World Maritime University

The Maritime Commons: Digital Repository of the World Maritime University

World Maritime University Dissertations | Dissertations

10-28-2023

Investigating the relevance of effectiveness of cybersecurity measures in the Philippine maritime industry

Marife S. Duatin

Follow this and additional works at: https://commons.wmu.se/all_dissertations

 Part of the Education Commons

This Dissertation is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact library@wmu.se.

WORLD MARITIME UNIVERSITY

INVESTIGATING THE RELEVANCE OF EFFECTIVENESS OF CYBERSECURITY MEASURES IN THE PHILIPPINE MARITIME INDUSTRY

MARIFE S. DUATIN

A dissertation submitted to the World Maritime University in partial fulfillment of the requirements for the award of the degree of Master of Science in Maritime Affairs

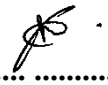
2023

Copyright Marife S. Duatin, 2023

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.

(Signature):  **.....**

(Date): **24 September 2023**

Supervised by: Dr. Dimitrios Dalaklis, Ph.D.
Professor, Safety and Security
World Maritime University

Supervisor's affiliation: Maritime Safety and Environmental Administration

Acknowledgments

First and foremost, I would like to give all the glory to our God Almighty. With Him, everything is possible.

I would like to express my gratitude to my family, who inspire me to keep pushing myself forward, for their unwavering support, love, and prayers. My father, Maximo Sr; my sister, Dang; my brother-in-law, Darwin; my niece, Darianne, and nephew Adrian; my cousin, Ate Monalisa. Thank you all so much! A special mention to my mother, Felicidad, who I know is smiling from heaven.

I would like to express my gratitude to my Commanding Officers, CG COMMO JOEVEN L FABUL, WMU Alumni SY 2004, for believing in me and pushing me to apply to the World Maritime University; to CG COMMO MARIFEM UBUNGEN-ISAAC, WMU Alumni SY 2017 for allowing me to go through my application at WMU and for her unwavering support. My Coast Guard Finance Service Family, my Bonkie (close buddy), CG CAPT NOEMIE G CAYABYAB, for assisting us with our application and her steadfast support.

I would also like to express my sincere appreciation and gratitude to the WMU S23 Philippine Team, led by Sir Jeth, to whom we all fondly address as our dear congressman, for all the support and always being there for each of us and ensuring all is well. For Lyn, Tony, Orly, Elgene, Gerico, Marge, Emma, Alrina, and Taka, for all the laughter and tears from foundation studies to the dissertation period. Thank you for your friendship. To the class of S23, I hope you enjoyed the taste of chicken adobo, pancit bihon, and Shanghai rolls. I am pleased to prepare it for you all for every gathering. To the COH team, led by our dear Chairman, Tebogo, and Sir Jeth, it was a pleasure working with you, gentlemen.

To all the faculty and staff of the World Maritime University, led by our very own WMU President, Prof Max Mejia Ph.D., thank you all for sharing your knowledge and for your patience with every one of us; special mention to Ms. Lyndell Lundahl, who is like a mother to every student, I hope you enjoy your retirement Ma'am; to Ms Ellin Sigurjonsdottir, who played a big part for my admission at WMU, I am forever grateful to you Ma'am. I sincerely thank our MLP Professors, led by Prof Maria Carolina Romero- Associate Professor- Head of Maritime Law and Policy Specialization, Prof Henning Jessen- Nippon Foundation Chair in Maritime Law and Digital Change, Prof George Theocharidis-Maritime Law and Policy Professor, Prof Aref Fakhry-MLP Associate Professor, and Prof Khanssa Lagdami- ITF Seafarer Trust Assistant Professor of Maritime Labour Law and Policy. To my dissertation supervisor, Dr. Dimitrios Dalaklis, Ph. D-Professor, Safety and Security, for his continued support, patience, and in providing me with relevant materials during the dissertation period. Thank you so much, Sir! To Prof Anne Pasaver and Prof Dale Smith for the proof reading, thank you so much! To BIMCO, especially Mr Jakob Larsen, Head of Maritime Safety and Security, for giving me a copy of the latest edition of the Cybersecurity Workbook during our field study in their prestigious office. To the crew and staff of World Bistro, led by Daniel, thank you for feeding us healthy food and for your friendship!

To all the Titos and Titas of Malmo, special mention to Tita Linda and Tito Bossy S, Tita Linda C, Ate Glo, Tita Dolores, Tito Carding and Tita Linda, and Ate Carol, for treating every Filipino student like the long-lost children, and for constantly feeding us, MARAMING MARAMING SALAMAT PO!

Furthermore, finally, to my sponsor, the Government of the United Kingdom, my heartfelt gratitude for sponsoring my academic journey here at WMU. Thank you very much!

Abstract

Title of Dissertation: **Investigating the Relevance of Effectiveness of Cybersecurity Measures in the Philippines Maritime Industry**

Degree: **Master of Science**

This study explores the importance and effectiveness of cybersecurity protocols in the maritime sector of the Philippines. It uses a narrative literature review methodology to synthesize information from various scholarly databases and relevant texts. The research aims to establish a foundational understanding of cybersecurity, explain pivotal notions, and examine the legal framework of the cybersecurity domain. It critically analyses instances of cybersecurity breaches across various industries, emphasizing the widespread existence of cyber threats. The study also investigates the sources of cyber threats in the maritime industry, assesses vulnerabilities, and delineates potential consequences of attacks. It evaluates factors influencing the effective implementation of cybersecurity measures, including human aspects, organizational policies, and technological obsolescence. The paper investigates real-life maritime cyberattack scenarios, such as the NotPetya cyberattack, and identifies best practices and existing conventions within maritime cybersecurity. The analysis of the cybersecurity landscape in the Philippines involves evaluating domestic policies, regulations, and standards enforced by maritime entities like the Maritime Industry Administration (MARINA), the Philippine Coast Guard (PCG), and the Philippine Port Authority (PPA). A benchmark analysis evaluates maritime cybersecurity protocols in Malaysia, Singapore, and the Philippines, examining the relative strengths and weaknesses of each nation's cybersecurity capabilities. The study provides significant insights into the development of strategies and policies aimed at bolstering the cybersecurity resilience of the maritime sector in the Philippines.

KEYWORDS: Cybersecurity, cyber threats, cyberattacks, cybersecurity measures, risk mitigation, cybersecurity best practices, and cybersecurity in the Philippines

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ABS	American Bureau of Shipping
AI	Artificial Intelligence
APCERT	Asia-Pacific Computer Emergency Response Team
ASEAN CERT	Association of Southeast Asian Nation Computer Emergency Response Team
BIMCO	Baltic and International Maritime Council
CERT	Computer Emergency Response Team
CERT-PH	Philippine National Computer Emergency Response Team
CII	Critical Information Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CMS	Cybersecurity Management System
CNII	Critical National Information Infrastructure
COS	Chamber of Shipping
CPA	Cybercrime Prevention Act
CSA	Cybersecurity Agency of Singapore
DDoS	Distributed Denial of Service
DICT	Department of Information and Communication Technology
DoC	Document of Compliance
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
IACS	International Association of Classification Societies
ICT	Information and Communication Technologies
IMO	International Maritime Organization
ILO	International Labour Organization
IoT	Internet of Things
ISACs	Information Sharing and Analysis Centres
ISAOs	Information Sharing and Analysis Organizations
ISM Code	International Safety Management Code
ISPS Code	International Ship and Port Facility Security Code

ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
MARINA	Maritime Industry Administration
MCAAG	Maritime Cybersecurity Assessment and Annex Guide
MITM	Man-in-the-Middle
MTS	Maritime Transport System
MyCERT	Malaysia Computer Emergency Response Team
NATO	North Atlantic Treaty Organization
NCIAC	National Cybersecurity Inter-Agency Committee
NCIWM	National Cyber Intelligence Web Monitoring
NCSI	National Cybersecurity Index
NCSP	National Cybersecurity Plan
NCSP	National Cybersecurity Policy
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OT	Operational Technology
PDPA	Personal Data Protection Act
PCG	Philippine Coast Guard
PPA	Philippine Port Authority
SDG	Sustainable Development Goal
SingCERT	Singapore Computer Emergency Response Team
SMS	Safety Management System
SOC	Security Operations System

Chapter 1. Introduction

1.1 Background

The maritime industry is vital to international trade and commerce, but unfortunately during recent years it is becoming increasingly susceptible to cyberattacks. These attacks may result in the loss of sensitive information (Elgan, 2021), the disturbance of operations (Vanguard, 2020), and even the substantial destruction of ships and port facilities (Nicaise, 2022). As a result, there is an increasing demand for effective cybersecurity procedures to protect the maritime industry against cyber threats.

Several studies regarding the effectiveness of cybersecurity in the maritime sector identify an increasing concern regarding the apparent impacts of cyberattacks on the industry. Research conducted by DNV to 801 maritime professionals representing 72 countries (*See Figure 1*) has shown that the maritime industry is particularly at risk of cyberattacks due to several factors, including outdated systems, a lack of investment in security, and a shortage of trained personnel (DNV, 2023).

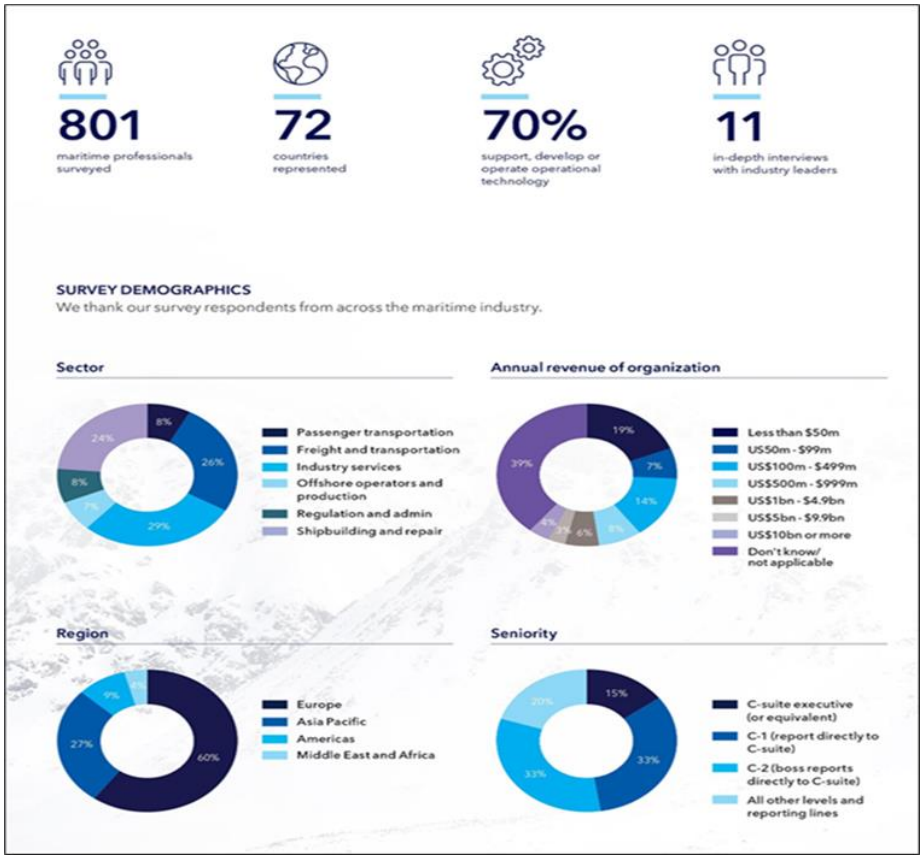


Figure 1. *DNV Survey Demographics*
Source: Maritime Cyber Priority Report 2023: Staying Secure in an Era of Connectivity
https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.htmln

According to a study by the International Association of Classification Societies (IACS), significant vulnerabilities must still be addressed. However, the maritime industry has already introduced specific measures that enhanced cybersecurity like the MSC.428(98) and MSC-FAL.1/Circ.3, which supplement the IMO ISPS (International Ship and Port Facility Security) Code for vessels and port facilities and work in tandem with the ISM Code, which is a highly influential risk mitigation instrument for the sector (Progoulakis et al., 2023). The investigation uncovered a need for more consistency and standardization in cybersecurity practices across the industry and inadequate training and resources for crew members to respond effectively to cyber incidents (The Editorial Team, 2022). Lloyd's Register and the University of Cambridge Centre for Risk Studies discovered in a separate study that maritime trade is highly vulnerable to virtual intrusion due to obsolete technology and a lack of investment in cybersecurity. The study also highlighted the potential for substantial financial losses from cyberattacks on ships and port facilities (Lloyd's Register and the University of Cambridge Centre for Risk Studies, 2017).

The maritime industry must improve its cybersecurity measures to tackle the growing cyberattack threat. These measures include utilizing new technologies and providing crew members with cyber incident training and resources (Chew, 2023). As discussed by Canepa et al. in their study, understanding security protocols and the importance of being vigilant about security risks is a significant challenge, mainly due to the constantly evolving technological landscape. Adequate training programs are crucial in maintaining security. These training programs must cater to the users' specific requirements to effectively develop their capabilities in response to the ever-changing risk scenarios. As humans are often considered to be the most fragile point in a computer system (Triplett, 2022), it is essential to provide professional training to enhance user awareness and technical expertise in operating various protection mechanisms (Canepa et al., 2021). The literature demonstrates a general concern about the effectiveness of cybersecurity within the business but a need for specific policies and procedures, training for seafarers, industry standardization, and additional research and development.

This research effort will focus on the relevance of the effectiveness of cybersecurity measures in the Philippines, particularly in the domain of the maritime industry, highlighting the legal frameworks in place and cybersecurity practices of the country's key implementing maritime government agencies. Additionally, it will attempt to identify the gaps and vulnerabilities in the industry. Furthermore, it will examine the best practices of other countries that can be enforced and implemented to improve the nation's cyber resilience, particularly in the maritime industry.

1.2 Research Aims and Objectives

The research effort aimed to analyse the effectiveness of cybersecurity measures in the maritime sector of the Philippines to ensure the safety and security of maritime operations, protect critical infrastructure, and ensure compliance with international regulations. The researcher identified three research objectives:

i. to identify the various types of cybersecurity threats and vulnerabilities in the maritime sector of the Philippines and investigate the extent to which these threats and vulnerabilities can be mitigated by implementing best practices, policies, and procedures.
ii. to examine the human, technological, and organizational aspects that instigate the effectiveness of cybersecurity measures in the maritime industry and to propose strategies to address these factors to improve the overall effectiveness of cybersecurity in the industry and
iii. to evaluate the different methods and mechanisms that can be used to measure the effectiveness of cybersecurity procedures in the maritime industry and identify the challenges and limitations associated with these evaluations to develop recommendations for improving the industry's overall cybersecurity effectiveness.

1.3 Research Questions

To address the objectives of this research, the researcher has explored the following research questions:

i. What are the cybersecurity threats and vulnerabilities in the maritime industry of the Philippines?

ii. How effective are the maritime industry's current cybersecurity guidelines and regulations, and what modifications are required to better protect against cyber threats?

1.4 Research Methodology

A narrative literature review was selected as the preferred methodology for research to assess the relevance of the effectiveness of cybersecurity measures in the maritime industry of the Philippines. Charles Sturt University in Australia defines a narrative or

conventional literature review as a thorough and impartial assessment of existing information on a particular topic. It forms a theoretical structure and provides the proper context for the research effort. Through a thorough examination of a range of scholarly works, a literature review can help identify patterns and trends, as well as gaps or contradictions in the current knowledge base. Literature reviews are an integral component of the research process and are essential in providing a solid foundation for subsequent analysis (Charles Sturt University, 2023). Further, Onwuegbuzie and Frels (2016) have identified four main types of narrative reviews. These reviews include comprehensive, theoretical, methodological, and historical literature review surveys. A comprehensive literature review involves evaluating and synthesizing the key components of existing information related to a specific subject matter. It is commonly found in the introduction of a thesis or dissertation, and it typically includes the study's purpose, underlying hypothesis or problem, or the reviewer's idea. On the other hand, a theoretical review aims to investigate the influence of theory on the formation and structure of research.

Moreover, the methodological literature review involves analyzing a particular study's research methodologies and design. This review highlights the strengths and limitations of the employed methods and provides insights into potential avenues for future research. Lastly, the historical literature review involves analysing research conducted over a specific timeframe. It begins by investigating the initial appearance of an issue, concept, theory, or phenomenon in literature and tracing its development within the academic discourse of a particular field. The principal purpose of this research is to place the study within a historical framework, thereby demonstrating a comprehensive understanding of the latest advancements in the area. Additionally, this type of analysis aims to identify potential avenues for future research (Onwuegbuzie & Frels, 2016).

The research began by effectively identifying relevant keywords that were essential in gathering information from academic databases. The keywords or research strings used in the different databases were *cybersecurity, cyber threats, cyberattacks, cybercrime, the effectiveness of cybersecurity, cybersecurity measures, risk mitigation, cybersecurity best practices, cybersecurity reports, cybersecurity in the maritime industry, and cybersecurity in the Philippines*. The extensive, thorough approach included searching through various databases, such as DNV, Google Scholar, HeinOnline, iLaw, IMO Documents, IMO Vega, Llyod's List Online, MPDI Open Access Journals, Researchgate, ScienceDirect, Scopus, Springer, Taylor & Francis Online, World Maritime University Digital Library, and WMU Maritime Commons, to find literature that was both high-quality

and pertinent. The use of search databases made the process more efficient and streamlined, allowing the researcher to identify and access the most valuable sources of information. Further, as part of the criteria for research, the literature used needed to have been published between 2000 to the present day, with the exemption of legal sources such as international conventions, laws (international and domestic), resolutions, and regulations. The year 2000 was specified as a benchmark year as the first well-known cybercrime was detected during that year in the Philippines. Lastly, the researcher also utilizes the reports of different credible and known media organization websites and different cybersecurity-related websites for information on the latest cybercrimes or cyberattack and collections of data.

1.5 Key Assumptions and Potential Limitations

The research assumes maritime industry organizations with cybersecurity management plans comply with cybersecurity guidelines and regulations. The limited resources of the maritime industry are a potential research limitation. Because of time restrictions, no questionnaire was utilized during the conduct of this research effort. Many organizations in the maritime sector may need more resources to invest in cybersecurity, limiting the efficacy of their actions. Furthermore, the study will focus only on the current cybersecurity measures implemented by the government agencies mentioned in this research effort.

Chapter 2. Review of Related Literature

As the world becomes more interconnected through technological innovations, the risk of cyberattacks has increased substantially, and the maritime field is no exception (Mraković & Vojinović, 2019). Cybersecurity in the maritime sector is a critical issue, and this literature review will examine its various facets. The literature review will define effectiveness and its relationship to cybersecurity, investigate the legal foundations of cybersecurity, and present related studies focusing on cybersecurity in the maritime industry. This chapter provides readers with valuable insights into the status of cybersecurity practices in the maritime industry and potential areas for improvement.

2.1 What is Effectiveness?

As defined by the Cambridge Dictionary, effectiveness is the ability to be successful and produce the intended result (Cambridge Dictionary, n.d.). It is the extent to which something achieves its intended purpose or desired outcome. It measures the degree to which a process, system, product, or strategy meets its objectives and produces the expected results. Frequently, it contrasts efficiency or being efficient, which is the capacity to complete a task or achieve a goal using the fewest resources, such as time, money, or effort (*Efficient Definition & Meaning - Merriam-Webster*, n.d.). Effectiveness is concerned with maximizing outputs or results, whereas efficiency is concerned with minimizing inputs. In other words, effectiveness refers to doing the right things, whereas efficiency refers to doing something correctly.

On the other hand, the NIST Computer Security Resource Center defines “Control Effectiveness” as a measure of whether a given control contributes to reducing information security or privacy risk (NIST, n.d.-a). In cybersecurity, effectiveness refers to the capability of established cybersecurity measures to protect against cyberattacks and preventing unauthorized access to sensitive data and systems. Effective cybersecurity measures must detect and respond to potential threats in real-time while easing the risk of data breaches and other security incidents.

2.2 Understanding Cybersecurity

Cybersecurity, as defined by the Computer Security Resource Center (CSRC) on their website, is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (NIST, n.d.). Then again, as cited by Taherdoost (2022) in his article "Cybersecurity vs. Information Security," ISO/IEC27032:2012 defined cybersecurity as preserving confidentiality, integrity, and availability of information in cyberspace (Taherdoost, 2022)

Based on the interpretation and understanding of the definitions above, cybersecurity safeguards digital systems, networks, and data against unauthorized access, use, disclosure, disruption, modification, or destruction. It includes technical, organizational, and legal controls to safeguard information and prevent cyber threats from jeopardizing digital assets' confidentiality, accessibility, and integrity.

Cybersecurity has become a significant concern for individuals, businesses, governments, and societies due to the widespread adoption of digital technologies and the Internet. In today's digital age, the maritime industry cannot overstate the significance of cybersecurity. Cyber threats such as hacking, data breaches, malware, ransomware, phishing, and social engineering, among others (*Types of Cyber Threat in 2022 | IT Governance UK*, 2023), pose substantial risks to the confidentiality, integrity, and accessibility of sensitive data, financial assets, intellectual property, and critical infrastructure.

2.3 Review of Cybersecurity Legal Basis

Several international Conventions, treaties, and legal frameworks address cybersecurity. The 2001 Budapest Convention is one of them. This Council of Europe treaty aims to harmonize national cybercrime laws and enhance international cooperation in cybercrime investigation and prosecution. It includes hacking, online fraud, and child pornography, among other cybercrimes (Council of Europe, 2001).

Resolution 70/237 of the United Nations General Assembly is another. This Resolution established the applicability of international law, including the United Nations Charter, to information and communication technologies (ICTs). It also encourages Member States to develop and implement measures to prevent the malicious use of ICTs and strengthen international cooperation (Assembly, 1969). Also, the General Data Protection Regulation (GDPR) is an EU regulation that seeks to safeguard EU citizens' privacy and personal data. It has extraterritorial reach and applies to any organization, regardless of location, that processes the personal data of EU citizens (Wolford, 2023). Moreover, the Tallinn Manual is a non-binding academic guide to applying international law to cyber operations. It was compiled by an international group of experts and published by the NATO Cooperative Cyber Defence Centre of Excellence (Schmitt, 2013).

The legal basis for cybersecurity varies by jurisdiction but generally consists of laws, regulations, standards, and guidelines that mandate or recommend cybersecurity practices. In the United States, for instance, the Cybersecurity Act of 2015, the Federal Information Security Modernization Act (FISMA) of 2014 (*Federal Information Security Modernization Act | CISA*, n.d.), and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (*Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC*, n.d.) are some essential legal frameworks that establish cybersecurity requirements for specific industries. Additionally, under the US Department of Commerce, the National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to satisfy the needs of the US industry, federal agencies, and the general public. Its activities range from producing immediate actionable information to conducting longer-term research that anticipates technological advancements and future challenges. Federal statutes, executive orders, and policies define some of NIST’s cybersecurity tasks. Their cybersecurity activities are also motivated by the requirements of the US business community and the general public. They actively engage with stakeholders to establish priorities and ensure their resources are allocated to vital issues. NIST also enhances knowledge and management of privacy hazards, some directly related to cybersecurity. Cryptography, education and workforce, emerging technologies, risk management, identity and access

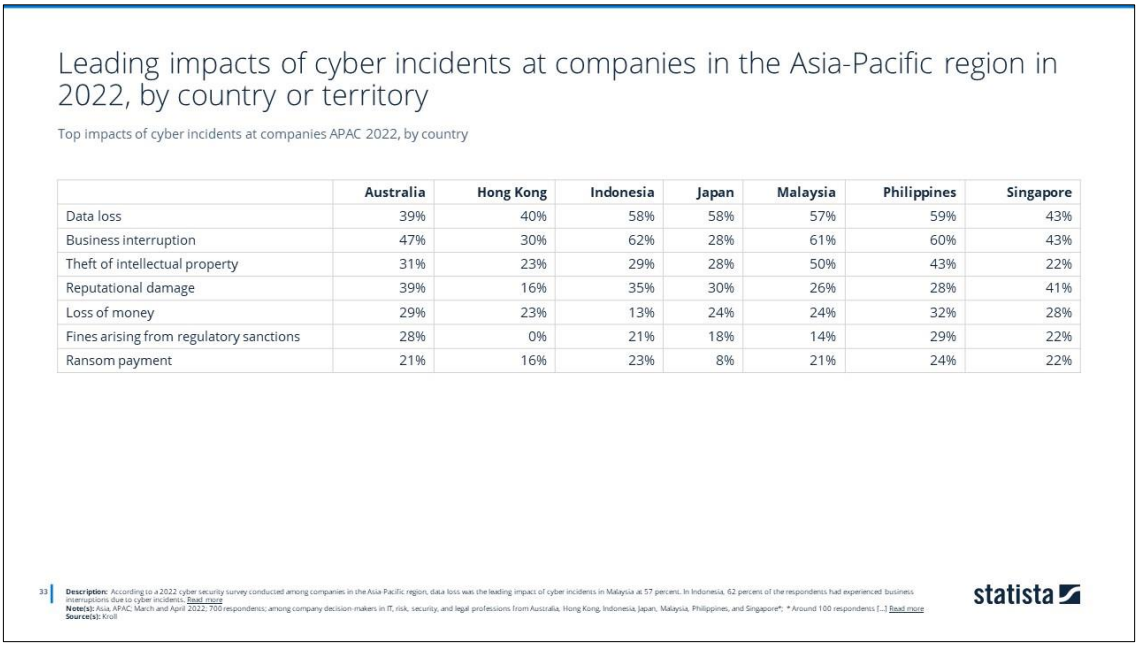
management, measurements, privacy, trustworthy networks, and reliable platforms are the areas that NIST contributes to and plans to prioritize (NIST, n.d.-b).

Moreover, international organizations such as the International Organization for Standardization (ISO) (Edition, 2015; *ISO/IEC JTC 1/SC 27 - Information Security, Cybersecurity and Privacy Protection*, n.d.) and the National Institute of Standards and Technology (NIST) have developed cybersecurity guidelines and standards that are widely recognized and adopted by organizations worldwide (NIST Cybersecurity Framework Team, 2018). Moreover, the International Maritime Organization (IMO) has developed Guidelines on Maritime Cyber Risk Management. The guidelines provide recommendations at a high level for maritime cyber risk management to protect shipping from existing and emerging cyber threats and vulnerabilities. Further, it contains functional elements that support effective cyber risk management (IMO, 2017).

Correspondingly, cybersecurity is likewise essential in implementing the mandates of the International Telecommunication Union (ITU), a specialized agency of the United Nations for information and communication technologies (ICTs). ITU is mandated to facilitate international connectivity in communication networks, allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide (*International Telecommunication Union (ITU)*, n.d.). Relatedly, ICTs can help accelerate progress toward every single one of the 17 United Nations Sustainable Development Goals (SDGs) (ITU, 2021). As stated in the report by the CyberPeace Institute, the 2030 Agenda for Sustainable Development Goals emphasizes the significance of information and communication technologies and global interconnectedness as potent growth drivers to accelerate human progress, reconcile the digital divide, and develop knowledge societies. Each of the SDGs incorporates a digital component, although some are more digitally focused than others. ICTs are explicitly mentioned as a goal under SDG 9 – "Build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation" and it is also said in the goals on climate change (SDGs 13, 14, and 15), gender equality and the empowerment of women and girls (SDG

5), economic growth (SDG 8), education (SDG 4), and health (SDG 3). Various research projects and initiatives have further emphasized the direct impact of transformative technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) on the SDGs (CyberPeace Institute, 2022).

The potential consequences of cyberattacks, which include financial loss, reputational harm, legal liabilities, and even harm to human life, highlight the significance of cybersecurity (*See Figure 2*). Investing in robust cybersecurity measures and remaining compliant with applicable laws and regulations is essential to protect digital assets, maintain trust, and ensure the security and resilience of digital systems and networks.



Leading impacts of cyber incidents at companies in the Asia-Pacific region in 2022, by country or territory

Top impacts of cyber incidents at companies APAC 2022, by country

	Australia	Hong Kong	Indonesia	Japan	Malaysia	Philippines	Singapore
Data loss	39%	40%	58%	58%	57%	59%	43%
Business interruption	47%	30%	62%	28%	61%	60%	43%
Theft of intellectual property	31%	23%	29%	28%	50%	43%	22%
Reputational damage	39%	16%	35%	30%	26%	28%	41%
Loss of money	29%	23%	13%	24%	24%	32%	28%
Fines arising from regulatory sanctions	28%	0%	21%	18%	14%	29%	22%
Ransom payment	21%	16%	23%	8%	21%	24%	22%

33 | **Description:** According to a 2022 cyber security survey conducted among companies in the Asia-Pacific region, data loss was the leading impact of cyber incidents in Malaysia at 57 percent. In Indonesia, 62 percent of the respondents had experienced business interruptions due to cyber incidents. Read more
Note(s): Asia, APAC; March and April 2022; 700 respondents; among company decision-makers in IT, risk, security, and legal professions from Australia, Hong Kong, Indonesia, Japan, Malaysia, Philippines, and Singapore*; * Around 100 respondents [...] Read more
Source(s): Kroll

statista

Figure 2*. Leading Impacts of Cyber Incidents at Companies in the Asia-Pacific Region in 2022*

Source: Cybersecurity and Cybercrime in the Asia-Pacific Region
https://www.statista.com/study/138955/cybersecurity-and-cybercrime-in-the-asia-pacific-region/

2.4 Cybersecurity Incidents in Different Industries

Over the last 21 years, from 2001 to 2021, cybercrime has victimized at least 6.5 million people, resulting in an estimated loss of almost $26 billion (Cabral, 2022). Below are some notable cybersecurity incidents that have impacted well-known companies in various industries, leading to substantial revenue losses,

reputational damage, and even geopolitical tensions. These incidents highlight the pervasive threat of cyberattacks across multiple industries and the critical significance of implementing robust cybersecurity measures to protect businesses and critical infrastructure.

2.4.1 Chinese Hackers Breach Telecoms

The US Cybersecurity and Infrastructure Security Agency warned at the start of June 2022 (CISA, 2022) that Chinese government-backed hackers had compromised several sensitive victims worldwide, including "major telecommunications companies." According to CISA, they exploited known router vulnerabilities and flaws in other network equipment, including Cisco and Fortinet products. The warning did not identify any specific victims. However, it alluded to alarm over the findings and the need for organizations to bolster their digital defenses, particularly when managing large amounts of sensitive user data. CISA further explained that the advisory details the targeting and compromise of major telecommunications companies and network service providers. The agency also mentioned that over the past few years, a series of high-severity vulnerabilities in network devices have enabled cybercriminals to exploit and obtain access to vulnerable infrastructure devices regularly. Moreover, these devices are frequently neglected (Newman, 2022)

A similar incident occurred in the Philippines in 2018 when the Philippine National Police Anti-Cybercrime Group detained Chinese nationals accused of telecom fraud. During the course of the apprehension, the team confiscated a variety of digital evidence that was used in the perpetration of cybercrime, including laptops, tablets, smartphones, basic phones, VOIP devices, routers/modems, landline phones, IP cameras, digital cameras, IT peripherals, identification cards, and various documentary evidence (Anti-Cybercrime Group, 2018b). After conducting thorough investigations and analysis, it has been revealed that the IP addresses associated with a series of telecommunication frauds in China have been traced back to the Philippines. The telecommunications company has been exploiting affluent individuals from various provinces in mainland China for an

extended period. The perpetrators impersonate law enforcement officers, sending fictitious arrest warrants to their victims and persuading them to transfer funds to a seemingly secure account, resulting in millions of dollars in illicit gains (Anti-Cybercrime Group, 2018a).

2.4.2 Ronin lost $600 Million of Cryptocurrency in Cyberattacks.

Ronin is a blockchain-based gaming platform that utilizes cryptocurrency, so It was unavoidable that those who are thinking ahead would direct their attention towards it from November 2021 to March 2022.. Axie Infinity, a game by Ronin, enables players to acquire digital currency and non-fungible tokens. As the game's popularity grew, the company reduced its security protocols so that its servers could accommodate a larger audience. This enabled Axie Infinity to accommodate the growing number of players and allowed criminals to steal $600 million worth of cryptocurrencies. The parent company of Ronin is collabourating with authorities to identify the perpetrators and recover the stolen funds, but any business can learn from this incident to never compromise your security standards (Sead Fadilpašić, 2022)

2.4.3 Hacked Systems at the Port of Antwerp

In 2013, criminals hacked the Port of Antwerp systems to manipulate container movement to evade detection and transport their drug cargo. Once the hackers gained access to the appropriate systems, they altered the location and delivery times of narcotic containers. The smugglers then dispatched their drivers to retrieve the narcotics-laden cargo containers before the authorized transporter could retrieve them. The hackers gained access to the systems through spear phishing and malware attacks directed at port authority employees and shipping corporations. Police uncovered the entire conspiracy after shipping companies noticed something was amiss (Shead, 2022).

With the scenarios mentioned above, cybersecurity is paramount due to the consequences of cyberattacks, including revenue loss, tarnished

reputations, legal liabilities, and even adverse effects on individuals. Investing in comprehensive cybersecurity measures and remaining compliant with applicable laws and regulations is necessary to safeguard the value of digital assets, preserve mutual confidence, and ensure the reliability and security of digital systems and networks.

Industry	Organization	Attack Type	Incident and Impact	Cost
Energy	Ukrenergo (Ukrainian Power Company)	OT-Specific Malware: Industroyer/ CrashOverride	Disrupted operations resulting in a blackout in the capital city of Kiev	225K Customers without power
Food & Beverages	Mondelez	Ransomware: NotPetya Targeted twice in a year	Lost sales, compromised electronic data, plus software and equipment damage	$150-$188M
Manufacturing	Reckitt Benckiser	Ransomware: NotPetya	Lost sales, disruptions to manufacturing & ordering systems, shipping terminals, IT networks, and other vital infrastructure in multiple markets	$117M
Pharmaceutical	Merck	Ransomware: NotPetya	Production shutdown, including the inability to fulfill vaccine orders, lost sales, and technology remediation	$670M
Shipping and Logistics	FedEx	Ransomware: NotPetya	IT operations disruption, impacted deliveries and sales, loss of revenue, and drop in earnings for one quarter	$300M

***Figure 3**. Cost of Prominent Industrial Cybersecurity Incident*

Source: Nozomi Networks: The Cost of OT Cybersecurity Incidents https://www.nozominetworks.com/blog/the-cost-of-ot-cyber-security-incidents#:~:text=%24300%20million&text=The%20incident%20temporarily%20shut%20down,business%20disruption%20and%20equipment%20damage.

Figure 3 illustrates an array of cybersecurity incidents that have impacted various types of industries. The financial losses incurred due to these breaches are a stark reminder of the gravity of the consequences that can arise. This underscores the crucial importance of implementing a robust cybersecurity framework and establishing the ability to recover from such incidents, a concept known as cyber resilience.

Chapter 3. Cybersecurity in the Maritime Industry

Chapter 3 examines the crucial aspect of cybersecurity in the maritime industry. As a result of the rapid digitization and integration of technology in maritime operations, the sector confronts an expanding array of cyber threats. This chapter explores the current landscape, commencing with an overview of cybersecurity in the maritime industry. It then examines the policies, regulations, and standards currently in place to safeguard the industry against cyber threats. Sources of cyber-based threats are analysed to obtain insight into the industry's potential weaknesses. In addition, the chapter investigates several cybersecurity cases that have affected the maritime industry, shedding light on the real-world consequences of such malicious attacks. This chapter delves deeper into the topic by examining the human element, organizational policies, and technological adaptation, which influence the effective implementation of cybersecurity in the maritime domain. The chapter concludes with a comprehensive examination of maritime cybersecurity best practices and standards to equip industry stakeholders with the knowledge and tools required to strengthen their cyber defenses.

3.1 Overview of Cybersecurity in the Maritime Industry

As defined in the digital book entitled Mission Secure, cybersecurity in the maritime industry is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to defend maritime organizations, their vessels, and the cyber environment (Mission Secure, 2020). Cybersecurity in the maritime sector is of the utmost significance for the movement of people and goods that support the global economy, such as food, medicine, and energy. Unfortunately, growing digitalization, automation, and efforts to find the optimal balance between security and usability introduce new cybersecurity threats. This balance can be difficult to maintain due to the maritime industry's swiftly evolving cybersecurity challenges (Cyber Risk GmbH, n.d.)

As stated in the special report of Lloyd's List on cybersecurity, following a sequence of high-profile assaults in recent years, cybersecurity has been elevated to the top of shipping's risk list. However, the industry's cyber resilience remains questionable. The results of a Lloyd's List survey examining

the extent of cyberattacks across the maritime industry and the measures being taken to combat this growing threat were appalling. Slow progress in addressing this cyber threat by the shipping industry continues to play into the hands of cybercriminals (Baker et al., 2022)

3.2 Key Actors Involved in Crafting Maritime Cybersecurity Policies, Regulations, and Standards

As stated in the Atlantic Council's report titled "Raising the Colors: Signalling for Cooperation on Maritime Cybersecurity" by Loomis et al., the maritime industry's Maritime Transportation System (MTS) holds significant importance in the global economy. It plays a crucial role in ensuring the secure transportation of seafaring passengers and most international trade. The MTS can be characterized as an extensive and heterogeneous transportation system. Each section has a distinct goal, tool set, and associated hazards. The MTS can be described as a complex network of interconnected systems that operates based on its participants' roles, actions, and goals. A comprehensive understanding of the MTS necessitates an initial examination of the diverse entities involved in regulating, advising, informing, and propelling the marine sector, including those expressly focused on maritime cybersecurity (Loomis et al., 2021).

Creating laws, agreements, and regulations for the marine industry requires the participation of various international and national organizations, governments, and industry stakeholders. As cited by the World Shipping Council, the main and secondary bodies involved in developing laws and policies for the sector have different roles, power, and influence. The primary entities, like IMO, ILO, national governments, coast guards and maritime authorities, have the highest authority and are responsible for governing the maritime sector, making and enforcing international and domestic laws and conventions (World Shipping Council, n.d.). On the other hand, the secondary entities, like the Intergovernmental Organizations (IGOs) (IMO, n.d.), Non-governmental Organizations (IMO, 2019), industry associations and organizations and classification societies, provide support through assistance, advocacy, and specialized knowledge. However, they do not have the same level of legislative authority and global influence as primary entities. Although

they contribute to policy development and improvement, their actions are limited by the parameters set by principal bodies (Global Policy Forum, 1999). The entities play a critical role in ensuring the safety and security of maritime operations and must work collabouratively to establish effective measures that address the unique challenges and risks associated with this industry.

3.2.1 International Maritime Organization (IMO)

The International Maritime Organization (IMO) is a United Nations-affiliated institution that aims to establish a comprehensive regulatory framework for the global maritime industry. Its primary functions include ensuring safety, addressing environmental concerns, managing legal matters, enhancing security measures, and promoting international technical cooperation. IMO is best known for its association with the Safety of Life at Sea (SOLAS) Convention, established in 1914. It is also recognized for its involvement in the International Convention for the Prevention of Pollution from Ships (MARPOL), which was adopted in 1983. (International Maritime Organization, n.d.) In 2017, IMO's Maritime Safety Committee issued recommendations for managing cyber risks in the maritime sector. These recommendations were intended to be incorporated into safety-management systems, and IMO urged shippers to implement them by the first annual verification of a vessel's Document of Compliance (DOC) and Safety Management in 2021 (International Maritime Organization, 2017).

3.2.2 International Labour Organization (ILO)

The International Labour Organization (ILO) has a vital role in ensuring fair labour practices and protecting the welfare of seafarers in the global maritime industry. Through conventions and regulations, the ILO establishes international labour standards in the industry, which are crucial in defining the legal framework governing marine activities. The Maritime Labour Convention, 2006 (MLC), also known as the "Seafarers' Bill of Rights," consolidates existing labour norms and modernizes them to cover critical aspects such as the minimum age requirement, working time regulations, intervals for rest, and the

repatriation process. By ratifying and implementing the MLC, nations can establish suitable and acceptable working conditions for seafarers and safeguard their rights.

3.2.3 Baltic and International Maritime Council (BIMCO)

BIMCO is recognized as the preeminent global organization that advocates for the interests of ship owners, charterers, brokers, and agents. The group's primary function is to develop international regulations and policy recommendations in various domains on shipping. These areas encompass environmental concerns, support for crew members, insurance matters, maritime safety and security, provision of information, and digitalization efforts. Additionally, the group is responsible for formulating guidelines on cybersecurity in the maritime sector. BIMCO membership is comprised of over 130 countries and encompasses around 62 percent of the worldwide merchant fleet, as assessed by the gross tonnage of the vessels. BIMCO, a global organization, has been officially recognized as a non-governmental organization (NGO) by the United Nations (BIMCO, n.d.).

3.2.4 Chambers of Shipping (COS)

All chambers of shipping are trade associations representing the interests of shipping enterprises within a particular nation. The Chamber of Shipping of America (CSA) and the Chamber of Shipping in the United Kingdom are two of the members of these non-governmental organizations. Around forty national COS organizations are part of the International Chamber of Shipping. These organizations work to advocate for the interests of the maritime shipping sector to various international regulatory and standards agencies. The International Chamber of Shipping (ICS) aims to promote best practices within the shipping industry and collabourates with stakeholders from the private and public sectors to achieve this objective. As a result of its efforts, the ICS possesses consultative status within IMO (International Chambers of Shipping, n.d.).

3.2.5 Classification Societies

Classification societies, sometimes known as class societies, are non-governmental organizations responsible for establishing and upholding technical criteria for the design, building, and operation of ships and offshore structures. The main emphasis of these standards pertains to the hull, propulsion, and steering systems of a ship, as well as power production and other systems associated with the operation of a vessel. Class societies utilize a comprehensive system of examination and validation to establish a fundamental benchmark for ship safety and dependability. This benchmark is a reference point for shipbuilders, brokers, operators, flag administrations, insurers, and the financial community. The International Association of Class Societies (IACS) comprises ten member organizations, including the American Bureau of Shipping (ABS), Bureau Veritas (BV) from France, China Classification Society, Lloyd's Register from the United Kingdom, Nippon Kaiji Kyokai (Class NK) from Japan, and the Russian Maritime Register of Shipping. Certain insurers mandate that a vessel possess a certification from a class society to obtain coverage. The IACS has issued advisory recommendations on the resolutions that have been enacted. Among these suggestions, Recommendation No. 166 focuses explicitly on cyber resilience (IACS, n.d.).

3.2.6 Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) is an organizational entity operating inside the United States Department of Homeland Security (DHS). CISA is responsible for overseeing and directing the development of cybersecurity strategies in the United States public sector. Its primary objective is to strengthen the nation's cyber defense capabilities by facilitating collabouration between each state's cybersecurity programs and enhancing the government's capacity to effectively counter various cyber threats, including ransomware attacks and supply chain breaches. The Cybersecurity and Infrastructure Security Agency (CISA) does not own an enforcement division or engage in enforcement activities. Instead, its

primary concentration lies in the realm of risk management and collabouration with both public and private sector entities. CISA's core functions involve disseminating threat intelligence and facilitating the development of a more robust and resilient cyber infrastructure. It focuses on mitigating various physical and cyber risks, which encompass the security of Industrial Control Systems/Operational Technology (ICS/OT) and cyber-physical systems (CPS) (Cybersecurity & Infrastructure Security Agency, n.d.).

3.2.7 European Union Agency for Cybersecurity (ENISA)

In 2004, the European Network and Information Security Organization was established, now known as ENISA. The said organization is responsible for ensuring that cybersecurity standards are consistent throughout Europe. ENISA has its headquarters in Athens and engages in various activities, such as creating cybersecurity policies, setting up cybersecurity certification programs for IT products and services, sharing information, improving capabilities, and providing cyber-awareness training programs (European Union Agency for Cybersecurity, 2005). To address the importance of the maritime sector in the European Union's economy and society, as well as the growing use of digital technologies in maritime facilities, the European Union Agency for Cybersecurity (ENISA) has actively participated in creating cybersecurity standards that are tailored specifically for ports (European Union Agency for Cybersecurity, 2019).

3.2.8 Information Sharing and Analysis Groups

Information-sharing and analysis centers (ISACs) and information-sharing organizations (ISAOs) collect, process, analyze, interpret, and share actionable intelligence on cyber and physical threats to maintain situational awareness. Established in 1998, they enhance private and public information sharing to protect critical infrastructure owners and operators. The National Council of ISACs (NCI) consists of 25 members, while ISAOs were formed in 2015 to promote voluntary information sharing within industry sectors. The International Association of Certified ISAOs (IACI) comprises fifteen organizations

(Loomis et al., 2021)

3.2.9 Maritime Insurers

The origins of maritime insurance can be traced back to the establishment of Edward Lloyd's Coffee House in London in 1686. The industry has undergone substantial transformation throughout the years to provide comprehensive coverage for ships and cargo, safeguarding against loss or damage to vessels, terminals, cargo, and passengers. Presently, many maritime insurers mandate compliance with cyber-safety regulations established by class societies, IMO, and regulatory authorities (Loomis et al., 2021).

3.2.10 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a government agency with a mission to enhance technology infrastructure security in the United States (National Institute of Standards and Technology [NIST], n.d.). In collabouration with public and private sector stakeholders, NIST has developed the Cybersecurity Framework (See Figure 4), a voluntary program aimed at reducing cyber risks to critical infrastructure by leveraging existing standards, guidelines, and practices. This framework is widely recognized as a leading standard program and is frequently utilized across various industries. It comprises three main components: the core, implementation tiers, and profiles. The core component of the Cybersecurity Framework provides a comprehensive framework for cybersecurity operations and easily understandable intended outcomes. Its primary objective is to assist organizations in mitigating their cyber risk. The implementation tiers support organizations in carrying out activities and achieving desired results by providing a practical understanding of how these processes are executed. The framework profiles enhance this process by outlining essential criteria and goals for various categories of businesses. Overall, the Cybersecurity Framework developed by NIST is a valuable resource for companies and other organizations seeking to enhance their cybersecurity posture. By leveraging the existing standards, guidelines,

and practices, organizations can effectively manage their cyber risks and protect themselves against cyber threats (NIST, n.d.-c).

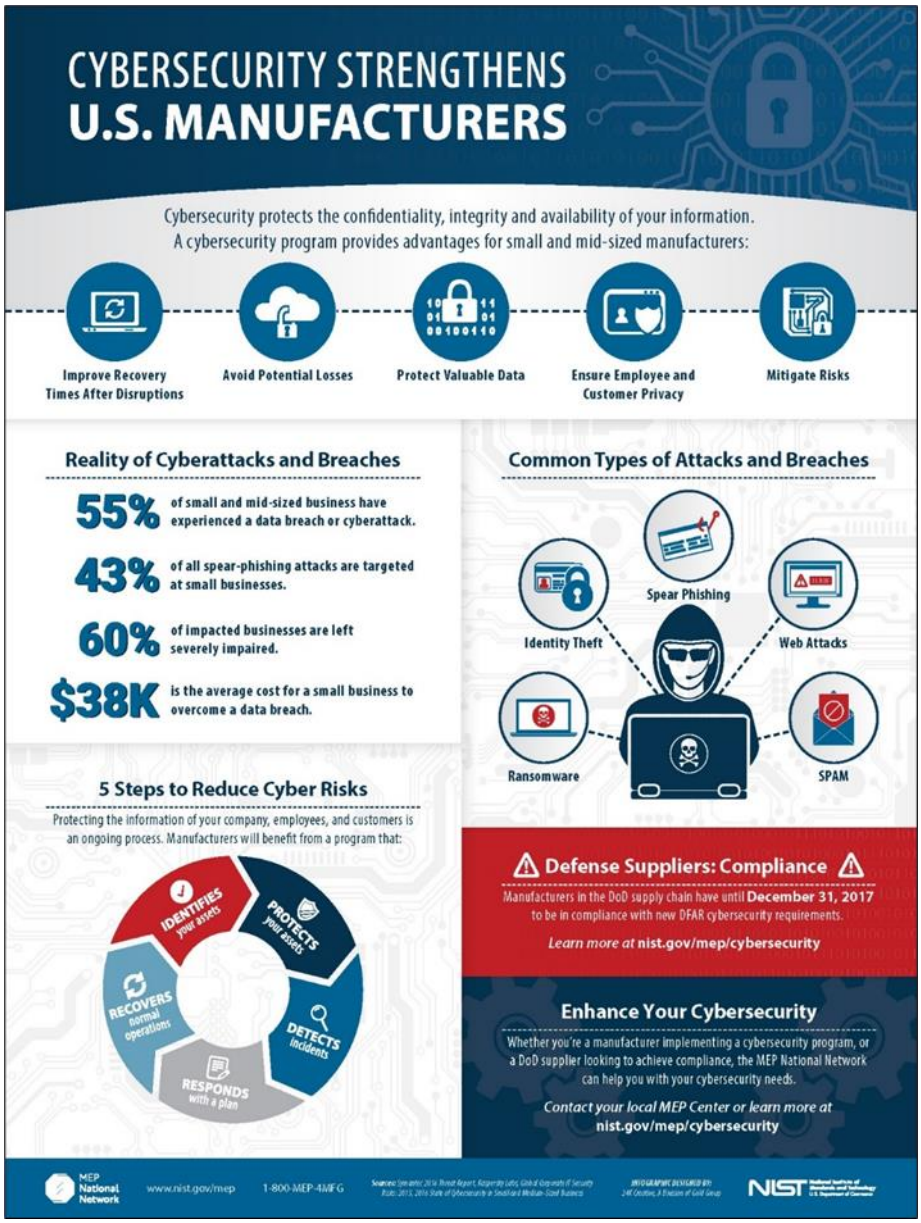


Figure 4. *NIST Cybersecurity Frameworks Infographics*
Source: https://www.nist.gov/blogs/taking-measure/things-make-me-wannacry

3.2.11 North Atlantic Treaty Organizations (NATO)

NATO is a military alliance of 31 member countries across Europe and North America, founded in 1949. One of the fundamental principles of the treaty is mutual defense (North Atlantic Treaty Organization, n.d.).

To tackle issues related to cyber warfare, NATO has created the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, Estonia. This organization has developed the Tallinn Manual, a comprehensive guide for applying legal frameworks to information operations in cyberspace (Schmitt, 2013). As emphasized on the CCDCOE website, the Tallinn Manual is a scholarly publication that reputable legal scholars and practitioners have authored. It is not legally binding but aims to provide an impartial account of international law concerning cyber activities. The manual remains unbiased in matters of policy and politics and does not represent the legal position of any nation or international organization, including the CCDCOE. The creators of the manual endeavor to maintain objectivity by thoroughly examining and incorporating multiple interpretations and applications of international law in the cyber domain with each new edition (The NATO CCDCOE, n.d.).

3.3 Review of Cybersecurity Policies, Regulations, and Standards in the Maritime Industry

Maritime Cyber Risk Management in Safety Management Systems

IMO adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems (SMS) in 2017. The resolution stated that an approved SMS should consider cyber risk management following the objectives and functional requirements of the International Safety Management (ISM) Code. It encourages administrations to ensure that cyber risks are appropriately addressed in SMS no later than the first annual verification of the company's Document of Compliance (DoC) after January 1, 2021. The same year, IMO developed MSC-FAL.1/Cir 3 guidelines that provide high-level maritime cyber risk management recommendations to safeguard shipping from current and emerging cyber threats and vulnerabilities.

The Guidelines on Cybersecurity Onboard Ships Version 4

Ships and shipping are susceptible to cyberattacks; hence, the industry collabourated to develop Guidelines on Cybersecurity Onboard Ships based on high-level principles. These regulations are intended to enhance the

protection and security of seafarers, the environment, cargo, and ships. The purpose of the guidelines is to aid in developing a cyber risk management strategy compliant with applicable regulations and best practices aboard a ship, focusing on work processes, equipment, training, incident response, and recovery management (BIMCO, 2021).

Code of Practice: Cybersecurity for Ships

Developed by The Institution of Engineering and Technology, with assistance from the Defence Science and Technological Labouratory and funding from the Department of Transport in the United Kingdom. The Code of Practice explains why cybersecurity must be considered part of a holistic approach throughout a ship's lifecycle and the potential consequences of ignoring threats. The Code of Practice is intended to be an integral element of a company's or ship's overall risk management system and subsequent business planning to ensure that the cybersecurity of the ship or fleet is managed cost-effectively as part of normal business operations (Boyes & Isbell, 2017)

Maritime Cybersecurity Assessment and Annex Guide

The US Coast Guard has published the Maritime Cybersecurity Assessment & Annex Guide (MCAAG) to assist Maritime Transportation Security Act (MTSA)-regulated facilities and other Marine Transportation System (MTS) stakeholders in addressing cyber threats. This voluntary guide is a resource for creating baseline cybersecurity assessments and plans, specifically the Facility Security Assessments (FSA) and Facility Security Plans (FSP) required by MTSA. The initial cybersecurity incorporation deadline into mandated FSAs and FSPs was October 1, 2022. During the implementation phase, stakeholders expressed an intention for the Coast Guard to continue developing guidance and providing support. MCAAG provides an additional resource for MTSA-regulated facilities to enhance and expand their ongoing cyber risk and vulnerability assessments (USCG, 2023).

IACS Unified Requirements (U.R.s) for Cybersecurity: E26 and E27

The International Association of Classification Societies (IACS) has recently published the E26 and E27 Unified Requirements (URs) for cybersecurity.

The new URs are founded on internationally recognized standards, such as IEC 62443, for the cybersecurity of industrial automation and control systems. The new URs cover the scope of applicability, which includes OT systems for critical vessel functions, the identification and protection against cyber threats, the detection of incidents, the means to respond and recover, as well as the hardening and security capabilities of systems and components (DNV, 2022).

3.4 Sources of Cyber-Based Threats

Sheldon Yates (2016) discussed the different sources of cyber-based threats in his book titled “National Critical Infrastructure Policy: Background and Select Cyber Issues”. As with other vital infrastructures, threats to the maritime information technology (IT) infrastructure can originate from various sources. For instance, advanced persistent threats — in which adversaries hold sophisticated expertise and substantial resources to pursue their objectives — pose a growing danger. Sources of risk include corrupt employees, illicit organizations, hackers, and terrorists. These threat sources differ in terms of the actors' capabilities, their willingness to act, and their motivation, which can include, among other things, monetary or political gain or disruption. The sources of cyber-based threats are detailed in Table 1.

Threat Source	Description
Bot-Network Operators	Bot-net operators use a network of compromised, remotely controlled systems, referred to as a bot-net, to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Business Competitors	Companies that compete against or do business with a target company may seek to obtain sensitive information to improve their competitive advantage in various areas, such as pricing, manufacturing, product development, and contracting.
Criminal Groups	Organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Insiders	A disgruntled or corrupt organization insider is a source of computer crime. The insider may not need a great deal of knowledge about computer intrusions because his or her knowledge of a target system is sufficient to allow unrestricted access to cause damage to the system or to steal system data. The insider threat includes malicious current and former employees and contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power— impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. A phisher may also use spam and spyware or malware to accomplish their objectives.
Spammers	An individual or organization that distributes unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or Malware Authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Terrorists	A terrorist seeks to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. The terrorist may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Table 1. *Sources of Cyber-based Threats*

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and Software Engineering Institute's CERT® Coordination Center

3.5 Analysis of Cybersecurity Threats and Vulnerabilities

Cybersecurity threats and vulnerabilities refer to the potential risks and weaknesses that malicious actors could exploit in computer systems, networks, and software. Understanding these threats and vulnerabilities is fundamental for implementing effective cybersecurity measures in the

interconnected digital landscape of today, where technology plays a vital role in numerous aspects of our lives. As discussed in the article by Boyan Mednikarov et al., entitled "*Analysis of Cybersecurity Issues in the Maritime Industry*," both targeted and untargeted cyberattacks do exist. Targeted attacks are cyberattacks on specific corporate internet networks and network components to gain unauthorized access to confidential information and impede the regular operation of ship systems. He further identified the different types of targeted attacks, which include the following:

Social Engineering - Social engineering, also known as human hacking, is deceiving employees and consumers into disclosing their credentials to gain access to their networks or accounts. It is a hacker's cunning use of deception or manipulation of people's tendencies to trust, be cooperative, or follow their curiosity and impulses to explore (Conteh & Schmick, 2016).

Attack scenarios	Description
Pretexting	A classical social engineering attack where attacker elicits classified or sensitive information from victims by using pretext scenarios (face to face or via some mediums,telephone typically). It can be very simple, e.g. posing as someone who needs help asking for help or information directly, or complex, e.g. posing as inner staff, technical support to obtain useful help with a prior survey to know better the lingo, organization and victims. (exploit e.g. kindness, credulity, ignorance, sympathy, helpfulness)
Shoulder surfing	The attacker collects information by surfing/observing over the victim's shoulder (e.g. snooping through username, password on computers, sticky notes or papers) when the victim is not paying attention or relax the vigilance during a social interaction. (exploit e.g. gullibility, friendliness, ignorance, carelessness)
Piggybacking	An authorized person provides access to an unauthorized person by keeping the secured door open (for providing help or other reasons. Most employees do not know every colleagues at large organizations and will hold a door for politeness).
Trailing & Pre-tending	Attacker who lacks the proper authentication by following individuals with permission into a restricted area of security, usually with suitable disguises such as uniform, fake badge to convince or bypass security guard. (exploit e.g. helpfulness, sloth)
Baiting	The attacker leaves a medium (e.g. USB stick) containing malicious codes in a location that is likely to be found and waits for the victims' trigger. Cases like Item Dropping, Road Apple [10, 16] are included. (exploit e.g. curiosity, greed)
Phishing	A network attack in which attackers use spoofed emails typically to trick, to lure victims into sharing sensitive information such as usernames and passwords (other actions, e.g. click a link). It is can be conducted by network mediums such websites, SNSs, instant messaging, pop-up windows and WiFi [92, 73, 67, 49, 19, 17].
Spear phishing	Spear phishing is a phishing that targets a specific organization or individual. Usually, attackers gather information about the targets, such as personal and professional relationships and other personal details from SNSs, job sites corporate websites, etc. to craft a personalized message that looks and sounds authentic to increase the probability of success.
Whaling	Whaling is a spear phishing attack directed specifically at high-value targets such as senior executives, CEO or CFO. Usually, the whaling baits such as emails and websites are highly customized and personalized, in which the target's name, job title, employee functions, internal phone numbers, organizational logos, email footer and other relevant information are incorporated. The high-level customization makes it difficult to detect a whaling attack.
Vishing	Voice phishing, in which victims are exploited to divulge sensitive information in voice form. Usually, it is conducted by mediums such as phone, Voice over IP (VoIP) and Interactive voice response (IVR).
Smishing	SMS phishing. Attacks uses Short Message Service (SMS), typically cell phone text messages, to deliver the bait to induce people to divulge sensitive information. Since the mobile phone market is now saturated with smartphones which all have fast internet connectivity, a malicious link sent via SMS can yield the same result as it would if sent via email, instant message, SNSs, etc.
Trojan attack	Trojan attack seeks to damage, disrupt, steal, control or in general inflict some other harmful action on targets' computer and network. In trojan attacks, malicious code or malwares are designed to disguise as legitimate software to lure or deceive targets into loading and activating on computer. Interesting malwares, fake mobile App are cases in point. E.g. an attacker (orally or via a note for a certain/tempting software) manages to convincing the victim to disable their firewall/anti-virus, under the pretext of allowing the software's installation, or further breaches cybersecurity by the software installed. (exploit human vulnerabilities credulity, greed, obey to authority/software note, etc.)
Water-holing	A watering hole attack is a strategy, in which attacker infects websites that targets are likely to visit (mainly by exploiting websites vulnerabilities), then waits for the targets to visit and be compromised by e.g. by downloading malwares or click malicious links (exploit targets' visit habits that they often or regularly visit the websites and trust in familiar websites).

Figure 5*.The Analysis of Popular Social Engineering Attacks Scenarios in Cybersecurity*
Source: Defining Social Engineering in Cybersecurity
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9087851

Zuoguang Wang cited in his article that the twelve prominent social engineering attack scenarios are summarized in Figure 5. Most studies acknowledge some of them, such as pretexting, shoulder

surfing, phishing, and vishing (typical instances or prototypes). Each row's description of the attack scenario exemplifies the characteristics of social engineering in cybersecurity, and some annotations are included to facilitate comprehension (Wang et al., 2020).

Brute Force - In this type of attack, the perpetrator repeatedly attempts to log in to a device or edge device using a variety of passwords, typically with the aid of specialized software designed to generate a variety of password combinations (Otoom et al., 2023).

Distributed Denial of Service (DDoS) – DDoS attacks are a type of cyberattack that aims to exhaust the target system's resources, thereby rendering the target unreachable or inaccessible and prohibiting legitimate users from gaining access to the service (MS-ISAC, 2022).

Man-in-the-middle (MITM) - A MITM attack is a cyberattack in which attackers intercept an ongoing conversation or data transmission by eavesdropping or posing as a legitimate participant. An attacker can stealthily intercept information without the victim's knowledge by inserting themselves in the "middle" of a conversation or data transmission. An MITM attack seeks to retrieve confidential data such as bank account information, credit card numbers, and login credentials, which may be used to commit additional crimes such as identity fraud and illegal fund transfers. Since MITM attacks are conducted in real-time, they are frequently undetected until it is too late (Panda Security, 2022).

Supply chain - A supply chain attack occurs when an outside provider or partner with access to your data and systems is exploited to compromise your digital infrastructure. Because the external party has been granted permission to access and manipulate portions of your network, your applications or sensitive data, an attacker only needs to breach the third party's defenses or program a security flaw

into a vendor-provided solution to gain access to your system. As with the target security breach, supply chain attacks are diverse, affecting large corporations and typically reliable methods, such as when malware is utilized for stealing cash from automated teller machine (ATM) machines. The Stuxnet computer virus, designed to infiltrate Iran's nuclear facilities, is an example of its use against governments (Fortinet, 2023).

Spoofing - Spoofing is the act of a cybercriminal masquerading as a trusted entity or device to spur you into performing an action that is advantageous to the hacker but harmful to the victim. Spoofing occurs whenever an online con artist disguises their identity as something else. Spoofing applies to numerous communication avenues and can involve varying degrees of technical complexity. The technique of social engineering is typically a component of spoofing attacks, in which scammers psychologically manipulate their victims by exploiting human weaknesses such as fear, greed, or lack of technical knowledge (Kaspersky, 2023).

On the other hand, untargeted attacks are carried out using internet environments and software tools to detect unprotected communication components (Mednikarov et al., 2020). The most popular types of untargeted cyberattacks are as follows:

Malware - Malware, short for malicious software, is any intrusive software created by cybercriminals (often called hackers) to steal data and harm or destroy computers and computer systems. Viruses, worms, Trojan horses, spyware, adware, and ransomware are examples of common malware. Malware is designed to steal information, including emails, plans, and especially private data like passwords. On top of that, it disables PCs and networks by locking them and can cause damage to the infrastructure of your network, subsequently ruining computer systems. Likewise, it uses a computer’s resources to launch botnets, cryptocurrency mining software, or spam email campaigns. Company intellectual property can be sold on the dark web (CISCO, 2023).

Ransomware – Ransomware is a type of malware that encrypts a victim's data or device and threatens to keep it encrypted or worse unless the victim pays the attacker a ransom. Ransomware attacks made up 17% of all cyberattacks in 2022, according to the IBM Security X-Force Threat Intelligence Index 2023. The encryption key required to recover access to the impacted data or utilize the infected device was sought in exchange for a ransom during the initial ransomware attacks. A firm could reduce the costs of these ransomware attacks and frequently avoid paying the ransom demand by creating regular or continuous data backups (IBM, 2023).

Phishing- These attacks trick consumers into divulging personal information like passwords or credit card details to steal or corrupt sensitive data. It comes from fraudsters posing as reliable sources which can make ganing access to confidential data easier. Email phishing is the most common type, in which scammers use fake hyperlinks to trick email recipients into divulging their personal information. Attackers pretend to be familiar names such as Microsoft, Google, or even as a fellow employee frequently poses as integral account providers. Malware phishing is another variation. This attack entails inserting malware within an email attachment that looks like a legitimate document (such as a resume or bank statement). Sometimes, opening a malicious attachment might bring down the entire IT infrastructure.

In contrast, spear phishing targets certain people by looking at data acquired via research into their social and professional lives. Due to their high level of customization, these assaults are extremely good at getting beyond basic cybersecurity. Another form of phishing is "whaling," in which scammers frequently target "big fish" like a company executive or famous person. The scammers investigate their target to determine the best time to take crucial data or login credentials. Texting and phishing are combined to create “smishing”. It entails sending texts that appear to be official correspondence from organizations like FedEx or Amazon. Since text messages are given

in plain text and seem more personal, people are particularly susceptible to SMS fraud. “Vishing” is the last. Attackers in fake call centers try to coerce victims into giving up personal information over the phone in this phishing style. These scams frequently employ social engineering to trick victims into downloading malware in an app and installing it on their devices (Microsoft Security, n.d.).

3.6 Three Types of Information Infrastructure Attacks

Rattray (2001) has provided a comprehensive analysis in his book *Strategic Warfare in Cyberspace*, regarding the possibility for adversaries to engage in strategic attacks on information infrastructure through diverse mechanical, electromagnetic, and digital methods. The author further supports this argument by citing the following examples:

Mechanical Attacks – According to Rattray's (2001) research, information systems and networks have been intentionally disrupted and destroyed through physical means during both wartime and peacetime. Command and control systems are susceptible to physical attacks, such as bombings, the deliberate severing of fiber-optic connections, damage to microwave antennae, and the physical destruction or shutdown of computers. Throughout history, the physical interception of messengers has played a significant role in determining the outcomes of battles, with electronic communications being vulnerable to mechanical disruption during the Civil War, as cavalry units cut telegraph lines. To carry out mechanical attacks, adversaries must achieve immediate physical proximity to their targets (Rattray, 2001).

Electromagnetic Attacks- Rattray (2001) has identified that information systems and networks that rely on electrical components are vulnerable to damage and disruption caused by targeted electromagnetic energy. Military operations have been observed to employ tactics aimed at disrupting electronic communications since the inception of radio technology during World War I. During the Cold War era, considerable efforts were made to address the use of an electromagnetic pulse (EMP) caused by nuclear detonations with the aim of enhancing the

effectiveness of U.S nuclear command and control communications in the event of an attack. A nuclear detonation significantly perturbs the electromagnetic field, which generates an electric current within any conductive medium. This current has the potential to interfere with or incapacitate various communication and information systems. In the 1990s, experts drew attention to the potential for producing EMP-like effects in a more limited and targeted manner (Rattray, 2001).

Digital Attacks- According to Rattray's (2001) analysis, strategic information attacks primarily aim to exploit the potential risks that arise from the intrusion and disruption of computer systems and networks, which form the backbone of advanced information infrastructures. The objectives of these attacks can range from rendering the targeted information systems and networks completely immobile to causing intermittent shutdowns, erratic data inaccuracies, unauthorized information acquisition, unauthorized service utilization, covert system monitoring, unauthorized system control assumption, unauthorized data access, and dissemination of fabricated information. Furthermore, potential attackers may attempt to introduce compromised system elements into the opposing party's information infrastructure, thereby allowing them to observe, obstruct, or obliterate the target's system and networks (Rattray, 2001).

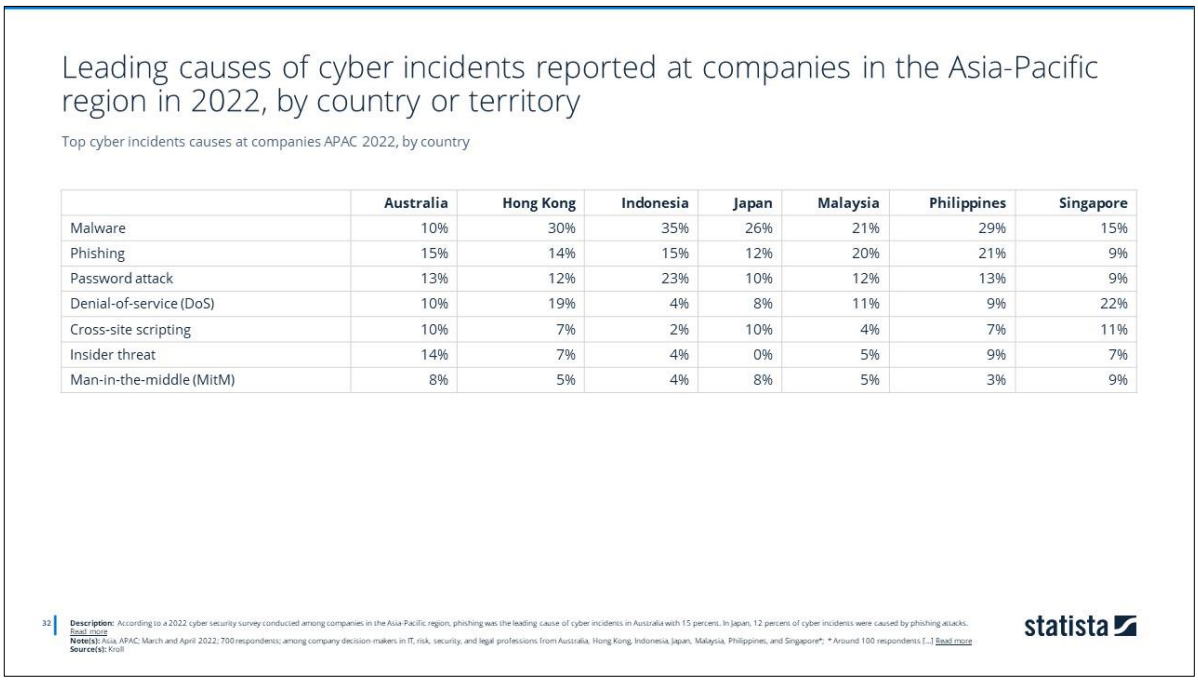


Figure 6. *Leading Causes of Cyber Incidents Reported at Companies in the Asia Pacific Region in 2022*

Source: Cybersecurity and Cybercrime in the Asia-Pacific Region
https://www.statista.com/study/138955/cybersecurity-and-cybercrime-in-the-asia-pacific-region/

According to Figure 6, malware was the most prevalent form of cyberattack in the ASIA Pacific Region in 2022. This data serves as a reminder of the continued risk posed by malicious software to regional organizations. Businesses and institutions must remain vigilant in preventing, detecting, and responding to cyber threats, including malware attacks. By implementing robust security measures and staying up-to-date with the latest trends and best practices in cybersecurity, entities can reduce their susceptibility to these types of incidents.

3.7 Factors Influencing the Effective Implementation of Cybersecurity in the Maritime Industry

Digitalization in the maritime industry aims to optimize the efficient operation of maritime assets, enabling continuous and interactive monitoring of key technical and operational parameters and achieving greater efficiencies and environmental conformance. Digitalization improves stakeholder communication onboard the vessel at the terminal facility, and within the transportation infrastructure (Progoulakis et al., 2023). The following subtopics

are some of the elements or factors influencing the effective implementation of cybersecurity in the maritime industry.

3.7.1 Human Element

Cybersecurity is not solely concerned with information technology systems, according to Triplett (2022). It also considers how humans use information systems and the susceptible actions that contribute to vulnerabilities. Human inaccuracy can be unintentional if the strategic implementation is inaccurate, or the plan of implementation is accurate, but unsatisfactory. According to his investigation, humans are the weakest link in secure data transmission. In addition, he asserts that the lack of cybersecurity awareness among employees can have significant consequences, such as when they are easily distracted, agitated, and exhausted, resulting in security incidents (Triplett, 2022).

Moreover, according to Nobles (2018) cited by Nobles (2019) in his research paper, malicious threat actors obtain a strategic advantage by exploiting human vulnerabilities and weaknesses. He identifies the contributing factors of human exposures in cybersecurity as (a) disproportionate investments in people compared to technologies, (b) inadequate cybersecurity and awareness training, (c) the underappreciation of human factor engineering, (d) the use of technologies to enforce end-user behavior, (e) the absence of a security culture, and (f) the lack of human factors programs.

Likewise, as stated in the research conducted by Anwar et al. (2017), gender differences (*See Figure 7*) also play an essential component in mediating the factors influencing employees' cybersecurity attitudes and behaviors. As shown in Figure 6, they compare the features of their cybersecurity behavior model between male and female employees. In terms of computer skills (CS), prior experience (PE), cues-to-action (CA), security self-efficacy (SSE), and self-reported cybersecurity behavior (SRCB), the results indicate statistically substantial gender disparities. Given that women were shown to have significantly lower self-efficacy than males, women's self-efficacy may

be an intervention target. The practical application of their findings is the development of gender-specific cybersecurity training and interventions that target pertinent elements of the cybersecurity behavior model to enhance employee attitudes and behaviors (Anwar et al., 2017).

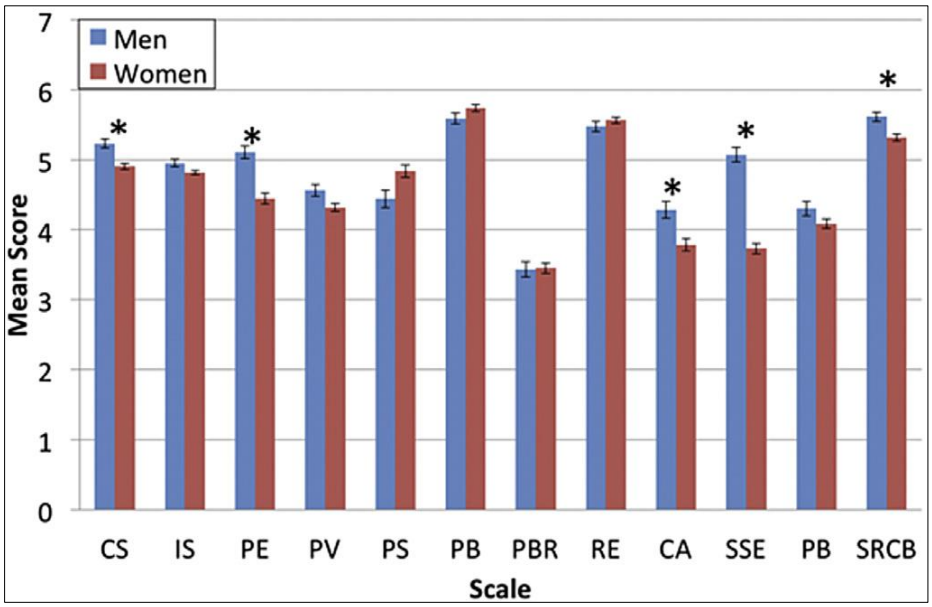


Figure 7. *Gender Differences*
Source: Gender Difference and Employees' Cybersecurity Behaviours
https://www.sciencedirect.com/science/article/pii/S0747563216308688

3.7.2 Organizational Policies, Regulations, and Standards Adaptation

The issue of cybersecurity has become a matter of significant concern in various industries globally, including the maritime sector. The maritime industry, which encompasses shipping, offshore operations, and ports, heavily relies on digital technologies and interconnected systems for efficient communication and operations (Ichimura et al., 2022). However, while digitalization has streamlined these processes, it has exposed the industry to diverse cyber threats. The successful implementation of cybersecurity in the maritime industry hinges on several factors, including adopting organizational policies, adherence to regulations, and standardization.

According to the report by Loomis et al. (2021), a crucial recommendation involves raising the baseline for cybersecurity. The report emphasizes the need to elevate the cybersecurity standard in

the maritime industry, which currently has a low baseline, by identifying four key problems that require attention. These issues include a more specific set of cybersecurity guidelines, a clear threat matrix for maritime incidents, more streamlined intelligence sharing, and a codified vulnerability disclosure program. Figure 8 provides a visual representation of these critical issues.

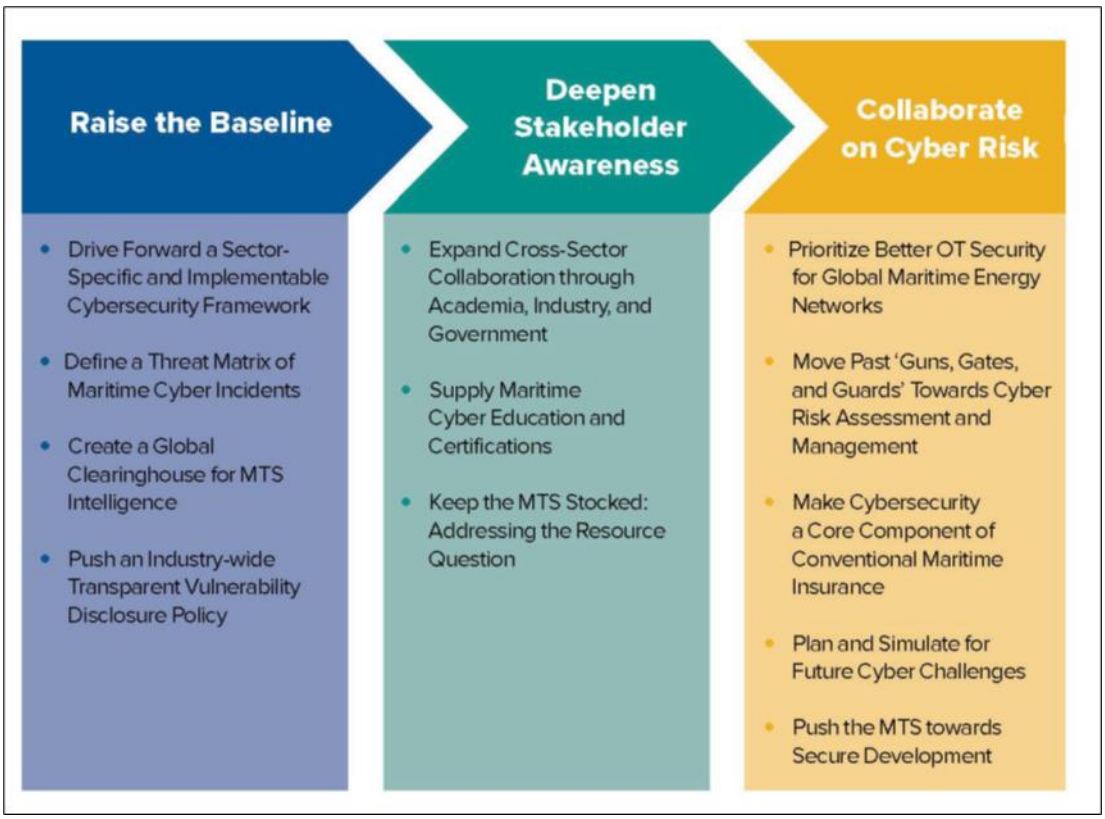


Figure 8. *Atlantic Council Recommendation on Signalling for Cooperation on Maritime Cybersecurity*
Source: Raising the Colours: Signalling for Cooperation on Maritime Cybersecurity https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/

The report further highlights that one of the challenges is how organizations approach security and guidelines for best practices. IMO, the primary international maritime body, issued cybersecurity guidelines as recently as 2017, drawing heavily on the NIST Cybersecurity Framework's five functions to provide high-level direction to maritime transport system stakeholders. However, varied

cybersecurity frameworks have been developed and promoted by both stakeholder organizations and multilateral bodies, such as BIMCO, the American Bureau of Shipping (ABS), and ENISA. Each framework introduces essential elements, but these modifications unintentionally create a tapestry of frameworks that clash at the operator level (Loomis et al., 2021).

Given the maritime sector's complexity, with a changing attack surface based on a ship or facility's type, functions, and age, cyber risk frameworks should not add confusion. The report underscores the importance of addressing these issues to ensure a more robust and practical approach to cybersecurity in the maritime industry.

3.7.3 Obsolete Technology

Another critical aspect that affects the successful implementation of cybersecurity measures is the willingness of stakeholders to upgrade their outdated technology and cybersecurity infrastructures. The NTT 2020 Global Network Insights Report (*See Figure 9*) has observed that the presence of outdated devices on networks has increased cybersecurity threats, resulting in more severe implications for cybersecurity concerns (NTT, 2020). On the other hand, as per The Agenda Weekly, cited on the World Economic Forum website, the widespread use of machine learning and artificial intelligence technologies, along with an increasing dependence on hardware, cloud infrastructure, and software, has resulted in digitalization having a significant impact on multiple aspects of our lives and industries (World Economic Forum, 2021). In addition, the World Economic Forum's Global Risks Report 2022 has identified a global risk related to technology, specifically outdated cybersecurity infrastructure. This risk is attributed to the increasing prevalence and complexity of cybercrimes, which can cause geopolitical strain, economic turmoil, social unrest, and financial damage. This risk had evaluated over a ten-year period. A global risk is an event or circumstance that can have significant adverse consequences across multiple nations or sectors (WEF, 2022).

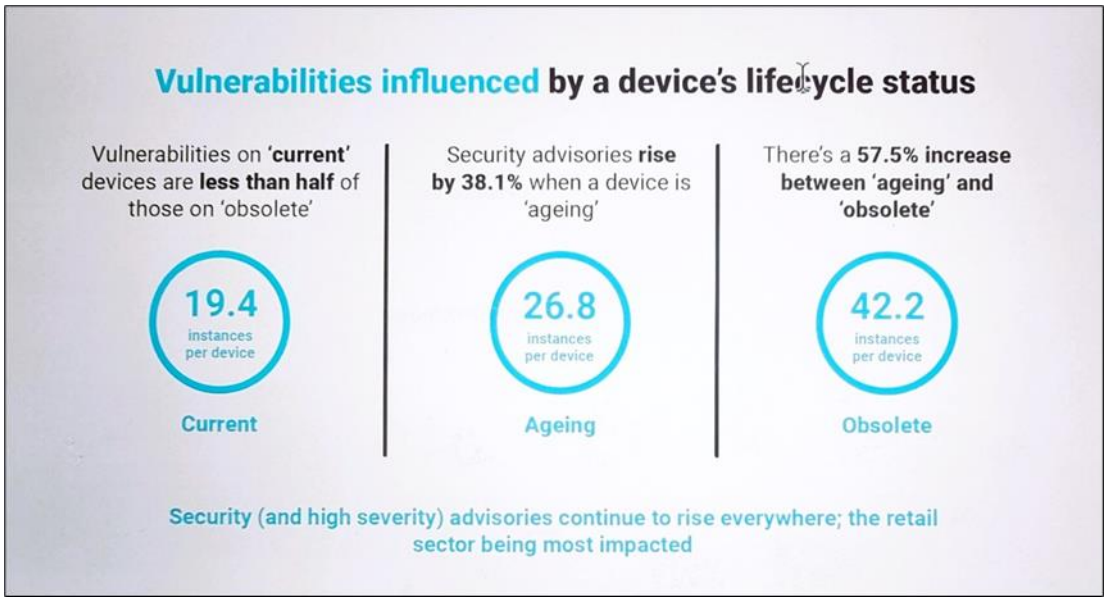


***Figure 9**. Vulnerabilities influenced by a device's lifecycle status*
Source: 2020 Global Network Insights Report- Security Threats and Vulnerabilities
https://services.global.ntt/en-us/insights/2020-global-network-insights-report?utm_source=NetworkingReport2020&utm_medium=PressRelease&utm_campaign=NetworkingReport2020&utm_term=&utm_content=Campaignlandingpage&campaignID=7014G000001n2rG&utm_SFDC_Offer=

To sum up, as the maritime industry adopts more digital and interconnected systems, it is crucial to prioritize effective cybersecurity measures. Educating and training people in cybersecurity and raising awareness is the first defense against cyber threats. Organizationally constant policies, procedures, and regulations also ensure compliance and resilience. It is also essential to address outdated technology to stay ahead of malicious actors. By managing these factors proactively, the maritime sector can navigate the complex cybersecurity landscape and ensure the continuous flow of goods and services around the world's oceans, ultimately securing its future in our digital age.

The Philippines' progress in implementing cybersecurity measures is still in its infancy stage, making it crucial to address the factors present in the maritime sector to prevent and mitigate cyberattacks effectively. Additionally, discussing

and acknowledging these concerns can aid in improving the industry's cyber resilience. It is therefore imperative to prioritize cybersecurity in the maritime sector and take proactive measures to safeguard against potential threats. By doing so, the industry can ensure the safety and security of its operations and maintain its reputation as a reliable and trustworthy entity.

3.8. Maritime Cybersecurity Cases

Cyberattacks have increasingly targeted the maritime industry in recent years, essential to global trade and economic stability. The following are a few cases of cyberattacks that show the severity of the impacts and serve as vital reminders of the imperative need for robust cybersecurity measures in the maritime industry to protect global trade, infrastructure, and economic stability.

3.8.1 Cyberattack on Port of Los Angeles

The number of monthly cyberattacks on the Port of Los Angeles has nearly doubled since the COVID-19 pandemic, reaching 40 million. The port processes more than $250 billion in cargo annually and it is primarily targeted by Europe and Russia to destabilize the American economy. The Port of Los Angeles has invested millions in cybersecurity, establishing one of the first Cyber Resilience Centers in the world. The Cyber Operations Security Centre, a component of the FBI's cyber watch program, provides enhanced intelligence gathering and protection against cyber threats to the maritime supply chain. Since the pandemic, supply chain bottlenecks have lessened, but the strain on supply chains will persist until the end of 2023 due to the high cargo volume and limited space. The vital function played by the Port of Los Angeles in the nation's infrastructure, supply chains, and economy is essential for maintaining national security (Fenwick, 2022).

3.8.2 Cosco Shipping Targeted in Ransomware Attack

Cosco Shipping Lines, the container transport division of China's Cosco Shipping Group, suffered a cyberattack that rendered its IT systems in the United States inoperable. The company has verified the outage, which affects services such as email and slot reservations. It is

uncertain what caused the system failure. Cosco Shipping's US website remained inaccessible, whereas its UK and primary corporate sites went online and became operational. The company advised US-based customers to submit booking requests, shipping instructions, and amendments through its e-commerce website. The business evaluated the incident and took steps to mitigate its impact on operations(Shen, 2018).

3.8.3 Maersk Shipping NotPetya Cyberattack

Maersk Line, a container shipping company, was targeted by a NotPetya Cyberattack in 2017, a ransomware strike that blocked individuals from accessing their data unless they paid $300 in bitcoin, costing them roughly $300 million in lost income. The ransomware exploited security flaws in Windows that Microsoft corrected after they were discovered. The main targets of the attack were Maersk Line, APM Terminals, and Damco. (Novet, 2017). It took Maersk over a week to restore most of its IT operations to normalcy. This resulted in a six-day backlog on its trading and liner services, with numerous terminals still recovering from outages. Ultimately, it resulted in a large financial loss and a significant dent in Maersk's consumer confidence (Wingrove, 2017). In the 2022 Annual Report of Information Fusion Center, it was cited that during the NotPetya cyberattack, Maersk experienced a complete global network breakdown, resulting in the inoperability of dozens of its 76 ports, 800 vessels, and drilling platforms, and the incapacitation of 95,000 employees in 130 countries. It is important to note that the attack was not specifically targeted at the corporation but was instead a result of deliberate targeting of Ukraine. The incident serves as a critical reminder of the potential risks that can arise from cyber threats and the need for appropriate measures to prevent and mitigate their impact (Information Fusion Center, 2022).

3.9 Maritime Cybersecurity Best Practices and Standards

IMO implemented resolution MSC.428(98) concerning the integration of

Maritime Cyber Risk Management into the Safety Management System (SMS) in the year 2017 (International Maritime Organization - IMO, 2017). The Resolution asserts that an authorised Safety Management System should incorporate cyber risk management and urges governing bodies to guarantee that cyber threats are adequately managed inside safety management systems. The same year, IMO published guidelines offering comprehensive maritime cyber risk management recommendations (IMO, 2017). These guidelines protected the shipping industry from existing and evolving cyber threats and vulnerabilities. As cited by Arampatzis (2020) in his article, it was emphasized in IMO recommendations that implementing comprehensive cyber risk management should commence at the senior management level. It was recommended that senior management implement a comprehensive cyber risk awareness culture throughout all levels and departments of a company. This should be accompanied by establishing a flexible and all-encompassing cyber risk management system that operates continuously and undergoes regular evaluation through effective feedback mechanisms (Arampatzis, 2020). Furthermore, BIMCO has formulated the Guidelines on Cybersecurity Onboard Ships (BIMCO, 2021), per the NIST Cybersecurity Framework (NIST, 2018). The primary objective of these rules is to provide comprehensive operational resilience to cyberattacks. The subsequent frameworks presented encompass well-established models employed by several businesses, including the maritime industry to develop and implement cybersecurity strategies.

3.9.1 NIST Cybersecurity Framework

Kessler and Shepard (2022) assert that the NIST Cybersecurity Framework has gained widespread recognition as a prominent point of reference for cyber defense guidelines and recommendations on best practices, both domestically and internationally. The authors stated that the framework should not be regarded as a mandatory requirement but as a discretionary framework comprising policy standards, recommendations, and optimal practices. Its purpose is to aid companies in evaluating their capacity to recognize, detect, mitigate, and address cyber incidents. The assessment additionally furnishes an organization with a strategic approach to discern vulnerabilities in its

cyber protection and a systematic plan for enhancement (Kessler & Shepard, 2022b).

The Framework consists of three primary components: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core, as seen in Figure 10, is a comprehensive repository that captures routine cybersecurity practices, resulting outcomes, and relevant references for the infrastructure and various sectors. The Elements of the Core offer explicit guidance in developing unique organizational profiles. Utilizing profiles within the framework will aid an organization in harmonizing and prioritizing its cybersecurity endeavors based on its business or mission necessities, risk tolerance, and the resources at its disposal. The tiers allow businesses to assess and understand the attributes of their cybersecurity risk management approach, therefore aiding in prioritizing and attaining cybersecurity objectives (NIST Cybersecurity Framework Team, 2018).

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

***Figure 10**. NIST Framework Core Functions and Categories*

Source: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 https://www.nist.gov/cyberframework/framework

3.9.2 NIST's National Initiative for Cybersecurity Education (NICE) Framework

NIST's National Initiative for Cybersecurity Education (NICE) framework focuses on training and educating the cybersecurity workforce. Its mission is to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development (NIST, n.d.-d). According to Kessler and Shepard (2022), the NICE Framework utilizes a blend of established criteria, shared vocabulary, and optimal methodologies that employers can use in the private or public sectors to delineate the roles and responsibilities of cybersecurity professionals. Additionally, academic institutions can employ this framework to develop educational curricula that align with industry requirements, while students and trainees can utilize it to identify suitable programs of study. The authors clarify that the architecture encompasses six overarching workforce categories: analysis, investigation, protection and defense, and secure provisioning. Every class consists of several specialized fields. Overall, there exist around thirty-six distinct specialization areas. Every technical field is linked to a specific occupational position as a job description. Every position is associated with a set of responsibilities inherent to the job, and each responsibility is delineated based on the requisite knowledge and abilities that an individual aspiring to or currently occupying this position should possess. Tasks will consist of various knowledge and skill statements, and each knowledge or skill may apply to multiple tasks and, thus, to different roles (*See Figure 11*) (Kessler & Shepard, 2022c)

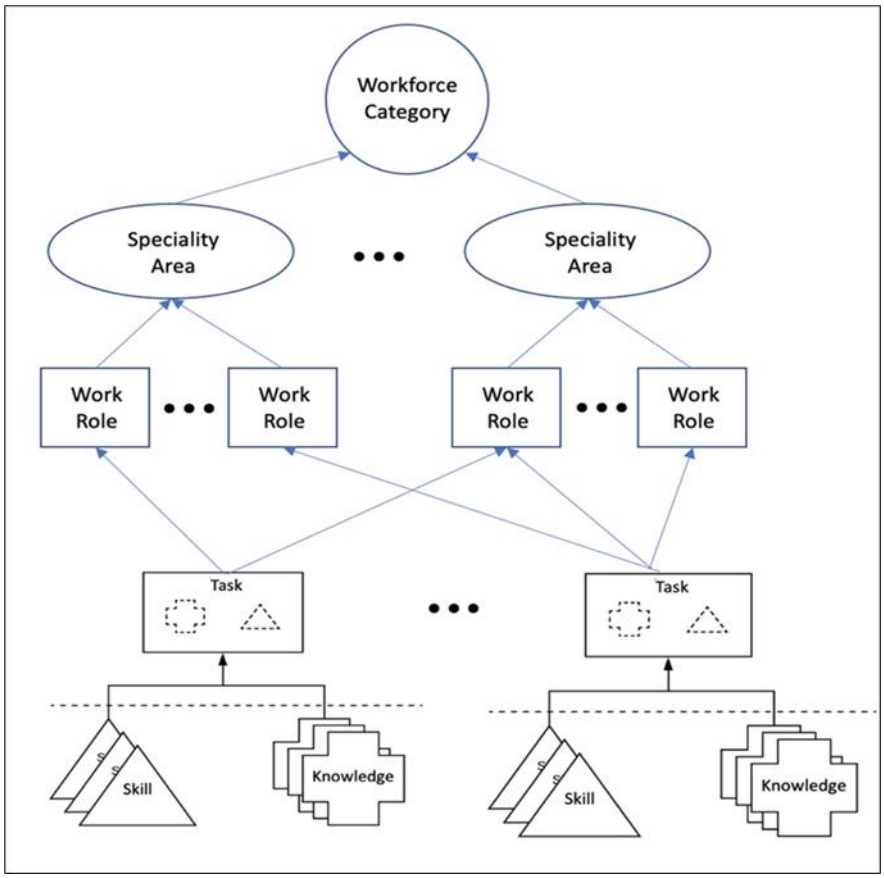


Figure 11. *NIST NICE Framework Building Blocks*
Source: Maritime Cybersecurity- A Guide for Leaders and Managers 2nd Edition by Gary C Kessler and Steven D Shepard https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

3.9.3 The MITRE ATT&CK® Framework

The MITRE ATT&CK® Framework is a comprehensive repository of adversary tactics and procedures derived from empirical observations in real-world contexts. The ATT&CK® knowledge base is a fundamental resource for developing targeted threat models and approaches within many sectors, including the business sector, government, and the cybersecurity product and service industry (MITRE, n.d.). In their book, Kessler and Shepard (2020) noted that an ATT&CK® matrix has been developed specifically for enterprise, mobile, and industrial control system contexts. The ATT&CK® Enterprise Matrix comprehensively categorizes techniques,

encompassing 14 distinct areas: reconnaissance, initial access, execution, persistence, privilege escalation, defensive evasion, lateral movement, command and control, and exfiltration. Each tactical category encompasses a collection of attack techniques, with the matrix providing a comprehensive description of over 220 distinct attack technique categories. This academic text defines various methods along with a collection of real-world instances, strategies for mitigating the associated risks, and ways to detect the occurrence of these techniques. The reconnaissance category encompasses a range of approaches: active scanning, phishing for information, acquiring the target's host, network, and organizational communication, exploring open websites, and examining the target's website, among others. Each approach may have sub-techniques, resulting in a categorization that encompasses over 30 attack strategies. The “Enterprise Matrix” includes a comprehensive compilation of around 600 distinct cyberattack strategies (Kessler & Shepard, 2022a).

3.9.4 The MITRE D3FEND™ Framework

Singer (2021) articulates in his article that the MITRE D3FEND™ knowledge graph thoroughly depicts various technical functionalities in cybersecurity, presented in a standardized language called "countermeasure techniques." MITRE carried out this study with financial support from the NSA to strengthen the cybersecurity measures for national security systems, the Department of Defense, and the defense industrial base. By making this framework available to the public, it aims to facilitate its widespread access and utilization, enabling the cybersecurity community to improve and refine continuously. The author further explains that D3FEND™ offers a comprehensive compendium of explanations for digital entities. These entities encompass the distinct technological components safeguarded or scrutinized by cyber products. Such definitions articulate cyber systems and their corresponding countermeasures, establishing a bedrock for digital engineering and the automated analysis of intricate relationships between computer network structures, susceptibilities,

and cyber defenses. This facilitates security architects in comprehending how a novel product may interconnect or collabourate within an integrated network defense system (Singer, 2021).

3.9.5 ABS Cybersafety ® Method

As presented on the website of the American Bureau of Shipping (ABS), with a focus on maritime and high-tech manufacturing control systems, the ABS CyberSafety® team boasts a wealth of cybersecurity knowledge. Leveraging their expertise, they have developed the industry's first comprehensive guidance for creating a customized cybersecurity plan that meets the unique needs of a fleet. The ABS CyberSafety® methodology offers a complete strategy for asset owners, operators, shipyards, equipment system suppliers, and integrators to assess and manage the risks associated with cyber-enabled equipment (American Bureau of Shipping, n.d.). According to Kessler and Shepard's (2022) research, the ABS CyberSafety® Method is a comprehensive maritime cyber guideline that utilizes a top-down risk management approach. Figure 12 outlines a framework including several fundamental tasks the maritime industry should integrate into its cybersecurity strategy. These tasks are grouped into three categories: practices and processes (Tasks 1-3), risk management (Tasks 4-6), and resource and asset protection (Tasks 7-9). Additionally, the authors discussed Task 10-23, which consists of 14 advanced capabilities spread across three categories. These capabilities enhance the organization's cybersecurity implementation by incorporating cyber defense standards, threat intelligence, vulnerability assessment, and system testing (Kessler & Shepard, 2022d).

Figure 12. *ABS CyberSafety® Method*
Source: ABS Cybersecurity: Guidance Notes for the Marine & Offshore Industries

3.9.6 BIMCO Risk Management Model

The Baltic and International Maritime Council (BIMCO) published *Guidelines on Cybersecurity Onboard Ships Version 4* in collabouration with the International Chamber of Shipping (ICS), the International Union of Marine Insurance, The World Shipping Council, and more than 20 maritime companies and organizations in 2020. These principles aim to enhance the safety and security of seafarers, cargo, vessels, and the environment. The recommendations can assist in developing an effective strategy to manage cyber risks aboard a ship by utilizing a risk assessment model and aligning it with applicable regulations and industry best practices. The guidelines stress the importance of addressing work processes, equipment, training, incident response, and recovery management to mitigate cyber risks. They comprehensively analyze the rationale and methodology for effectively

managing cyber threats within the maritime industry. The manuscript enumerates the necessary supporting paperwork for risk assessment and provides a comprehensive overview of the risk assessment process, explaining the role played by each constituent of cyber risk. The publication emphasizes the significance of assessing the probability, severity, consequences, and susceptibilities during the execution of a cyber risk evaluation. It guides readers in effectively addressing and mitigating the impacts of cyber events (BIMCO, 2021).

Figure 13. *BIMCO Cyber Risk Management Approach*

Source: The Guideline on Cybersecurity Onboard Ships
https://www.bimco.org/About-us-and-our-members/Publications/The-Guidelines-on-Cyber-Security-Onboard-Ships

The Cyber Risk Management Approach of BIMCO is depicted in Figure 13. This illustration provides a comprehensive overview of the approach taken by the organization to manage cyber risks. It highlights the various steps involved in the process and emphasizes the importance of a proactive and holistic approach to cyber risk management. By following this approach,

BIMCO can effectively mitigate the risks associated with cyber threats and ensure the safety and security of their operations. Implementing a sound cyber risk management strategy is essential for any organization that seeks to protect its assets and reputation in today's increasingly complex digital landscape.

To enhance cybersecurity in the Philippines' maritime industry, it is advisable to adopt a comprehensive cybersecurity framework incorporating globally accepted standards such as the NIST Cybersecurity Framework and ISO protocols and industry-specific guidelines from the International Maritime Organization (IMO). A successful cybersecurity strategy for this sector must be customized to tackle its distinctive challenges, adhere to local regulations, and prioritize teamwork, risk assessment, and incident response.

Chapter 4. Cybersecurity Landscape of the Philippines

The fourth chapter of this research examines the cybersecurity landscape of the Philippines, emphasizing specifically the maritime industry. This chapter will review the various legal instruments that govern cybersecurity in the Philippines' maritime sector, the domestic policies, regulations, and standards implemented by the nation's primary maritime agencies. It will also investigate the cybersecurity threats and vulnerabilities within the maritime industry. It will compare Malaysia and Singapore's maritime cybersecurity landscapes to obtain a broader perspective. This chapter seeks to present valuable views on cybersecurity in the Philippine maritime sector and how it compares internationally by conducting an in-depth assessment.

4.1 The Philippines Cybersecurity Landscape

In light of the inherent vulnerabilities that the nation faces within the digital realm, the Philippine government is taking measures to strengthen its information and communication technology (ICT) infrastructure and capabilities to effectively mitigate security threats that arise from the dynamic and ever-changing ICT landscape.

The Department of Information and Communication Technology (DICT) established the National Cybersecurity Plan 2022 in 2017. This plan serves as a strategic framework *(See Figure 14*) for safeguarding the operations of ICT infrastructure within the country. The proposal underscores the significance of establishing a comprehensive National Cybersecurity Strategy framework to formalize and implement internationally recognized standards. This endeavor aims to establish a systematic government approach for defending mission-critical and non-critical infrastructure from potential threats and attacks. The framework focuses on establishing a reliable and robust ICT infrastructure, with particular emphasis on the following stages: enhancing the trustworthiness and security of essential information infrastructure, ensuring the safety of the government's information environment, enhancing the security of enterprises, and promoting awareness and security among individuals (Department of Information and Communication Technology, 2017).

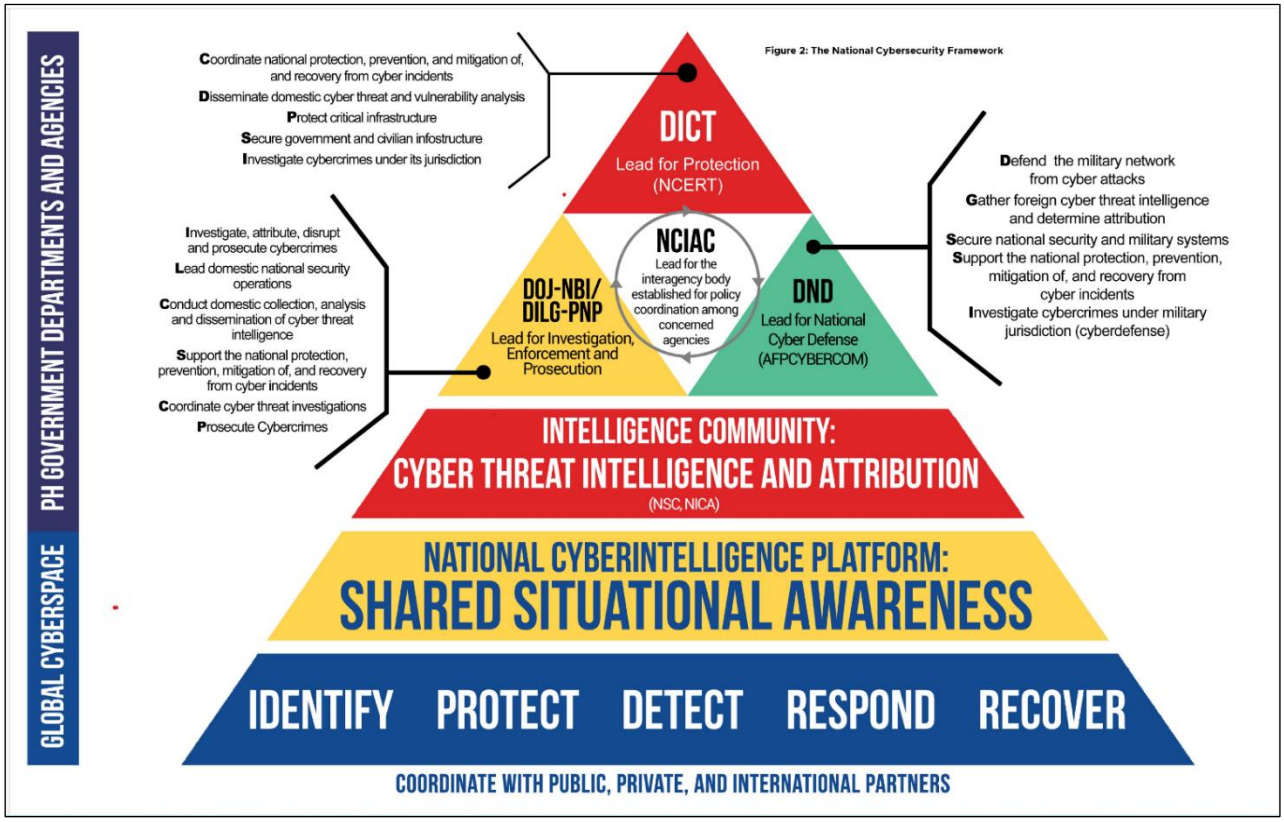


Figure 14. Philippines National Cybersecurity Framework

Source: Department of Information and Communication Technology
https://dict.gov.ph/national-cybersecurity-plan-2022/

The current state of the nation's cybersecurity capabilities is in its early developmental phase. As a result, the foundational structure for safeguarding critical infrastructure must be established by adopting the NIST Cybersecurity Framework (Department of Information and Communication Technology, 2017). This framework comprises five essential activities: identification, protection, detection, response, and recovery (NIST Cybersecurity Framework Team, 2018). By implementing this framework, organizations can ensure that they take the necessary steps to secure their digital assets and mitigate the risks associated with cyber threats. Businesses and academic institutions must prioritize cybersecurity to protect their operations,and reputation.

In addition, the government has implemented the Cybersecurity Management

System (CMS) Project and the National Cyber Intelligence Web Monitoring (NCIWM) initiative. The Cybersecurity Management System represents the inaugural cyber resiliency endeavor of the nation. It serves as a consolidated national framework for the exchange of intelligence, enabling the Department of Information and Communications Technology and its private-sector cybersecurity collabourators to aid government entities in addressing cybersecurity threats, attacks, and related concerns. The NCIWM, or Network-Centric Intrusion Warning Mechanism, is a valuable instrument capable of delivering instantaneous analysis of cyber assaults targeting government websites and other domain names that have been incorporated into the system. Further, the government has created the Computer Emergency Response Team (CERT) Training Program as an additional initiative. The initiative aims to enhance the capabilities of government ICT employees through training programs focused on information security. Furthermore, this initiative aims to build and enhance emergency response capabilities inside the nation (ASEAN Regional Forum, 2022).

4.1.1 National Cybersecurity Plan

The Department of Information and Communications Technology is presently engaged in soliciting public feedback, opinions, and recommendations from various stakeholders, advocates, and concerned individuals regarding the proposed National Cybersecurity Plan (NSCP) for 2023-2028. The aforementioned public consultation aims to enhance the NSCP 2023-2028 edition, scheduled for publication before the end of 2023. The draft National Cybersecurity Plan (NSCP) for the period 2023-2028 places emphasis on six key pillars. These pillars include: 1) The implementation of the "Cybersecurity Act" to enhance the policy framework; 2) The establishment of measures to secure and safeguard Critical Information Infrastructures (CII); 3) The proactive defense of government and individuals in the realm of cyberspace; 4) The development of an efficient and well-coordinated network of Computer Emergency Response Teams (CERT) and Security Operations Centres (SOC); 5) The enhancement of the cybersecurity workforce's

capabilities; and 6) The promotion of international cooperation in the field of cybersecurity. The necessity for collabourative efforts from all relevant parties to attain a reliable, robust, and protected digital environment for the Filipino population was emphasized by Ivan John Uy, the Department Secretary. Additionally, he emphasized that NSCP 2023-2028 highlights the significance of collabouration among various governmental entities in effectively fulfilling our objective. This document delineates a series of procedural measures that elucidate how each governmental entity can effectively synchronize its respective cybersecurity endeavors through the National Cybersecurity Inter-Agency Committee (NCIAC). Additionally, it facilitates the coordination of all organizational Computer Emergency Response Teams (CERTs) and establishes two CERTs at the national level (Department of Information and Communication Technology, 2023).

4.1.2 Cybersecurity Legal Instruments in the Philippines

The dynamic nature of the cyber environment poses many challenges, risks, and threats. The Philippine government recognizes the complexity of this landscape and acknowledges the critical nature of information as an asset to individuals, the public, the private sector, and the government. Consequently, it is imperative to safeguard its computers, networks, and application systems from any form of compromise or breach. As a proactive measure, the Philippine government has implemented measures to ensure the safety and security of its cyberspace. As early as 1965, legislation has been enacted to safeguard individuals and assets and hold accountable those who infringe upon the right to information privacy or attempt to undermine its system. Some notable examples include the Anti-Wire Tapping Act of 1965 (Congress of the Philippines, n.d.) and the Electronic Commerce Act of 2000 (Congress of the Philippines, 2000).

As mentioned in the National Cybersecurity Plan 2022, establishing the first National Cybersecurity Plan was identified as a key agenda by the Arroyo Administration in 2004. The plan emerged as a primary point of reference during the development of the Information Security Incident

Response Manual in 2013 under the auspices of the Information and Communication Technology Office (Department of Information and Communication Technology, 2017). In 2012, the Philippines enacted the Cybercrime Prevention Act, also known as Republic Act 10175 (Congress of the Philippines, 2012). It is an act defining cybercrime, providing for the prevention, investigation, suppression, and imposition of penalties and other purposes (Republic Act No. 10175 | Official Gazette of the Republic of the Philippines, n.d.) It deals with legal matters regarding online interactions and the internet in the Philippines.

According to Sy (n.d), the process of developing, passing, and enacting cybercrime law in the Philippines has been characterized by a prolonged and arduous nature. The convergence of technical challenges and the determined efforts of various factions, notably bloggers and online users, to protect their rights to freedom of speech and expression has given rise to extensive public discourse and legal proceedings. The Department of Justice (DOJ), in collabouration with the Information and Communications Technology office of the Department of Science and Technology (ICTO-DOST) and the Department of Interior and Local Government (DILG), drafted the implementing rules and regulations (IRR) of the Cybercrime Prevention Act (CPA) in accordance with Section 28 of the CPA. This drafting process involved the active participation and cooperation of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP). Consultations were also conducted with academia, government, and the private sector. The IRR, designed to be transparent and inclusive, aims to reconcile the provisions of the CPA with other legislations, namely the Access Devices Regulation Act of 1998, E-Commerce Act of 2000, Anti-Child Pornography Act of 2009, and Anti-Photo and Voyeurism Act of 2009. It also aims to address any existing gaps in law enforcement protocols concerning cybercrimes (Sy, n.d.).

4.1.3 Domestic Policy, Regulation, and Standards of Maritime Agencies

Cybersecurity is crucial in the maritime sector as technology reliance

increases, making it susceptible to cyberattacks. This section analyzed the policies implemented by vital maritime agencies in the Philippines to safeguard against cyber threats. It examined the cybersecurity strategies of the Maritime Industry Administration, the Philippine Coast Guard, and the Philippine Port Authority to understand the measures taken to protect their ICT systems. This section provides a detailed analysis of the proactive actions taken by these agencies to address the growing cybersecurity risks in the industry.

4.1.3.1 Maritime Industry Administration (MARINA)

Despite the diligent effort of the researcher, no information was provided on the initiatives undertaken by MARINA in implementing its cybersecurity measures. The only information acquired was the advisory of the agency to all shipowners, operators, and ship managers with Philippine registered ships regarding the requirement of incorporating cyber risk management in their safety management system in compliance with the IMO issuance of Resolution MSC 428(98) which was adopted on 16 June 2017.

4.1.3.2 Philippine Coast Guard (PCG)

The PCG is implementing NHQ-PCG/CG-11 Circular Number 11-19, which was issued on October 7, 2019, under the title "Philippine Coast Guard Cybersecurity Policy." This policy is backed by relevant sources, including the National Cybersecurity Plan 2022 of the government, ISO 27002-Code of Practice for Information Security Controls, and the Cyber Strategy of the United States Coast Guard. Its goal is to set up a framework of principles and regulations that govern the conduct and responsibilities of those associated with the PCG Information Infrastructure (infostructure), including PCG personnel, civilian employees, and third-party stakeholders with access to infostructure assets. The policy aims to inform these individuals about their mandatory obligations, limitations, privileges, and responsibilities. It is a formal

agreement that serves as a fundamental framework for developing and implementing exact policies, processes, and recommendations. It aims to implement cybersecurity best practices and norms effectively. The document offers direction, strategic goals, and structures to support and enhance activities, foster confidence in collabourations across different agencies and regions, and develop diverse cyber capabilities and jurisdictions. It also serves as a foundation for maintaining uniform decision-making and resource allocation. It is a chosen approach or action plan used to direct and shape current and future decisions to achieve the functions prescribed by the PCG (Philippine Coast Guard, 2019).

4.1.3.3 Philippine Port Authority (PPA)

The Philippine Port Authority is presently implementing the newly approved PPA Memorandum Circular No 012-2023, released on August 10, 2023, titled "Updated PPA Information and Communication Technology (ICT) Security Policy." The memorandum establishes a comprehensive Information and communication technology security framework within the PPA. This framework aligns with the State's policy as outlined in the National Cybersecurity Plan 2023, supporting its goals and objectives. The PPA's ICT security policy comprises defined standards, procedures, and regulations to ensure compliance among all relevant parties. Its primary aim is to effectively maintain a secure and safe ICT domain within the PPA while preserving and sustaining the operability and integrity of the agency's information systems. The policy applies to all individuals who use PPA ICT services, including PPA officials and employees, clients, contractors, third-party service providers, and other users of information systems. The policy aims to provide necessary safeguards and cohesive administration against internal and external security vulnerabilities to PPA's ICT system, services, facilities, and infrastructure.

Moreover, the policy allows PPA officials and workers to securely transmit and receive official and confidential information, materials, and documents using internet channels while ensuring adequate backup storage provisions. Clients can also securely participate in online business transactions with PPA through its ICT services, facilities, and infrastructure. Finally, the policy aims to enhance PPA's capacity to effectively manage a comprehensive and current record of its technological resources, regardless of their connection to the organization's network and ability to store or process data (Philippine Port Authority, 2023).

4.1.4 Cybersecurity Threats and Vulnerabilities in the Maritime Industry of the Philippines

Despite the researcher's diligent efforts, no significant cybersecurity attacks were uncovered within the maritime sector of the Philippines. The researcher posited that underreporting of incidents may be a contributing factor, potentially due to a desire to preserve the image or reputation of those affected. However, with the growing prevalence of digitalization and the heightened risk of cybersecurity breaches, an attack will probably occur. Proactive measures, such as initiating a comprehensive awareness campaign are crucial in preventing such incidents from transpiring.

4.2 A Brief Benchmark Analysis of Maritime Cybersecurity Landscape: Malaysia, Singapore, and Philippines

With increasing digitization and interconnectedness of the maritime industry, cybersecurity has become a critical component in ensuring the smooth and secure operation of maritime activities. A comparison of the cybersecurity landscapes of Malaysia, Singapore, and the Philippines reveals that each country has strengths and common issues affecting its individual strategies for safeguarding maritime operations. It is imperative for all stakeholders operating within the maritime industry to remain cognizant of the unique

challenges and solutions offered by each country's cybersecurity framework to ensure the protection of their assets and operations. As shown in Figure 15, as of July 2023, Malaysia reached the highest score on the National Cybersecurity Index (NCSI) among countries in the Asia-Pacific region, 79.22 out of 100, followed by Singapore with a score of 71.43. Meanwhile, the Philippines ranks 7th among 23 countries, scoring 63.64 in the index.

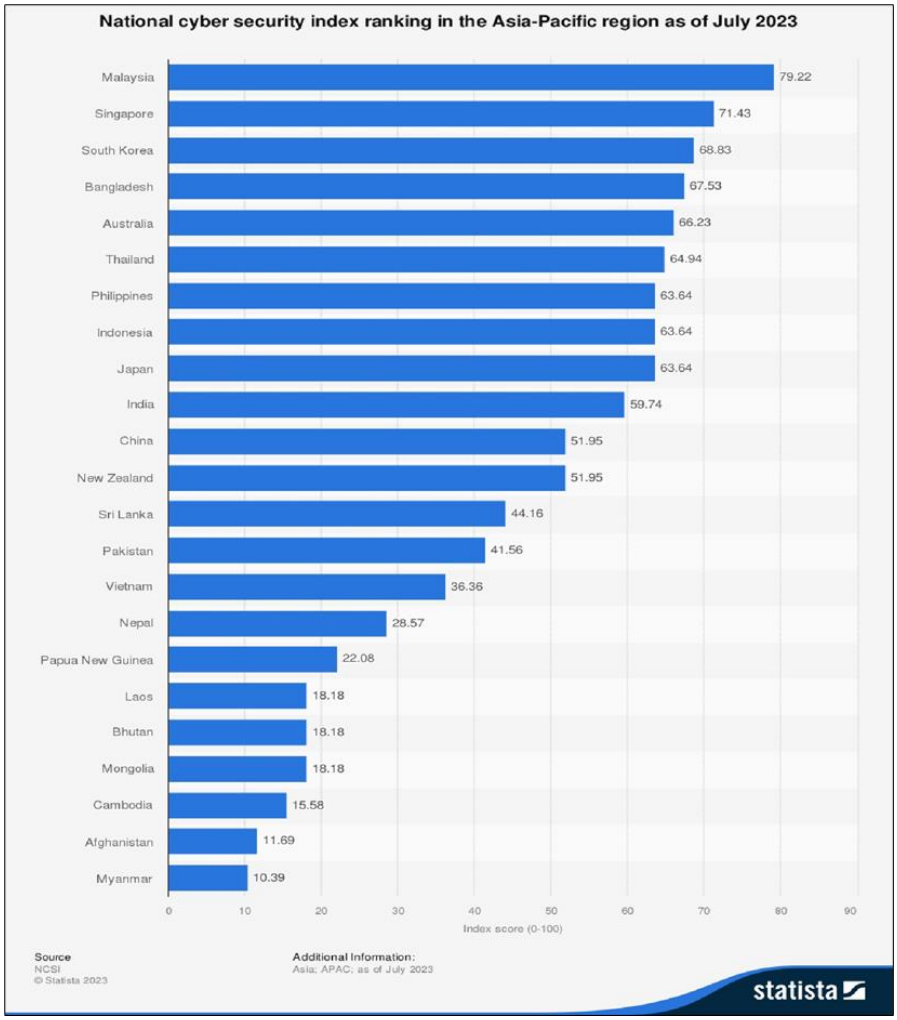


Figure 15. *National Cybersecurity Index Ranking in the Asia-Pacific Region as of July 2023*

Source: National Cybersecurity Index Ranking APAC 2023, by country https://www.statista.com/statistics/1400043/apac-national-cyber-security-index-ranking-by-country/#statisticContainer

The National Cybersecurity Index (NCSI) was implemented by the E-Government Academy in 2016 to serve as an instrument for assessing the preparedness and dedication of nations towards cybersecurity. The metric evaluates a nation's capacity to mitigate cyber threats and handle cyber

incidents by monitoring the established national cybersecurity capabilities adopted by the central government. The findings of the NCSI are derived from criteria that are both objective and measurable and are supported by publicly accessible information. This data includes legislative and policy tools, institutions, cooperative formats, activities, and tangible outcomes. The index assesses the performance of countries across 12 distinct categories related to cybersecurity capacity, which are further categorized into three overarching pillars: strategic capacities, preventive capacities, and responsive capacities. Strategic competencies encompass cybersecurity governance and policy dimensions, global involvement, education, and innovation. Preventive capabilities include establishing a secure digital infrastructure and analyzing cyber threats. The ability to respond to cyber threats of different types and magnitudes, as well as effectively handle cyber incidents and crimes, is closely associated with the third pillar,responsive capacities (National Cybersecurity Index, 2022).

4.2.1 Malaysia

Malaysia has implemented a wide range of cybersecurity measures to strengthen its cybersecurity capabilities and address the challenges of the digital era. Directive No. 26 of the National Security Council entitled National Cybersecurity Management (NSC Directive No. 26) is an executive directive that defines the overarching management of the cybersecurity ecosystem in the said country. The roles and responsibilities of each stakeholder are explicitly defined to ensure comprehension and seamless implementation of national cybersecurity initiatives and strategy (NACSA, 2023).

Hashim (2011) explains in his article that the National Cybersecurity Policy (NCSP) serves as a crucial framework for these efforts, covering essential aspects such as safeguarding vital information infrastructure, enhancing incident response capabilities, fostering collabouration between public and private sectors, and raising cybersecurity awareness. He further expounds that Malaysia’s NCSP entails identifying and categorizing significant industries and entities in the critical National Information Infrastructure (CNII). These sectors and

entities are subject to increased cybersecurity laws and surveillance (Hashim, 2011). The nation's Computer Emergency Response Team (MyCERT) plays a vital role by actively monitoring and rapidly addressing cybersecurity issues while providing valuable advice and assistance to companies in managing and mitigating cyber threats (MyCERT, n.d.).

Further, the country emphasizes promoting collabouration between government agencies, the private sector, and academia. One of its efforts is the Malaysia Cybersecurity Strategy (MCSS), which aims to disseminate knowledge and facilitate collabouration to address and mitigate cyber threats effectively. In addition, Malaysia prioritizes cybersecurity education and awareness, conducting various campaigns, training programs, and workshops to impart knowledge on cybersecurity best practices to individuals and enterprises (National Security Council, 2020).

Moreover, Malaysia actively participates in international cybersecurity forums and initiatives, fostering collabouration with neighbouring countries and worldwide partners. It is affiliated with regional entities such as the ASEAN CERT (Cybersecurity ASEAN, 2022) and the Asia-Pacific Computer Emergency Response Team (APCERT) (APCERT, n.d.), which serve as platforms for sharing threat intelligence and disseminating best practices. Moreover, Malaysia has implemented cybersecurity-related laws such as the Personal Data Protection Act (PDPA) (Government of Malaysia, 2010) and the Communications and Multimedia Act (CMA) (Communications and Multimedia Act 1998, 2004), which strengthen its efforts in safeguarding data and promoting cybersecurity. With all Malaysia's initiatives, programmes and established mechanisms in cybersecurity, it maintains its leadership position as indicated in the latest National Cybersecurity Index Ranking in the Asia-Pacific Region as of July 2023 (*See Figure 15*).

Malaysia and the Philippines have taken significant steps to strengthen their cybersecurity efforts. However, the effectiveness of their protocols may vary due to factors such as the distribution and availability of

financial and other resources, as well as the constantly evolving nature of cyber threats. Both countries must continue modifying and improving their cybersecurity plans to combat the increasing threats in the digital world efficiently.

4.2.2 Singapore

Singapore has adopted a comprehensive and diverse approach to address cybersecurity challenges effectively. The Cybersecurity Agency of Singapore (CSA) coordinates and supervises the country's cybersecurity efforts. The CSA's objective includes establishing policies, monitoring threats, and coordinating incident responses. Legal frameworks are a significant aspect of Singapore's cybersecurity strategy (Cybersecurity Agency Singapore, 2022a). The Cybersecurity Act provides a comprehensive legal framework, granting the CSA the authority to efficiently oversee and address cybersecurity threats and incidents (Republic of Singapore, 2018). Likewise, the Personal Data Protection Act (PDPA) includes rules on data breaches and cybersecurity, ensuring personal data security (The Law Revision Commission, n.d.).

Furthermore, Singapore's cybersecurity strategy involves identifying and categorizing Critical Information Infrastructure (CII) sectors, including telecommunications, electricity, water, healthcare, and other industries. Organizations in these sectors must comply with rigorous cybersecurity standards and reporting obligations. Public awareness and education are crucial to enhancing Singapore's cybersecurity resilience (Cybersecurity Agency Singapore, 2022b).

The country has also implemented cybersecurity guidelines and best practices to encourage enterprises to adopt optimal cybersecurity measures. Organizations can pursue certification to demonstrate their adherence to these standards, strengthening their overall cybersecurity stance and ability to withstand threats (Cybersecurity Agency Singapore, 2022b). Innovation plays a significant role in Singapore's cybersecurity policy, as the government actively supports cybersecurity

research and development through initiatives like the National Cybersecurity R&D Program. Local startups and research projects in cybersecurity also receive support, enhancing the nation's capabilities in this domain (National Cybersecurity R&D Lab, n.d.).

Singapore actively engages in several international collabourations and partnerships regarding cybersecurity, such as the ASEAN CERT through incident drills. By fostering alliances with other nations, it exchanges threat intelligence and promotes adopting best practices, thus making valuable contributions to global cybersecurity endeavors (Ocampo, 2022).

Efforts to cultivate a proficient cybersecurity workforce are evident in Singapore's implementation of diverse educational initiatives, provision of scholarships, and establishment of collabourative alliances with industry stakeholders. The presence of highly skilled and well-trained personnel is crucial in effectively mitigating the constantly evolving landscape of cyber risks. Singapore has established a comprehensive framework that clearly outlines the roles and duties of different stakeholders in incident response and coordination. Regular cybersecurity exercises and drills are carried out to evaluate the preparedness and response capabilities of governmental and private sector entities.

To sum up, Singapore and the Philippines both recognize the significance of cybersecurity but have different approaches and levels of advancement in their programs. As discussed above, Singapore has established a centralized governing body, the Cybersecurity Agency of Singapore (CSA), to supervise and coordinate the country's cybersecurity efforts. This centralized approach ensures a highly organized and effective solution of cyber risks. Singapore has also enacted the Cybersecurity Act, which empowers CSA to oversee cybersecurity issues and implement a robust legal framework. Implementing rigorous cybersecurity standards in Singapore's Critical Information Infrastructure (CII) sectors also guarantees the

implementation of protective measures in critical domains such as telecommunications and healthcare. Singapore has also taken steps such as public education campaigns, certification programs, innovation assistance, international collabouration, and an incident response system to enhance its cybersecurity posture.

On the other hand, the Philippines has traditionally used a decentralized approach to cybersecurity, with various government entities engaging in related initiatives. The Cybercrime Prevention Act is in place to address cybercrime offences, but it may not have the same comprehensive cybersecurity regulations as Singapore. Although the Philippines has defined critical infrastructure sectors, the enforcement of cybersecurity regulations and protection measures may differ. Public awareness and education campaigns are being developed to enhance cybersecurity in the Philippines. The country is also promoting innovation and research, while certification and compliance with cybersecurity standards are evolving. The Philippines actively collabourates internationally, like Singapore, to strengthen cybersecurity resilience.

In summary, Singapore, Malaysia, and the Philippines each adopt diverse cybersecurity strategies designed to address their individualized obstacles and priorities. Singapore is renowned for its highly established ecosystem, encompassing a thorough regulatory framework and proactive best practices, thus setting a notable benchmark. Malaysia progressively enhances its cybersecurity capabilities by engaging in collabourative initiatives and undertaking capacity-building endeavors. The Philippines significantly emphasizes improving its cybersecurity measures and regulatory framework while prioritizing public awareness and fostering international cooperation. These nations collectively exemplify the significance of flexible cybersecurity measures in protecting vital infrastructure, data, and national security within a constantly evolving digital environment.

Chapter 5. Conclusion and Recommendation

Developing a comprehensive cybersecurity framework holds the utmost importance for the maritime industry in the Philippines. The Philippines lacks comprehensive cybersecurity measures explicitly tailored to the maritime industry, considering the various government agencies and business stakeholders involved. However, the government is actively working on a comprehensive plan to establish the requisite measures for this framework.

To further strengthen cybersecurity, it is highly recommended to establish a maritime cybersecurity agency within either the Department of Transportation or the Philippine Coast Guard. A dedicated Information Sharing and Analysis Center (ISAC) should also be established, focusing solely on maritime matters, similar to the one in the United States of America. Moreover, developing a comprehensive national strategy that involves a strong commitment and systematic coordination and collabouration from political authorities to enforce relevant legal frameworks effectively is crucial. Establishing partnerships with key governmental maritime entities and relevant stakeholders is also critical in promoting a culture of cybersecurity awareness. This can be achieved through various means, such as training programs, facility modernization, and adopting best practices observed in other countries and international organizations. Above all, the primary objective is to enhance knowledge regarding cybersecurity through a holistic approach and to ensure the safety and security of the Philippine maritime sector through cyber resiliency.

For a more thorough exploration of the subject at hand, it is suggested that future researchers concentrate on the status of the vital information and communication technology (ICT) infrastructure within the maritime industry of the Philippines. Additionally, it would be beneficial to draft a policy regarding assessing the proficiency of cybersecurity specialists in this field. Moreover, a policy on the strict reporting system of any cybersecurity incident should be introduced to monitor the status and the severity of cyberattacks to be able to mitigate and prevent such their impact.

References

American Bureau of Shipping. (n.d.). ABS CyberSafety® Program. Retrieved September 12, 2023, from https://ww2.eagle.org/en/Products-and-Services/cyber/abs-cybersafety.html

Anti-Cybercrime Group. (2023). Cybercrime Threat Landscape in the Philippines. Anti-Cybercrime Group, National Headquarters, Philippine National Police. https://acg.pnp.gov.ph/main/about-us/20-publications/42-cybercrime-threat-landscape-in-the-philippines.html

Anti-Cybercrime Group. (2018a). 73 Chinese Nabbed for Telecom Fraud to be Deported. https://acg.pnp.gov.ph/main/press-releases/245-73-chinese-nabbed-for-telecom-fraud-to-be-deported.html

Anti-Cybercrime Group. (2018b). PNP-ACG Nets 151 Chinese Nationals Linked to Telecom Fraud. https://acg.pnp.gov.ph/main/press-releases/243-pnp-acg-nets-151-chinese-nationals-linked-to-telecom-fraud.html

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

APCERT. (n.d.). Asia Pacific Computer Emergency Response Team. Retrieved September 14, 2023, from https://www.apcert.org/

Assembly, T. G. (1969). General Assembly. *International Organization*, *23*(2), 363–557. https://doi.org/10.1017/s0020818300031660

ASEAN Regional Forum. (2022). ASEAN Regional Forum Annual Security Outlook 2022. 151-153. https://aseanregionalforum.asean.org/librarycat/arf-annual-security-outlook-2022/

ASEAN Regional Forum. (2022). ASEAN Regional Forum Annual Security Outlook 2022. 188–189. https://aseanregionalforum.asean.org/librarycat/arf-annual-security-outlook-2022/

Baker, J., Bakhsh, N., Bush, D., Chen, X., Clayton, R., Diakun, B., Lowry, Ni., Osler, D., Porter, J., Sharpe, A., Shen, C., Watkins, E., Bockmann, M. W., Williams, F., & Willmington, R. (2022). A Special Report: Cybersecurity. Lloyd's List Intelligence, 1–28. https://doi.org/10.1057/978-1-137-53675-4_9

BIMCO. (n.d.). About Us and Our Members. Retrieved August 8, 2023, from https://www.bimco.org/about-us-and-our-members

BIMCO. (2021). The Guidelines on Cybersecurity Onboard Ships. *International Chamber Shipping of Shipping*, *4*, 1–53.https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Booth, A., Clowes, A. S. M., & St James, M. M. (2022). Systematic Approaches to a Successful Literature Review (A. Owen (Ed.); Third Edit). SAGE Publications Ltd.

Boyes, H., & Isbell, R. (2017). Code of Practice: Cybersecurity for Ships. In *IET Standards and Department for Transport*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

Cabral, A. R. (2022). Cybercrime Rate in the UK was higher last year than in other developed nations. The National. https://www.thenationalnews.com/business/technology/2022/05/08/cyber-crime-rate-in-the-uk-higher-last-year-than-in-other-developed-nations/

Cambridge Dictionary. (n.d.). Retrieved April 18, 2023, from https://dictionary.cambridge.org/dictionary/english/effectiveness

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021). Assessing the Effectiveness of Cybersecurity Training and Raising Awareness Within the Maritime Domain. INTED2021 Proceedings, 1(March), 3489–3499. https://doi.org/10.21125/inted.2021.0726

Charles Sturt University. (2023). Literature Review: Traditional or Narrative Literature Reviews. https://libguides.csu.edu.au/review/Traditional#:~:text=A%20narrative%20or%20traditional%20literature,or%20context%20for%20your%20research

Chew, T. S. (2023). Considerations for Developing Cybersecurity Awareness Training. ISACA Journal, 2, 1–3. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training

CISA. (2022). People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a

CISCO. (2023). What is Malware? CISCO. https://www.cisco.com/site/us/en/products/security/what-is-malware.html

Computer Security Resource Center. (n.d.). Retrieved April 20, 2023, from National Institute of Standards and Technology US Department of Commerce: https://csrc.nist.gov/glossary/term/cybersecurity

Communications and Multimedia Act 1998. (2004). Laws of Malaysia Act 588: Communications and Multimedia Commission Act 1998. https://www.mcmc.gov.my/en/legal/acts

Congress of the Philippines. (n.d.). Republic Act No. 4200. The LAWPHiL Project. Retrieved August 21, 2023, from https://lawphil.net/statutes/repacts/ra1965/ra_4200_1965.html

Congress of the Philippines. (2012). *Cybercrime Prevention Act of 2012*. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Congress of the Philippines. (2000). Republic Act No. 8792. Official Gazette. https://www.officialgazette.gov.ph/2000/06/14/republic-act-no-8792-s-2000/

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

Council of Europe. (2001). *The Budapest Convention (ETS No. 185) and its Protocol*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

CyberPeace Institute. (2022). Cyber Peace and the UN SDGs. https://cyberpeaceinstitute.org/news/cyber-peace-and-the-un-sdgs/

Cyber Risk GmbH. (n.d.). *Cybersecurity for the Maritime Industry*. Retrieved June 27, 2023, from https://www.maritime-cybersecurity.com/#:~:text=Identifying%20and%20evaluating%20key%20ship,vulnerabilities%2C%20and%20operational%20data%20in

Cybersecurity Act. (n.d.). Retrieved April 20, 2023, from https://www.csa.gov.sg/legislation/Cybersecurity-Act

Cybersecurity Agency Singapore. (2022a). Our Identity. CSA Singapore. https://www.csa.gov.sg/Explore/who-we-are/our-identity

Cybersecurity Agency Singapore. (2022b). Singapore Cyber Landscape 2022. Urban Forest Design Pte Ltd. https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022

Cybersecurity Agency Singapore. (2022b). What is Singapore Doing for a Trusted, Resilient, and Safer Cyberspace? In Singapore Cyber Landscape 2022 (pp. 34–83). Urban Forest Design Pte Ltd. https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022

Cybersecurity & Infrastructure Security Agency. (n.d.). About CISA. America's Cyber Defense Agency. Retrieved August 8, 2023, from https://www.cisa.gov/about

Department of Information and Communication Technology. (2023). DICT seeks the public's input on the draft National Cybersecurity Plan 2023-2028. https://dict.gov.ph/dict-seeks-publics-inputs-on-draft-national-cybersecurity-strategy-2023-2028/

Department of Information and Communication Technology. (2017). National Cybersecurity Plan 2022. https://dict.gov.ph/national-cybersecurity-plan-2022/

DNV. (2022). IACS Unified Requirements for Cybersecurity is mandatory from January 1, 2024. DND Technical and Regulatory News, No.17/2022. https://www.dnv.com/news/iacs-unified-requirements-for-cyber-security-mandatory-from-1-january-2024-227429

DNV. (2023). Maritime Cyber Priority 2023: Staying secure in an era of connectivity - DNV. DNV. https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.htmln

Efficient Definition & Meaning - Merriam-Webster. (n.d.). Retrieved April 18, 2023, from https://www.merriam-webster.com/dictionary/efficient

Elgan, M. (2021). Maritime Cybersecurity: A Rising Tide Lifts all Boats. Security Intelligence. https://securityintelligence.com/articles/maritime-cybersecurity-rising-tide/

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

European Union Agency for Cybersecurity. (2005). About ENISA-The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/about-enisa

Federal Information Security Modernization Act | CISA. (n.d.). Retrieved April 20, 2023, from https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

Fenwick, S. (2022). Cyberattacks on Port of Los Angeles have doubled since the pandemic. BBC News. https://www.bbc.com/news/business-62260272

Fortinet. (2023). Supply Chain Attacks: Examples and Countermeasures. Fortinet, Inc. https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks

Global Policy Forum. (1999). NGOs and the United Nations. GPF. https://archive.globalpolicy.org/component/content/article/176-general/31440-ngos-and-the-united-nations.html#2

Government of Malaysia. (2010). Personal Data Protection Act 2010. https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en

Hashim, M. S. B. (2011). Malaysia's national cybersecurity policy: The country's cyber defense initiatives. 2011 2nd Worldwide Cybersecurity Summit, WCS 2011.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) | *CDC*. (n.d.). Retrieved April 20, 2023, from https://www.cdc.gov/phlp/publications/topic/hipaa.html

IACS. (n.d.). About International Association of Classification Societies. Retrieved August 8, 2023, from https://iacs.org.uk/about/

IBM. (2023). What is Ransomware? IBM. https://www.ibm.com/topics/ransomware

Ichimura, Y., Dalaklis, D., Kitada, M., & Christodoulou, A. (2022). Shipping in the era of digitalization: Mapping the future strategic plans of major maritime commercial actors. Digital Business, 2(1), 100022. https://doi.org/10.1016/j.digbus.2022.100022

IMO. (n.d.). Relations with Observer Organizations. Retrieved September 18, 2023, from https://www.imo.org/en/OurWork/ERO/Pages/Relations-with-Observer-Organizations.aspx

IMO. (2017). Guidelines on Cyber Risk Management. *Imo*, *MSC-FAL*(1/Circ.3),1–6. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-GuidelinesOnMaritimeCyberRiskManagement(Secretariat).pdf

IMO. (2019). Rules and Guidelines for Consultative Status of Non-Governmental International Organizations with the IMO. December. https://www.imo.org/en/OurWork/ERO/Pages/Relations-with-Observer-Organizations.aspx

International Association of Classification Societies (IACS). (n.d.).Cybersecurity in the Maritime Industry. https://www.iacs.org.uk/our-work/cyber-security-in-the-maritime-industry/

Information Fusion Center. (2022). IFC ANNUAL REPORT 2022. https://www.ifc.org.sg/ifc2web/app_pages/User/commonv2/pubsProductsFiles.cshtml?parent=2022&prevParent=Annual%20Report

International Maritime Organization - IMO. (2017). Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems. Web Site IMO, 428(June 2017), 2017. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

International Chambers of Shipping. (n.d.). About ICS. Retrieved August 8, 2023, from https://www.ics-shipping.org/about-ics/

International Maritime Organization. (n.d.). Brief History of IMO. Retrieved August 9, 2023, from https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx

ISO/IEC JTC 1/SC 27 - Information security, cybersecurity, and privacy protection. (n.d.). Retrieved April 20, 2023, from https://www.iso.org/committee/45306.html

International Telecommunication Union (ITU). (n.d.). ITU Committed to Connecting the World. Retrieved July 28, 2023, from https://www.itu.int/en/about/Pages/default.aspx

ITU. (2021). Digital Technologies to Achieve the UN SDGs. ITU Committed to Connecting the World. https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx

Kaspersky. (2023). What are Spoofing-Definition and Explanation? AO Kaspersky Lab. https://www.kaspersky.com/resource-center/definitions/spoofing

Kessler, G. C., & Shepard, S. D. (2022a). ATT&CK and D3FEND Frameworks. In *Maritime Cybersecurity - A Guide for Leaders and Managers* (2nd ed., pp. 56–57). Amazon Distribution GmbH, Leipzig.

Kessler, G. C., & Shepard, S. D. (2022b). NIST Cybersecurity Framework. In *Maritime Cybersecurity - A Guide for Leaders and Managers* (2nd ed., pp. 58–59). Amazon Distribution GmbH, Leipzig.

Kessler, G. C., & Shepard, S. D. (2022c). NIST NICE Framework. In *Maritime Cybersecurity - A Guide for Leaders and Managers* (2nd ed., pp. 60–62). Amazon Distribution GmbH, Leipzig.

Kessler, G. C., & Shepard, S. D. (2022d). Policy and Procedure Framework Documents. In *Maritime Cybersecurity - A Guide for Leaders and Managers* (2nd ed., p. 198). Amazon Distribution GmbH, Leipzig.

Lloyd's Register and University of Cambridge Centre for Risk Studies. (2017). Cyber risk in the maritime industry. https://www.lloydsregister.com/en/insights/industry-trends/shipping/cyber-risk-in-the-maritime-industry

Loomis, W., Singh, V. V., Kessler, G. C., Bellekens, X., & Atlantic Council of the United States. (2021). Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity. https://www.atlanticcouncil.org/in-depth-research-

reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/

Mednikarov, B., Tsonev, Y., & Lazarov, A. (2020). Analysis of Cybersecurity Issues in the Maritime Industry. *Information & Security: An International Journal*, *47*(1), 27–43. https://doi.org/10.11610/isij.4702

Mengist, W., Soromessa, T., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. MethodsX, 7, 100777. https://doi.org/10.1016/j.mex.2019.100777

Microsoft Security. (n.d.). What is Phishing? Microsoft. Retrieved July 5, 2023, from https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing

MITRE. (n.d.). MITRE|ATT&CK. Retrieved September 12, 2023, from https://attack.mitre.org/versions/v13/

Mission Secure. (2020). A Comprehensive Guide to Maritime Cybersecurity. Mission Secure. https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach?utm_term=%2Bmaritime%2Bcybersecurity&utm_campaign=Maritime+Cyber+Security&utm_source=adwords&utm_medium=ppc&hsa_acc=9936888968&hsa_cam=11247064448&hsa_grp=115882845

Mraković, I., & Vojinović, R. (2019). Maritime cybersecurity analysis – How to reduce threats? Transactions on Maritime Science, 8(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

MS-ISAC. (2022). Understanding and Responding to Distributed Denial of Service Attacks. Cybersecurity Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Medical Research Methodology, 18(1), 1–8. https://doi.org/10.1186/s12874-018-0611-x

MyCERT. (n.d.). MyCert-Who We Are. Cybersecurity Malaysia. Retrieved September 14, 2023, from https://www.mycert.org.my/portal/full?id=d8032294-04b2-4ba0-9e46-62c898bb4983

NACSA. (2023). National Security Council's Directive No. 26. National Cybersecurity Agency (NACSA). https://www.nacsa.gov.my/directive26.php

National Cybersecurity Index. (2022). Upgrading National Cyber Resilience. E-Government Academy. https://ega.ee/publication/updating-national-cyber-resilience/

National Cybersecurity R&D Lab. (n.d.). About NCL. Retrieved September 16, 2023, from https://ncl.sg/about

National Security Council. (2020). Malaysia: Cybersecurity Strategy 2020-2024. https://rakyatandrights.my/paper/malaysia-cyber-security-strategy-2020-2024/

Newman, L. H. (2022). The Worst Hacks and Breaches of 2022. WIRED. https://www.wired.com/story/worst-hacks-breaches-2022/

Nicaise, V. (2022). Cybermaretique: a short history of cyberattacks against the port. Stormshield. https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/

NIST. (n.d.). Control Effectiveness. Information Technology Labouratory Computer Security Resource Center. Retrieved July 11, 2023, from https://csrc.nist.gov/glossary/term/control_effectiveness?fbclid=IwAR3xDMYVQfSbwUlyCjVf9VduX6cKVENV2GAoopLycP1TKu0R7xr0Fi6lqM0

NIST. (n.d.). CYBERSECURITY. National Institute of Standards and Technology. Retrieved July 13, 2023, from https://www.nist.gov/cybersecurity

NIST. (n.d.). National Initiative for Cybersecurity Education (NICE). Retrieved September 12, 2023, from https://www.nist.gov/itl/applied-cybersecurity/nice

NIST Cybersecurity Framework Team. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nobles, C. (2019). Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity. Midwest (MWAIS) 2019 Proceedings, December 1–6. https://www.researchgate.net/publication/346962076_Establishing_Human_Factors_Programs_to_Mitigate_Blind_Spots_in_Cybersecurity_Establishing_Human_Factors_Programs_to_Mitigate_Blind_Spots_in_Cybersecurity

Novet, J. (2017). Shipping company Maersk says the June cyberattack could cost is up to $300 million. CNBC. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

North Atlantic Treaty Organization. (n.d.). What is NATO? Retrieved August 9, 2023, from https://www.nato.int/nato-welcome/index.html

NTT. (2020). 2020 Global Network Insights Report. https://services.global.ntt/en-us/insights/2020-global-network-insights-report?utm_source=NetworkingReport2020&utm_medium=PressRelease&utm_campaign=NetworkingReport2020&utm_term=&utm_content=Campaignlandingpage&campaignID=7014G000001n2rG&utm_SFDC_Offer=

Ocampo, Y. (2022). Singapore Establishes ASEAN Regional Computer Emergency Response Team. OpenGov ASIA. https://opengovasia.com/singapore-establishes-asean-regional-computer-emergency-response-team/

Onwuegbuzie, A. J., & Frels, R. (2016). 7 Steps to a Comprehensive Literature Review: A Multimodal and Cultural Approach. Sage Publication.

Otoom, A. F., Eleisah, W., Abdallah, E. E., Otoom, A. F., Eleisah, W., & Abdallah, E. E. (2023). Deep Learning for Accurate Detection Networks of Brute Force Attacks on IoT Networks. Procedia Computer Science, 220, 291–298. https://doi.org/10.1016/j.procs.2023.03.038

Panda Security. (2022). What is a Man-in-the-Middle (MITM) Attack? Definition and Prevention. Panda Media Center. https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/

Philippine Coast Guard. (2019). Philippine Coast Guard Cybersecurity Policy. PCG.

Philippine Port Authority. (2023). PPA ICT Security Policy. PPA.

Progoulakis, I., Nikitakos, N., & Dalaklis, D. (2023). Digitalization and Cyber-Physical Security Aspects in Maritime Transportation and Port Infrastructure. Springer International Publishing. https://doi.org/10.1007/978-3-031-25296-9

Rattray, G. J. (2001). Strategic Warfare in Cyberspace. The MIT Press.

Republic Act No. 10175 | Official Gazette of the Republic of the Philippines. (n.d.). Retrieved April 24, 2023, from https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Republic of Singapore. (2018). Singapore Cybersecurity Act. 9, 1–75. https://sso.agc.gov.sg/Acts-Supp/9-2018/

Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare (First). Cambridge University Press, New York.

Sead Fadilpašić. (2022). The maker of Axie Infinity just suffered one of the largest heists in crypto history. In Techradar Pro. https://www.techradar.com/news/the-maker-of-axie-infinity-just-suffered-one-of-the-largest-heists-in-crypto-history

Shead, S. (2022). Hackers can bring ships and planes to a grinding halt. And it could become much more common. CNBC. https://www.cnbc.com/2022/06/27/hackers-can-now-bring-cargo-ships-and-planes-to-a-grinding-halt.html

Shen, C. (2018). Cosco Shipping Targeted in Ransomware Attack. Llyod's List. https://lloydslist.maritimeintelligence.informa.com/LL1123581/Cosco-

Shipping-targeted-in-ransomware-attack?vid=Maritime&processId=d905e2e8-4da4-475f-b4c1-4af229860553

Singer, J. (2021). D3FEND Knowledge Graph Guides Security Architects to Design Better Cyber Defenses. MITRE News & Insights. https://www.mitre.org/news-insights/impact-story/d3fend-knowledge-graph-guides-security-architects-design-better-cyber

Sy, G. (n.d.). Short History of the Development of Cybercrime. https://www.scribd.com/document/475544325/Short-History-of-the-Dvlpt-of-Cybercrime#

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*(2022), 483–487. https://doi.org/10.1016/j.procs.2022.12.050

The Editorial Team. (2022). IACS: New Requirements on Cyber Safety. SAFETY4SEA. https://safety4sea.com/iacs-new-requirements-on-cyber-safety/

The Law Revision Commission. (n.d.). Personal Data Protection Act 2012. Retrieved September 16, 2023, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

The NATO CCDCOE. (n.d.). The Tallinn Manual. Retrieved September 16, 2023, from https://ccdcoe.org/research/tallinn-manual/

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2(3), 573–586. https://doi.org/10.3390/jcp2030029

Types of Cyber Threat in 2022 | IT Governance UK (2023). https://www.itgovernance.co.uk/cyber-threats

USCG. (2023). Maritime Cybersecurity Assessment and Annex Guide (MCAAG). January. https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

Vanguard. (2020). Maritime Cyberattacks Increase by 900% in Three Years. Vanguard. https://www.vanguardngr.com/2020/07/maritime-cyberattacks-increase-by-900-in-three-years/

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. IEEE Access, 8, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

WEF. (2022). The Global Risks Report 2022. 17th Edition. In World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Wingrove, M. (2017). Maersk Attack: Wake up Shipowners to the Cyber Threats. Riviera. https://www.rivieramm.com/news-content-hub/news-content-hub/maersk-attack-wake-up-shipowners-to-the-cyber-threats-28013

Wolford, B. (2023). *What is GDPR, the EU's new data protection law?* GDPR.EU. https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

World Economic Forum. (2021). These are the top cybersecurity challenges of 2021. The Weekly Agenda. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

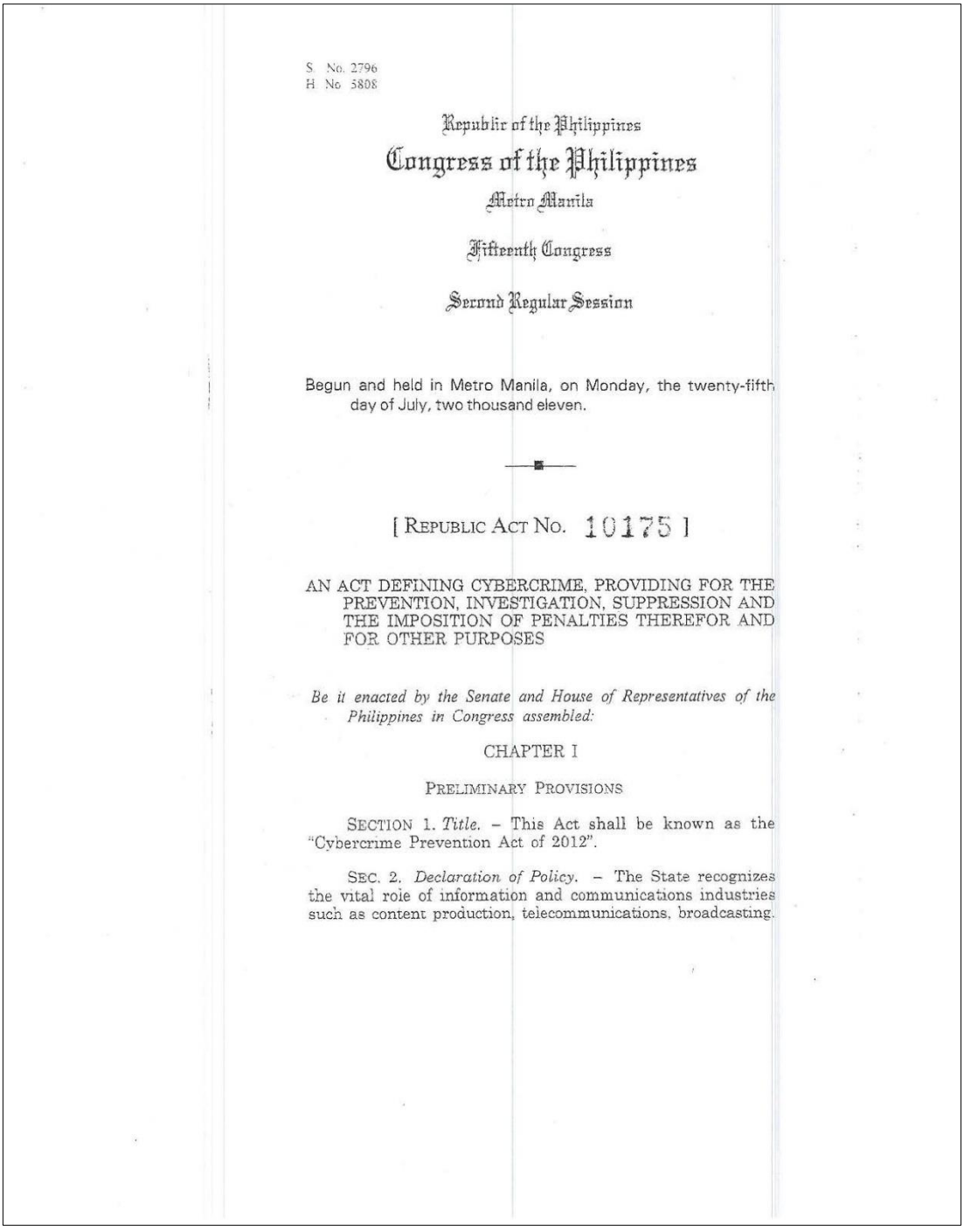
World Shipping Council. (n.d.). Shipping Regulation. Retrieved September 18, 2023, from https://www.worldshipping.org/shipping-regulation

Yates, S. (2016). National Critical Infrastructure Policy: Background and Select Cybersecurity Issues. Nova Science Publishers, Inc.

Appendices

A. RA 10175 (Cybersecurity Prevention Act of 2012)
B. Philippine Coast Guard Cybersecurity Policy

A. RA 10175 (Cybersecurity Prevention Act of 2012)



S. No. 2796
H. No. 5808

Republic of the Philippines
Congress of the Philippines
Metro Manila

Fifteenth Congress

Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10175]

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I

PRELIMINARY PROVISIONS

SECTION 1. *Title.* – This Act shall be known as the "Cybercrime Prevention Act of 2012".

SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting.

electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

SEC. 3. *Definition of Terms.* – For purposes of this Act, the following terms are hereby defined as follows:

(a) *Access* refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.

(b) *Alteration* refers to the modification or change, in form or substance, of an existing computer data or program.

(c) *Communication* refers to the transmission of information through ICT media, including voice, video and other forms of data.

(d) *Computer* refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.

(e) *Computer data* refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

(f) *Computer program* refers to a set of instructions executed by the computer to achieve intended results.

(g) *Computer system* refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media.

(h) *Without right* refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law.

(i) *Cyber* refers to a computer or a computer network, the electronic medium in which online communication takes place.

(j) *Critical infrastructure* refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

(k) *Cybersecurity* refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

(l) *Database* refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system.

(m) *Interception* refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

(n) *Service provider* refers to:

(1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

(o) *Subscriber's information* refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established:

(1) The type of communication service used, the technical provisions taken thereto and the period of service;

(2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and

(3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

(p) *Traffic data* or *non-content data* refers to any computer data other than the content of the communication including, but not limited to, the communication's origin,

destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II

PUNISHABLE ACTS

SEC. 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) Illegal Access. – The access to the whole or any part of a computer system without right.

(2) Illegal Interception. – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

(3) Data Interference. – The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

(4) System Interference. – The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(5) Misuse of Devices. –

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(6) Cyber-squatting. – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

(i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(iii) Acquired without right or with intellectual property interests in it.

(b) Computer-related Offenses:

(1) Computer-related Forgery. –

(i) The input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or

(ii) The act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

(2) Computer-related Fraud. – The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided*, That if no

damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided*, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(c) Content-related Offenses:

(1) Cybersex. – The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) Child Pornography. – The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: *Provided*, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

(3) Unsolicited Commercial Communications. – The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

(i) There is prior affirmative consent from the recipient; or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(4) Libel. – The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

SEC. 5. *Other Offenses.* – The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. – Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. – Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

SEC. 7. *Liability under Other Laws.* – A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

CHAPTER III

PENALTIES

SEC. 8. *Penalties.* – Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(1) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

SEC. 9. *Corporate Liability.* – When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power of representation of the juridical person provided

the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00).

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (PhP5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

CHAPTER IV

ENFORCEMENT AND IMPLEMENTATION

SEC. 10. *Law Enforcement Authorities.* – The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

SEC. 11. *Duties of Law Enforcement Authorities.* – To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

SEC. 12. *Real-Time Collection of Traffic Data.* – Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed; (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

SEC. 13. *Preservation of Computer Data.* – The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension for another six (6) months: *Provided*, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the

Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

SEC. 14. *Disclosure of Computer Data.* – Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

SEC. 15. *Search, Seizure and Examination of Computer Data.* – Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

(a) To secure a computer system or a computer data storage medium;

(b) To make and retain a copy of those computer data secured;

(c) To maintain the integrity of the relevant stored computer data;

(d) To conduct forensic analysis or examination of the computer data storage medium; and

(e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the

necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

SEC. 16. *Custody of Computer Data.* – All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

SEC. 17. *Destruction of Computer Data.* – Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination.

SEC. 18. *Exclusionary Rule.* – Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

SEC. 19. *Restricting or Blocking Access to Computer Data.* – When a computer data is *prima facie* found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

SEC. 20. *Noncompliance.* – Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of *prision correccional* in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.

CHAPTER V

JURISDICTION

SEC. 21. *Jurisdiction.* – The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

CHAPTER VI

INTERNATIONAL COOPERATION

SEC. 22. *General Principles Relating to International Cooperation.* – All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense shall be given full force and effect.

CHAPTER VII

COMPETENT AUTHORITIES

SEC. 23. *Department of Justice (DOJ).* – There is hereby created an Office of Cybercrime within the DOJ designated as the central authority in all matters related to international mutual assistance and extradition.

SEC. 24. *Cybercrime Investigation and Coordinating Center.* – There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, for policy coordination among concerned agencies and for the formulation and enforcement of the national cybersecurity plan.

SEC. 25. *Composition.* – The CICC shall be headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson with the Director of the NBI as Vice Chairperson; the Chief of the PNP; Head of the DOJ Office of Cybercrime; and one (1) representative from the private sector and academe, as members. The CICC shall be manned by a secretariat of selected existing personnel and representatives from the different participating agencies.

SEC. 26. *Powers and Functions.* – The CICC shall have the following powers and functions:

(a) To formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);

(b) To coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in this Act;

(c) To monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;

(d) To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;

(e) To coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other related projects;

(f) To recommend the enactment of appropriate laws, issuances, measures and policies;

(g) To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions; and

(h) To perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of this Act.

CHAPTER VIII

FINAL PROVISIONS

SEC. 27. *Appropriations.* – The amount of Fifty million pesos (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

SEC. 28. *Implementing Rules and Regulations.* – The ICTO-DOST, the DOJ and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act, for its effective implementation.

SEC. 29. *Separability Clause.* – If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 30. *Repealing Clause.* – All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly. Section 33(a) of Republic Act No. 8792 or the "Electronic Commerce Act" is hereby modified accordingly.

SEC. 31. *Effectivity.* – This Act shall take effect fifteen (15) days after the completion of its publication in the *Official Gazette* or in at least two (2) newspapers of general circulation.

Approved,

FELICIANO BELMONTE JR.
Speaker of the House of Representatives

JUAN PONCE ENRILE
President of the Senate

This Act which is a consolidation of Senate Bill No. 2796 and House Bill No. 5808 was finally passed by the Senate and the House of Representatives on June 5, 2012 and June 4, 2012, respectively.

MARILYN B. BARUA-YAP
Secretary General
House of Representatives

EMMA LIRIO-REYES
Secretary of the Senate

Approved: SEP 12 2012

BENIGNO S. AQUINO III
President of the Philippines

0

Office of the President of the Philippines
PNOY006250

B. PHILIPPINE COAST GUARD CYBERSECURITY POLICY

PAMBANSANG PUNONGHIMPILAN TANOD BAYBAYIN NG PILIPINAS
(National Headquarters Philippine Coast Guard)
139 25th Street, Port Area,
1018 Manila

NHQ-PCG/CG-11 07 October 2019

CIRCULAR
NUMBER 11-19

PHILIPPINE COAST GUARD CYBERSECURITY POLICY

I. REFERENCES:

a. PCG Regulations G200 – 001, (Security of classified matters) Dated 23 Sept 2002.

b. GHQ Letter directive Nr 287 dated 30 August 2013, Subj; Adopting cyberspace as one of the domains of AFP Operations.

c. CEIS Directive 2012-001, Subj: PN Standard LAN and network security.

d. National Cyber Security Plan 2022.

e. ISO 27002, Code of Practice for information Security Controls.

f. Certificated Information Systems Security Professional V1.1

g. NHQ-PCG/CG11 Standard Operating Procedures (SOP) Nr.: 05-19 (Utilization of PCG Provided Email Services).

h. NHQ-PCG/CG11 Standard Operating Procedures (SOP) Nr.: 09-19 (Utilization of issued PCG Mobile / Cellular Phones

i. Executive Order No. 189, s. 2015 – Creating The National Cybersecurity Inter-agency Committee

j. United States Coast Guard Cyber Strategy

II. PURPOSE:

The purpose of this policy is to govern set of principles, provide rules and higher guidance by which PCG organic personnel, civilian employees, third party stakeholder who are given access to the PCG Information infrastructures (infostructure) assets must abide, inform their obligatory requirements, limitations, privileges and responsibilities.

This publication shall serve as covenant and basis for the issuance of specific policies procedures, and guidelines to efficiently and effectively implement cyber

1

security best practices and norms. This will provide directions and strategic priorities; framework enablers; promote confidence for both interagency and regional collaborations; and develop and leverage a diverse set of cyber capabilities and authorities.

Finally, this will provide a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions in attaining PCG mandated functions

III. SCOPE:

This policy provides guidance to administrators, maintainers, operation, and third-party stakeholder of the PCG C4IS infostructure for effective administration, operations, maintenance, and security of C4IS system.

IV. DEFINITION OF TERMS:

a. **Administrator** - Refers to the person responsible for managing the PCG network. The responsibilities of the administrator typically include installing and upgrading software; and backup and recovery tasks.

b. **Baseline Configuration –** is a fixed reference in the development cycle or an agreed-upon specification of a system at a point in time. It serves as a documented basis for defining incremental change and encompasses many different aspects of the system. It is the center of an effective configuration management program whose purpose is to give a definite basis for change control in a project controlling various configuration items like work, system performance and other measurable configuration, basically, it is a defined specification that is considered as the baseline for all changes that follow.

c. **Bring Your Own Device (BYOD) –** portable computing device – such as smartphones, laptops ad table – brought by personnel to the workplace for use and connectivity to the PCG network.

d. **Closed Network (Red network) –** Also known as the PCG RED network, this refers to the PCG internet makes use of the Virtual Private Network (VPN). It is a closed and secured network, and not accessible via internet. This shall be primarily used for internal communications and mission-critical information system of the organization.

e. **Confidential/Restricted (CONRES)** – Term used for the categorization of electronic document, computer system, service, storage, and mobile devices contained or stored with confidential or restricted information.

f. **Controlled Open Public Network (Network) –** also known as the PCG Network (Gray Network), the network that is open to the internet. It is an open and public yet a secured network. This shall be used for internet browsing and internet-facing applications such as

the PCG website and the PCG collaboration suite (PCGCS), or PCG Emails System.

g. **Cyberspace** – used to described the virtual world of computers

h. **Cybersecurity** – refers to the collection of tools, policies, risk management, approaches, actions, trainings, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

i. **C4IS Infrastructure** - refers to command, control, communications, computer, intelligence, surveillance, target acquisition, and reconnaissance systems equipment and services.

j. **Domain Service** – in active domain services (AD DS), it is a server role in active directory that allows admin to manage and store information about resources from a network, as well as application data, in a distributed database.

k. **End User** – refers to all sailors, marines and employees, guest, and contractors who use computer and other electronic device to access PCG ICT infrastructures and to accomplish assigned task or functions.

l. **Guest Mobile Phone** – personal mobile devices that are installed with either customized applications or confidential, restricted, and unclassified information within the PCG organization, other units, government agencies, and third-party stakeholders.

m. **Guest Network** – a separate non-secured network provided by the PCG to visitors, guest, and end users requiring limited internet access only.

n. **Information infrastructures (infostructures)** – refers to the communications networks and associated information systems that support operational and administrative activities of the PCG.

o. **Information Security Officer** - refers to appointed officer who assists the commanding officer in discharging his responsibilities of safeguarding classified information and material

p. **Infrastructure** – refers to the fundamental facilities and system serving a country, city, or area, including the services and facilities necessary for its economy to function

q. **Internet of things (IoT) Devices** – also something referred to as the Internet of Everything (IoE), consist of all the web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware. These devices can interact with humans to get instructions to set them up and access the data, but the devices also generate massive amounts of Internet traffic, including loads of data that can be used to make the devices useful, but can

also be mined for other purposes. All this new data, and the Internet accessible nature of the devices, raises both privacy and security concerns. Examples of this device are smart TV, air conditioning unit, refrigerator, electrical plug, locks, light, etc.

r. **PCG Collaboration Suite (PCGCS)** - it is an email platform installed in Network utilized by PCG units/offices for communicating unclassified information to other government agencies and third-party stakeholders.

s. **PCG Messenger System** - is the PCG customized application software developed for chat and file transfer used by PCG units and offices in daily official communications (future development).

t. **PCG RED network** - is described as PCG internet which uses Virtual Private Network (VPN) but at the same time accessible via internet.

u. **Regular Mobile Phone** - PCG issued managed mobile devices that are installed with either customized applications or authorized third party software used for communication and collaboration of confidential, restricted, and unclassified information within the PCG organization, other AFP units, government agencies, and third party stakeholders.

v. **Secured Email System** - it is an email platform installed in PCG Gray Network utilized by PCG units/offices for communicating confidential and restricted information to other AFP units and Uniformed Service.

w. **Secured Mobile Phone** - PCG issued secured and managed mobile devices that are installed with either customized applications or authorized third party software used for communication and collaboration of classified information within the PCG organization.

x. **Supervisory Control and Data Acquisition (SCADA)** – generally refers to vessel computer system that monitors and controls a process. In the case of the transmission and distribution elements not limited to the following systems: Ships Combat System, and Propulsion and Power Monitoring and Control System. SCADA will monitor substances, transformers and other electrical assets. SCADA systems are typically used to control geographically dispersed assets that are often scattered over thousands of square kilometers.

y. **Third Party Stakeholders** – refers to a person or company who may be indirectly involved but is not a principal party to an arrangement, contact, deal, lawsuit, or transaction.

z. **Untrusted Network** – A setting that is not secure and shows evidence of vulnerabilities such as public wifi, and networks other than categorized in this policy.

aa. **Workstations** – are computing devices directly connected to the PCG network/s, owned and managed by the PCG. The term can refer to desktop computers, and laptops.

bb. **Virtual Private Network (VPN) -** is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

V. POLICY:

The Philippine Coast Guard shall ensure the resiliency of its infrastructure and shall provide necessary safeguards to guarantee the confidentiality, integrity, and availability of digital information transmitted in the information infrastructure. It is therefore, the responsibility of the unit commanders to implement security controls in order to insure and maintain credible of the cyber security posture. Hence, the PCG shall adhere to basic function in cybersecurity, which are identify, detect, protect, respond, and recover.

In general, PCG shall implement classification and management of its critical ICT assets in order for the effective and efficient implementation of cybersecurity.

1) Network Management

PCG classifies and categorizes electronic document, computer system and storage media according to its utilization. The PCG shall employ domain services for effective management and administration computers, service and network devices. In order to standardize the development of information network, the PCG information network shall be categorized as closed (Red), Controlled Open Public (Gray), Demilitarized Zone (DMZ), and Guest Networks

a) Closed Network (Red Network)

i. Closed Network shall be properly monitored, protected, hardened, and secured with appropriate security systems and devices;

ii. Secret and CONRES computer and servers shall be connected in this type of network;

iii. Unclassified servers and computer are prohibited to be connected in this type of network;

iv. Top secret computer shall be prohibited to be connected in this type of network;

v. Guest computer are prohibited in this type of network

vi. All PCG mission critical information system shall utilize this type of network

vii. PCG shall develop, implement, secure and maintain email system for exchanging secret information in this type of network;

viii. PCG shall develop, implement, secure, and maintain email system for exchanging CONRES information in this type of network

ix. White listing of application, services, protocols and ports shall be implemented in this type of network;

x. Internet services shall be prohibited in this type of network, however point to point connectivity through internet shall be allowed provided it shall employ secured connectivity thru VPN tunneling;

xi. PCG closed network shall be physically separated from other type of network; and;

xii. Shall employ identification, authentication, authorization, and accountability (IAAA) system for the access to network resources.

b) Controlled Open Public Network (GRAY Network)

i. This type of network shall be properly monitored, protected, hardened, and secured with appropriate security system and devices;

ii. CONRES and Unclassified computer and servers may be connected in this type of network;

iii. Top secret computer shall be prohibited to be connected in this type of network;

iv. PCG shall employ email and collaboration systems for CONRES and unclassified communication;

v. PCG shall implement logical separation of networks;

vi. PCG Shall employ email and collaboration systems for CONRES and classified communications;

vii. PCG controlled open Public network shall be physically separated from the closed network, however it could be logically separated from guest network and demilitarization zone; and;

viii. Shall employ identification, authentication, authorization, and accountability (IAAA) system for the access to network resources.

c) Demilitarized Zone (DMZ)

i. This type of network shall be properly monitored, protected, hardened, and secured with appropriate security system and devices;

ii. PCG shall regulate and implement white listing of ports, protocols and services; and;

iii. All public facing service such as email, website, and customized services shall utilized this type of network;

d) Guest Network

i. This type of network shall be properly monitored, protected, hardened, and secured with appropriate security systems and devices;

ii. PCG shall regulate and implement white listing of ports, protocols and services;

iii. This type of network shall only be utilized by the guest of third party stakeholder;

iv. All computer not yet configured with baseline configuration shall utilize this type of network; and;

v. Top secret, secret, CONRES, and Unclassified computer are prohibited to be connected in this type of network.

vi. Network access must not exceed to more than three (3) hours;

2) Computer Management

PCG computer system shall be managed and configured in accordance to its purpose and use. The PCG shall implement policy that classify, monitor, audit, and secure all computer system in the infrastructure

a) Computer system with Top Secret electronic document shall be classified as Top Secret and shall be tagged as green;

b) Computer system with secret electronic documents shall be classified and shall be tagged with Red;

c) Computer system with confidential and restricted electronic documents shall be classified as confidential/restricted (CONRES) and shall be tagged with Blue;

d) Top secret computer shall be prohibited to be connected to any network;

e) Secret computer shall be connected to close Network;

f) Secret computer shall be prohibited to be connected to Controlled open public network;

g) CONRES computer shall be connected either in closed network or controlled open network;

h) Unclassified computer shall be connected only to controlled open public network;

i) Unclassified computer shall be prohibited to be connected to closed network;

j) Computer system with unclassified electronic documents shall be classified as unclassified and shall tagged with Gray;

k) All computers shall be managed and administered by CGWCEISC;

l) All computers shall be properly configured with baseline configuration prior issuance to the end-user

m) All servers shall be configured with baseline configuration prior its deployment;

n). Baseline configuration shall be determined, configured, and implementation by CGWCEISC only;

o) CGWCEISC shall employ identification, authentication, authorization, and accountability (IAAA) system for the access to network resources;

p) All servers and computer shall be employed with protocol and services white listing;

q) Servers and computer shall be monitored, accounted, configured, and administered property and securely; and;

r) Servicing of servers and computers outside of PCG premises shall be prohibited unless authorized by Unit commanders

s) Usage of counterfeit software or Operating System is prohibited

t) All computers must undergo cleaning procedure prior connecting to the network

3) Storage Management

PCG storage system shall be managed and configured in accordance to its purpose and use. The PCG shall implement policy that classify, monitory, audit, network, and secure all storage system in the infrastructure.

a) Storage system stored with top secrete electronic documents shall be classified as top secret and tagged with Green;

b) Top Secret storage system shall be prohibited to be connected to any networks or to a computer system other than top secret;

c) Storage system stored with secret electronic documents shall be classified as secret and tagged with Red;

d) Secret storage system shall be connected to closed network;

e) Secret storage system shall be prohibited to connect to controlled Open Public Network;

f) Storage system storage with confidential/Restricted electronics document shall be classified as CONRES and tagged with Blue;

g) CONRES storage system shall be connected to closed and controlled open public networks;

h) Remote access to the CONRES storage system shall employ encryption protocols such as VPN tunneling;

i) Storage system stored with Unclassifie electronic documents shall be classified as unclassified and tagged with Gray;

j) Unclassified storage system shall be connected to controlled open public network;

k) Unclassified storage system shall be prohibited to be connected to closed network;

l) Network storage shall be the primarily media for storing electronic documents and it shall be properly secured and managed;

m) Network storage shall be managed and administered by CGWCEISC;

n) Network storage Back-up shall be conducted regularly;

o) Files and folder stored at network devices shall be shared to specific office and on need to know basis;

p) Top secret and CONRES computer shall prohibited the utilization of portable storage devices;

q) Secret documents shall be stored in secret network storage installed at PCG closed network;

r) Unclassified computer shall regulate the utilization of portable storage devices; and;

s) File extension white listing and storage quota shall be implemented;

t) Storage system must be protected by Anti-Malware and Anti-Virus service/s or any equivalent security protection.

4) Bring Your Own Devices (BYOD)

PCG shall implement security controls to the BYODs to maintain the confidentiality, integrity and availability of information stored in it;

a) All BYOD shall be regulated and registered, monitored, accounted and audited;

b) BYOD devices connected to PCG infrastructure that utilizes its services shall employ utmost security;

c) PCG shall employ mobile device management system;

d) BYOD shall maintain secure access to PCG infrastructure;

e) BYOD shall maintain visibility in the PCG networks;

f) BYOD shall be prohibited to be connected to closed network;

g) BYOD owners shall adhere to the PCG usage policies;

h) BYOD owner shall take full responsibility for the protection of their own device; and;

i) Intentional/Unintentional introduction of malware that may result to security breach caused by BYOD will constitute a punishable act under existing Philippine laws

j) All devices from end user shall undergo scanning prior connecting to the PCG network

5) Internet of Things Device (IoT) Device

a) All IoT shall be regulated, registered, monitored, accounted and audited;

b) PCG shall employ protection system to all IoT devices;

c) IoT devices firmware/operating system shall be regularly updated;

d) IoT shall be prohibited to be connected to PCG closed network;

e) PCG shall implement policy control that disable unwanted features;

f) PCG shall implement managed access to IoT data ;

g) PCG shall implement appropriate protection for all potential attack surface

h) PCG shall implement secure connectivity and encrypted data transmission

i) PCG shall restrict access to or control of the devices;

j) Owner of the IoT device shall take responsibility for the protection of their own device; and;

k) Intentional/Unintentional introduction of malware that resulted to security breach to PCG network through IoT constitute a Punishable act under existing Philippine laws.

6) Mobile Phone Management (Future Development)

a) Mobile phones issued to all PCG Units/Offices shall be managed and secure according to the following;

1) Secured Mobile Phone

i) Shall be issued to all PCG Units/Offices for communicating and collaborating classified (top secret/secret/confidential/restricted) information;

ii) Shall be used for communication and collaboration within the PCG. It shall be connected to PCG closed network through a secured connectivity by employing tunneling technology such as VPN;

iii) Internet use such as browsing and downloading of mobile applications shall be prohibited however, internet shall be used only as a medium of secured connectivity to PCG closed network via VPN tunneling

iv) Shall be installed with PCG customized application for mobile device and/or authorized third party mobile applications for voice and data communication;

v) Shall be manage by mobile management system installed at the PCG closed network and shall be accounted, audited, managed, and secured by PCGICT Personnel;

vi) Shall be employed with multi-factor authenticate system and all files and phonebooks can be remotely destructed/erased /formatted if the device will be lost; and;

vii) Shall be tagged as RED mobile device thru customized sticker and/or mobile background.

`2) Regular Mobile Phone

i) Shall be issued to all PCG Units/Offices for communicating and collaborating confidential, restricted and unclassified information; but not limited to coordination, monitoring, queries, assistance and rendering support to maritime stakeholders.

ii) Shall be used for communication and collaboration within the PCG, other AFP units, government agencies, and third party stakeholders. It shall be connected to PCG controlled Open Public Network however, it shall be managed through a mobile management system deployed in PCG Gray network;

iii) Shall be installed with PCG customized application for mobile devices and/or authorized third party mobile application for voice and data communication;

iv) Shall be accounted, audited, managed, and secured by PCGICT personnel. It shall be employed with multi-factor authentication system and all files and phonebooks can be remotely destructed/erased/formatted if the device will be lost, and,

v) Shall be tagged as GRAY mobile device thru customized sticker and/or mobile background.

3) Guest Mobile Phone

i. Shall only be allowed to be connected to the guest network and shall be monitored when connected to the PCG Gray network; and,

ii. Shall only be allowed to access Internet services

b) Mobile devices shall be monitored, accounted, configured, and administered properly and securely;

c) PCG shall employ Mobile Management System to effectively secure and manage all PCG issued mobile devices;

d) Classified information shall not be stored in mobile devices; and,

e) PCG shall ensure the proper disposal of mobile devices issued to PCG personnel.

7) SCADA SYSTEMS

a) PCG shall implement security controls for the SCADA Systems (Ships' Combat System, Propulsion Advance Bridge Management System, Mission management System and Power Monitoring and Control System) to maintain the confidentiality, integrity and availability of information stored in it;

b) All SCADA Systems shall be regulated, registered, monitored, accounted and audited;

c) PCG shall employ protection system to all SCADA Systems devices;

d) The mobile storage devices (USB flash Disk or External Hard Disk Drive) shall be prohibited from attaching to Computing devices in SCADA Systems unless authorized by the Unit Commander as necessary for the operation and upgrade of the system; and,

e) The SCADA Systems shall be physically separated from any networks.

8) Printers, Scanners, and Photocopying Machines

a) Printers, scanners, and photocopying machine shall be classified in accordance to the Computer Systems and networks attached to it;

b) Network printers and photocopying machines shall be monitored, audited, and secured properly;

c) Photocopying machines that store information shall properly checked and monitored;

d) All data stored in the rented photocopying machine shall be deleted/shredded;

e) Firmware updated shall be implemented to all printers, scanners and photocopying machines; and,

f) All printers, scanners, and photocopying machines shall be regulated, registered, monitored, accounted and audited.

9) Electronic Documents Management

Official electronic documents that reside in computer system, and stored in storage devices in the PCG network require protection. The electronic documents shall be categorized as Classified and Unclassified as provided in the PCG Regulations G200 – 001, ("Security of Classified Matters"). Classified documents are categorized as Top Secret, Secret, Confidential, and Restricted. PCG shall implement the following security controls to secure its electronic documents:

a) Top Secret shall be drafted in a computer system categorized as Top Secret;

b) Top Secret electronic documents shall be transmitted via courier as prescribed by existing policy on Security of Classified Matters;

c) Top Secret electronic documents shall be stored in an encrypted and isolated network or in a storage device employed with the highest encryption standards and physical security (e.g. vault);

d) Secret documents shall be drafted in a computer system categorized as Secret;

e) Secret electronic documents shall be transmitted over PCG Closed Network;

f) Secret electronic documents shall be stored in a storage device either it is networked or through removable storage and shall be employed with the highest encryption standard;

g) Secret electronic document shall be communicated through Red Network Email System or PCG Messenger System only;

h) Confidential documents shall be drafted in a computer system categorized as Confidential/Restricted (CONRES);

i) Confidential electronic documents shall be transmitted on both Closed and Controlled Open Public Network;

j) Confidential electronic document shall be stored in a storage device either networked or through removable storage and shall be employed with encryption;

k) Confidential electronic document shall be communicated either on Secured Email System or PCG Messenger System in Gray Network or Email System or PCG Messenger System in Red Network;

l) Restricted electronic documents shall be drafted in a computer system categorized as CONRES;

m) Restricted electronic documents shall be transmitted on both Closed and Controlled Open Public Network;

n) Restricted electronic documents shall be stored in a storage device either networked or through removable storage and shall be employed with encryption;

o) Restricted electronic document shall be communicated either on Secured Email System or PCG Messenger System in Gray Network or Email System or PCG Messenger System in Red Network;

p) Unclassified documents shall be drafted in a computer system categorized as Unclassified;

q) Unclassified electronic documents shall be transmitted on both Closed and Controlled Open Public Network;

r) Unclassified electronic documents shall be stored in a storage device either networked or through removable storage and do not need employment of encryption;

s) Philippine Coast Guard Collaboration Suite shall be used to communicate unclassified electronic documents with other government agencies, and commercial sectors;

t) Access to classified electronic documents shall be prohibited over un-trusted network;

u) Remote access of CONRES electronic documents shall employ appropriate security schemes such as Virtual Private Network (VPN; and,

v) All electronic document shall have an onsite and offsite backup and recovery system,

VI. GENERAL GUIDANCE

The following are general guidelines to ensure the cybersecurity posture of the PCG and maintaining information assurance in the PCG infrastructure. These guidelines were intentionally accepted cybersecurity standards published by the National Institute of Standard and Technologies (NIST) to address compliance of all layers of cybersecurity spectrum.

a) Asset Management

The data personnel, devices, system, and facilities that enable the PCG to achieve operation purposes are identified and manage consistent with their relative

important to PCG objectives and the organization's risk strategy. The PCG shall develop and implement following controls;

1) The PCG shall employ a system or means for an automated asset management where inventory of physical devices connected into the network can be monitored.

2) The PCG shall conduct regular inventory of all physical devices and systems;

3) The PCG shall conduct regular inventory of all software platforms and applications;

4) The PCG shall map network, communication and data flow;

5) The PCG shall audit all external and internal information system;

6) The PCG ICT resources shall be prioritized based on their classification, critically, and operational and administrative value; and;

7) The PCG shall establish cybersecurity roles responsibilities for the entire workforce and third-party stakeholders.

b) Operational and administrative Environment

The organization's mission, objective stakeholders, and activities should be understood and prioritized, and risk management decisions. Hence, PCG shall implement the following control;

1) The PCG shall identify and communicate the organization's role in the operation:

2) The PCG shall identify and communicate the organization's place in critical infrastructure and in the government sector;

3) The PCG shall establish and communicate the priorities for organizational mission, objectives, and activities;

4) The PCG shall establish dependencies and critical functions for delivery of critical service; and;

5) The PCG shall establish resilience requirements to support delivery of critical service

c) Governance

The policies, procedures, and processes to manage and monitor the organization`s regulatory, legal, risk, environmental, and operational requirements shall be understood and shall inform the management of cyber security risk. Hence, the PCG shall implement the following controls;

1) Organizational cyber security related policy shall be established;

2) Information security roles & responsibility shall be coordinated and aligned with internal roles and external partners;

3) Legal and regulatory requirement regarding cybersecurity, including privacy and civil liberties obligations, shall be understood and managed; and;

4) Governance and risk management processes shall address cybersecurity risk.

d). Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, function, image, or reputation), organizational assets, and individuals. Hence, the PCG shall implement the following controls;

1) The PCG shall conduct Cyber Risk Assessment (CRA) to determine the gap between industry standards and current unit cybersecurity posture.

2) The PCG shall adopt the NIST 20 Critical Security Controls as mentioned in the PCG cyber warfare Doctrine as the de facto yardstick by which the cybersecurity posture of a unit can be measured

3) The result of the CRA shall be the unit's basis for programming C4IS requirements;

4) The PCG shall identify asset vulnerabilities and property document it;

5) The PCG shall engage with local and international partners to maintain threat and vulnerability information through information sharing forums and sources;

6) All threats, boat internal and external, are identified and documented;

7) Potential operational and administrative impacts and likelihoods shall be promptly and properly identified;

8) Threats, vulnerabilities, likelihoods, and impacts shall be used to determine risk; and,

9) Risk responses shall be identified and prioritized.

e). Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions shall be established and used to support operational risk decisions. Hence, the PCG shall implement the following controls:

1) Risk management processes shall be established, managed, and agreed to by organizational stakeholders;

2) Organizational risk tolerance shall be determined and clearly expressed; and;

3) The organization's determination of risk tolerance shall be informed by its role in critical infrastructure and sector specific risk analysis.

f). Access Control

Access to assets and associated facilities is limited to authorized users, processes, device and to authorized activities and transactions. Hence, the PCG shall implement the following controls:

1) Identities and credentials shall be managed for authorized devices and users;

2) Physical access to assets shall be managed and protected;

3) Remote access shall be managed;

4) Access permission shall be managed and incorporating the principles of least privilege and separation of duties; and,

5) Network integrity shall be protected, incorporating network segregation where appropriate.

g). Awareness and Training

The organization`s personnel and partners shall be provided cybersecurity awareness education and shall be adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Hence, the PCG shall implement the following controls:

1) All PCG personnel shall be cybersecurity aware and trained;

2) All privileged users should understand their respective roles and responsibilities;

3) Third-party stakeholders (e.g., suppliers, customers, partners) should understand their respective role and responsibilities;

4) Staff and Unit Commanders shall understand roles and responsibilities;

5) Physical and information security personnel should understand their respective roles and responsibilities; and,

h). **Data Security**

Information and records (data) shall be managed consistent with the PCG risk strategy to protect the confidentiality, integrity, and availability of information. Hence, the PCG shall implement the following controls:

1) Data at rest shall be protected;

2) Data-in-transit shall be protected;

3) Assets shall formally be managed throughout removal, transfers, and disposition;

4) Adequate means to ensure confidentially, integrity, and availability of information shall be maintained;

5) Protections against data leaks shall be implemented;

6) Integrity checking mechanisms shall be used to verify software, firmware, and information integrity; and

7) The development and testing environment shall be separated from the production environment.

i). **Information Protection Processes and Procedures**

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures shall be maintained and used to manage protection of information systems and assets. Hence, the PCG shall implement the following controls;

1) Baseline configuration of information technology/industrial management system shall be created and maintained;

2) System development life cycle to manage systems shall be implemented;

3) Configuration change control processes shall be in place;

4) Backups and information shall be conducted, maintained, and tested periodically;

5) Policy and regulations regarding to physical operating environment for organizational assets shall be met;

6) Data shall be destroyed according to policy;

7) Protection processes shall be continuously improved;

8) Effectiveness of protection technologies shall be shared with appropriate parties;

9) Response plans (Incident Response and Business Continuity) and recovery plans (Incident Response and Disaster Continuity) shall be in place and managed;

10) Response and recovery plans shall be tested;

11) Cybersecurity shall be included in human resources practices (e.g., de-provisioning, personnel screening); and,

12) A vulnerable management plan shall be developed and implemented.

j). Maintenance

Maintenance and repairs of information system components shall be performed consistent with policies and procedures. Hence, the PCG shall implement the following controls:

1) Maintenance and repair of organizational assets shall be performed and logged in a timely manner, with approved and controlled tools; and,

2) Remote maintenance of PCG ICT assets shall be approved, logged, and performed in a manner that prevents unauthorized access.

k). Protective Technology

Technology security solutions shall be managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Hence, the PCG shall implement the following controls:

1) Audit/log records shall be determined, documented, implemented, and reviewed in accordance with policy;

2) Removable media shall be protected and its use restricted according to procedures and guidelines;

3) Access to systems and assets shall be controlled, incorporating the principle of least functionality; and;

4) Communications and control network shall be protected.

l). Anomalies and Events

Anomalous activity shall be detected in a timely manner and the potential impact of events shall be understood. Hence, the PCG shall implement the following controls:

1) A baseline of network operations and expected data flows for users and systems shall be established and managed;

2) Detected events shall be analyzed to understand attack targets and methods;

3) Event data shall be aggregated and correlated from multiple sources and sensors;

4) Impact of events shall be determined; and,

5) Incident alert thresholds shall be established.

m). Security Continuous Monitoring

The information system and assets shall be monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Hence, the PCG shall implement the following controls:

1) PCG information network shall be monitored to detect potential cybersecurity events;

2) The physical activity shall be monitored to detect potential cybersecurity events;

3) Personnel activity shall be monitored to detect potential cybersecurity events;

4) Malicious code shall be detected;

5) Unauthorized mobile code shall be detected;

6) External service provider activity shall be monitored to detect potential cybersecurity events;

7) Monitoring for unauthorized personnel, connections, devices, and software shall be performed; and,

8) Vulnerability scans shall be performed.

n). Detection Processes

Detection processes and procedures shall be maintained and tested to ensure timely and adequate awareness of anomalous events. Hence, the PCG shall implement the following controls:

1) Roles and responsibilities for detection shall be well defined to ensure accountability;

2) Detection activities comply with all applicable requirements;

3) Detection processes shall be tested;

4) Event detection information shall be communicated to appropriate parties; and,

5) Detection processes shall be continuously improved

o). Response Planning

Response processes and procedures shall be executed and maintained to ensure timely response to detected cybersecurity events. Hence, there will be a separate SOP for the PCG computer emergency team (PCG CERT).

p). Response Communication

Response activities shall be coordinated with internet and external stakeholders, as appropriate, to include external support law enforcement agencies. Hence, the PCG shall implemented the following controls:

1) Personnel should know their roles and order of operations when a response is needed;

2) Events shall be reported consistent with established procedures and guidelines;

3) Information shall be shared consistent with response plans;

4) Coordination with stakeholders shall occur consistent with response plans; and,

5) Voluntary information sharing shall occur with external stakeholders to achieve broader cybersecurity situational awareness.

q). Analysis

Analysis shall be conducted to ensure adequate response and support recovery activities. Hence, the PCG shall implement the following controls:

1) Notifications from detection systems shall be investigated;

2) The impact of the incident should be understood;

3) Forensics shall be performed; and,

4) Incidents shall be categorized consistent with response plans.

r). Mitigation

Activities shall be performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. Hence, the PCG shall implement the following:

1) Incidents shall be contained;

2) Incidents shall be mitigated; and,

3) Newly identified vulnerabilities shall be mitigated or documented as accepted risks.

s). Response Improvements

The PCG organizational response activities shall be improved by incorporating lessons learned from current and previous detection/response activities. Hence, the PCG shall implement the following controls:

1) Response plans shall incorporate lessons learned; and,

2) Response strategies shall regularly updated.

t). Business Continuity and Recovery Planning

Recovery processes and procedures shall be executed and maintained to ensure timely restoration and continuity of systems or assets affected by cybersecurity events. Hence, PCG shall execute recovery plan during or after an event. Hence, PCG shall execute recovery plan during or after an event.

u). Recovery Improvements

Recovery planning and processes shall be improved by incorporating lessons learned into future activities. Hence, the PCG shall implement the following controls:

1) Recovery plans shall incorporate lessons learned; and,
2) Recovery strategies shall be updated.

v). Recovery Communications

Restoration activities shall be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Hence, the PCG shall implement the following controls:

1) Public relations shall be managed;

2) Reputation after an event shall be repaired; and,

3) Recovery activities shall be communicated to internal stakeholders and executive and management teams.

VII. RESPONSIBILITIES:

a. Head of Offices and Commanders/Operational/Support Command and Units

1) Ensure all PCG personnel, civilian employees, Third Party Stakeholders, and guests adhere to the provisions of this policy;

2) Develop appropriate procedures on the operation ensure implementation of this policy;

3) Designate Document Security Officer;

4) Develop procedures and guidelines on the operations of systems implemented in this policy;

5) Coordinate with the DCS for MCWEIS, CG-11 on the formulation and review of this policy and other relevant cyber security policies;

6) Plan and program all activities pertaining to the implantation of this policy in the APB; and,

7) Investigate and recommend appropriate punishment on the violation of this policy.

b. Coast Guard Weapons, Communication, Electronics and Information System Command (CGWCEISC)

1) Tagging of the computers and establish procedures and guidelines for base-lining and white listing;

2) Develop plans, designs, milestone, and technical requirements of this policy to the PCG Cybersecurity Plan;

3) Develop plans, designs and technical and budgetary requirements of this policy to the Information System Strategic Plan;

4) Formulate appropriate procedures and guidelines on the installation, configuration, administration, and maintenance of all systems implemented in this policy; and,

5) UPR for the implementation and enforcement of this policy

c. Deputy Chief of Coast Guard Staff for Maritime Communication, Weapons, Electronics and Information System, CG-11

1) Ensure all PCG Personnel, civilian employees, and Third party stakeholders adhere to the provisions of this policy;

2) SPR for the supervision and monitoring of the implementation and enforcement of this policy;

3) Conduct annual inspection on PCG units compliance to this policy;

4) Conduct a regular review of this policy.

d. Deputy Chief of Coast Guard Staff for Intelligence, Security, and Law Enforcement, CG-2

1) Ensure all PCG personnel. civilian employees, and Third Party Stakeholder adhere to the provisions of the policy;

2) SPR for the conduct background investigation of the Third Party Stakeholders; and,

3) Coordinate with the DCS for MCWEIS, CG-11 on the formulation and view of this policy and other relevant cyber security policies.

e. The PCG Legal Service

1) Review and evaluate the legal context of this policy and other relevant cyber security policies in ensuring compliance to laws, statutory, and regulation; and,

2) Recommend sanctions to erring personnel based on existing national cyber-related laws.

VIII. ADMINISTRATIVE SANCTIONS:

PCG personnel and third party contractors who are found deliberately violating this policy shall be dealt with accordingly. Appropriate filing of case shall be pursued against individuals or those that contribute to the defilement or sabotage of PCG infostructure.

IX. EFFECTIVITY: This circular shall take effect upon publication

BY COMMAND OF ADM HERMOGINO PCG:

OFFICIAL:

EDUARDO D FABRICANTE
COMMO PCG
Chief of Coast Guard Staff

LIEZEL B BAUTISTA
CDR PCG 18 JAN 2019
Coast Guard Adjutant