Global Journal of Arts Humanity and Social Sciences ISSN: 2583-2034

GSAR PUBLISHERS
GLOBAL SCIENTIFIC AND ACADEMIC RESEARCH

Glob. J.Arts.Humanit.Soc.Sci
ISSN: 2583-2034
Vol-2 Iss-2, page 63-73
Doi:-

Mass Media and Cyber Security in the Maritime Industry: Analysing the Threats and Prevention

[1]Jammy Seigha GUANAH, Ph.D. [2]Jammy Seigha GUANAH, Jnr.

[1]Department of Mass Communication University of Benin, Benin City, Nigeria
[2]Department of Nautical Science Liverpool John Moores University, Liverpool, UK

Article History
Received : 8/01/2022
Accepted : 16/02/2022
Published : 24/02/2022

Corresponding author:

Jammy Seigha GUANAH, Ph.D.

Abstract

Cyberspace is important to every sphere of human life or operations, including the maritime industry; there is hardly anything that can be done today without the use of cyberspace. Howbeit, it is susceptible to cybercrimes. For this reason, this study appraised the roles of cyber security in the maritime industry, and how the mass media can assist in curbing maritime cybercrimes. Survey Monkey and library methods were used to gather data for the study. For the Survey Monkey method, the questionnaire link was sent through various social media platforms to the respondents made up of seafarers, maritime companies (shore-based)personnel, and selected journalists. Through the library method, guidelines and procedures published by maritime companies like Baltic and International Maritime Council (BIMCO), Cruise Line International Association (CLIA), and International Association of Independent Tanker Owners (INTERTANCO) were analysed. The study was based on the mediamorphosis theory. Findings revealed the different vulnerabilities of maritime systems to cyber-attacks, both on-board and ashore, and also highlighted the steps being taken to address cyber security issues in the maritime domain. Equally, it was discovered that the mass media's awareness creation level about cyber security in the maritime industry was very low. The study concluded that cyber security plays an important role, not only to the maritime industry but to other sectors as well, as with security in general there must be threats to these systems. Recommendations made include that security agencies and technical experts should cooperate to come up with procedures that will help to mitigate these threats, and that the media carry out intensive awareness campaigns to ensure that both seafarers and personnel at the shore can be aware of the dangers that a cyber-breach poses to the system.

Key Words: Cyberspace, Industry, Media, Maritime, Prevention, Security.

Introduction

Cyber is a new frontier, and it is opening up new opportunities for individual nation-states to interact with each other across natural and national boundaries. The relevance of cyberspace to a nation's growth politically, socially, economically, and security-wise, is quite significant. Hence, countries all over the world are always interested in influencing whatever goes on in cyberspace (Guanah, 2019). However, there are a lot of security issues associated with cyberspace. This calls for functional cyber security, cyber security having been defined by the Oxford Online Dictionary (2014) as the state of being protected against unauthorized or criminal use of electronic data, or the procedures which are taken to achieve this. Guanah (2017) also cites the International Telecommunication Union (ITU) as defining it "as the collection of best practices, guidelines, tools, security concepts, technologies and policies which can be used to ensure that user and organization's assets and the maritime cyber environment is protected" (p.1).

Cyberspace can be utilized for the development of any society; in the same vein, it can be anathema if not properly channeled towards development goals; especially now that the world's growing cyberspace is driven by innovations that are increasingly being aided by modern computer technologies, the Big Data phenomenon and the Internet of Things (IoT). Akinkugbe (2019) asserts that technology and innovation are accelerating and being disrupted every day and that by 2020, 21 billion "things" will be connected; from phones, music, lighting, cars, cameras, home appliances because "we no longer exist in isolation" (p.2).

The environment in which communication network over computer networks occurs is known as cyberspace; security on the other hand is the state of being free from danger. With the understating of the two definitions, it can be said that cyber security is a state in which computer network systems are free from threats. Kemmerer (2003) says that cyber security consists largely of defensive methods used to identify and respond to would-be intruders. Noting that cyber security is quickly becoming one of the most important industries to safeguard our democratic values, Zabierek and Pipikaite (2021) emphasize that the demand for cyber security professionals is rising globally, as cyber-attacks are increasing in scale and severity. They admit that this has led to the global demand for cyber security professionals in all aspects of the field, and across all sectors. Hence, the media can intervene in curbing the menace of cyber insecurity.

Cyber security plays a critical role in the maritime industry, as it will help to ensure that appropriate procedures are put in place to minimize the risks to computer systems or networks. Although technology has greatly improved the maritime industry, it still has its risks and vulnerabilities. There is the need to help minimize cyber threats, which are becoming a growing menace, spreading to all industry sectors that are relying on International Communication Technology (ICT) systems (European Network and Information Security Agency-ENISA, 2011). According to the Protection and Indemnity Club-P&I Club (2016), "the risk of cyber-attack is the biggest potential threat to both ships and their owners as the use of information technology spread into all areas of the business" (p.1).

According to a report published by the European Network and Information Security Agency-ENISA (2011), maritime cyber security awareness is currently low to non-existent; current maritime regulations and policies consider only physical aspects of security and safety, maritime governance is currently fragmented between different levels (i.e. international, European, national), and due to the high ICT complexity, it is a major challenge to ensure adequate maritime cyber security.

Therefore, what is the place of the mass media in preventing cyber security threats in the maritime industry? Interestingly, they have some significant roles they can play, especially the social media branch of the mass media. These functions can be carried out via various platforms like facebook, Instagram, WhatsApp, Twitter, Snapchat, Blogs, SoundCloud, Hulkshare, 2go, Zoom, GooglePlus, Facebook Messenger, Tencent, Telegram, Tik Tok, Skype, LinkedIn, Pinterest, Evernote, YouTube, even email, and many more, because they operate through the cyberspace (Internet) too just like maritime cyber communication.

Through these outlets, the media can create awareness about the existence of cybercrimes that can affect the maritime industry, go ahead to expose the identity of the perpetrators and their modus operandi, and finally proffer some solutions to tackle the challenges. Sailors and mariners on the high seas can access such information being passed across through the various platforms enabled by the Internet. Though the mainstream media like Newspapers, magazines, radio, television, and others may not play many roles here, the online versions of these media can also be very effective in helping to curb the activities of maritime cyber threats.

This paper reviewed some cyber security guidelines and procedures published by maritime companies and provided the best methods to help respond to, resolve, and recover from a cyber-attack. The scope of this study is limited to the understanding of the important roles played by cyber security in the maritime industry, and the role of the mass media. This will help to enhance the awareness of external and internal threats, risks, and vulnerabilities relating to the security of data and digitally held information in marine organizations.

The objectives of the study

The major objective of the study was to analysis cyber security, specifically cyber threats in the maritime industry, too:

i. identify the different vulnerabilities of maritime systems, both on-board and ashore;

ii. pinpoint methods to prevent and resolve cyber-attacks, and

iii. find out mass media's awareness creation level about cyber security in the maritime industry.

Review of Relevant Literature

Theoretical Consideration

This research is based on the mass communication metamorphosis theory, sometimes known as the "digital metamorphosis." Roger Fiedler proposed it in 1997 as a way to understand and quantify the changes in the digital world and culture. Roger Fidler coined the term "metamorphosis" in 1990, but it was not until his book in 1997 that he defined it as the alteration of communication media, frequently caused by the complex interaction of perceived demands, competitive and political forces, and social and technological advancements (Blogspot, 2012).

Metamorphosis, according to Fidler (1997), is a coherent way of thinking about the technological growth of communication media. From the concepts of co-evolution, convergence, and complexity, he derived his metamorphosis principles. Fidler argues that as new media forms evolve and develop, they affect the development of other existing media over time and to varying degrees, such that instead of the emergent media displacing the old ones, the current media converge with it to improve its operations.

According to Guanah, Agbanu, and Obi (2020), the theory "explains and estimates the chances of the digital world and its culture" (p.701); it also "talks about the changes that take place in the ways through which information is transmitted at present"

(p.702). This theory's application in this research is that it explains how traditional mainstream media and social media can be employed in the processes of fighting cyber threats in the maritime industry.

Concept of Cyber Security and Maritime Cyber Threats

Some criminal activities take place in cyberspace, which poses threats to man's security in various forms. These crimes are referred to as cybercrime because they occur in cyberspace, these entails everything one does illegally with computing devices like mobile phones, tablets, and personal computers, and other criminal activities in cyberspace, including spamming, Subscriber Identity Module (SIM card) frauds, credit card frauds, Automated Teller Machine (ATM) frauds, phishing, identity theft, unauthorised access, distribution of obscene and indecent contents, cyberbullying, and many more. Cyber-attack risks have been around for as long there have been computers, but these attacks skyrocketed at the end of the 20th century with the introduction of the Internet and the vast use of closed computer networks as an important business tool (Marsh, 2014). Some cyber-attacks and crimes also have something to do with maritime cyber security.

Rouse (2016) defines cyber security as the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorised access. Merriam-Webster's online Dictionary (2021) defines cyber security as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (p. 1). We can hereby say that maritime cyber security is a measure taken to protect the network and computer assets both on ships, terminals, ports, and all computerized equipment supporting maritime operations. Ensuring cyber security requires coordinated efforts throughout an information system. Elements of cybersecurity include Operational security, Information security, Application security, network security, end-user education, and disaster recovery/business continuity planning. (Rouse, 2016).

A maritime cyber threat is the possibility of a malicious attempt to damage, disrupt, or gain unauthorized access to a maritime computer system, or electronic communications network. One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security risks. Adam Vincent, a CTO-public sector at Layer 7 Technologies, says, "the threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It is no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly…." (as cited in Sen, 2017, p.62).

The cyber threat is specific to the ship, operation, company, and/or trade. When assessing threats, companies should be aware of any specific aspect of their operations that might increase their vulnerability to cyber accidents. Why do individuals or states conduct maritime cyber-attacks? According to Jensen (2015), an expert in maritime cyber security, an attacker's motivation ranges from financial, smuggling in contraband, to stealing company's secrets from different marine industries.

Types of Cyber Attacks

Cyber-attacks on the Maritime industry take place regularly. Cybercriminals use different methods of vectors or malware that may affect a ship or maritime company, but all are grouped into Targeted and Untargeted attacks. Untargeted attacks are attacks that occur through the Internet; the company or ship's systems are usually one of the many potential targets. Some examples include Malware and Social engineering. There are numerous types of malware, which include Worms, Trojans, Spyware/adware, Ransomware, and Viruses. Social engineering examples are Phishing and Water Holing/Pharming. However, our focus here is targeted attacks.

According to TrendMicro (2015), targeted attacks can be considered one of the biggest cyber threats to an organization in today's Internet-connected landscape. It is the worst-case scenario for any company of any size, as not only does the targeted company lose reputation, it could also cost millions in damages. As the reports of these are made known, past incidents will be attached to some of the examples of targeted attacks:

a. Spear-Phishing: This process is similar to Phishing, but the victims are targeted with personal emails, often containing malicious software or links that automatically download the malicious content. The "Icefog" incident is an example of a Spear-Phishing attack. In spear-phishing attacks, the targets included governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies.

b. USB as infection carriers: The Universal Serial Bus (USB) devices such as thumb drives or portable hard disks "which are employee-owned are an excellent medium for carrying infection from one place to another when critical systems are not connected to the Internet" (Sood & Enbody, 2014, p.17). This occurs when an employee plugs a corrupted USB into a system.

c. Ghost Shipping: According to CyberKeel (2014), this attack involves the process of creating remote access to terminal systems, and thereby the criminals were able to release containers to their truckers without the knowledge of the port or the shipping line. The Port of Antwerp was a victim of Ghost Shipping between 2011 and 2013.

d. Distributed denial of service (DDOS)/Denial of service (DOS): A DOS attack is one, which prevents authorized and legitimate users from accessing information. A DDOS attack is similar, but it takes control of servers and/or multiple computers to implement a DOS attack.

e. Zero-Day Exploit: A zero-day exploit defined by FireEye (2010) is an unknown exploit that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong.

There are more examples of targeted and untargeted attacks, "The potential number and sophistication of tools and techniques used in cyber-attacks will continue to evolve and is only limited by the ingenuity of those organizations and individuals developing them"(BIMCO, 2016, p.14).

Cyber Vulnerabilities in the Marine Sector

Techopedia (2012) defines vulnerability as a cyber-security term that refers to a flaw in a system that can leave it open to an attack. It can also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. Today's maritime companies and seafarers rely on outside sources, systems, and networks heavily for navigation. A significant amount of cyber threats are the result of vulnerabilities in equipment carried and used by the maritime industry worldwide (Hayes, 2016).

Vulnerabilities on a ship might be caused by any of the following reasons: (i) if safety-critical systems or equipment are always connected to shore-based facilities, (ii) if there is inadequate access to controls for service providers, contractors, and other third parties, (iii) if the present antivirus software is either outdated or missing, (iv) if the computer networks used by the ship lacks segmentation of networks and boundary protection measures, and (v) if operating systems that are unsupported or obsolete are present (BIMCO, 2016).

It is recommended that shipping companies should initially perform assessments of the potential threats that may realistically be faced. This should be followed up by an assessment of the systems and the procedures used on-board to map their usefulness to handle the current level of threat (BIMCO, 2016). An argument might be made that the relatively low public profile of the majority of marine businesses means that they are less likely to be the subject of a cyber-attack than financial institutions, energy companies, public utilities, or airlines. That may be the case, but the threat is real, and the results of a successful attack could be catastrophic (Marsh, 2014).

According to a guideline produced by BIMCO (2016) systems attached to uncontrolled networks, or directly to the Internet, are more vulnerable to cyber-attacks than stand-alone systems; this is because on the stand-alone systems there are fewer connections to other systems thereby reducing the risk of spread of the virus if it is infected. Care should also be taken to understand how important shipboard systems might be connected to uncontrolled networks (BIMCO, 2016).

Ship System Vulnerabilities

Control systems are vulnerable to cyber-attacks from both inside and outside the control system network. For systems associated with vulnerabilities to be understood, the types of operations and communication associated with these control systems must be made known; as well as achieving an understanding of how the cyber attackers use the vulnerabilities found to their advantage (ICS-CERT, 2011). These systems include:

A. Navigation Systems: A report by Oliver Wyman has shown that significant weaknesses have been identified in the various navigation systems that are used at sea. The report highlights that the Automatic Identification System (AIS), Electronic Chart Displays and Information Systems (ECDIS), Global Positioning Systems (GPS) are all critical aids to navigation, and each of them is potentially vulnerable to attacks (Wyman, 2015). Below are a few examples of how an attack on a navigation system will affect it:

i. Electronic Chart Display & Information System (ECDIS): The ECDIS serves as an alternative to paper nautical charts as it complies with the International Maritime Organisation (IMO) and has a geographic information system. An ECDIS vulnerability might allow a cyber-attacker to modify and access files and charts ashore and on-board (CyberKeel, 2014).

ii. Automatic Identification System (AIS): This system used by both ships and vessel traffic services (VTS) helps in the automatic tracking of other ships by electronically exchanging data. There are many known vulnerabilities of the AIS, which were proven by Trend Micro in 2013 when they demonstrated how easy it was to penetrate the AIS of a ship.

iii. Global Positioning System (GPS). Garmin(2001) defines the global positioning system as a satellite-based navigation system. The data provided by the GPS is crucial to maintaining the safety of navigation at sea for all vessels. The main vulnerabilities of the GPS are jamming and spoofing; jamming involves the attacker intentionally blocking GPS signals while spoofing is an electronic attack, which involves signals that are sent to a receiver to control navigation. (Hayes, 2016).

B.Communication Systems: The availability of Internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defense mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard system and data. (BIMCO, 2016).

C.Cargo management systems: Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore. An example of such a system is the shipment-tracking tool available to shippers via the internet. Interfaces of this kind make data in cargo manifests and cargo management systems vulnerable to cyber-attacks (BIMCO, 2016).

D.Crew welfare and administrative systems: On-board computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide Internet access and email. They can be exploited by cyber attackers to gain access to onboard systems and data (BIMCO, 2016).

E.Access control systems: Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic "personnel-on-board" systems (BIMCO, 2016).

F.Passenger servicing and management systems: Digital systems used for property management, boarding, and access control may likely hold valuable passenger-related data. Intelligent devices such as handheld scanners and tablets are themselves an attack vector as the confidential data collected will likely be passed on to other systems (BIMCO, 2016).

G.Passenger facing public networks: Fixed or wireless networks connected to the Internet, installed on board for the benefit of

passengers, for reasons like guest entertainment systems should be considered uncontrolled and should not be connected to any safety-critical system on board (BIMCO, 2016). The same should apply to networks provided in ports.

H.Bridge systems: The increase in the use of digital, network navigation systems, with interfaces/connections to shoreside networks for update and provision of services, allow such systems to be vulnerable to cyber-attacks. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media such as the Universal Serial Bus (USB) are often used to update such systems from other uncontrolled or controlled networks (BIMCO, 2016).

I.Propulsion and machinery management and power control systems: The digital systems used to monitor and control onboard machinery; steering and propulsion allow these systems to be vulnerable to cyber-attacks. The vulnerability of these systems might increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with communications and navigation equipment on ships using integrated bridge systems (BIMCO, 2016).

Methods to Prevent and Resolve Cyber Attacks

Although there are various vulnerabilities and methods of attack used to gain unauthorized access to systems and cause damage, there are also plans, guidelines, and procedures that, if followed regularly, will help to minimize the risk of a cyber-attack. For instance, A Cyber Incident Response Plan is the type of contingency plan that can be used, as it establishes procedures that will be used to respond to cyber-attacks against a company or a ship. Its procedures are designed to enable security technicians to identify, mitigate and recover from malicious computer incidents. However, these contingency plans must be tested periodically.

Apart from contingency plans, other measures can be used to minimize risks and address security vulnerabilities. These guidelines will help to ensure that the risks to various ships and shore equipment are minimized. The Centre for Internet Security (CIS) provided a guideline containing a list of Critical Security Controls (CSC), which includes both procedural and technical controls:

Procedural controls: These security controls focus on how the onboard systems are used by seafarers. All procedures and plans that contain sensitive information should be kept confidential with access to a few people and handled based on the organization's policy (CIS, 2016). These procedural controls include:

- **Administrator privileges-** Administrator privileges are special privileges that allow a user full access to system configuration settings and all data. These privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or on-board, to log into systems using such privileges.
- **Removable media and physical control policy-** The transfer of data by personnel from uncontrolled systems to controlled systems serves as a major risk in introducing malware to the system. Organisations should produce a security policy for the use of removable media devices.
- **Awareness and training-** Cyber threats from internal parties should be considered and never be underestimated. Personnel, even with the best of intentions, can make mistakes, for instance by using infected removable media to transfer data from computer to computer; mistakes can also be made by mishandling data and disposed of files incorrectly.
- **Updates for anti-malware and anti-virus tools-** For anti-virus tools to detect and deal with viruses efficiently, they need to be updated regularly. Senior-level management should establish procedural requirements to ensure updates are distributed to ships on regular basis and that all relevant computer systems on-board are updated.
- **Support services from ashore-** Organisations should ensure that owned ships have access to expert support from the shore in the event of a cyber-attack. The details/guidelines for this support and associated procedures should be produced by the senior management level and made available onboard.
- **Disposal of equipment (Information Deletion) -** Equipment which are outdated may contain data which are confidential or commercially sensitive. Organisations should have procedures in place to ensure that the data held in this outdated equipment are properly destroyed before disposing of the equipment thereby ensuring that the confidential information cannot be retrieved.
- **Software maintenance and upgrades-** Updates would not be received for any software or hardware that stops being supported by its software developer or producer. Companies/organisations should carefully evaluate the cyber risk assessment for software and hardware that are no longer supported before using them.

Technical Controls: Technical controls are security controls that when executed by a computer facilitates the detection of security violations, supports security requirements for data and applications, and provides automated protection from unauthorised access or misuse (Federal Aviation Administration, 2016). These controls require significant operational considerations:

- **Network device configuration such as routers and firewalls**- It should be determined which systems should be attached to controlled or uncontrolled networks.
- **Communication through radio and satellite** – The procedures to ensure the security of satellite and radio connections should be planned in collaboration with the producer and service provider. When an uplink connection for the ship's navigation and control system is to be established, it should be reviewed on how to prevent unauthorised parties from gaining access to the systems onboard and ashore.
- **Capability to recover data-** The capability to recover data is about possessing the ability to restore a system and or/data from a secure copy or image thereby allowing

the restoration of a clean system (CIS, 2016). Software-adequate backup systems and all necessary information should be available to ensure it can be recovered after a cyber-incident has occurred.

- **Defenses against malware-** Antivirus and antimalware software should be installed, updated, and maintained on all personnel-owned work-related computers on-board.
- **Create defence of boundary-** A structure containing expected data flows and network operations for personnel should be created and managed so that cyber incident alert thresholds can be also.
- **Hardware and software secure configuration** - The senior officers on-board and in companies should be the only personnel that has access to administrator profiles so that they are in charge of control of the setup and the disablement of normal user profiles.
- **Software security for applications (Patch management)** - All necessary security and safety updates should be made available to onboard systems.
- **Network design security-** Networks on-board should be divided into parts by firewalls to create different safe sectors.
- **Physical security**- As physical security is an important aspect of cyber security, safety-critical equipment, and cable runs should be protected in form of manned watches from unauthorised access.
- **Browser protection for web and email** – Personnel that makes use of emails should make sure that any information exchange carried out is properly connected to ensure that confidentiality and integrity of data are secure.
- **Wireless Access control-** Only appropriate authorised devices should possess wireless access to networks.
- **Control and Limitation of network services and protocols**- Access lists to network systems should be created and utilised to execute the company's security policy. This ensures that only necessary traffic would be permitted through the controlled network based on the security policy of that network.

Communication, Mass Media, and the Maritime Industry

Communication is an essential aspect of human life. Today, human beings are perpetuating cybercrimes; they can only commit these crimes because they can communicate. Before now, Guanah (2018) has defined communication as the movement of information from Person, Medium, or Point A to another Person, Medium, or Point B through a dedicated channel to bring about a desired effect or reaction.

Either on land (ashore), or the high sea (on-board), Mariners (sailors) do communicate. However, the communication is mostly done through communication gadgets (Walkie Talkie, email, VHF radio etcetera) more than on face-to-face bases, whether it's in the land-to-sea vessel or sea-to-sea communication. These are the most convenient ways to communicate in the maritime industry, and all these operate through cyberspace. It is the interruption, interception, and manipulation by unauthorised entities to commit a crime that brings about maritime cyber insecurity.

This is a situation where there is a security breach on the communication that takes place in cyberspace. When such comprise occurs, it may jeopardise the lives of crewmembers and goods that may be in the process of being transported from one location to the other. It is through communication that the mass media operates.

Recommending that communication lines should be kept open as a means to improve cyber security awareness, Volyntseva (2021) emphasises the need to establish a system to communicate cybersecurity policies and raise awareness throughout an organisation, adding that emails and other media help to achieve this. He adds that posters, printed from the Internet, tailored with contact details of cyber-attack response teams (either in-house, or outsourced), will act as a visual reminder. These communication tools, including posters, can cover best practices, password security policies, or how to respond in case of a cyber-attack.

The significant role the mass media play in all aspects of society cannot be overemphasized. Saddled with the core duties of informing, entertaining, and educating the masses, among others, the mass media engender and ensure the safety of lives and property, as it is tenable even in the marine industry. Media contents are like the life-giving water that quenches the information thirst of their audiences' lungs; hence, they look forward to and are eager to hear from the media daily.

Just as in every other field of human endeavour, the mass media have roles they play in the prevention of maritime cyber breaches, and in enhancing maritime cyber security. The media educate the maritime stakeholders that all unnecessary default user accounts must be deleted or disabled. If an account is reviewed, and it is found out to be unnecessary, it should be deleted, as the default user accounts lack adequate security and therefore act as a vulnerability to the system. This in turn endangers all other systems.

Backup policies are necessary and should be in place. The media have the responsibility to enlighten stakeholders that backup of systems helps to ensure quick recovery capabilities of the system in case of a cyber-attack. Systems, which possess a large amount of confidential information, should be backed up regularly. If an attack occurs that prevents access to system information or deletes this data, backup systems would enable the ship to quickly regain operational and navigational capabilities.

The current policies of most companies do not require that all antivirus software should have all malware and engine updates applied regularly. The media should concentrate on emphasising the call for the installation of anti-malware software and the configuring to run regularly; at least should be daily scans basis to update and protect the systems that are not done regularly. There is always an increase in the risk of an attack if vulnerabilities to the outdated malware system are found.

Through their reportage, especially via feature and opinion articles, the media can assess and manage cyber risks in order to ensure

risks are minimised, and any vulnerabilities of systems found are patched. Risk assessment tests that are carried out by either the organization's personnel or a third party, will help to review and analyse systems to ensure their reliability in case an attack should occur. These assessment tests are necessary as the results gained from them can be publicised by the media to produce a more secure contingency plan.

At all times, network security must be implemented or tested for systems. The media should draw the attention of stakeholders to this fact periodically. This is important because the focus should be placed on controlled networks as these are designed to prevent any security risks from connected devices by making use of switches, routers, and firewalls. Network systems that should be placed on controlled networks include networks that are used to provide suppliers with remote access to Operation Technology (OT) software and navigation equipment and networks that are necessary to the operation of the ship (BIMCO, 2016).

Research Method

The Survey Monkey method was employed as the research design in this study. This method was chosen because the research work was based on assessing the response of both on-board and ashore personnel in the marine industry, and journalists, using an online survey on current maritime security levels in their current workplaces. The researchers did not require face-to-face interviews or an experiment, instead, a questionnaire was used. The researchers signed up on the site of Survey Monkey.Com, typed in their questionnaire to generate a link. This link was sent to respondents through various social media platforms.

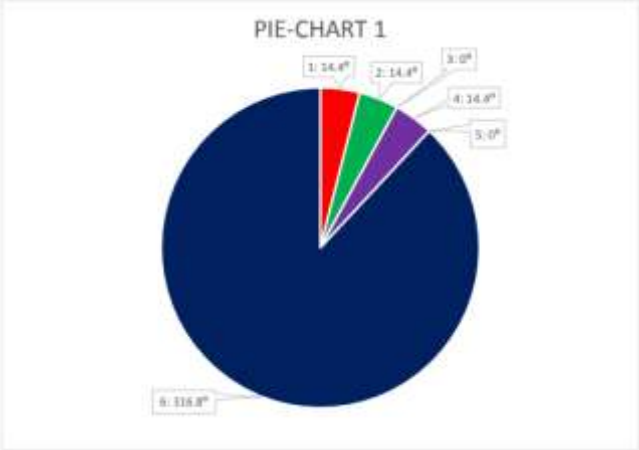
This quantitative survey was conducted on the current maritime cyber security level on board a ship and in the office, and the role of the media in curbing maritime cyber security. Every survey respondent was informed before the survey, the purpose of the data collection, and how it would be used. No information was collected which was sensitive to any company. All personal information collected from the survey was destroyed once used and was not passed on to any other person or organisation.

Since the issues of concern in this research specifically involved those in the fields of marine and mass communication(media) expert reviews were necessary, therefore, the researchers purposively selected 15 mariners and 15journalists, who are professionals in these two fields to form the population. This population was also the sample size of the study since the population is small (Ifeakor, 2009).The mariners are made up of Masters, Chief Officers, on-shore administrative staff of marine organisations, and vessel managers while the journalists are made up of reporters, editors of online and mainstream media, feature writers, and journalism lecturers in the university.

A 14-item structured questionnaire was used as the data-gathering instrument for this study. For the survey to be both reliable and valid, the questions in the questionnaire were properly constructed, as recommended by Hale (2013). A pilot test was conducted, and the reliability of the Cronbach alpha reliability coefficient value of 0.87 was recorded. Senior mariners and newspaper editors validated the questionnaire through peer review before it was circulated. The researchers purposively selected 15mariners and 15 journalists. Out of this,25, representing a response rate of 83.33%, completed and returned the copies of the questionnaire. The data collated were analyzed, using degrees and a pie chart.

Data Presentation

Fig. 1: Different vulnerabilities of maritime systems, both on-board and ashore



Scale 1%=3.6º, **Source:** Fieldwork, 2017

Key:

1: If safety-critical systems or equipment are always connected to shore-based facilities

2: If there is inadequate access to controls for service providers, contractors, and other third parties

3: If the present antivirus software are either outdated or missing

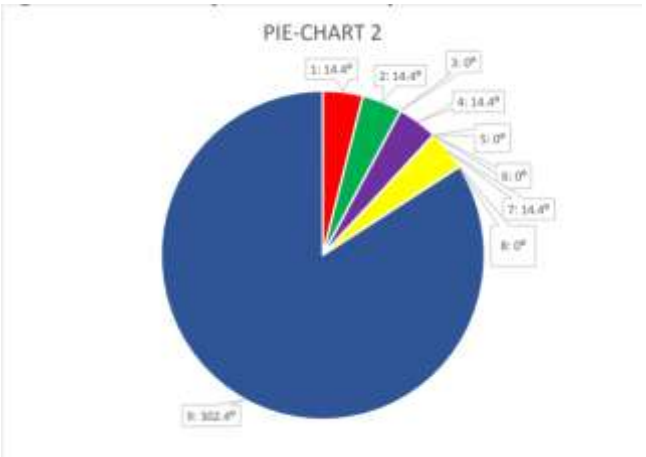
4: If the computer networks used by the ship lacks segmentation of networks and boundary protection measures

5: If operating systems that are unsupported or obsolete are present

6: All of the above

Fig. 1 indicates that the maritime industry is quite vulnerable to different types of cyber-attacks.

Fig. 2: Some methods to prevent and resolve cyber-attacks

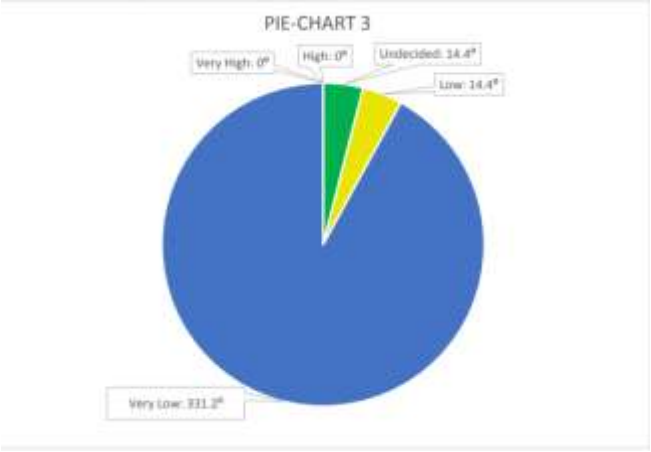


Scale 1%=3.6º, **Source:** Fieldwork, 2017

Key:
1: Testing contingency plans periodically
2: Awareness and training
3: Updates for anti-malware and anti-virus tools
4: Regular software maintenance and upgrades
5: Hardware and software secure configuration
6: Network design security- Physical security
7: Browser protection for web and email
8: Control and Limitation of network services and protocols
9: All of the above

The data in Fig.2 reveal that both procedural and technical controls are needed to prevent and resolve cyber-attacks on maritime facilities.

Fig. 3: Level to which the mass media create awareness about cyber security in the maritime industry.



Scale 1%=3.6º, **Source:** Fieldwork, 2017

Key: Very High High Undecided Low Very Low

Fig. 3 shows that the mass media have not been doing much in creating awareness about cyber security in the maritime industry.

Discussion of findings

The first finding of this study indicated that there are many vulnerabilities of maritime systems, both on-board and ashore. For instance, ashore, modern ports rely a whole lot on computer networks; various complex networked logistics management systems track maritime cargo overseas. These networked systems are also often involved in the unloading and loading of containers at ports. Optical recognition and other technologies are also used on modern gantry cranes to scan, locate and manage all aspects of port terminal operations (Kramek, 2014).

The GPS is also used by automated container terminal systems to facilitate the movement and automatic placement of containers. All these technologies and more used by ports make them vulnerable from loading and unloading of cargo to crane jobs. Brookings Report in 2013 said, "Easily available jammers could close down a port at cost of more than 1 billion dollars per day" (Kramek, 2014, p. 4).

This study also revealed that there are various methods through which maritime cyber-attacks can be prevented and resolved. They include technical and procedural controls. According to (2016), Administrator privileges should always be constrained to the execution of functions requiring such access. Access to this information should only be allowed to relevant authorised personnel. To protect this access to confidential data and safety-critical systems, organisations should prepare a standard password policy system. This policy system should ensure that passwords created by personnel are strong and changed periodically when necessary. Also, awareness programmes should be in place for all personnel on-board covering, risks related to emails, Internet usage, personal devices, poor data security practices, and maintaining software on company hardware.

CIS (2016) suggests further that all software and hardware installations on-board should be updated regularly to ensure a sufficient level of security is kept. Guidelines for scheduled updating of software, like the computer operating system and hardwires, should be put in place, taking into account the time spent at sea, speed of Internet connectivity, and type of ship. Likewise, manufacturers of communication equipment and terminals for satellite communication on-board should provide management interfaces with security control software that are available on the network. The protection of this equipment should be considered when reviewing the security of a ship's installation. Other preventive steps to be taken against maritime cyber security suggested by CIS (2016) includes Capability to recover data, Defences against malware, Defence of boundary, and Software security for applications (Patch management).

In finding out mass media's awareness creation level about cyber security in the maritime industry, it was discovered that it was very low. This finding corroborates the report made by ENISA (2011) that "the awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent" (p.1). This means that the mass media have not been doing much as regards maritime cyber security.

Stressing the importance of ensuring that cyber security awareness is promoted consistently, Volyntseva (2021) advocates that employees of organisations be educated about how a personal mobile device or insecure browsing can result in data breaches. This major lack of public awareness of the threats involved in cyber security has been having its toll on the maritime industry because of the momentous role the media play in society. It is of critical importance the mass media carry out an intensive awareness drive to ensure that both seafarers and personnel on-board and ashore can be aware of the dangers that a cyber-breach poses to the system to reduce this threat.

Some maritime staff lacks management systems for cyber security; this shows that the organisations lack risk management programs even though these programs provide the ability to communicate and quantify adjustments to the cyber security framework of an organisation (Natural Institute of Standard and Technology- NIST,

2018). The mass media need to make such personnel understand that risk management processes make it possible to inform and prioritise decisions relating to cyber security. The media should let them know that for the risks to be managed; ship owners and on-board personnel should know and understand the chances of a cyber-attack occurring as well as the aftermath. With this knowledge in mind, a level of risk, which is unacceptable and should trigger action, is determined.

A high percentage of personnel may lack the necessary procedures to handle a cyber-security incident, the media must provide these procedures to appropriate levels which include shore-side personnel whose duty is to support the operation and management of the ship and on-board personnel i.e. seafarers, officers, and the Master.

The media's duties include letting all stakeholders realise the advantages of performing regular training programs on cyber security which is good as this will help to improve awareness and thereby evolve the cybersecurity levels. These training programs will create defences that will emerge to stop older threats; as information technology becomes more integrated into the system, the incentives to compromise the security of deployed IT systems will grow (Berson, 2014).

Conclusion and Recommendations

The study set out to appraise the roles cyber security plays in the maritime industry, hence the researchers analysed the guidelines on cyber security onboard ships produced and published in 2016, and supported by various shipping associations like BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO. Based on findings that showed that the current cyber risk awareness levels is low, the media must carry out intensive awareness campaigns in order to ensure that both seafarers and personnel at the shore can be aware of the dangers that a cyber-breach poses to the system.

This study also highlighted the risks of cyber-attacks and the vulnerabilities of maritime systems; it showed that a large number of systems used onboard and ashore possess vulnerabilities that could be exploited. These vulnerabilities may be caused if the current anti-malware software installed is outdated, if protections measures and division of networks systems are absent, if systems required for the safe operation and navigation of a ship is in constant connection with ashore systems, and if any computer system which is no longer in use are still available. Therefore, drastic steps must be quickly taken to address these foregoing issues. With the cooperation of security agencies and technical experts, coupled with the involvement of the mass media, procedures can be made that will help to mitigate these threats.

References

1. Akinkugbe, N. (2019). Money Matters with Nimi: Cyber Security, Your Digital Footprint & Your Personal Finances. Retrieved from https://www.bellanaija.com/2019/04/money-matters-with-nimi-cyber-security/.
2. Baltic and International Maritime Council- BIMCO (2016). *Guidelines on cyber security onboard ships.* Denmark: BIMCO.
3. Blogspot (2012). Understanding the future. Retrieved from http://understandingthefutur3.blogspot.com.ng/2012/10/defined-by-its-creator-as.html?m=1.
4. Center For Internet Security- CIS (2015). *Controls.* Retrieved from https://www.cisecurity.org/controls/
5. Clark, D., Berson, T., &Lin, H.S., 2014. *Committee on Developing a Cybersecurity Plan. Findings and Conclusion.* Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK223216/
6. CyberKeel(2015). *Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas.* Retrieved from http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf.
7. European Network and Information Security Agency- ENISA (2016). *Critical Infrastructures and Services.* Retrieved from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts
8. Federal Aviation Administration- FAA. (2016). Develop Primary ISSP. Retrieved from https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/operations/isse/items/c_prelim_issp/
9. Fidler, R. F. (1997). *Metamorphosis: Understanding New Media (Journalism and Communication for a New Century Ser*). London: Pine Forge Press.
10. FireEye (2012). *What is a Zero-Day Exploit?*. Retrieved from https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
11. Garmin (2001). *What is GPS?* Retrieved from http://www8.garmin.com/aboutGPS/
12. Guanah, J. S., Agbanu, N. V., &Obi, I. (2020). Artificial intelligence and journalism practice in Nigeria: Perception of journalists in Benin City, Edo State. *International Review of Humanities Studies*, 5(2): 698-715. Available at: www.irhs.ui.ac.id.
13. Guanah, J. S. (2019 October). Cybercrime as a security ambivalence of the digital media: The framing of *Yahoo-Yahoo Business* (YYB) stories by Nigerian newspapers. Paper presented at the 21st International Conference/Annual General Meeting (AGM) of African Council for Communication Education (ACCE), held at National Open University of Nigeria (NOUN), Jabi Campus, Abuja, Nigeria, from 22nd - 25th.
14. Guanah, J. S. (2018). Book as a communication medium: Using Barclays Ayakoroma's *Dance on the Grave* to discuss salient gender issues. *International Review of Humanities Studies*, 3 (2):385-403. Retrieved from: www.irhs.ui.ac.id.

15. Guanah, J. S. (2017). The role of cyber security in the maritime industry: An analysis on cyber threats and its prevention. Unpublished B.Sc. (Hons.) Nautical Science Dissertation of Liverpool John Moores University, Liverpool, United Kingdom.
16. Hale, J. (2013). The 3 Basic Types of Descriptive Research Methods. Retrieved *from*https://psychcentral.com/blog/archives/2011/09/27/the-3-basic-types-of-descriptive-research-methods/.
17. Hayes, C. R. (2016). *Maritime Cybersecurity: The Future of National Security.* Retrieved fromhttps://www.hsdl.org/?view&did=794596
18. Industrial Control System-ICS-CERT (2011).*Overview of Cyber Vulnerabilities.* Retrieved from https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities
19. Ifeakor, C. Amaechi (2009). Population, sample, and sampling techniques. In: I. E. Osegbo, A. C. Amaechi, & J. O. Enemuo (Eds) *Research methodology in education: Basic issues & techniques*. (Pp. 98-117). Odoakpu-Onitsha: Folmech Printing and Publishing Co. Ltd.
20. Jensen, E.T. (2015). Cyber Sovereignty: The Way Ahead. *Texas International Law Journal*, 50(2): 275-304.
21. Kemmerer, R. A., (2003). *Cybersecurity* in Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715. Retrieved fromhttp://dx.doi.org/10.1109/ICSE.2003.1201257
22. Kramek, J., (2014). *The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities*. *Brookings Report.* Retrieved from http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-securitykramek
23. Marsh, O. (2014). *The Risk of Cyber Attack to the Maritime Sector*. Retrieved from https://uk.marsh.com/Portals/18/Documents/The%20Risk%20of%20Cyber-Attack%20to%20the%20Maritime%20Sector.pdf
24. Merriam-Webster (2021)Definition of *Cybersecurity*. Retrieved from: https://www.merriam-webster.com/dictionary/cybersecurity.
25. Natural Institute of Standard and Technology-NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: https://doi.org/10.6028/NIST.CSWP.04162018.
26. Oxford Online Dictionary (2014). *Cybersecurity*. Oxford: Oxford University Press. Retrieved from http://www.oxforddictionaries.com/definition/english/Cybersecurity
27. Rouse, M. (2016). *Cyber Security.* Retrieved from http://whatis.techtarget.com/definition/cybersecurity
28. Sen, J. (2017). *Advances in security in computing and communications*. McFarland-Wisconsin: Books on Demand.
29. Sood, A.K., & Enbody, R.(2014). Chapter 2-Intelligence Gathering. In A. K. Sood, & R. Enbody (Eds.). *Targeted Cyber Attacks*. Boston: Syngress.
30. Swanson, M., Bowen, P., Philips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.
31. Techopedia (2012). *Vulnerability.* Retrieved from https://www.techopedia.com/definition/13484/vulnerability
32. Protection and Indemnity Club- P&I Club (2016). *Cyber Risk A new area of vulnerability for the maritime industry.* Retrieved from https://www.londonpandi.com/media/2025/5633stoploss67september.pdf
33. TrendMicro (2015). Understanding Targeted Attacks: What is a Targeted Attack.Retrieved fromhttps://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack
34. Volyntseva, Y. (2021). Ten tips to improve Cyber Security Awareness amongst your employees. Retrieved from https://www.businesstechweekly.com/hr-and-recruitment/cyber-security-awareness/.
35. Wyman, O. (2015). Cyber Gap Insurance: Cyber Risk: Filling the Coverage Gap. Retrieved from https://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/Navigating%20a%20Shifting%20Risk%20Landscape%20Expert%20Perspectives%20on%20the%20Marine%20Industry.pdf.
36. Zabierek, L. & Pipikaite, A. (2021). Why cybersecurity needs a more diverse and inclusive workforce. Retrieved from https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/?utm_source=sfmc&utm_medium=email&utm_campaign=2761050_Agenda_weekly-29October2021&utm_term=&emailType=Agenda%20Weekly.