2019

Awareness of cypersecurity threats in the Port of the Freetown, Sierra Leone

Malik Abdul Karim Sesay

WORLD MARITIME UNIVERSITY

Malmö, Sweden

AWARENESS OF CYBERSECURITY THREATS IN THE PORT OF THE FREETOWN, SIERRA LEONE

By

MALIK ABDUL KARIM SESAY
SIERRA LEONE

A dissertation submitted to the World Maritime University in partial fulfilment of the requirement for the award of the degree of

MASTER OF SCIENCE
In
MARITIME AFFAIRS

(SHIPPING MANAGEMENT & LOGISTICS)

2019

Declaration

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

Name: Malik Abdul Karim Sesay

Specialisation: Shipping Management & Logistics

(Date):

Supervised by**:** Professor George Theocharidis

Supervisor Signature: …………

Acknowledgements

My first gratitude will go to God Almighty for his Grace, Mercy and Guidance in allowing me go through this past fourteen months' tedious Academic pursuit in the World Maritime University (WMU). Though it was not easy but I will would love to extend my thanks and appreciation to the WMU faculty, staff and administration for their support.

This dissertation will have not been successful without the personal effort of my supervisor, Professor George Theocharidis for your valuable understanding and advice, time and supervision received during the writing of this dissertation. Apart from that I do appreciate your moral support giving to me, I am grateful for your knowledge and expertise during the entire work.

To my late Mother Mrs. Aziza Sesay and my father Mr. Abdul Karim Sesay I do appreciate your advice and courage during my study and a special thanks to my lovely wife Salamatu Hassanatu Sesay for giving me the courage, motivation and love throughout this entire course and onto this very moment which was meaningful to the success of this programme.

Abstract

Title of Dissertation: **Awareness of Cybersecurity Threats in the Port of Freetown, Sierra Leone.**

Degree: Master of Science

Taking into consideration the advancement in port infrastructure and technology as well as the importance of ports in not only a country's economy, but also the global economy and the increasing cybersecurity threats on such systems, it was considered important to study the awareness of cybersecurity threats in the Port of Freetown, Sierra Leone, a port that has hardly been researched when it comes to the awareness of cybersecurity threats. The research assumed a descriptive design in order to fulfil its aim and objectives. The research used both primary and secondary data. The primary data was collected by distributing close-ended questionnaires to different respondents electronically at the Port of Freetown and the secondary data was collected through reviewing different scholarly publications, and authoritative publications from governments, the International Maritime Organization, the United Nations, etc. The research sought to include anywhere between 50 to 100 participants; only 71 interviewees managed to successfully respond to all the survey questions. The main conclusion of this dissertation was that cybersecurity awareness at the Port of Freetown was below average as the Port is considerably exposed to cybersecurity threats. Effectively, the presence of the threats and even their materialization makes it difficult to comprehensively understand when a maritime operator has been attacked and the type of actors involved. It is hereby recommended that authorities in Sierra Leone start by adopting the universally acceptable International Maritime Organization (IMO) practices and then plan to invest in implementing measures supported by the provisions of IMO.

KEYWORDS: **Security, Threat, Ports, Awareness, Cyber attack**

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AIS	Automatic Identification System
ECDIS	Electronic Chart Display System
EU	European Union
ICT	Information Commination Technology
IMO	International Maritime Organization
ISPS	International Ship & Port Security Code
IOTS	Internet of Things
MGCI	Maritime Global Critical Infrastructure
MTS	Maritime Transport System
SOLAS	Safety of Life at Sea
US	United State
UNCTAD	United Nation Conference on Trade & Development

CHAPTER ONE – INTRODUCTION

Taking into consideration the advancement in port infrastructure and technology as well as the importance of ports in not only a country’s economy, but also the global economy and the increasing cybersecurity threats on such systems, it was considered important to study the awareness of cybersecurity threats in Sierra Leone, a country that has hardly been researched when it comes to awareness of cybersecurity threats in African shipping ports. This section will serve as the first chapter of the research and it will contain the following topics: background, research problem, research aim and objectives, research questions, brief methodology, research rationale, research assumptions and delimitations, and dissertation organization.

1.1. Background

In recent years, the interest in cybersecurity, which normally refers to the protection of both physical and technological assets of organizations, has increased all over the globe because of several factors. First, digitalization is continuously growing, which implies people are greatly relying on efficient information systems; second, information systems, including the data stored in them, have overly complex characteristics (DiRenzo et al., 2015). Third, the dependence on information systems and their technology as a whole has made societies and organizations vulnerable to the functionality of the systems (Jones et al., 2016). Fourth, each year, the number of cyberattacks on organizations are said to be increasing as companies continue reporting more and more financial losses due to cyberattacks (Jensen, 2015). The issue is made much more complex when you take into consideration the fact that the world is moving towards the "Fourth Industrial Revolution," a phrase coined by Schwab (2016) referring to how technologies like artificial intelligence, autonomous vehicles, and the Internet of Things (IoTs) are merging with the day to day activities of humans, including running organizations.

The emergence of these new information systems has brought about a fundamental shift in the manner in which countries and their citizens are involved in global economic activities, e.g., how they communicate, and how they control critical infrastructure (Chiappetta & Cuozzo, 2017). Nonetheless, cybercriminals are exploiting these activities by carrying out malicious activities, some of which are considered as natural disasters and acts of terrorism

(Tam & Jones, 2018). Furthermore, the motives behind cyberattacks vary greatly from one attack to another, including monetary gain, political agendas, and acts of excitement (Tam & Jones, 2018). Today, it has been identified that cyberattacks not only include cybercrime and identity thefts, but also threats to national and international security (Chiappetta, 2017).

Some of the most far-reaching cyberattacks in 2017, i.e., the NotPetya and WannaCry, revealed the vulnerabilities of critical infrastructures, for instance how networks and their assets can impact the economic and social functionalities of different countries (Jović et al., 2019). Since the maritime industry plays a considerable role in the global transport network, many consider it as the backbone of global trade as well as part of a country's critical transport infrastructure (Kessler, 2019; Newman, 2019; Jović et al., 2019). Globally, roughly 80% of the world trade is transported by sea (Kessler, 2019). Contemporary information technologies and systems play a leading role in all modes of transport. They significantly affect the efficiency, consistency, and performance of transport networks (Newman, 2019).

1.2. Problem Statement

In the maritime sector, ports are today heavily depending on networked computers and information systems to control the flow of maritime commerce on which the economy, national and homeland security depend on (Jović et al., 2019); this has also increased cyberattacks towards maritime systems, as it was seen in the NotPetya cyberattack that crippled operations of Maersk's 17 APM Terminals across the globe (Jović et al., 2019). The attack also highlighted how ports have no specific responses or guidelines to prevent or mitigate major cyberattacks. In Africa, the International Maritime Organization (IMO) notes that while governments rush to expand their shipping ports and make them more technologically dependent, they still continue employing workers who are less aware of cybersecurity and the threats that come with the phenomenon making the countries overly vulnerable (United Nations, 2015). A survey carried out by European Union Agency for Cybersecurity (ENISA) on the level of preparedness among African shipping ports when it comes to dealing with cybersecurity threats revealed that only 23% of African shipping ports are using the Resolution MSC.428(98) of the IMO, which provides a safety management system for shipping and shipping ports to protect themselves against any cybersecurity threat (ENISA, 2019). The Resolution MSC.428(98) was a development of the IMO, which requires all shipping and shipping ports to implement in their operations by 1st January, 2021 (IMO, 2019). By focusing on Sierra Leone's largest shipping port, i.e., the Port of Freetown, it was, therefore, considered important to study the country ports' awareness of cybersecurity in the age of increased cyberattacks.

1.3. Research Aim and Objectives

The research will seek to fulfil the following aim:

- To study the current state of cybersecurity awareness in the Port of Freetown, Sierra Leone

The above aim will be guided by the following objectives:

1. To identify cybersecurity risks and threats against the Port of Freetown
2. To examine whether the Port of Freetown is prepared to deal with cybersecurity risks and threats they face
3. To suggest policy recommendations that can improve cybersecurity management in the Port of Freetown
4. To propose an effective framework of protecting the Port of Freetown from cybersecurity risks and threats

1.3.1. Research Questions

The research will be guided by the following questions:

1. To what extent is the Port of Freetown exposed to cybersecurity threats?
2. How serious are cybersecurity breaches for the Port of Freetown?
3. To what extent is the Port of Freetown prepared to mitigate or prevent cybersecurity threats?

1.4. Brief Methodology

The research will assume a descriptive design in order to fulfil its aim and objectives. The research will use both primary and secondary data. The primary data will be collected by distributing close-ended questionnaires to different respondents electronically at the Port of Freetown. Secondary data will be collected through reviewing different scholarly publications, and authoritative publications from governments, the International Maritime Organization (IMO), the United Nations, etc. Since the research will focus on the Port of Freetown, each and every research participant will either have to be a manager or employee at the Port. The research sought to include around 50 to 100 participants. Random sampling will be applied to recruit the participants from the Port whereby managers and employees will freely be invited to take part in the research. Both qualitative and quantitative methods will be applied in analyzing the primary findings. Microsoft Excel will be used to tabulate the data by coming up with graphs and tables that illustrate the findings of the extent of cybersecurity awareness of managers and employees at the Port of Freetown.

1.5. Research Rationale

The maritime sector is reactive in setting procedures and standards based on catastrophic events. To cite one of the most famous cases, on April 15th, 1912, the 'unsinkable' RMS *Titanic* collided with an iceberg during her maiden voyage from Southampton, UK, to New York City. Dubbed by her builders as 'indestructible,' the *Titanic* sailed on her maiden voyage with minimum lifeboats and lifejackets for passengers and crew; this lack of safety equipment led to over 1,500 deaths (Brasington & Park, 2016). As a result, the international community came together in 1913 to set international shipping practices and regulations for seafaring vessels in an event called the Safety of Life at Sea (SOLAS) (McGillivary, 2018). Maritime leaders all over the globe also mandated safety requirements such as loading capacity, durability, lifeboat and lifejacket ratio, etc. as a response to the *Titanic* disaster (Brasington & Park, 2016).

Today, the maritime sector is still being affected by what scholars term as the *'Titanic* syndrome' (Zăgan et al., 2018; Trimble et al., 2017; Svilicic et al., 2019). In relation to cybersecurity threats, this implies that the international community normally comes together and acts in response to catastrophic events that cause cyber panic. What the international community does not know is that maritime cyberattacks are happening more frequently, and this lack of awareness is caused by attacks going unreported or undetected (Zăgan et al., 2018). Even though researchers have suggested that the maritime sector is vulnerable to cybersecurity threats, very little has been done to deter or prevent these threats. The importance of the current research is that it will help shade off this *'Titanic* syndrome' by recommending ways that some of the least researched, yet overly important shipping ports in the world can prepare themselves for dealing with cybersecurity threats by increasing awareness among its stakeholders. The research also hopes to pave the way for further research into increasing cybersecurity awareness among African shipping ports.

1.6. Research Assumptions and Delimitations

Research assumptions are things that are considered as true, or at least plausible, by researchers and the peers who read or review other people’s research. In other word, any other person reading a research will believe that certain aspects of the research are true given the population, tests carried out, research design, limitations, etc. (Quinlan et al., 2019). For the current research, it will be assumed that all the primary data presented by the participants will be a true reflection of the current state of cybersecurity awareness in the Port of Freetown, Sierra Leone.

Research delimitations, on the other hand, refer to the definitions researchers set for their own research, which are in their control. Delimitations help researchers to set goals that are not impossibly large to complete (Quinlan et al., 2019). For the current research, it will only include respondents from the Port of Freetown, Sierra Leone, and no other port. It will be assumed that the findings of the research reflect on other West African region ports that assume a similar level of cybersecurity awareness as the Port of Freetown.

1.7. Dissertation Organization

This section has presented the first chapter of the research, the research of the research will include four more chapters, which will be laid out as follows: Chapter two will be the literature review chapter, and it will include the following topics: identifying maritime risk, vulnerability and threats, maritime safety and security, maritime sector in general, main information systems of the maritime sector, development of the Sierra Leone maritime sector, definition and conceptual illustrations of cybersecurity, cyberattacks and the actors, current state of maritime cybersecurity, and cybersecurity regulations in the maritime sector. Chapter three will be the methodology chapter, and it will include the following topics: research design, research philosophy and approach, case study design, data collection, data analysis, reliability and validity of a qualitative study, and ethical approach. Chapter four will be the results and discussion chapter. It will include only those two major sections. Chapter five will be the conclusion chapter, and it will include the following sections: summary, main conclusions, research recommendations, research limitations, and suggestions for further research.

CHAPTER TWO – LITERATURE REVIEW

2.1. Introduction

This chapter will review existing literature on the cybersecurity threat in the maritime industry from previous researchers and authors. Although the focus of this dissertation is on the Freetown Port in Sierra Leone, the review will not be restricted to publications of research on that particular port alone. The rationale for taking a wider-focused approach towards the literature review is to contextualize the characteristics of the larger industry both in developed and developing countries and lay down a verifiable background against which the Freetown Port can be compared and contrasted. The discussion of security in the cyberspace will be against the background of the conceptual illustration adapted from the works of Zăgan et al. (2018) as demonstrated in Figure 1 later within this chapter.

2.2. Maritime Sector in General

A functional maritime industry is an essential element for an economically sound society especially when viewed from the perspective of globalization. This argument was presented by the United Nations Conference on Trade and Development (UNCTAD, 2017) who reported that up to 90% of the raw materials and finished products that go through the global supply chain are conveyed via maritime transport. According to the report, the maritime sector is made up of globally distributed entities including state departments; port authorities; privately owned shipping companies; telecommunications and energy networks; and transport infrastructures such as seaports, roads, rail and airports. However, the significance of seaports is that they are not only an element of the global maritime supply chain but they are also the hub of other forms of global cargo transportation, hence a driving factor of international trade and economy (UNCTAD, 2017). Such positioning makes the maritime industry part and parcel of worldwide and continuously evolving networks. According to Hareide et al. (2018), the various actors and operations that characterize the maritime sector can be identified as either Maritime Global Critical Infrastructure (MGCI) or Maritime Transport System (MTS). MGCI includes infrastructures (ports and straits) which have the potential to impose multi-sector and boundary consequences on society in terms of disturbance (Hareide et al., 2018). The significance of MGCI is that it includes all assets and systems that depend on certain maritime activities and can have global implications for economy and system security as well as public safety and health. MTS includes seaports and waterways and their operators and it underpins the criticality of the maritime industry to the worldwide economy (Hareide et al., 2018). However, the problem still remains that awareness of the significance of a functional maritime industry, and especially with regards to its security, is low in many countries particularly in the developing world.

Tam and Jones (2018) classified maritime industry operations into shipping operations and land operations. On one hand, the shipping industry and the associated shipping companies run the shipping operations that are the primary aspect of maritime transport. On the other hand, the port authorities and port operators are the main actors in the land operations whereby they, respectively, manage and maintain port infrastructure, and handle cargo operation in relation to loading and discharging vessels (Tam & Jones, 2018). As already noted by UNCTAD (2017), ports form the nucleus of maritime operations including shipping; therefore, they entail vital intermodal nodes for both passenger and cargo transportation networks and critical border control points. It follows, therefore, that there is unconditional need to install functional and effectual security policies and systems. Because of the port connectivity between states, according to Svilicic et al. (2019), they are a strategic interface within the maritime industry and it is imperative that the business environment (both physical and cybernetic) is effectively secured so that the maritime operators can deliver their services efficiently. The cybernetic environment is made up of port infrastructure including the information and communication technology (ICT) systems and the associated hardware, software, networks, data, services and the users (Polemi, 2017). Because of the large-scale nature of port infrastructure as well as the impairment, degradation and disruption of both the physical and cybernetic environments and systems, Kessler, Craiger and Haass (2018) consider ports as components of the transport-critical infrastructure that potentially impacts on national security, safety, health, economy and citizen’s welfare. Further, the large amounts of data handled by the maritime industry and especially at the port level make the entire industry vulnerable to cyberattacks as well as accidents, but there are still poor levels of awareness of the problem.

2.3. Definition and Conceptual Illustrations of Cybersecurity

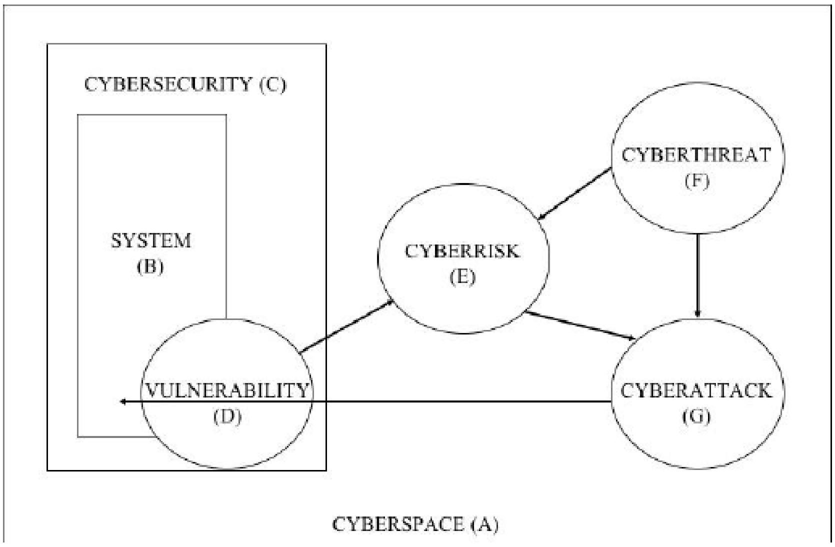

Figure 1: Conceptual Illustration of Cybersecurity Framework

Source: Adapted from Zăgan et al. (2018)

Zăgan et al. (2018) gave a concise illustration of the role of cybersecurity represented by (C) in Figure 1 above. Summarily, all the cyber operations take place in the cyberspace (A) in which is located the system (B) and protected by cybersecurity (C). (D) represents the vulnerabilities of the system, (F) represents the cyber threats while (E) represents the cyber risk (all of which are discussed further in the next section, "Identifying Maritime Risk, Vulnerability and Threats") at any given time. Cyberattack (G) may cause (E) to materialize at any point in which (C) is inadequate. Typically, (G) targets (B) via identified (D). Ideally, (G) is refered to as materialized (F) which represents specific technical ways of inflicting harm (Zăgan et al., 2018). (B) is used in reference to all the hardware and associated software used in the maritime cybernetic environment. As explained by Lagouvardou (2018), the systems are part of the cyber technology in reference to the use of digital systems to transmit, manipulate, store and monitor data. A critical feature of cyber technology is that the systems are further connected to other external systems that present opportunities for interception, access and modification of software or the data itself by unauthorized parties.

The most abstract definition of cyberspace, according to Daum (2019), is a three-dimensional domain in which information moves between individual computers and computer groups. However, more recent definitions have included technological dimensions as well as other features such as computing devices that not only mean computers but also network devices. As Chiappetta and Cuozzo (2017) argue, the inclusion of the concept of “network” makes cyber security and particularly information security an extremely wide area of interest. However, Bothur, Zheng and Valli (2017) add that it is imperative to consider the topic in the wider context of cybersecurity because it goes beyond the limited scope of information security and includes the involved assets, even the human operators and consumers of the information. In agreement, Tam and Jones (2018) point out that the humans in cybersecurity are considered as an additional dimension and potential cyberattack targets who may even be inadvertent victims.

The ministries concerned with the maritime industry and trade in European Union (EU) Member States and also state departments and agencies in the United States (US) identify an acceptable state of cybersecurity as one in which risks and threats against the essential operations of societies that depend on the cybernetic environment are under control (Hopcraft & Martin, 2018). There is general consensus among maritime scholars (Fowler et al., 2017; Jacq et al., 2018; Meyer-Larsen & Müller, 2018) that states and private shipping companies must focus on the security of their critical infrastructures associated with the cyber environment in which the maritime industry operates so as to ensure business resilience against cyberattacks. In that sense, Jacq et al. (2018) define cybersecurity as a concept that addresses the access to data and its storage and control. The objective of cybersecurity, therefore, according to Fowler et al. (2017), is to realize a stable state by installing essential and reliable protections.

Cyber risks, according to Meyer-Larsen and Müller (2018), entail a complex combination of operational and strategic risks. On one hand, operational risks entail organizational the performance while, on the other hand, strategic risks concern an organization’s overall direction and they typically appear from its positioning in the larger business environment (McGillivary, 2018). Cyber risk is an indication of the vulnerability or opportunity that has potential to harm the cyber environment and when it materializes or is exploited against a particular operation depending on the cyber environment, it can result in disruption, damage or harm (Tam & Jones, 2019). According to Mraković and Vojinović (2019), a realized risk in practice arising from failure of information systems may cause a shipping company or port authorities to suffer disruptions, financial losses and reputational injury.

2.4. Identifying Maritime Risk, Vulnerability and Threats

According to Kessler (2019), shipping ports have in recent years acknowledged the significance of using modern technologies and especially with regards to data and information security. For instance, the Port of Long Beach, Port of San Diego and Port of Barcelona have all been targets of cyberattacks in the past two years whereby their IT systems were infiltrated and the authorized users blocked from the servers and systems (van Erp, 2017). In acknowledgement of the serious consequences of such attacks on terminal operations, Kessler (2019) studied the concepts of risk, vulnerability and threat in relation to the maritime industry so as to understand how key security and safety regulations have influenced the remodeling of the entire industry. Risk is described as the likelihood of harm that can be suffered under the conditions of exposure or use and the likely degree of the harm (Jacq et al., 2018). Besides operational risks such as labor strikes, accidents, equipment failure and mishandling of dangerous cargo, Beaumont (2018) points out that the maritime industry is also vulnerable to security breaches involving hacking, theft, physical attacks and sabotage. Similarly, Newman (2019) also studied the implications of risks and threats in the maritime industry and found that they impact on business processes globally and create shipping process imbalances. This finding is consistent with that by Kessler (2019) who also found that risks and threats affect business processes by restricting the authorized users' access to servers and systems in lieu of ransom payment. Global imbalances occur when ships cannot access their ports of destination and are forces to reroute, effectively disrupting shipping schedules (Newman, 2019).

Trimble, Monken and Sand (2017) identified five risk categories that occur in the maritime industry including 1) environmental, 2) financial, 3) market, 4) political, and 5) technical. In the context of this dissertation, technical risks are seen to arise from constructions and ICT and, as demonstrated by Trimble, Monken and Sand (2017), they may lead to any or all of the other four categories. The most common vulnerability factors in the maritime industry identified by Eiza and Ni (2017) include 1) cargo, 2) money, 3) vessels, 4) people, and external impacts. Expanding on the findings, Ahokas et al. (2017) explain that the cargo vulnerability factor is implemented by way of smuggling weapons, people and drugs while the money vulnerability factor is implemented by ways such as funding terrorist activities using revenues from shipping. The vessel vulnerability factor is implemented by way of disrupting the infrastructure by sinking vessels, possibly using weapons, while the people vulnerability factor is implemented by way of attacking the vessels to incite human casualties (Ahokas et al., 2017). Svilicic et al. (2019) define threat as an act (or the actor) which can cause harm and, in relation to the maritime industry, threats include theft of information and cargo, financial losses, sabotage and terrorist attacks. These threats are embodied in the activities of states, criminal groups, terrorists and individuals but awareness levels of countermeasures are still considerably low.

2.5. Maritime Safety and Security

None of the literature consulted for this review has presented a clear safety and security theory; rather, there is a tendency for most of the researchers to address safety and security as distinct but interrelated concepts of the cyberspace, whether in the maritime industry or any other. Chiappetta (2017), for instance, asserts that safety is a much wider and more comprehensive idea while Śliwiński and Piesik (2018) place security within safety measures. Perhaps a clearer explanation is that given by Wilshusen (2015) in which it is noted that maritime safety comprises a set of preventive/security measures designed and expected to protect the globalized maritime industry against risk, harm and loss and also reduce the effects in the invent that such risks materialize. Ahokas et al. (2017) also define maritime safety as the protection of assets and life at sea from operational and environmental threats, including the safety of the physical maritime environment from pollution. It follows, therefore, that maritime safety often entails all the aspects relating to the combination of security and safety. In that context, one may agree with Chiappetta (2017)) that safety is a wider concept that also covers security as one of its measures. Wilshusen (2015) describes maritime safety from the four factors of internal safety; external safety; environmental impacts and human factor. In explanation, they point out that internal safety is an influencing factor for the damage and structure stability of vessels and the evaluation of business premises while external factors include the environment, ports, fairways and the related equipment. The significance of the human factor is that it is related to maritime safety since more than 75% of the accidents and incidents are a function of the human factor (Wilshusen, 2015). Environmental impacts result from the complicated interactions of all the factors highlighted above.

Śliwiński and Piesik (2018) describe security as an assurance of availability, reliability, confidence and integrity but points out that is has multidimensional meanings. With specific regards to the maritime industry, Śliwiński and Piesik (2018) observed that security is a concept traditionally used to point out intentional threats as opposed to intentional ones or those that arise from natural causes. Before the turn of the 21st century, maritime security was not a strictly critical topic of security debates especially in developing countries. However, Svilicic et al. (2019) notes that the 9/11 terrorist attacks set off a chain of security-related concerns and reactions across the developed, developing and least developed countries, including the formation of the International Ship and Port Security Code (ISPS). These were further heightened by the frequent pirate attacks in the Strait of Malacca in the early 2000s and high-visibility terrorist acts against vessels, e.g. USS Cole (2001), the French tanker Limburg (2002) and the Filipino civilian ship Super Ferry 14 (2004). Maritime security is thus defined as the set of preventative policies, strategies and measures implemented to protect the maritime industry against hazards and deliberate illegal acts. Equally importantly, Eiza and Ni (2017) add that maritime security must also include a sense of secure feeling of the port operators, shipping companies, their vessels, passengers and crew against threats such as terrorism and piracy. According to Beaumont (2018), these threats cannot be isolated from technology (hence the cybernetic environment) because of the increasing reliance on ICT systems which are also advancing exponentially. Essentially, maritime operations are information-driven and the protection of information is one of the first stages of ensuring port cybersecurity as aptly captured by Zăgan et al. (2018) in the conceptual illustration. Yet, only the most developed countries are appreciably aware of what needs to be done to be done to protect information in the cyber industry.

2.6. Main Information Systems of the Maritime Sector

Information flow in the maritime industry traditionally relied on paper which, necessarily, translated into higher operational costs and lower customer satisfaction levels. However, as Beaumont (2018) reported, electronic information systems have considerably cut down logistics costs and increased customer satisfaction by promoting higher levels of industry-wide coordination. The rolling out of innovative technologies every other day has compelled maritime operators to adapt their infrastructure so as to facilitate and support operations that are responsive to market dynamics. Such adaptations, according to Trimble, Monken and Sand (2017), have made it possible for the maritime industry to increase efficient productivity. The industry-wide coordination of operations pointed out by Beaumont (2018) is supported by various applications ranging from the most basic to the most sophisticated, including text messaging, automatic identification system, email, collaborative planning voice, video and web surfing. These applications are typically used in operations such as traffic control, navigation, tracking, monitoring loading/offloading processes and freight management.

Apart from the applications pointed out above, van Erp (2017) notes that there are the key ICT systems essential for vessels in the maritime industry. These include Global Positioning System (GPS), Automatic Identification System (AIS) and Electronic Chart Display Information System (ECDIS), and the common feature of these systems is that they are not directly connected to the Internet. AIS is very high frequency (VHF) radio and is mandatory in vessels, both passenger and cargo, with a gross capacity of 300 tons and is instrumental inter-ship data exchanges especially in poor visibility conditions. GPS is mainly used in logistics operations for real-time detection and tracking of objects in transit such as vessels or even individual containers as well as aid in route planning and navigation (Fowler et al., 2017). However, Ahokas et al. (2017) have criticized a number of national and regional jurisdictions especially in developing countries for not using GPS technology to its full capability in logistics operations. ECDIS integrates GPS data with data from a vessel's radar, speed log and gyrocompass to help mariners navigate coastal waterways and it is mandatory for large vessels. However, Ahokas et al. (2017) point out that there is no universally accepted definition of the term "large vessel" which still makes the use of ECDIS ambiguous in some vessels.

2.7. Development of the Sierra Leone Maritime Sector

Sierra Leone is a sovereign state with its national laws. The Sierra Leone Maritime Administration was established in 2000 through an act of parliament and the Merchant Shipping Act of 2003 and mandated to register sea vessels and regulate and develop maritime practices in the country's coastal and inland waters (Ministry of Transport and Aviation, 2019). However, since it is part of the larger global maritime industry and because of the forces of globalization, it ports are not markedly different from others across the world although regional developmental factors cannot be ignored (Boggero, 2018). Ports in Sierra Leone, like any other in the world, evaluate organizational forms, implement emerging technologies and adopt industry trends in order to increase effectiveness, efficiency and the ease of being incorporated into global logistics chains. However, with specific regards to port cybersecurity, Sierra Leone has been in an ongoing process of developing a national maritime policy but there is still no Maritime Security Act in place (Ministry of Transport and Aviation, 2019). The proposed legislation, though, is commended for its focus on safety issues because, as argued by Śliwiński and Piesik (2018), safety is a wider concept that encompasses security measures.

Over 60% of the cargo into and out of Sierra Leone is by sea freight through three ports: Port of Freetown, Port of Pepel and Port of Sherbro Island. Therefore, according to studies by Okeke-Ogbuafor, Gray and Stead (2018), this makes Sierra Leone one of the countries in which the maritime industry is a key player in the performance of the country's economy and the people's quality of life. Further, for Sierra Leone, the maritime industry has been the facilitator of new graduate courses in tertiary education including marine engineering, navigation, fishing technology and refrigeration engineering. According to Diggins (2018), the higher the number of university students a country produces, the greater the potential for foreign direct investment they generate. In Sierra Leone, the graduates in the mentioned courses demonstrate to potential investors that there is a reliable pool of trainable manpower in the country's maritime industry. With such developments, the Ministry of Transport and Aviation acknowledges the need for functional cybersecurity policies and measures. Therefore, it may be inferred that there is an appreciable level of port cybersecurity in Sierra Leone.

2.8. Cyberattacks and the Actors

As described in the conceptual illustration, a cyberattack is the materialization of cyber risk. According to Zăgan et al. (2018), a cyberattack has the fundamental elements of cyber threats in relation to the intentions and goals of the actor and these are categorized into targeted and untargeted attacks. While there will be at least one intended target such a system and the data it contains or even an entire organization in a targeted cyberattack, an untargeted cyberattack will typically have multiple random targets. Targeted attacks are characterized by techniques such as brute force, spear-phishing, denial of service (DoS), subverting the supply chain and distributed DoS (Ahokas et al., 2017). Untargeted attacks, on the other hand, entail malware, scanning, social engineering, water holing and phishing. The most common forms of attack are DoS, phishing and malware. Boggero (2018) describes phishing are emails randomly sent to multiple recipients typically with a request to confidential and sensitive information to lure the unsuspecting targets to a given phony website. The targeted form of phishing is spear-phishing, in which specific individuals are targeted via email onto which malicious links or software are attached (Boggero, 2018). Opening the attachments or accessing the given links can enable the actor to gain access into the targets systems and cause authenticated by unwanted and injurious actions to the systems without the victim's knowledge. As explained by Chiappetta (2017), a DoS attack will flood a network with data, effectively preventing authorized users from accessing and using the data therein. Short DoS attacks (quantified in hours) disrupt operations that rely on real-time data while mid-term attacks (days or weeks) escalate security-related issues with regards to fuel and food shipments. According to Daum (2019), a distributed DoS uses similar methods to DoS but targets multiple victims. Scanning, brute force, water holing, subverting the supply chain and social engineering are less common but also have undesirable consequences.

The actors can be summarized on the basis of their motivations, their objectives and the cyber threats they present as illustrated in the table below.

Table 1: Cybercrime Actors' Profile

ACTOR	**MOTIVATION**	**OBJECTIVE**	**CYBER THREAT PRESENTED**
• Government • Terrorist	• Social • Ideological • Egoism • Religious • political	• Disruptions • Critical infrastructure • Military systems • National institutions	• Cyber war • Cyber terrorism
• Hacktivist • Hacker • Insider	• Reputation • Egoism • Political	• Knowledge • Attention • Disruptions	• Hacktivism
• Government • Industrial spy • Insider • Organized criminals	• Informational • Ideological • Economical • Political	• Cargo • Knowledge • Digital assets • Organizational data	• Cyber espionage • Cyber criminality

Source: Eiza and Ni (2017)

2.9. Current State of Maritime Cybersecurity and Regulations

As already observed by Beaumont (2018) earlier in this chapter, the maritime industry has appreciably adopted technological advancements and shifted to modern ICT from the traditional paper-based communications. However, with the advancements also come considerable security challenges relating to data about cargo, vessels and personnel as well as the overall operations of the entire industry (Hareide et al., 2018). Different risks have been identified ranging from deliberate to opportunistic to completely unintended attacks resulting in devastating losses. Typically, the cyberattacks exploit the vulnerabilities inherent in MTS including telecommunication systems, information networks and individual computers and devices involved in maritime operations (Jacq et al., 2018). In a typical example from Somalia, classified by the United Nations (UN) among the least developed countries, pirates have occasionally taken advantage of navigation data available online to track vessels using radar, AIS and ECDIS to locate and hijack ships. Maritime cyberattacks take the form of infiltrating port computers; sending fake GPS signals to reroute a vessel; modifying AIS signals to falsely report a vessel's location; and accessing ECDIS software to amend maps (Kessler, Craiger and Haass, 2018). There is general consensus among researchers that the increasing reliance of the maritime industry on ICT systems has exposed it to cyber risks and the associated operational vulnerabilities and disruptions.

Although studies into the topic of cybersecurity and the associated protective measures are wide and vast, specific awareness into the cyber environment surrounding the maritime industry is comparatively low (Zăgan et al., 2018). This phenomenon is further complicated by the fact that new technologies are emerging at such a high rate that keeping up with the most current protective measures creates a new cost center which maritime industry operators especially in developing countries consider as avoidable (van Erp, 2017). In contrast, the developed countries and economic blocks (such as the EU) have developed appropriate region-wide legislations aimed at protecting the marine cybernetic environment. For example, the EU Directive on the Security of Network Information Systems (refered to as the NIS Directive) aims at providing legal measures to reinforce the general extent of cybersecurity in all Member States. However, given that it was enacted relatively recently (July 2016), the implication is that the maritime industry has remained exposed to threat for long. This literature review appreciates that there is considerable knowledge of the security aspect of the general cyberspace; however, implementing security measures based on the available knowledge is still not happening at the desired rate at least going by the conclusions by Diggins (2018); Svilicic et al. (2019); Tam and Jones (2019); Trimble, Monken and Sand (2017); UNCTAD (2017). The least developed and developing countries are the ones recognized as the slowest in implementing universally acknowledged cybersecurity measures.

CHAPTER THREE - RESEARCH METHODOLOGY

3.1. Introduction

This chapter will discuss the methodological approach that was assumed by this research. It will contain discussions on the following sections: research design, research philosophy and approach, case study design, data collection, data analysis, reliability and validity of a qualitative study, and ethical approach.

3.2. Research Design

Research design refers to the framework of research methods and techniques selected by a researcher that allows them to choose research methods suitable for their research problem and set their studies up for success. There are different types of research designs, including qualitative research and quantitative research, which can further be broken down into descriptive researches, experimental researches, correlational researches, and diagnostic researches (Quinlan et al., 2019). The current research chose a descriptive design due to the qualitative nature of the research problem. The other three research designs mentioned above are quantitative in nature, thus were not suitable for this research.

3.3. Research Philosophy and Approach

Research philosophy is defined as the perceptions assumed by researchers when collecting data for their studies (Kumar, 2019). There are two types of research philosophies, including positivism, and interpretivism. The positivism approach compels researchers to collect data based on pre-formulated hypotheses generated through quantifiable methods whereas the interpretivism approach is derived from the fact that human behavior cannot be quantified and analyzed the same way as physical sciences (Gray, 2019). Positivist researchers view the world as having one reality that everyone is part of making them subjective, whereas interpretists believe that factors of social science, e.g., humans, are different from natural sciences (Gray, 2019). The current research assumed an interpretivism approach due to its qualitative nature.

Research approach, on the other hand, is defined as a researcher's way of thinking. Similar to research philosophies, there are also two broad groups of research approaches, including deductive and inductive. Inductive approaches compel researchers to move from specific to general conclusions whereby they make initial observations concerning a research problem, then generalize the findings in line with the existing patterns from the collected data. A deductive approach, on the other hand, compels researchers to generalize theories and the conduct a study to analyze or test the pre-existing hypotheses based on those theories (Silverman, 2016). The current research assumed the inductive approach, because no hypotheses were formulated. In addition to this, the inductive approach is best suited for the interpretivism philosophy as it allows researchers to enjoy flexibility when collecting and analyzing their data since it does not depend on a single theory (Silverman, 2016).

3.4. Case Study Design

A case study refers to a type of empirical inquiry that investigates a phenomenon within its real-life context. As it is mostly used in social sciences, case studies are derived from a thorough investigation of a single individual, group, or event to study the causes of underlying principles. By making use of a case study design, a research can investigate a phenomenon in its historical, social, economic, technological, and/or cultural contexts (Glesne, 2016). As discussed earlier, the current research assumed a qualitative approach because of the nature of the research problem. The case study design, on the other hand, was chosen because the aim of the research was to investigate and observe the research problem in the environment of the key operators of the Sierra Leone maritime sector. The case study approach allowed one to collect the opinions and views of different stakeholders at the Port of Freetown with regards to the awareness of cybersecurity threats faced by shipping ports. Finally, the case study approach was deemed important as it would allow to one form a comprehensive conception of the current state of cybersecurity at the Port of Freetown, Sierra Leone.

3.5. Data Collection

Since the research focused on the Port of Freetown, each and every research participant had to either be a manager or employee at the Port. The research sought to include around 50 to 100 participants. Random sampling was applied to recruit the participants from the Port whereby managers and employees were freely invited to take part in the research. The current research used structured interviews to collect data from the participants. Structured interviews are a type of data collection method used in survey research wherein every interviewee is presented with exactly the same questions in a similar order. The advantage of such an approach is that it allows researchers to reliably aggregate their data and make confident comparisons between sample subgroups and/or between different survey periods (Mohajan, 2018).

The survey instrument was developed with three themes in mind that were identified while conducting the preliminary literature review: (1) operational environment of the Port of Sierra Leone, and (2) the current state of cybersecurity at the Port of Freetown, and (3) the awareness of cybersecurity threats at the Port of Freetown and mitigation measures. The survey instrument consisted of 19 questions, which can be retrieved from Appendix One of this research. The Port was contacted via telephone and the researcher was channeled to the responsible authority who was informed of the objective of the research, wherein they provided an email that a link to the survey and consent form would be shared with other members of the Port. The survey instrument and consent form were sent to the participants via SurveyMonkey, which would allow the participants to freely respond to the questions online at a time of their choosing.

3.6. Data Analysis

Both qualitative and quantitative methods were applied in analyzing the primary findings. Microsoft Excel was used to tabulate the data by coming up with graphs and tables that illustrate the findings of the extent of cybersecurity awareness of managers and employees at the Port of Freetown. The research, however, did not look into the statistical significance of the results and the level of heterogeneity, which can only be confirmed through advanced statistical analysis.

3.7. Reliability and validity

In a qualitative research, issues about reliability and validity are evaluated using means such as reflexivity, confirmability, dependability, transferability, and credibility (Attia & Edge, 2017). In this research, reflexivity was not a concern, because the survey was carried out online, thus there was no way of telling how the researcher-researched relationship affected the data collection. Nonetheless, it was important to look into the other four factors mentioned above. Credibility of a research is the confidence level one places on its findings (Attia & Edge, 2017). Credibility was confirmed by looking at persistent observations, which is the process of identifying the most relevant elements and traits relating to the research problem. Confirmability and dependability, on the other hand, is the extent to which the results of a study can be confirmed by other researchers or the stability of the results over time (Attia & Edge, 2017). For the current research, the confirmability and dependability will be established by comparing the results to the results of other similar studies. This will be done in the discussion section. Finally, transferability is the extent to which the results of a research can be transferred to a different context or setting (Attia & Edge, 2017). In order to establish the transferability of this research, the results will be compared to studies that have focused on cybersecurity awareness in other types of organizations so as to check the level of awareness and mitigation measures of cybersecurity threats in place.

3.8. Ethical Approach

The ethical approach of this study considered three important factors, including competing agendas, confidentiality and privacy, and informed consent. Before this study was conducted, employees and managers at the Port of Freetown were made aware of what the research will involve to ensure they have all the relevant information prior to agreeing to taking part. Consent was sought from the managers and employees at the Port to use the information they will present so as to come up with the findings of this study, which might be shared in other academic publications. The participants were also provided with contact details of the lead researcher and lead research supervisor in case they wanted further clarifications concerning the research.

For the confidentiality and privacy of the participants, the research did not collect any personal information from the interviewees such as their names, email or phone numbers, and even their position at the company. All the participants remained anonymous.

Finally, when it came to competing agendas, it was important to balance between professional obligation and intellectual curiosity by the lead research. Thus, the research was approach with a sense of 'doublemindedness.'

CHAPTER FOUR - RESULTS AND DISCUSSION

4.1. Introduction

The methodological approach of the current research was presented in the previous chapter. This chapter will present the primary findings of the research, including a discussion of how the results relate to past studies.

4.2. Results

This results section will be layout according to the three themes, which were earlier identified during the preliminary review that assisted in formulating the survey questions. The sections include: (1) operational environment of the Port of Sierra Leone, and (2) the current state of cybersecurity at the Port of Freetown, and (3) the awareness of cybersecurity threats at the Port of Freetown and mitigation measures. It is important to remember that the research sought to include anywhere between 50 to 100 participants; only 71 interviewees managed to successfully respond to all the survey questions.

4.2.1. Operational Environment of the Port of Freetown

The first four questions were meant to evaluate the operational environment of the Port of Sierra Leone in order to for the reader to understand whether the environment is vulnerable to cybersecurity threats.

Question 1: Which of the following, if any, does the Port of Freetown currently use or have?

This question sought to understand the most prevalent online service at the Port of Freetown. 'Email addresses for managers and employees' was ranked as the most prevalent online service (80.1%), followed by use of 'website' (60.3%) and then 'online banking' (38.7%) (see Fig. 2 below). It was a concern as most respondents did not take into consideration business transactions by customers as important factors, i.e., placement of orders and booking along with other financial transactions.

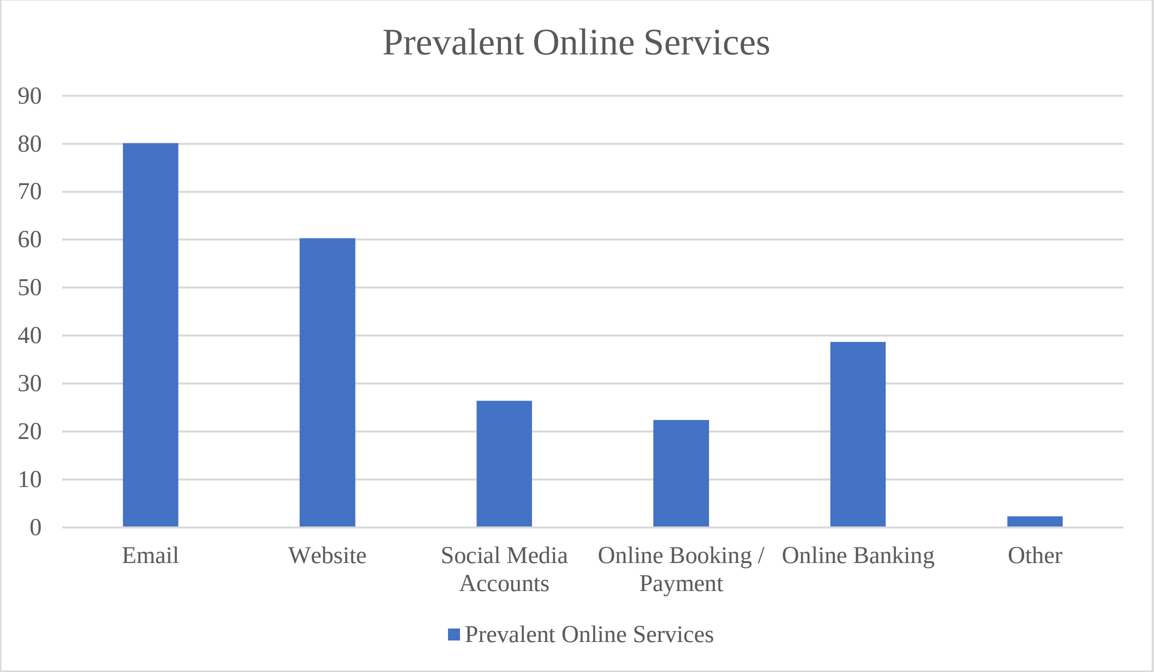

Figure 2: Prevalent Online Services at the Port of Freetown

Question 2: To what extent are online services an important part of the operations at the Port of Freetown provides?

This question was meant to establish whether the Port of Freetown highly depends on online services as much as they actually use them. A combined total of 32.6% of the respondents felt that online services were either 'important' or 'very important' to the Port operations (see Fig. 3 below). A combined total of 46.0% of the respondents felt that online services are not at the core of the Port’s operations, i.e., 'not very important' or 'not at all important.' Only 21.3% of the respondents chose the neutral option. This implies that the negative responses were more than the positive responses; such a finding might be viewed as a common-sense expectation taking into consideration the fact that the Port’s employees do not highly deem online services as an important part of their operations. It also highlights the fact that the Port does not recognize their business dependence on online services as much as they use them.

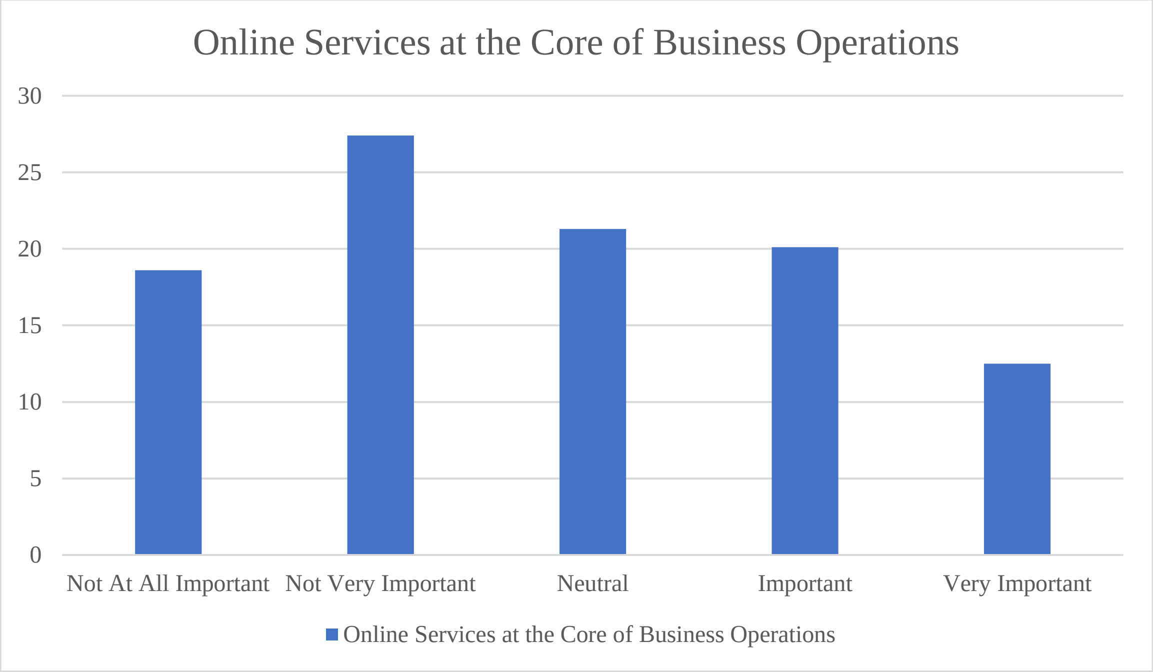

Figure 3: Online Services at the Core of Business Operations

Question 3: How many employees in the Port of Freetown use personally-owned devices?

The use of personally-owned devices is considered as one of the major causes of cybersecurity threats especially in organizations that have not implemented the necessary measures for employees to protect themselves against any cybersecurity breach (Herrera et al., 2017). It should be noted that while a majority of the respondents believed that employees used their own devices at the Port for work, the proportion decreased as the value went up (see Fig. 4 below).

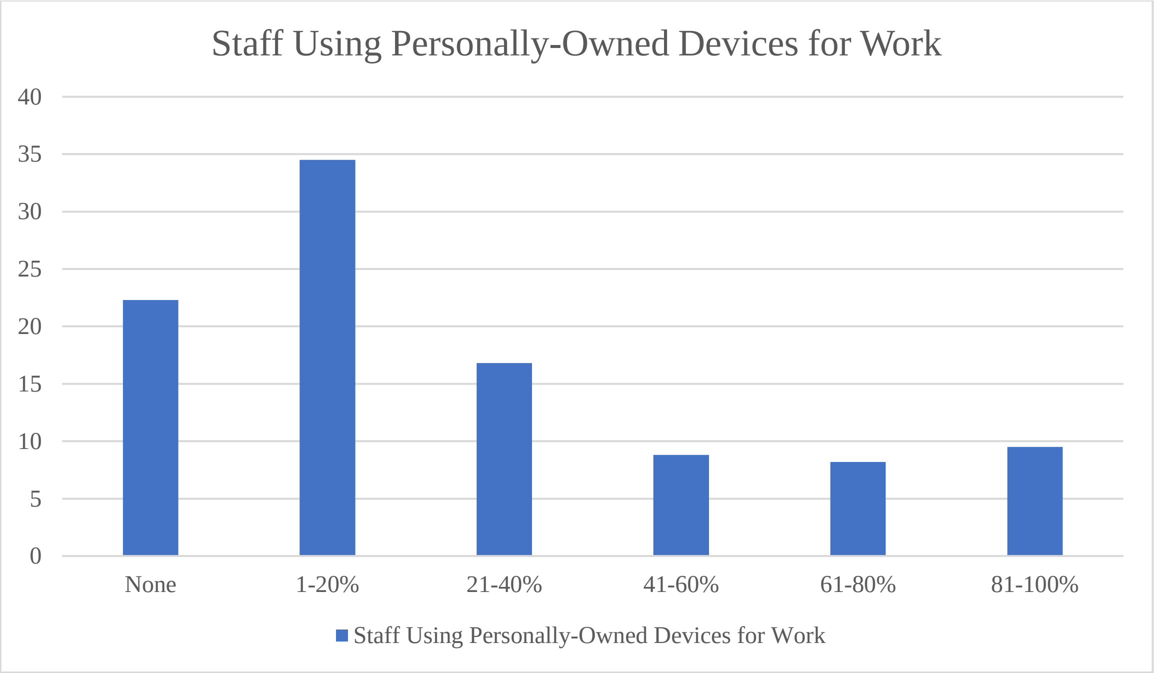

Figure 4: Staff Using Personally-Owned Devices for Work

Question 4: How important are these externally-hosted web services to the Port of Freetown?

Less than half the respondents (42.4%) deemed externally-hosted web services as a 'important' part of the Port's operations. 39% of the respondents considered externally-hosted web services as either 'not at all important' or 'not very important' to the Port's operations. A further 18.6% were 'neutral' to the criticality of externally-hosted web services (see Fig. 5 below).

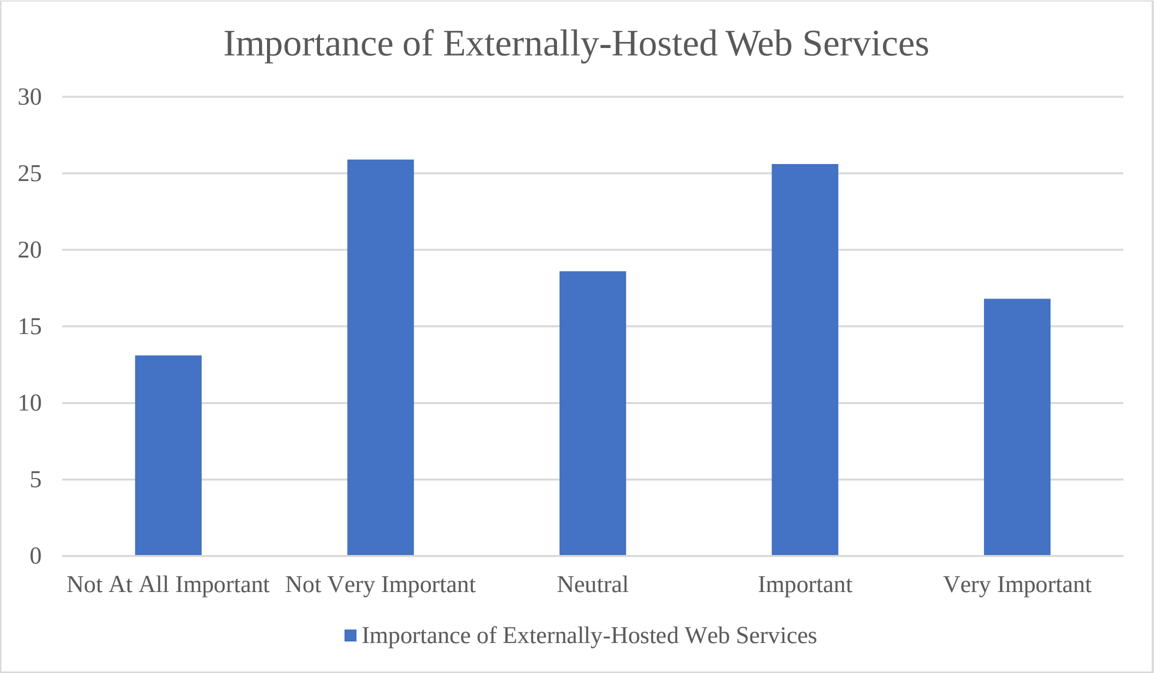

Figure 5: Importance of Externally-Hosted Web Services

4.2.2. The Current State of Cybersecurity at the Port of Freetown

Questions 5 to 9 were used to evaluate the current state of cybersecurity at the Port of Sierra Leone in order to for the reader to understand some of the cybersecurity incidents the Port has faced in the past and their implications.

Question 5: Which of the following have happened to at the Port of Freetown in the last 1 year? and Question 6: As far as you know, what or who was the source of the attack or breach?

The most common type of attack or breach experienced at the Port over the last 12 months was malware, spyware or viruses (75.8%) as well as stealing money through fake websites or fraudulent emails (33.5%). Other breaches noted by the respondents include: denial-of-service attacks (17.6%) and unauthorized access (19.2%) (see Fig. 6 below). Fig. 6 below is comparable to Fig. 7 below in that the main source most of the breaches and attacks was emails, attachments on the emails, and websites (53.8%). The other major source of breach was malware authors (38.5%). This pointed to the fact that the Port of Freetown was massively plagued by viruses and malware sent via websites and email attachments. Considering that the Port operation heavily depends on networked computers.

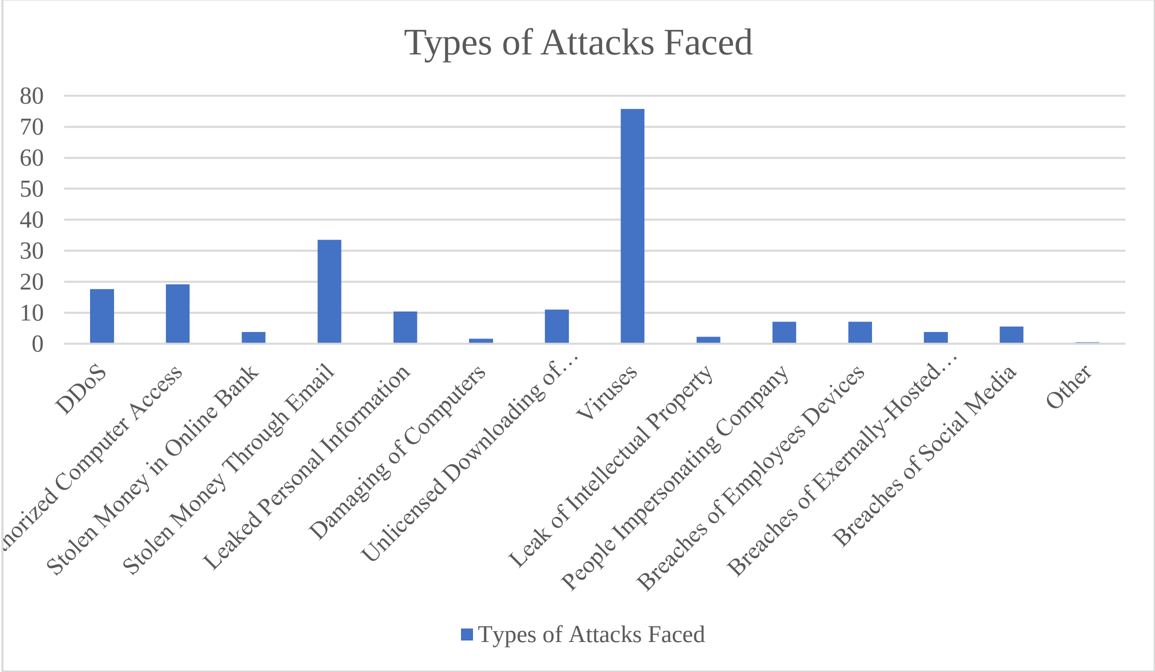

Figure 6: Types of Attacks Faced

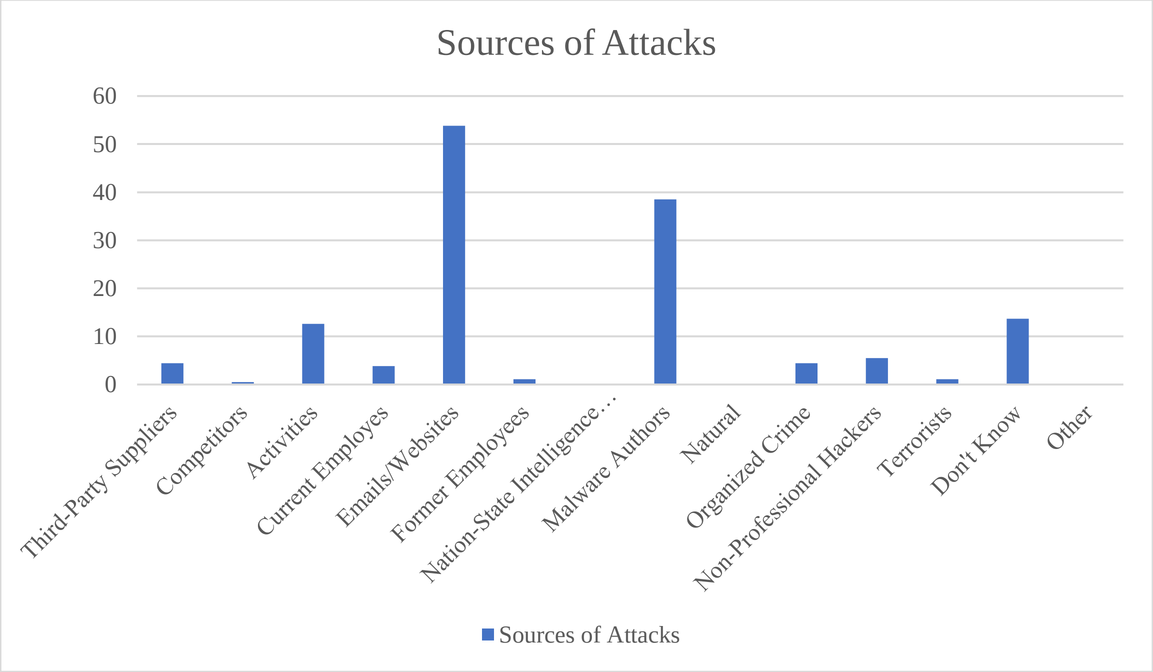

Figure 7: Sources of Attacks

Question 7: Roughly how much do you believe the attacks or breaches you have selected in Question 5 cost the Port of Freetown financially?

Over a third of the respondents (34.1%) were not aware of the financial costs of the attacks, with almost a similar number of respondents (33.5%) projecting the that attacks costed less the $500. Even though the average cost of an attack could not be measured correctly, because of insufficient information, most of the respondents had a feeling that the attacks cost the Port less than $1,000 (70.8) (see Fig. 8 below).

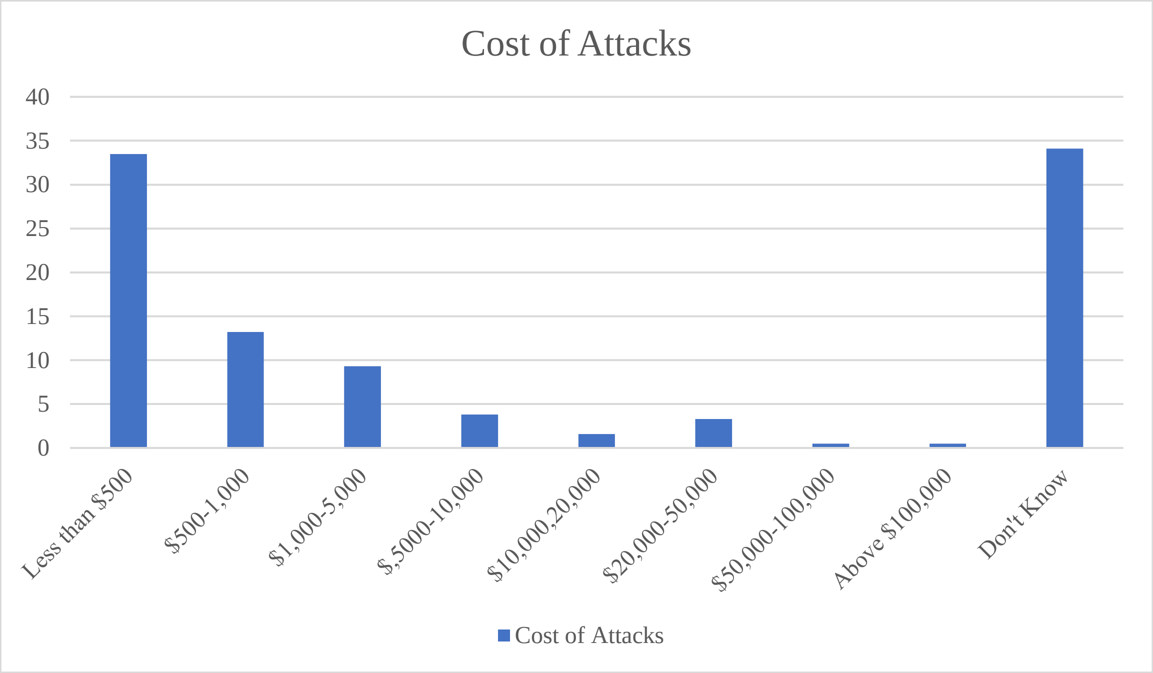

Figure 8: Cost of Attacks

Question 8: How was the attacks or breach in Question 5 identified?

Nearly half (48.4%) of the attacks were detected by anti-malware or anti-virus program. The second most common method of identification was business disruption (22.5%), i.e., whenever there was a disruption to the Port's operations, they look into possibility of a cyberattack as the cause of disruption. The third most common method of identification as noted by the respondents was an accident (21.4%). The fact the 21.4% of the incidents were identified through accident implied that a large number of the breaches were not detected. The more proactive methods, i.e., internal security monitoring and reports from staff or contractors, were ranked at 13.2% and 14.8%, respectively (see Fig. 9 below). Even though a small percentage of the attacks were identified through internally set measures, it still indicates that the Port has an organizational structure for cybersecurity threats, i.e., internal control mechanisms are active within the Port to some extent.

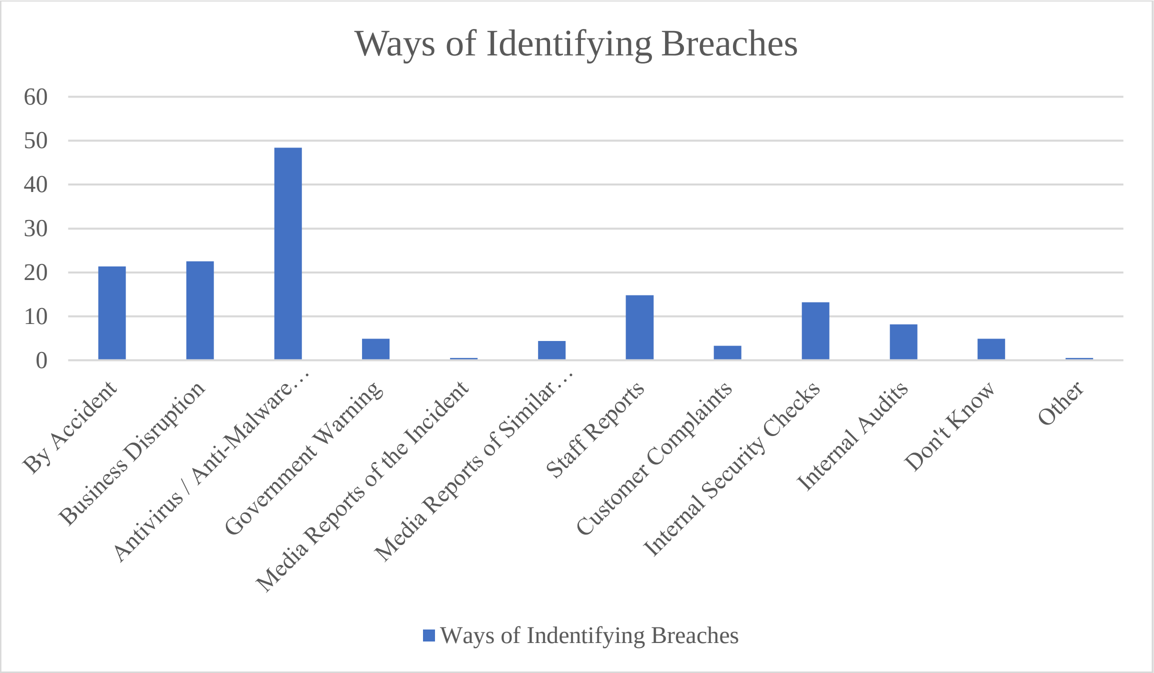

Figure 9: Ways of Identifying Breaches

Question 9: In which of the following ways below have the attacked you experienced in Question 5 have these impacted the Port of Freetown?

Even though, according to Fig. 10 below, there was a considerable variety in replies regarding the impact of the attacks, two impacts stood out including high recovery costs (46.2%) and preventing staff from carrying out their daily tasks (53.8%). These impacts can be considered as direct consequences of disruption to the Port's continuity. Also, being forced to implement new ways of mitigating future attacks was also an impact of the attacks (22.0%). Only 1.6% of the respondents felt that the attacks caused loss of revenue to the Port, while an additional 6.6% of the respondents felt that the attacks damaged the reputation of the port.

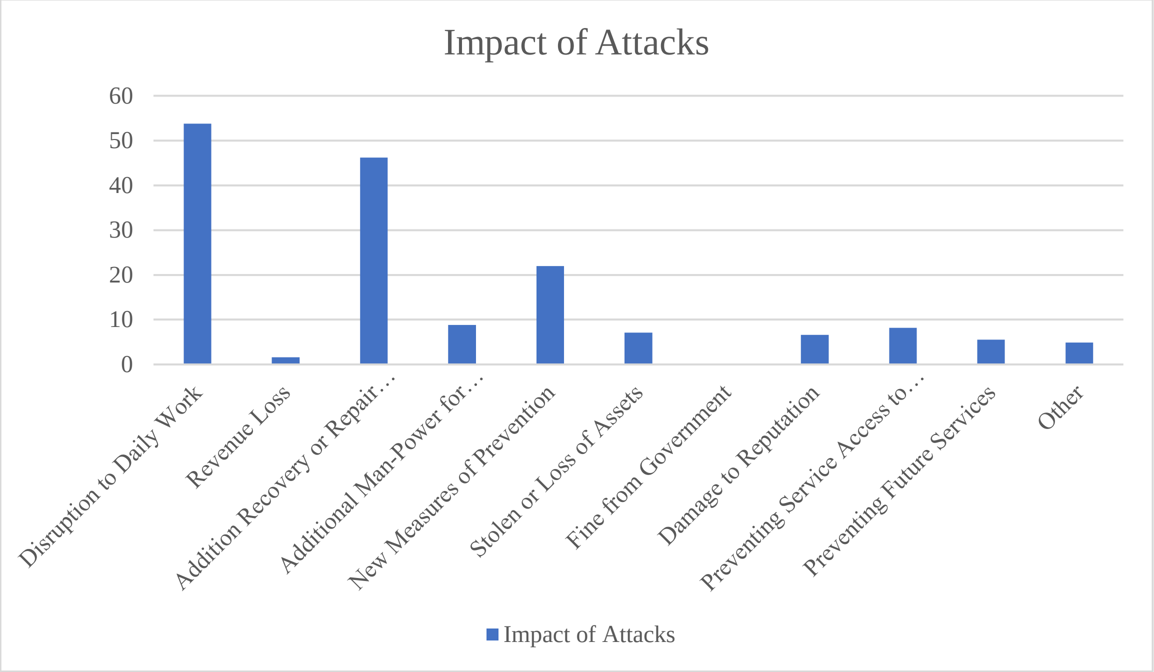

Figure 10: Impact of Attacks

4.2.3. The Awareness of Cybersecurity Threats at the Port of Freetown and Mitigation Measures

The rest of the questions in the survey instrument were used to evaluate the level of cybersecurity threats at the Port of Freetown and the mitigation measures put in place by the Port.

Question 10: Which of the following issues are included in your cyber security-related policies, or policy?

Less than half of the participants (42.4%) were not aware of any formal cybersecurity policies within the Port. 44.5% of the respondents were aware of the security aspects of removable devices and 32.9% were aware of the acceptable behavior of Port staff. 29.6% of the participants were aware of the fact that personally-owned devices can cause security problems to the Port. Others (24.1%) were also aware of the potential problems that cloud computing might bring to the Port as well as remote working (29.9%) (see Fig. 11 below).

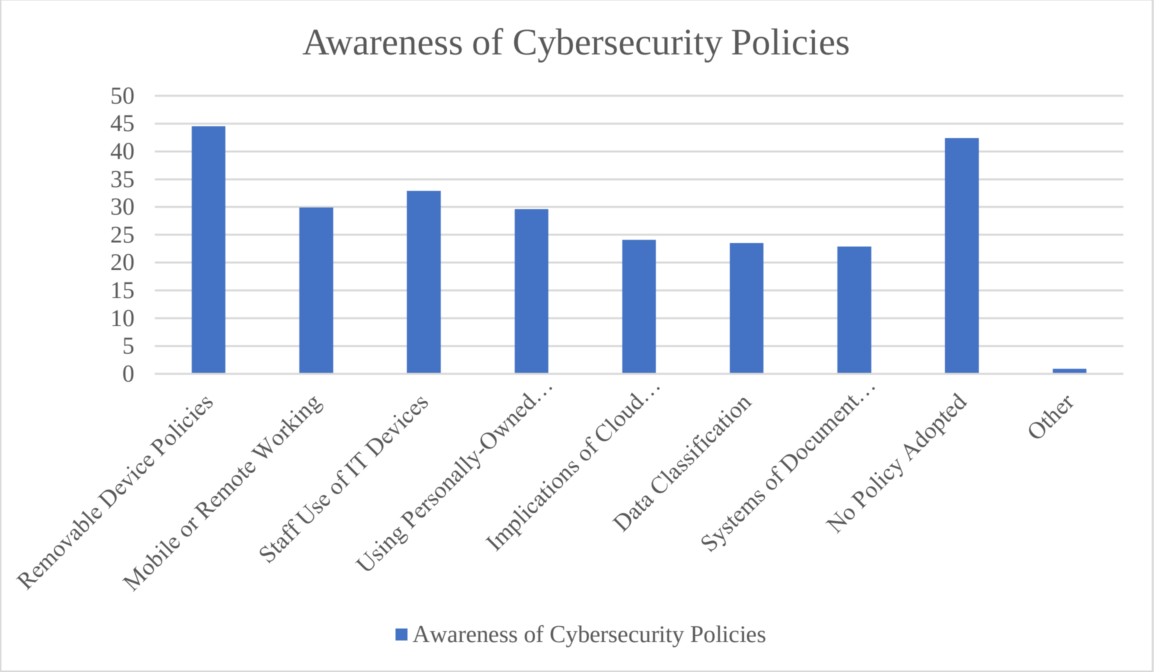

Figure 11: Awareness of Cybersecurity Policies

Question 11: How low or high of a priority is cybersecurity the Port of Freetown's management?

Exactly 35.4% of the respondents felt that cybersecurity was a 'very low' or 'low' priority to the management of the Port. Another 32.1% of the persons surveyed felt that cybersecurity was a 'very high' or 'high' priority to the management of the Port, while the rest 32.6% were neutral (see Fig. 12 below).

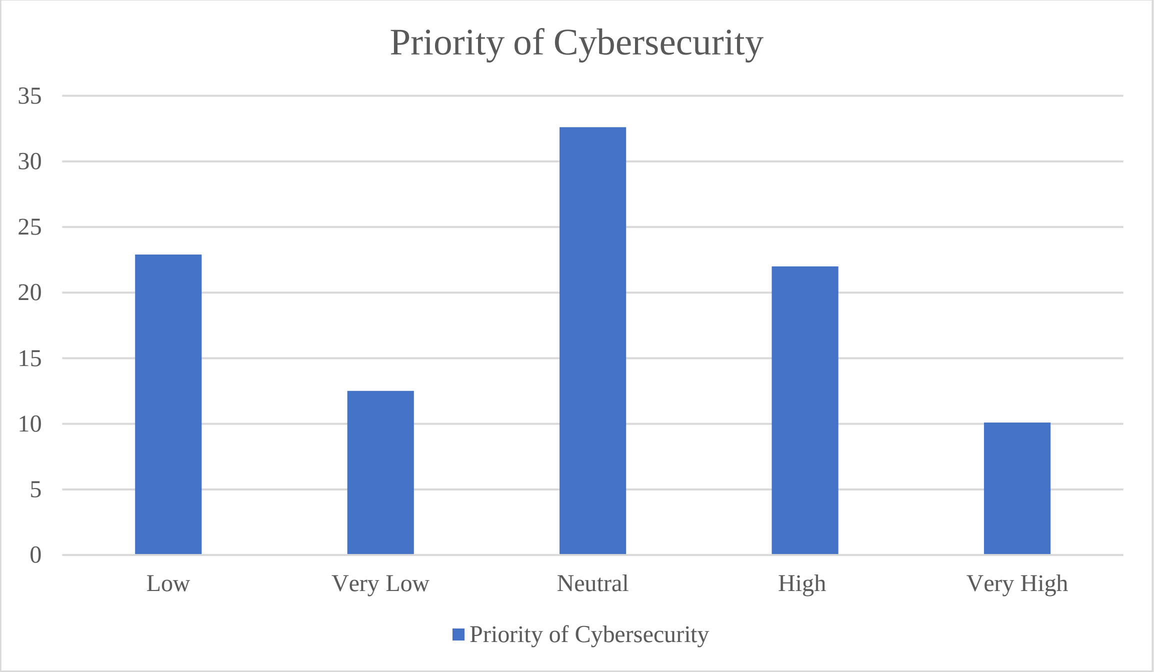

Figure 12: Priority of Cybersecurity

Question 12: Over the last 1 year, has the Port of Freetown provided workers with internal cyber security trainings?

36.9% of the respondents were not aware of any internal cybersecurity training that had taken place in the Port within the last 12 months. 55.8% of the respondents were aware of at least one training of cybersecurity awareness training that had taken place at the Port within the last 12 months (see Fig. 13 below). The lack of awareness can be attributed to the fact that perhaps not each and every employee at the Port of Freetown is trained on cybersecurity issues.

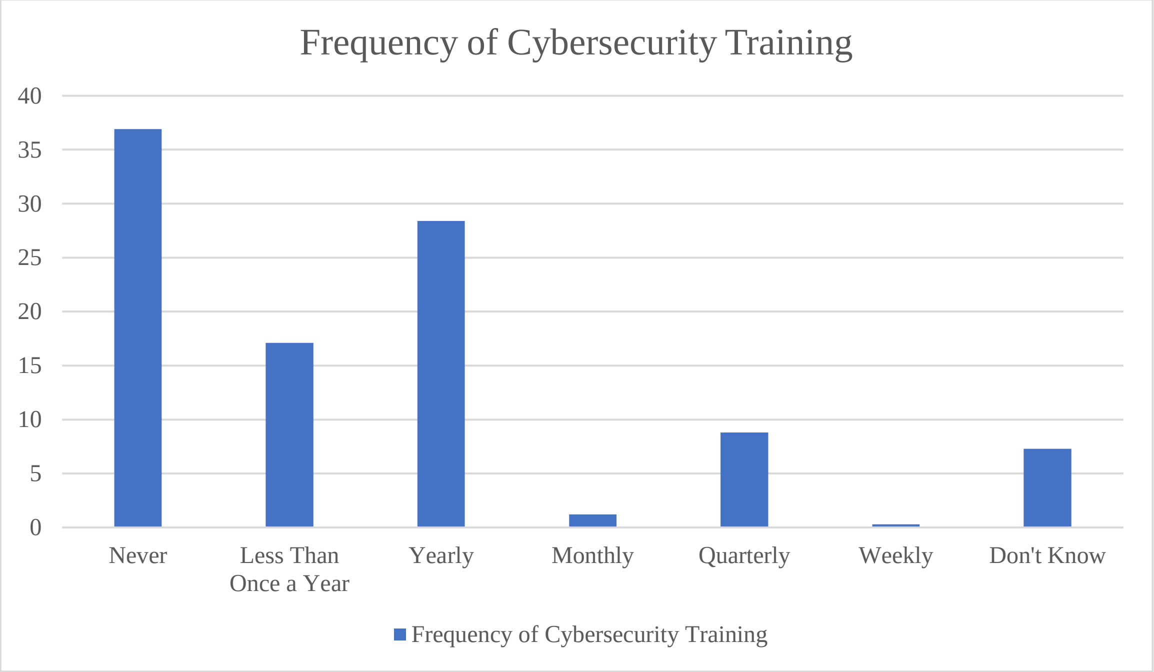

Figure 13: Frequency of Cybersecurity Training

Question 13: Please select some of the risk management or governance arrangements you have in place

28.% of the respondents were not aware of the existence of any risk management or governance arrangements at the Port (Chiappetta, 2017). The respondents who were aware of the risk management or governance arrangements present at the Port ticked employees tasked with dealing with cybersecurity (41.8%), board members tasked with dealing with cybersecurity (36.0%). This meant that cybersecurity within the Port was mainly managed through internal mechanisms involving human factors. Nearly 30.2% of the respondents claimed to be aware of the policies dealing with cybersecurity, and 22.6% of the respondents seemed to be aware of the fact that the Port outsources cybersecurity experts. Finally, 14.0% of the participants claimed that a business continuity plan was in place in case of a cyberattack (see Fig. 14 below).

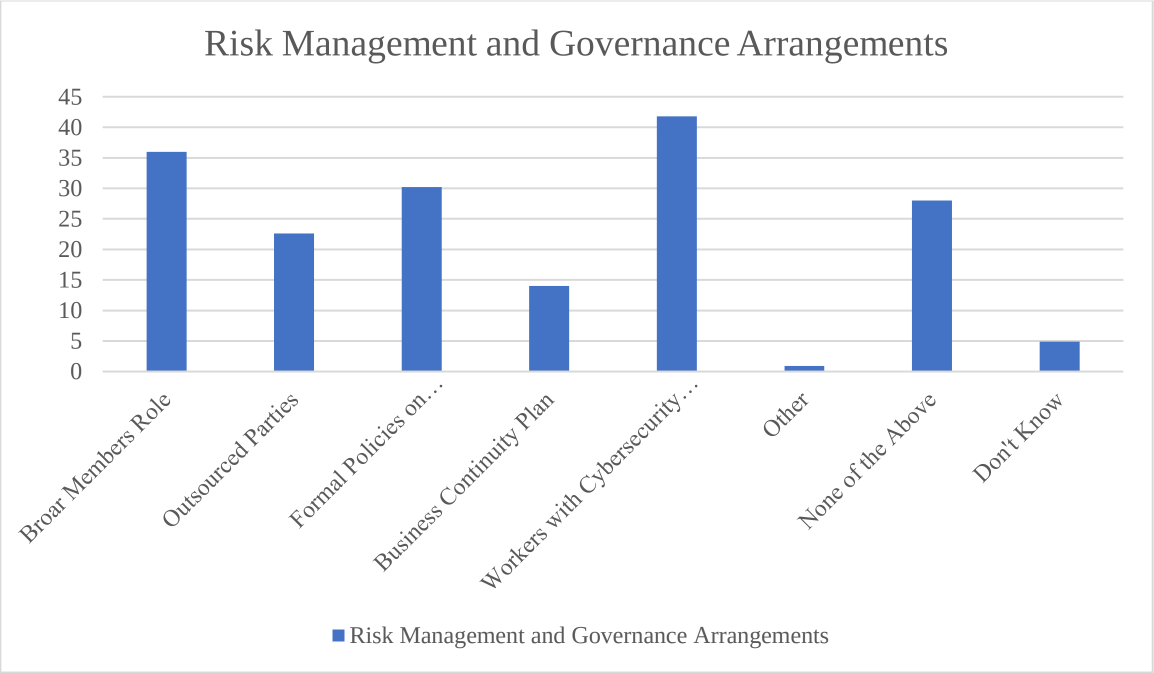

Figure 14: Risk Management and Governance Arrangements

Question 14: Please select all of the rules that you have in place from the list below

82.0% of the respondents confirmed that the Port had some form of rule to manage cybersecurity risks. Along the rules chosen by the respondents included regular checks (68.3%), ad-hoc checks (27.4%), and internal audits (22.6%). This pointed to the fact that the Port carried regular checks on their cybersecurity threats (see Fig. 15 below).

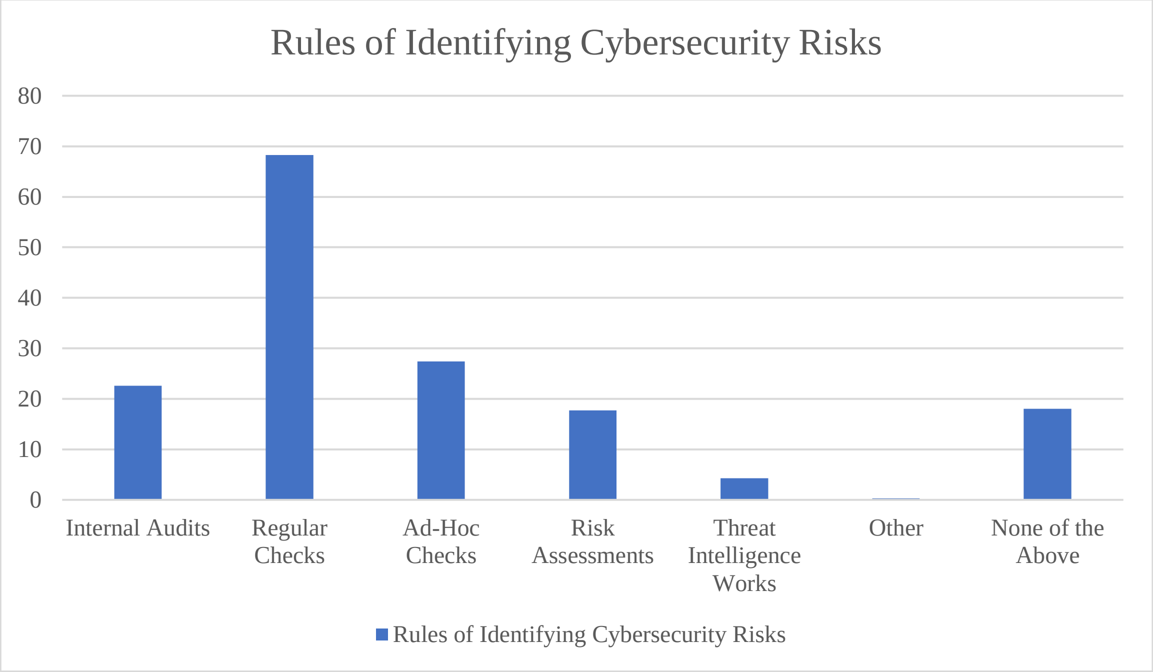

Figure 15: Rules of Identifying Cybersecurity Risks

Question 15: Do you have insurance which would cover you in the event of a cyber security breach or attack?

Insurance grants businesses an extra layer of protection in case of financial loss as a way of risk management (Chiappetta & Cuozzo, 2017). Nonetheless, insurance seemed to not be a crucial part of the Port's operations as only 9.1% of the respondents were aware of the fact that the Port has an insurance cover on cybersecurity (see Fig. 16 below).

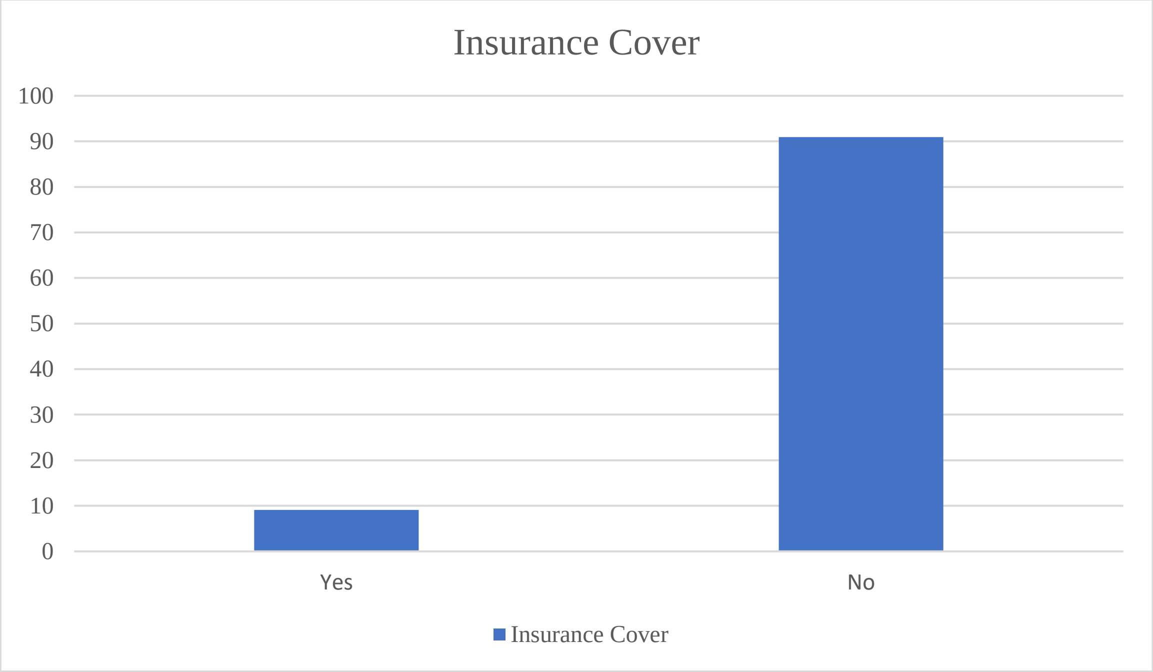

Figure 16: Insurance Cover

Question 16: Where are the attacks or breaches reported to?

More than 50% of the respondents thought that the best place of reporting any attack or breach is to the police. Other respondents (17.4%) chose the National Intelligence Service (NIS). Antivirus companies were ranked at 30.5% while credit card companies and bank were ranked at 19.2%. Other options included website administrators (17.7%), ISPs (18.9%), and outsources cybersecurity providers (27.1%). The above findings pointed to the fact that the Port reported both to public and private agencies when faced with cyberattacks (see Fig. 17 below).

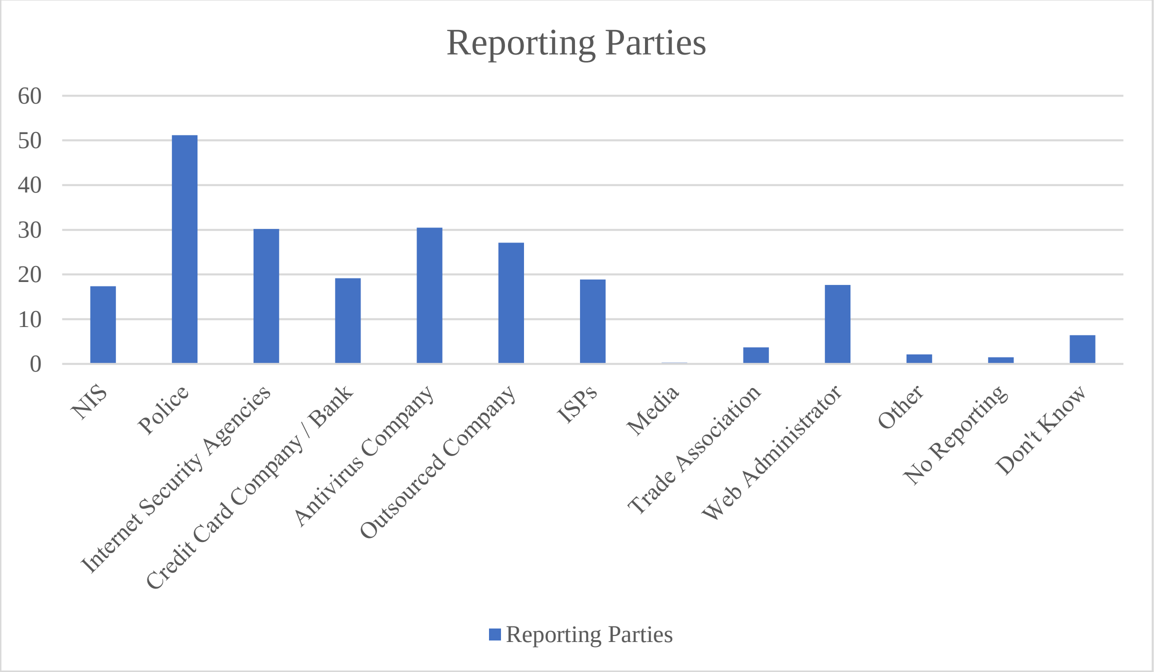

Figure 17: Reporting Parties

Question 17: From where have you sought guidance, advice or information on the cybersecurity threats that the Port of Freetown faces?

A majority of the respondents (54.3%) searched for information on major web portals on ways of managing cybersecurity threats. 29.6% of the respondents used government websites and a further 29.9% of the respondents consulted with their colleagues and other experts at the Port. 12.2% of the respondents sought information from the senior management. This finding meant that information sharing was more frequent among staff compared to staff and the senior management at the Port. When it came to public organizations, the NIS (6.4%) and police (6.7%) were not used to a large extent (see Fig. 18 below).

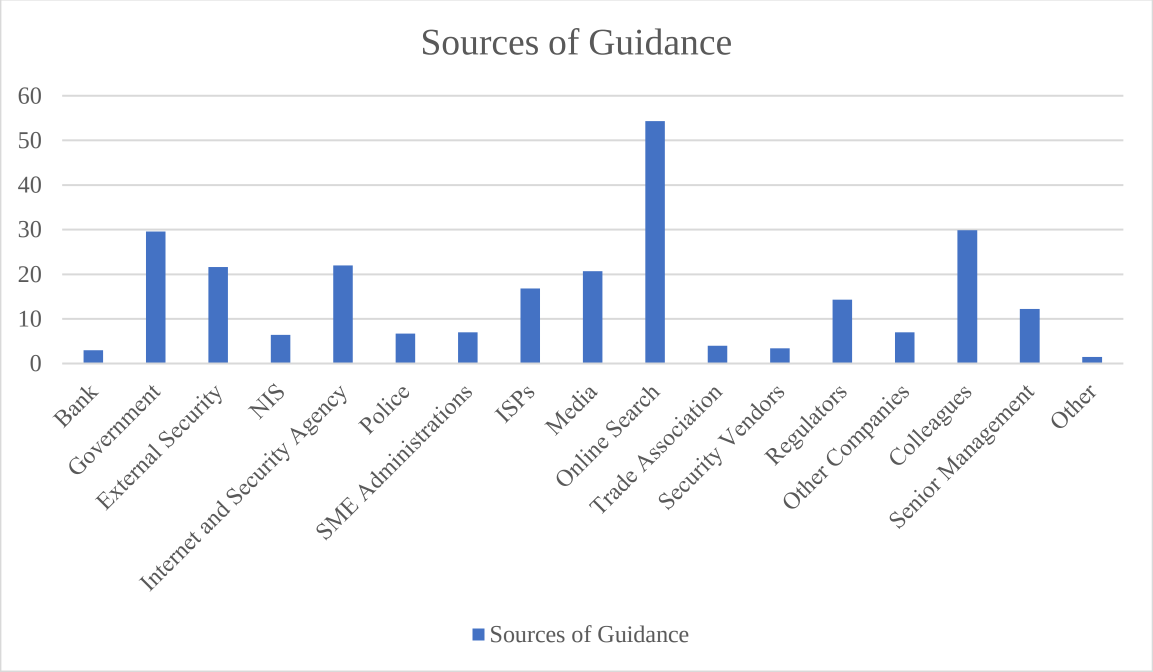

Figure 18: Sources of Guidance

Question 18: Are you aware of any of the following initiatives and standards?

44.8% of the respondents were not aware of any accreditation standards or schemes relating to cybersecurity. 31.4% of the respondents were aware of the ISO 27001 and 44.8% were aware of NIST Cybersecurity Framework. Government guidance was familiar to 6.7% of the respondents, while a further 13.1% of the respondents were aware of a Security Operation Center that can help the Port. The apparent lack of Sierra Leone’s Government guidance might point to poor support from the government (see Fig. 19 below).

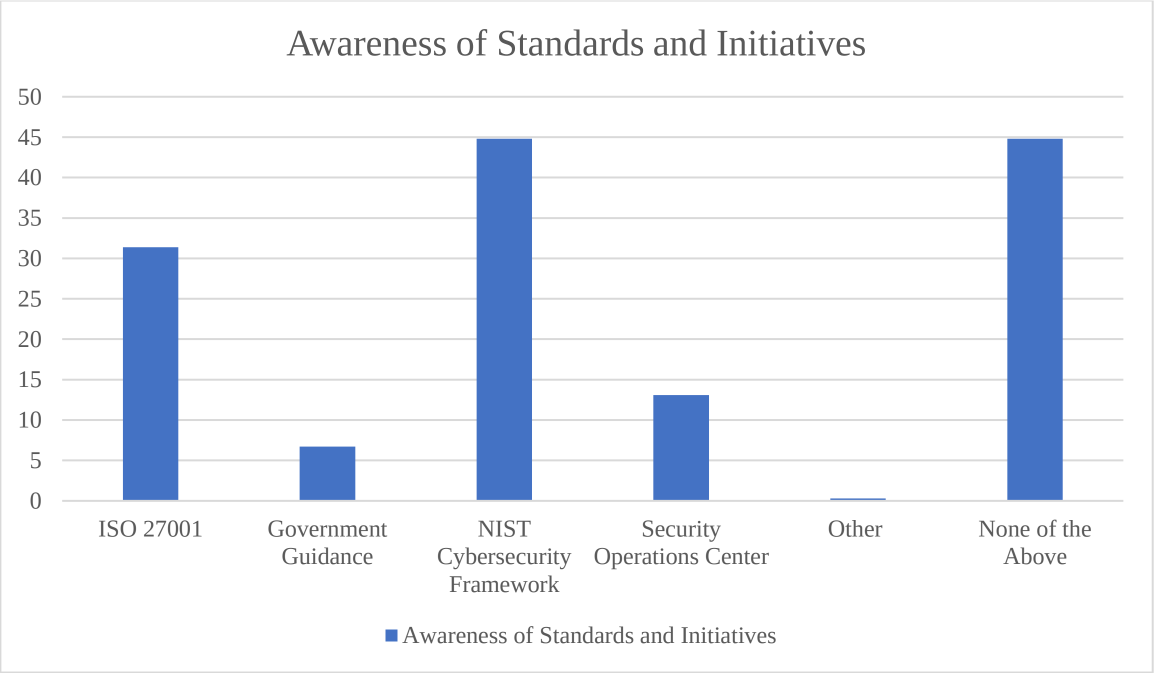

Figure 19: Awareness of Standards and Initiatives

Question 19: Which of the following, if any, do your clients require you to have or adhere to?

63.7% of the respondents were not aware of the Port's client were supposed to adhere to any cybersecurity standard. 26.8% of the respondents claimed that the clients need to adhere to Government's schemes while 18.0% of the respondents claimed that the clients need to adhere to the NIST Cybersecurity Framework (see Fig. 20 below).

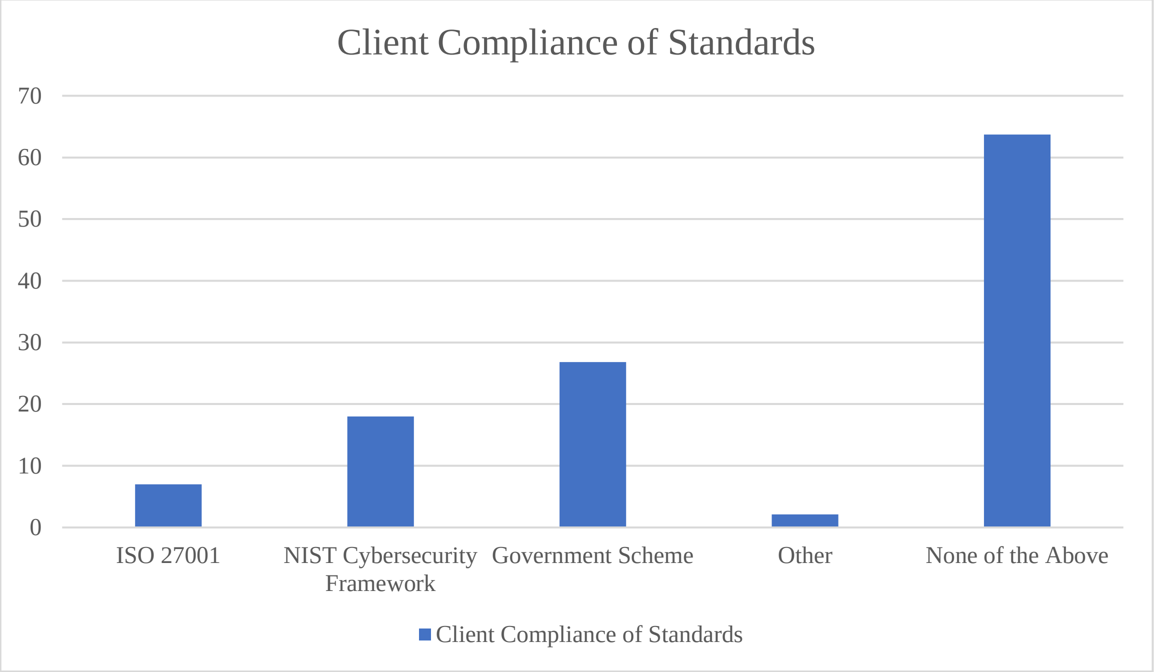

Figure 20: Client Compliance of Standards

4.3. Discussion

When it came to understanding the extent to which the Port of Freetown is exposed to cybersecurity risks, it was noted that the Port highly depends on online services, use of externally-hosted web services, and use of personally-owned devices as work, which makes them highly susceptible to risk. 77.7% of the respondents used personally-owned devices to some extent in their work operations, plus the Port also heavily relied on externally-hosted web services. The dependence of online services blurs spatial and temporal boundaries of traditional business management, something which most developing countries such as Sierra Leone are accustomed to. This trend has also encouraged the use of externally-hosted web services and personally-owned devices, which poses a great risk to organizations such as the Port of Freetown (DiRenzo et al., 2015). Personally-owned devices that retain business information can be lost or misplaced, and as a result, it can lead to companies losing sensitive data or their intellectual property. Furthermore, the use of personally-owned devices might offer a criminal opportunity to workers with malicious intentions (Jones et al., 2016). For externally-hosted web services, it implies that all a company's information is stored in third-party servers, which are vulnerable to outsider threats. Organized criminals and hackers are known to target servers that store business information for personal reasons, economic intelligence, and/or pecuniary gains.

When it came to understanding the seriousness of cybersecurity breaches at the Port of Freetown, two issues were taking into consideration, including the frequency of the attacks and the impact of the attacks. The analysis revealed that the respondents were aware of at least one cyberattack that had taken place at the Port in the last 12 months. Others noted that the Port had experienced more than one cyberattack in the last 12 months. The findings were in line with (Newman, 2019) who claimed that 52.5% of shipping ports the world over had experienced cyberattacks in 2018. The reason behind this is the shipping ports in most developing countries do not have sufficient resources to effective detect and prevent cyberattacks (Tam & Jones, 2018). Tam and Jones (2018) attributed this trend to the asymmetric nature of cyberattacking arguing that a disproportionately large number of cyberattacks are executed prior to the attackers penetrating the security and damaging the system. This implies that shipping ports in developing countries such as Sierra Leone, with their minimal resources, tend to accept as a norm a huge volume of attempted attacks, and this cannot be prevented because of the nature of cyberattacks. The apparent lack of awareness was related to how shipping ports from developing countries perceive cyberattacks.

Finally, when it came to understanding the Port of Freetown's preparedness to cybersecurity attacks, this research focused on two issues including the Port's approach to cybersecurity risks and how they deal with attacks. The first issue focuses on the Port's general readiness to risks, including their employees' perceptions, internal practices and policies, decision-making processes, and organizational culture. The second issue focuses involves arrangements made by the Port to deal with breaches. The overall view from the survey was that the Port was not prepared to manage cybersecurity risks, because all the questions were full of negative responses from the respondents. This reflects with other studies that suggest that shipping ports that are mostly affected by cybersecurity issues have poorly trained employees (Herrera et al., 2017), no risk management policy or practices (Ahokas et al., 2017), and poor updates by the senior management on ways of dealing with cyber security (Beaumont, 2018). This implies that such shipping ports do not merit organizational responses to cybersecurity, which makes them more vulnerable.

The blindness or lack of awareness towards maritime cybersecurity in Sierra Leone and other ports neighboring country's sea ports, e.g., Guinea, Guinea Bissau, Liberia, Cote d'Ivoire, and The Gambia, has been attributed to the poor lack of awareness of the roles oceans play when it comes to the development of a country. Such countries shipping ports can positively contribute to their economic development, but are usually crippled with stories of stolen resources, drowning refugees, and missed opportunities (Pretorius & van Niekerk, 2016). The consequences are overly astounding. Cyber-attacks are estimated to cost West African states roughly US$1 billion annually in lost revenue. An estimated 50-60 tons of cocaine moves from West African ports to Europe annually blindly due to poor systems of checks (Zăgan et al., 2018). Despite of this, states continue depending on sea trade to improve their economic state and food security.

Most West African states lack policies for ocean governance. None of the countries mentioned above, i.e., Sierra Leone, Guinea, Guinea Bissau, Liberia, Cote d'Ivoire, and The Gambia, have dedicated coast guards or a body charged with improving the state of cybersecurity within the ports. Over 90% of the abovementioned countries' trade is seaborne. Fishing and food import contributes to a majority of the food security in the abovementioned countries, as well as importation of oil and gas. The lack of extensive maritime cybersecurity has made it impossible for West African states to effectively monitor their operations (Doyon-Martin, 2015). The implications are not only damaging to the ports, but the states as a whole.

CHAPTER FIVE - CONCLUSION

5.1. Summary

This dissertation has found that the incidence of cyberattacks across the globe has increased and that while technological advances are welcome, they also bring with them more risks and threats. Further, there is a noted increase in the awareness of the concept of cybersecurity although there are still gaps in implementing functional and sustainable policies and measures especially in the least developed and developing countries. The research questions were:

1. To what extent is the Port of Freetown exposed to cybersecurity threats?
2. How serious are cybersecurity breaches for the Port of Freetown?
3. To what extent is the Port of Freetown prepared to mitigate or prevent cybersecurity threats?

The above research questions were designed to understand the thoughts and attitudes held by stakeholders in the maritime industry in Sierra Leone in general and the Port of Freetown in particular given that it is the biggest and busiest in the country. This understanding helped the researcher contextualize the extent to which the stakeholders are aware of the cyberspace aspect of the environment in which they operate and how they perceive their roles and responsibilities. The dissertation described the concepts of risk, threat and vulnerability as well as maritime safety and security and how they relate to the maritime industry in Sierra Leone. The dissertation also presented critical maritime-related information systems so as to highlight the different information systems that the industry operators depend on in safeguarding maritime transport. Using questionnaire interviews, the research found that maritime operators in Sierra Leone are considerably aware of both the physical and cybernetic environments in which they operate. The significance of the mention of the physical environment is that it is the venue of all the maritime operations, including the cyber aspect. From the literature review, it was inferred that there is considerable knowledge of the security aspect of the general cyberspace although the implementation of security measures based on the available knowledge is not happening at the desired rate. The types of actors have been profiled as government terrorist; hacktivist; hacker; insider; government; industrial spy; and organized criminals. Their motivations are social; ideological; egoism; religious; political; economical; and informational. The main cyber threats they present are cyber war; cyber terrorism; hacktivism; cyber espionage and cyber criminality.

5.2. Main Conclusions

The main conclusion in this dissertation is that cybersecurity awareness at the Port of Freetown is below average because the port itself is considerably exposed to cybersecurity threats. Effectively, the presence of the threats and even their materialization makes it difficult to comprehensively understand when a maritime operator has been attacked and the type of actors involved. It is also concluded from the questionnaire interviews that that while the critical information systems and technologies in use in maritime operations in Sierra Leone are numerous, most of the cyberattacks are email-based. Besides the emails, there are also attacks that exploit the vulnerabilities of ICT systems installed in vessels although these were found to be less common. However, it was a considerable challenge to make an authoritative conclusion on whether cybersecurity in the Sierra Leonean maritime industry should be appraised from the perspective of maritime security or maritime safety. On one hand, cybersecurity has been viewed as a component of maritime safety aimed at mitigating natural and unintended risk, threat and injury. On the other hand, as seen in the literature review, some cyberattacks have specifically targeted a particular maritime operator. The implication, as supported by some responses in the interviews, is that cybersecurity should be investigated and appraised from the perspective of maritime cybersecurity because its aim is to protect the industry against hazards and illegal and deliberate acts including terrorism and piracy.

It is also concluded that only the major maritime operators have the capacity to go beyond simply specifying cybersecurity but also implementing practical and sustainable security operations. More specifically, Port of Freetown currently does not have the required capacity to actually detail cybersecurity as its own security operation; rather, it is still evolving although the progress cannot be underrated. Summarily, it is concluded that no upper ceiling can be set for awareness on the procedures of cybersecurity. It is a dynamic concept and the onus is on the maritime operators to update the protective measures they use. The bottom line, though, is that the Sierra Leonean maritime industry is generally taking the right direction to raise awareness of the significance and implications of maritime cybersecurity, or the lack thereof.

5.3. Research Recommendations

It is hereby recommended that authorities in Sierra Leone start by adopting a universally acceptable IMO practices and then plan to invest in implementing measures supported by the provisions of IMO. Looked in the same view as other comparative jurisdiction such as Somalia, Sierra Leone has made noteworthy advances in port operations. Therefore, in order to improve efficiency and economic growth, it is recommended that the authorities benchmark using standards from other jurisdictions in the EU.

Fortunately, West African states have been paying increasing attention to maritime cybersecurity. The countries are increasingly becoming aware of the fact that they cannot secure their maritime domain alone. Not even highly advanced nations such as the U.S. and the U.K. are capable of that kind of control over their ports. This is because the cyberspace does not have a fence and everyone is a player, including cybercriminals (Greenberg, 2018). The best chance to ensure a secure port in terms of its cyberspace is through international cooperation. The AU Agenda 2063 considers the marine economy as a leading contributor to growth, and the 2050 Africa's Integrated Maritime Strategy (2050 AIMS), acknowledges the vast potential of wealth creation of African's shipping ports. The initiatives call for maritime education and development of African shipping ports with regards to their views towards cybersecurity (Peura, 2017). Such African countries as South African, Tanzania and Mozambique, which record the lowest rate of successful cyberattacks have signed cooperation agreements among each other to establish maritime domain awareness centers so as to share information on cybersecurity threats. The information includes detailed plans to improve cybersecurity in the following areas: marine manufacturing and transportation, aquaculture and marine protection, offshore oil and gas exploration, and ocean governance (Cheng et al., 2018).

5.4. Research Limitations

The key limitations of this study included its focus on just one port in a developing country and the small number of interviewees. The focus on a single port may have failed to generate results that can comprehensively be generalized to other ports even within the same region given the sharp discrepancies in economic status between developing countries. Then, the small number of interviewees limited the amount of primary input directly from the concerned stakeholders. However, the choice of the Port of Freetown was also considered to be practical given that up to 60% of the country's inbound and outbound freight passes through it. By virtue of being one of the busiest ports in the West African region, it provides a realistic scenario for investigation.

5.5. Suggestions for Further Research

This study, like most of the existing works that were used in the literature review, focused on the technical dimension of cybersecurity. This is an important approach given that the entire idea is driven by technology and the fact that technology is a dynamic rather than static notion. However, it is imperative to note that operation of technology cannot be investigated in isolation of the human factor. It is therefore recommended that further research focuses on the role of the human factor in compromising cybersecurity in the maritime industry. This is to say that besides natural threats, future studies should focus on both intentional and unintentional threats posed by humans.

REFERENCES

Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L. M. (2017). Cybersecurity in ports: a conceptual approach. In *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* (pp. 343-359). Berlin: epubli GmbH.

Attia, M., & Edge, J. (2017). Be (com) ing a reflexive researcher: a developmental approach to research methodology. *Open Review of Educational Research*, *4*(1), 33-45.

Beaumont, P. (2018). Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR. In *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 497-516). IGI Global.

Boggero, M. (2018). Sierra Leone: Continuity and Change. In *The Governance of Private Security* (pp. 149-159). Palgrave Macmillan, Cham.

Bothur, D., Zheng, G., & Valli, C. (2017). A critical analysis of security vulnerabilities and countermeasures in a smart ship system.

Brasington, H., & Park, M. (2016). Cybersecurity and ports: Vulnerabilities, consequences and preparation. *Ausmarine*, *38*(4), 23.

Cheng, Q., Cunningham, C., Gacayan, F., Gu, A., Hall, A., Lee, O., ... & Yi, J. (2018). Hacking Democracy: Cybersecurity and Global Election Interference.

Chiappetta, A. (2017). Hybrid ports: the role of IoT and CyberSecurity in the next decade. *Journal of Sustainable Development of Transport and Logistics*, *2*(2), 47-56.

Chiappetta, A. (2017). Hybrid ports: the role of IoT and CyberSecurity in the next decade. *Journal of Sustainable Development of Transport and Logistics*, *2*(2), 47-56.

Chiappetta, A., & Cuozzo, G. (2017, June). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* (pp. 206-211). IEEE.

Chiappetta, A., & Cuozzo, G. (2017, June). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* (pp. 206-211). IEEE.

Daum, O. (2019). Cyber Security in the Maritime Sector. *Journal of Maritime Law and Commerce*, *50*(1), 1-19.

Diggins, J. (2018). *Coastal Sierra Leone: Materiality and the Unseen in Maritime West Africa* (Vol. 55). Cambridge University Press.

DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015, July). The little-known challenge of maritime cyber security. In *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)* (pp. 1-5). IEEE.

Doyon-Martin, J. (2015). Cybercrime in West Africa as a result of transboundary e-waste. *Journal of Applied Security Research*, *10*(2), 207-220.

Eiza, M. H., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, *12*(2), 45-51.

Fowler, D. S., Cheah, M., Shaikh, S. A., & Bryans, J. (2017, March). Towards a testbed for automotive cybersecurity. In *2017 IEEE International Conference on Software Testing, Verification and Validation (ICST)* (pp. 540-541). IEEE.

Glesne, C. (2016). *Becoming qualitative researchers: An introduction*. Pearson. One Lake Street, Upper Saddle River, New Jersey.

Gray, D. E. (2019). *Doing research in the business world*. Sage Publications Limited.

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*, *August*, *22*.

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *The Journal of Navigation*, *71*(5), 1025-1039.

Herrera, A. V., Ron, M., & Rabadão, C. (2017, June). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-4). IEEE.

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region*, *14*(3), 354-366.

International Maritime Organization (IMO). (2019). *Resolution MSC.428(98): Maritime cyber risk management in safety management systems*. Retrieved from http://www.imo.org/en/OurWork/Facilitation/docs/FAL%20related%20nonmandatory%20instruments/RESOLUTION%20MSC.428-98.pdf

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018, October). Detecting and hunting cyberthreats in a maritime environment: specification and experimentation of a maritime cybersecurity operations centre. In *2018 2nd Cyber Security in Networking Conference (CSNet)* (pp. 1-8). IEEE.

Jensen, L. (2015). Challenges in maritime cyber-resilience. *Technology Innovation Management Review*, *5*(4), 35.

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security.

Jović, M., Tijan, E., Aksentijević, S., & Čišić, D. (2019, May). An Overview Of Security Challenges Of Seaport IoT Systems. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1349-1354). IEEE.

Jović, M., Tijan, E., Aksentijević, S., & Čišić, D. (2019, May). An Overview Of Security Challenges Of Seaport IoT Systems. In *2019 42nd International Convention on*

Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1349-1354). IEEE.

Kessler, G. C. (2019). Cybersecurity in the Maritime Domain. *USCG Proceedings of the Marine Safety & Security Council*, *76*(1), 34.

Kessler, G. C. (2019). Cybersecurity in the Maritime Domain. *USCG Proceedings of the Marine Safety & Security Council*, *76*(1), 34.

Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *12*(3), 429.

Kumar, R. (2019). *Research methodology: A step-by-step guide for beginners*. Sage Publications Limited.

Lagouvardou, S. (2018). Maritime Cyber Security: concepts, problems and models. *Kongens Lyngby, Copenhagen*.

McGillivary, P. (2018). Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed. *Marine Technology Society Journal*, *52*(5), 44-57.

McGillivary, P. (2018). Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed. *Marine Technology Society Journal*, *52*(5), 44-57.

Meyer-Larsen, N., & Müller, R. (2018, February). Enhancing the Cybersecurity of Port Community Systems. In *International Conference on Dynamics in Logistics* (pp. 318-323). Springer, Cham.

Ministry of Transport and Aviation. (2019). *Sierra Leone Maritime Administration*. Retrieved from https://mta.gov.sl/sierra-leone-maritime-administration

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23-48.

Mraković, I., & Vojinović, R. (2019). Maritime Cyber Security Analysis–How to Reduce Threats?. *Transactions on maritime science*, *8*(01), 132-139.

Newman, N. (2019). Cyber pirates terrorise the high seas. *Engineering & Technology*, *14*(4), 54-57.

Newman, N. (2019). Cyber pirates terrorise the high seas. *Engineering & Technology*, *14*(4), 54-57.

Okeke-Ogbuafor, N., Gray, T., & Stead, S. M. (2018). The controversial role of foreign fisheries consultants in Sierra Leone's coastal waters. *Marine Policy*.

Peura, R. (2017). Maritime Cybersecurity and Improvement of Project Execution Process.

Polemi, N. (2017). *Port cybersecurity: securing critical information infrastructures and supply chains*. Elsevier.

Pretorius, B., & van Niekerk, B. (2016). Cyber-security for ICS/SCADA: a south African perspective. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *6*(3), 1-16.

Quinlan, C., Babin, B., Carr, J., & Griffin, M. (2019). *Business research methods*. South Western Cengage.

Schwab, K. (2017). *The fourth industrial revolution*. Currency.

Silverman, D. (Ed.). (2016). *Qualitative research*. Sage.

Śliwiński, M., & Piesik, E. (2018). Functional safety with cybersecurity for the control and protection systems on example of the oil port infrastructure. *Journal of Polish Safety and Reliability Association*, *9*.

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.

Svilicic, B., Rudan, I., Frančić, V., & Mohović, D. (2019). Towards a Cyber Secure Shipboard Radar. *The Journal of Navigation*, 1-12.

Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129-163.

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

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

The European Union Agency for Cybersecurity (ENISA). (2019). *Port cybersecurity: Good practices for cybersecurity in the maritime sector*. Retrieved from https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport

Trimble, D., Monken, J., & Sand, A. F. (2017, November). A framework for cybersecurity assessments of critical port infrastructure. In *2017 International Conference on Cyber Conflict (CyCon US)* (pp. 1-7). IEEE.

United Nations Conference on Trade and Development (UNCTAD). (2017). *Review of Maritime Transport 2017*. UNCTAD, New York.

United Nations. (2015). Review of Maritime Transport. *United Nations Conference on Trade and Development (UNCTAD)*. New York and Geneva.

van Erp, J. (2017). New governance of corporate cybersecurity: a case study of the petrochemical industry in the Port of Rotterdam. *Crime, Law and Social Change*, *68*(1-2), 75-93.

Wilshusen, G. C. (2015). *Maritime critical infrastructure protection: Dhs needs to enhance efforts to address port cybersecurity* (No. GAO-16-116T).

Zăgan, R., Raicu, G., Hanzu-Pazara, R., & Enache, S. (2018). Realities in maritime domain regarding cyber security concept. In *Advanced Engineering Forum* (Vol. 27, pp. 221-228). Trans Tech Publications.

Zăgan, R., Raicu, G., Hanzu-Pazara, R., & Enache, S. (2018). Realities in maritime domain regarding cyber security concept. In *Advanced Engineering Forum* (Vol. 27, pp. 221-228). Trans Tech Publications.

APPENDICES

Appendix One – Survey Questions

Question Relating to Operational Environment of the Port of Freetown

1. Which of the following, if any, does the Port of Freetown currently have or use? (multiple choice)
   A. Email addresses for the port or its employees
   B. A website or blog
   C. Accounts or pages on social media sites (e.g. Facebook or Twitter)
   D. The ability for your customers to order, book or pay for products or services online
   E. An online business bank account the port pays into
   F. Other
2. To what extent, if at all, are online services a core part of the goods or services the Port of Freetown provides?
   A. Not at all important
   B. Not very important
   C. Neutral
   D. Important
   E. Very important
3. How many employees in the Port of Freetown use personally-owned devices such as smartphones, tablets, home laptops or desktop computers to carry out regular business-related activities?
   A. None
   B. 1-20%
   C. 21-40%
   D. 41-60%
   E. 61-80%
   F. 81-100%
4. How important, if at all, are these externally-hosted web services to the Port of Freetown?
   A. Not at all critical
   B. Not very critical
   C. Neutral
   D. Critical
   E. Very critical

Questions Relating to the Current State of Cybersecurity at the Port of Freetown

5. Which of the following have happened to at the Port of Freetown in the last 1 year? (multiple choice)
   A. Denial-of-service attacks
   B. Access to computers, networks or services without permission (i.e., hacking)
   C. Money stolen electronically (e.g. through online banking)
   D. Money stolen through fraudulent emails or fake websites
   E. Personal information (e.g. customer data) stolen electronically
   F. People damaging or stealing software from your computers or network, even if accidentally
   G. People downloading unlicensed or stolen software to your computers or network, even if accidentally
   H. Computers becoming infected with viruses, spyware or malware
   I. Theft of intellectual property

J. Others impersonating company in emails or online
K. Breaches from personally-owned devices
L. Breaches from externally-hosted web services
M. Breaches on social media
N. Other

6. As far as you know, who or what was the source of the breach or attack? (multiple choice)
   A. Third party suppliers
   B. Activists
   C. Competitors
   D. Emails/email attachments/websites
   E. Current employees
   F. Former employees
   G. Malware authors
   H. Nation-state intelligence services
   I. Natural (flood, fire, lightening etc.)
   J. Non-professional hackers
   K. Organised crime
   L. Terrorists
   M. Other
   N. Don’t know
7. Roughly how much do you believe the attacks or breaches you have selected in Question 6 cost the Port of Freetown financially?
   A. Less than £500
   B. £500 to less than £1,000
   C. £1,000 to less than £5,000
   D. £5,000 to less than £10,000
   E. £10,000 to less than £20,000
   F. £20,000 to less than £50,000
   G. £50,000 to less than £ 100,000
   H. £100,000 or more
   I. Don’t know
8. How was the attacks or breach in Question 5 identified? (multiple choice)
   A. By accident
   B. By antivirus/anti-malware software
   C. Disruption to business/staff/users/ service provision
   D. From warning by government/law enforcement
   E. Our breach/attack reported by the media
   F. Similar incidents reported in the media
   G. Reported/noticed by customers/customer complaints
   H. Reported/noticed by staff/contractors
   I. Routine internal security monitoring
   J. Other internal control activities not done routinely (e.g. reconciliations, audits etc.)
   K. Other
   L. Don’t know
9. In which of the following ways below have the attacked you experienced in Question 5 have these impacted the Port of Freetown? (multiple choice)
   A. Stopped staff from carrying out their day-to-day work
   B. Loss of revenue or share value
   C. Additional staff time to deal with the breach or attack, or to inform customers or stakeholders

D. Any other repair or recovery costs
E. New measures needed to prevent or protect against future breaches or attacks
F. Lost or stolen assets
G. Fines from regulators or authorities, or associated legal costs
H. Reputational damage
I. Prevented provision of goods or services to customers
J. Discouraged you from carrying out a future business activity you were intending to do
K. Other

Questions Relating to the Awareness of Cybersecurity Threats at the Port of Freetown and Mitigation Measures

10. Which of the following aspects, if any, are covered within your cyber security-related policy, or policies? (multiple choice)
A. What can be stored on removable devices (e.g. USB sticks, CDs etc.)
B. Remote or mobile working (e.g. from home)
C. What staff are permitted to do on your company's IT devices
D. Use of personally-owned devices for business activities
E. Use of new digital technologies such as cloud computing
F. Data classification
G. A Document Management System
H. Other
I. No policy adopted

11. How low or high of a priority is cybersecurity the Port of Freetown's management?
A. Very low
B. Low
C. Neutral
D. High
E. Very high

12. Over the last 1 year, has the Port of Freetown provided workers with internal cyber security trainings?
A. Never
B. Less than once a year
C. Annually
D. Quarterly
E. Monthly
F. Weekly
G. Don't know

13. Please select some of the risk management or governance arrangements you have in place? (multiple choice)
A. Board members with responsibility for cyber security
B. An outsourced provider that manages your cyber security
C. A formal policy or policies in place covering cyber security risks
D. A Business Continuity Plan
E. Staff members whose job role includes information security or governance
F. Other
G. None of these
H. Don't know

14. Please select all of the rules that you have in place from the list below (multiple choice)
A. Applying software updates when they are available

B. Up-to-date malware protection

C. Firewalls with appropriate configuration

D. Restricting IT admin and access rights to specific users

E. Any monitoring of user activity

F. Encrypting personal data

G. Security controls on company-owned devices (e.g. laptops)

H. Only allowing access via company-owned devices

I. A segregated guest wireless network

J. Other

K. None of these

L. Don’t know

15. Do you have insurance which would cover you in the event of a cyber security breach or attack?

A. Yes

B. No

16. Where are the attacks or breaches reported to? (multiple choice)

A. National Intelligence Service

B. Police

C. Antivirus company

D. Bank or credit card company

E. Outsourced cyber security provider

F. Internet/network service provider

G. Professional/trade/industry association

H. Media

I. Website administer

J. Other

K. No intention to report

L. Don’t know

17. From where have you sought information, advice or guidance on the cyber security threats that the Port of Freetown faces? (multiple choice)

A. Business bank/bank’s IT staff

B. External security/IT consultants

C. National Intelligence Services

D. Police

E. Small and Medium Business Administration

F. Internet Service Provider

G. Newspapers/media

H. Online searching generally

I. Professional/trade/industry association

J. Regulator

K. Security product vendors

L. Other companies

M. Within your company – senior management/board

N. Within your company – other colleagues or experts

O. Other

18. Are you aware of any of the following initiatives and standards? (multiple choice)

A. International Standard for Information Security Management (ISO 27001)

B. Any government’s guidance

C. NIST Cybersecurity Framework

D. Other

E. None of these

19. Which of the following, if any, do your clients require you to have or adhere to? (multiple choice)

    A. A recognised international standard (e.g. ISO 27001/PCIDSS)
    B. NIST Cybersecurity Framework
    C. Any government's scheme
    D. Other
    E. None of these

Appendix Two – Consent Form

Dear Participant,

Thank you for agreeing to participate in this research survey, which is carried out in connection with a Dissertation which will be written by the interviewer, in partial fulfilment of the requirements for the degree of Master of Science in Maritime at the World Maritime University in Malmo, Sweden.

The topic of the Dissertation is **Awareness of Cybersecurity Threats in the Port of the Freetown, Sierra Leone.**

The information provided by you in this interview will be used for research purposes and the results will form part of a dissertation, which will be published online and made available to the public. Your personal information will not be published. You may withdraw from the research at any time, and your personal data will be immediately deleted.

Anonymised research data will be archived on a secure virtual drive linked to a World Maritime University email address. All the data will be deleted as soon as the degree is awarded.

Your participation in the interview is highly appreciated.

Student's name	Malik Abdul Karim Sesay
Specialization	Shipping management & Logistics
Email address	w1701637@wmu.se
Supervisor:	Professor George Theocharidis

* * *

I consent to my personal data, as outlined above, being used for this study. I understand that all personal data relating to participants is held and processed in the strictest confidence, and will be deleted at the end of the researcher's enrolment.

○ Yes:

○ No: