MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

OAS | More rights for more people

MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

OAS | More rights for more people

COPYRIGHT (2021) Organization of American States.

Prepared and published by the Maritime and Port Security Program of the Inter-American Committee against Terrorism (CICTE).

The contents of this publication are presented exclusively for informational purposes and do not represent the official position of the Organization of American States, its General Secretariat, or its Member States.

This publication has been made possible thanks to the financial support of the Government of Canada.

We welcome your interest in this guide. Your feedback on how you have used this guide and whether it helped improved maritime cybersecurity incident response would be valuable information we can use to help design future projects.

Please contact CICTE's Maritime and Port Security Program at CICTE@oas.org to share your feedback.

OAS Cataloging-in-Publication Data

Maritime cybersecurity in the Western Hemisphere : an introduction and guidelines / [Prepared and published by the Maritime and Port Security Program of the Inter-American Committee against Terrorism (CICTE)].

v. ; cm. (OAS. Official records ; OEA/Ser.D/XXV.17)

ISBN 978-0-8270-7242-8

1. Computer security. 2. Security, International. 3. Transportation--Security measures. 4. Cyberterrorism. 5. Shipping--Security measures. 6. Harbors--Security measures. I. Inter-American Committee against Terrorism. II. OAS/CICTE Maritime and Port Security Program. III. Organization of American States. Secretariat for Multidimensional Security. IV. Series. OEA/Ser.D/XXV.17

CREDITS

Luis Almagro

Secretary General
Organization of American States (OAS)

Arthur Weintraub

Secretary for Multidimensional Security
Organization of American States (OAS)

Alison August Treppel

Executive Secretary
Inter-American Committee against Terrorism
Organization of American States (OAS)

Violanda Botet

Deputy Executive Secretary
Inter-American Committee against Terrorism
Organization of American States (OAS)

OAS Technical Team

OAS Maritime and Port Security Program

Lisbeth Laurie
Ricardo Desgarennes

OAS Cybersecurity Program

Kerry-Ann Barrett
Diego Subero
Sofia Hunter

Intern

Karen Grubb

Contributors

Hudson Trident
Max Bobys
Andrew Baskin

Graphic Design

María Paula Lozano

CONTENTS

EXECUTIVE SUMMARY

The growth in digitalization and automation in the maritime domain[1] has brought increases in efficiency and competitiveness as well as the industry's overall cyber risk. In the Western Hemisphere, the maritime sector is crucial to the flow of commerce and protecting operations and data that underpin those operations is of growing importance to national and regional economies.

The Organization of American States ("OAS"), an international organization, through the Inter-American Committee against Terrorism ("CICTE") has developed this overview document to assist in the following:

1. Assist maritime stakeholders in the Western Hemisphere understand maritime cyber risk;
2. Provide a brief overview of the key international rules and standards under development today by international organizations and states to address these risks;
3. Lay out initial steps maritime organizations can take to manage cyber risk; and
4. Highlight some best practices to consider as maritime organizations implement cyber risk management programs.

High-level considerations include:

- Maritime organizations are targets for cyber attacks for many reasons, such as their growing information technology and operational technology complexity and their role as hubs for data from shipping lines, trucking, and logistics, and off-dock storage providers.

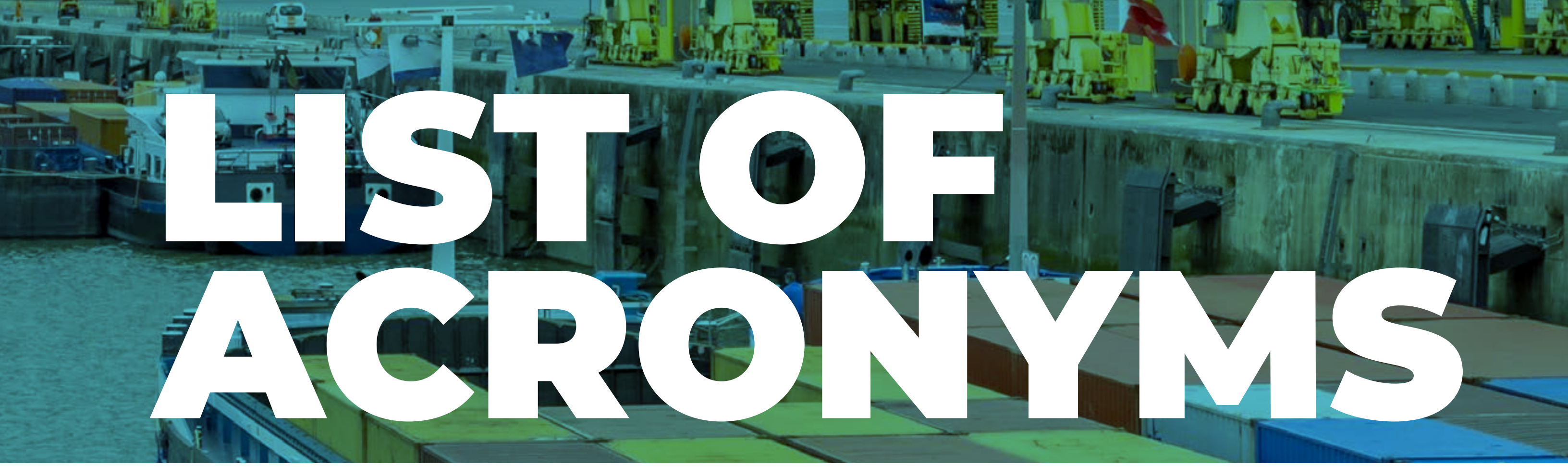
- A variety of Western Hemisphere maritime stakeholders, including ports, carriers, and logistics providers, have been victims of significant and costly cyber attacks.

- International rules on how to manage maritime cybersecurity risk are evolving but lag behind operational needs. Non-binding guidance and standards can help maritime organizations develop their own effective cyber risk management and cybersecurity programs.

- Best practices to improved cyber risk management and cybersecurity already exist and are described in this document in order to assist entities in the region in performing an initial baseline cybersecurity capability assessment to measure existing cybersecurity capabilities.

- Greater awareness of international rules and best practices to manage cybersecurity risk in the maritime area can be of particular use to OAS member states, some of whom are in the earliest stages of considering and implementing maritime digitalization programs, and

- States in Western Hemisphere, particularly in Latin America, are rapidly developing national cybersecurity plans and increasing ways to share information and respond rapidly to cybersecurity incidents. CICTE's maritime and cybersecurity programs are assisting states in these efforts and this publication is one of a series of reports that address various aspects of cyberspace in the region.



LIST OF ACRONYMS

AIS	Automatic Identification System
CERT	Computer Emergency Response Teams
CICTE	Inter-American Committee against Terrorism
CIO	Chief Information Officer
CIS	Center for Information Security
CISO	Chief Information Security Officer
CSC	Cybersecurity Steering Committee
DMARC	Domain-based Message Authentication, Reporting and Conformance
ERP	Enterprise resource planning
EU	European Union
GDPR	General Data Protection Regulation
ICS	Industrial control systems
IEC	International Electrotechnical Commission
IoT	Internet of things
IMO	International Maritime Organization
ISO	International Organization for Standardization
ISMS	Information Security Management System
ISPS	International Ship and Port Facility Security
IT	Information technology
OAS	Organization of American States
OT	Operational technology
MTSA	Maritime Transportation Security Act
MTS-ISAC	Maritime Transportation Systems Information Sharing and Analysis Center
NIS	Network and information systems
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NVIC	Navigation and Vessel Inspection Circular
PCS	Port community system
PFSA	Port facility security assessments
PFSO	Port facility security officers
PFSP	Port facility security plan
RFID	Radio frequency identification
SCADA	Supervisory control and data acquisition
SMS	Short Message Service
SOLAS	Safety of Life at Sea
SPF	Sender Policy Framework
TOS	Terminal operating system
USCG	United States Coast Guard

MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

1.0 INTRODUCTION

Maritime transport is critical to the movement of goods that underpin the global economy. Maritime infrastructure facilitates the flow of vital goods, such as foods, medicines, and energy. As part of the backbone of global trade and the global economy, the maritime industry is increasingly digitalizing, and in some cases automating, its operations, and there are growing calls for the industry to accelerate this process[2]. As the just-in-time supply chain relies on efficiencies provided by digitalization, this will result in additional efficiency gains and an industry that is more responsive to the needs of an evolving global economy.

As seen in other industries, the movement toward a more digitalized environment, such as electronic commerce and data exchange, brings a corresponding increase in cyber risk. Maritime operations and data are vulnerable to cyber threats. States in the Western Hemisphere are increasingly conscious of this and in response are expressing their concerns politically on a regional level. Practically they also are developing national level cybersecurity plans to address such risks on an operational level[3]. But more work remains to be done to develop and tailor those national plans to address increasing cybersecurity concerns in the maritime area.

Cyber threats affect all industrial sectors, and in the Western Hemisphere much attention has been focused on increasing the security of financial and banking systems and governmental services. Equally important is the need to promote cybersecurity in the maritime area as marine infrastructure presents its own particular set of risks and vulnerabilities. For example, the maritime sector is heavily reliant on systems such as complex information technology (IT) and operational technology (OT) and increasingly dependent on the use of Internet of Things (IoT)-enabled devices and automated systems that integrate communications, control, and information processing. Cyber threats to this digital infrastructure can generate operational interruptions and data corruption in the maritime industry, which can have serious effects for trade, economies, and security. As a result, maritime organization leaders need to be aware of the maritime cyber risk landscape and take actions to mitigate cyber risk both internally and to the maritime industry as a whole.

This document is intended for use by those executives, senior managers, and others responsible for land-based maritime infrastructure or related facilities involved in the logistics of seaborne cargos and people in the Western Hemisphere, including:

- Executive leadership, such as Chief Executive Officers and Managing Directors,

- Governance and oversight, such as Boards of Commissioners or Directors,

- Technical managers without information technology responsibilities, such as terminal operations managers, and

- Administrative managers, such as finance, legal, and human resources.

This document informs maritime leaders about requirements, guidelines, and best practices that their organizations can use and incorporate to manage cyber risk, drive organizational cybersecurity capability maturity, and develop operational resilience. This document also identifies and analyzes maritime-specific case studies, including some in the Western Hemisphere, that illustrate key cybersecurity and cyber risk management issues maritime organizations confront. Since maritime organizations are unique and vary in numerous ways, and most relevant national regulatory frameworks are still under development, there is no one-size-fits all set of guidelines and recommendations. Instead, maritime organizations should implement best practices based on their operating environment, financial resources, and risk appetite.

Maritime organizations across the world, including those throughout the Western Hemisphere, are continuing on the path toward increased digitalization and automation. This document aims to assist maritime organizations in the Western Hemisphere with ensuring that their cyber risk management capabilities grow with and adapt to their increased competitiveness and efficiency.

2.0 CYBER RISK IN THE MARITIME DOMAIN

2.1 Why cybersecurity is important to ports in the Western Hemisphere

Maritime organizations serve a critical function in the Western Hemisphere in facilitating domestic and international supply chain activities by connecting sea and inland transport services. According to IHS World Trade Service, seaborne trade in the Western Hemisphere accounts for roughly U.S. $3.75 trillion[4], with the combined economic value of port activities to be far greater. The Western Hemisphere includes a large number of ports and major maritime installations (e.g., the Panama Canal) at various levels of technological developments, and some states, including in the Caribbean, are heavily dependent on efficient ports and cargo container traffic for their well-being.

States in the region are increasingly digitalizing their maritime logistics operations and adopting new technologies, such as the implementation of port community systems (PCS)[5] (e.g., Peru and Jamaica) and the adoption of a maritime single window system (e.g., Panama and Antigua and Barbuda). These systems are designed to help streamline and process information at ports more rapidly. In addition, the 2020 pandemic, which had widespread effects on Latin American economies, is accelerating this digitalization trend as states are rapidly starting to digitalize many processes, such as permits, licenses, and social service applications. Cyber threats, if ignored, jeopardize these advances and the economic health and viability of port operators and other maritime organizations.

Recognizing these risks, the 34 member states of the Organization of American States (OAS) have taken steps to improve cybersecurity policy in all sectors, including the maritime sector. The OAS supports these efforts through its cybersecurity and maritime security programs. These programs are multi-facetted and focus on policy development, capacity building (including training and exercises), research, and outreach to States. Inter-American Committee against Terrorism (CICTE) has focused on identifying threats to the region's critical infrastructure generally. In particular, the CICTE Cybersecurity Program assists OAS member states in developing national or regional cybersecurity strategies, and the CICTE Maritime and Port Security Program focuses on assisting States develop national maritime security strategies. Together these initiatives lay the groundwork for addressing maritime cybersecurity risks and vulnerabilities in the region.

Over the last ten years, for example, thirteen states in the Western Hemisphere, with CICTE assistance, have adopted national cybersecurity strategies. Those national plans generally lay the policy groundwork for addressing cyber risks in critical infrastructure sectors, including the maritime sector. In addition, CICTE over the last five years has operated an information sharing network called "CSIRTAmericas"[6] to help states share information and coordinate rapid 24/7 responses to cybersecurity threats and vulnerabilities. In this sense, a report describing this information exchange model is being developed, and addresses its five pillars: Community, Taxonomy, Level of Information, Communication Channels and Traffic Light Protocol (TLP). In conjunction with this, CICTE also conducts cybersecurity crisis management exercises, including an exercise in Panama tailored to addressing cybersecurity risks its maritime sector.

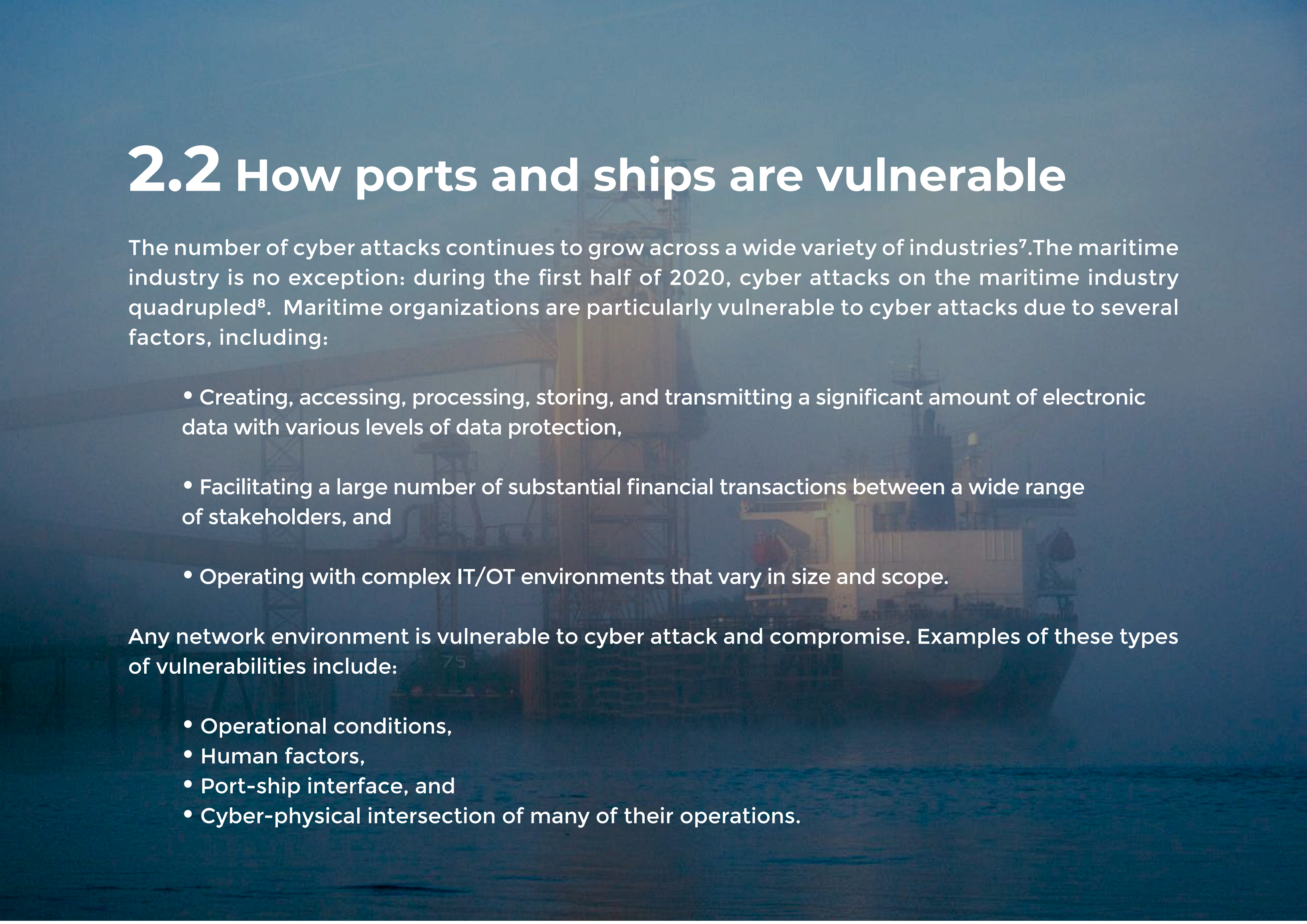
As these efforts unfold on the regional level, more attention needs to be paid to how maritime authorities can implement operational measures to address cybersecurity risk on a day-to-day basis. Before addressing what steps those authorities can take, it may be useful to take a step back and review two key developments that make maritime organizations attractive targets for cyber-attacks all over the world: (1) port and maritime operational digitalization and automation, and (2) maritime organizations as logistics data hubs and repositories.

2.1.1 Port and maritime operational digitalization and automation

Port and maritime operations are complex and involve a wide variety of fixed, technological, and communication assets that interconnect to support an array of vessel operations, cargo handling, supply chain, and governmental services. As maritime organizations in the Western Hemisphere become increasingly digitalized (and sometimes automated) in order to improve efficiency and competitiveness and, in some cases, comply with national requirements, their operations become increasingly vulnerable to cyber threats. This increase in digitalization means that a compromise of a maritime asset or group of maritime assets can have grave consequences for a maritime organization's operations, safety, finances, and reputation. In addition, because maritime organizations are growing increasingly interconnected, such as with the growing adoption of PCS, a compromise of one maritime organization's assets can lead to compromises of many maritime organizations' assets.

2.1.2 Maritime organizations as logistics data hubs and repositories

Further, because maritime organizations serve as a nexus of global trade, they have become information hubs, integrating data from their users, including terminal operators, carriers, logistics companies, and government authorities, among others. As data and information hubs, maritime organizations create, process, transmit/receive, and store a wide variety of data and information across their networks and in their systems. This data is commercially valuable to many, including competitors seeking an advantage or criminals seeking to steal data or compromise data to facilitate fraudulent transactions or smuggling. In addition to ensuring the digital security of their operations, maritime organizations need to protect the confidentiality, integrity, and availability of the data that reside on their networks and in their systems, just like other transportation hubs, such as airports.



2.2 How ports and ships are vulnerable

The number of cyber attacks continues to grow across a wide variety of industries[7].The maritime industry is no exception: during the first half of 2020, cyber attacks on the maritime industry quadrupled[8]. Maritime organizations are particularly vulnerable to cyber attacks due to several factors, including:

- Creating, accessing, processing, storing, and transmitting a significant amount of electronic data with various levels of data protection,

- Facilitating a large number of substantial financial transactions between a wide range of stakeholders, and

- Operating with complex IT/OT environments that vary in size and scope.

Any network environment is vulnerable to cyber attack and compromise. Examples of these types of vulnerabilities include:

- Operational conditions,
- Human factors,
- Port-ship interface, and
- Cyber-physical intersection of many of their operations.

2.2.1 Operational conditions

Maritime port and terminal operating environments are composed of complex infrastructure, public and private organizations, and various networked systems. Control systems moving cargo, optical recognition technology operating on cranes and at gates, Wi-Fi-enabled radio frequency identification devices (RFID) containing cargo data as they are scanned at the port, and security systems that are tied to personnel data as well as Terminal Operating Systems (TOS) and customs systems, all enhance the flow of international maritime commerce. This increase in digitalization has created significant efficiencies for maritime organizations.

Unfortunately, this technological connectivity breeds cyber vulnerability. Maritime organizations present attractive targets for cyber threat actors because there are so many stakeholders and networks operating in a complex IT/OT terminal environment. Many maritime organizations have IT systems that support every aspect of the organization, including its critical operational activities, such as cargo handling and fuel transfer and storage. Many, but not all, use technologies that are poorly secured or systems that are old and not updated and linked with other systems, which can increase cyber vulnerabilities. In this way, a maritime organization can be a "one-to-many" cyber threat vector to its stakeholders.

One entity can potentially expose third parties operating in the terminal environment, including terminal operators, port authorities, customs officials, logistics companies, agents, vendor representatives, and many others. Each of these stakeholders can have varying levels of cyber risk management, and one weak link can break the chain of cybersecurity. This is particularly true of maritime stakeholders operating in port communities employing a PCS, which connects numerous port community members in a single, integrated electronic system.

Further, unlike office network environments, compromised supervisory control and data acquisition (SCADA) devices or industrial control system-managed marine infrastructure can result in environmental damage, first- and third-party property losses, and physical injury or death. Moreover, successful attacks that result in the unauthorized disclosure of confidential or sensitive third-party information can generate compliance and policy consequences that can trigger fines and lawsuits.

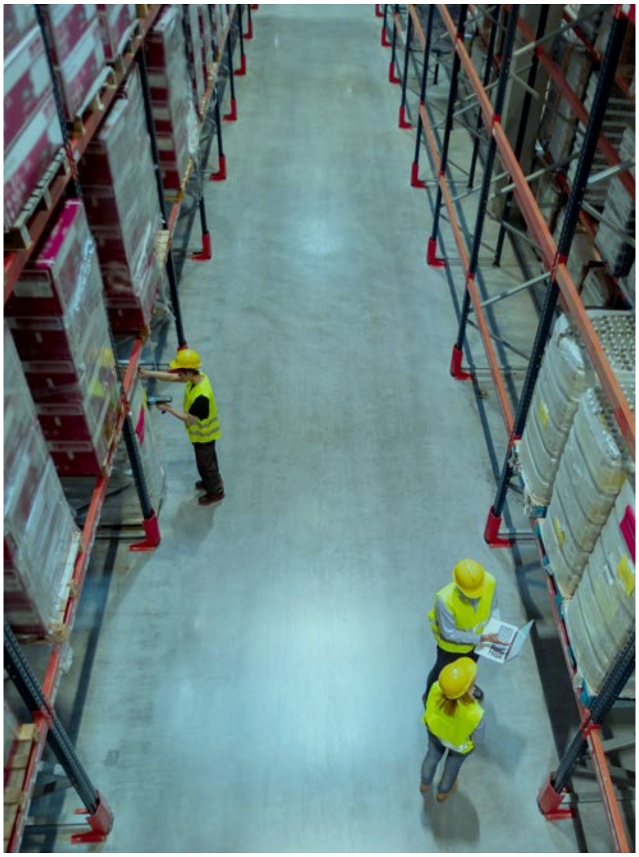
2.2.2 Human vulnerabilities

In addition to these previously mentioned vulnerabilities, maritime organizations, like other organizations, face vulnerabilities due to human factors. However, maritime organizations confront human-factor challenges because of the wide variety of administrative and operational roles their personnel undertake.

Administrative personnel engage with the corporate IT network endpoints, such as computers, printers, and servers, across which flow sensitive business data. As such, administrative personnel may be targeted by phishing scams or other social engineering exploits.

Operational personnel work in networked environments, such as Wi-Fi-enabled cargo-handling systems, mobile scanners, and gate access control. They also work with complex critical industrial control systems (ICS) servicing vessels (such as cranes and conveyor systems) and need to manage and efficiently operate increasingly complex systems while remaining vigilant for cyber threats. Further, OT systems in complex terminal environments are especially vulnerable to human error because an untrained or careless operator or an overcomplicated procedure can result in sensitive information leaking and potentially falling into the hands of an attacker. In addition, automated cargo management processes that are integrated with office-based enterprise resource planning (ERP) systems could be compromised, leading to broader data breaches.

Maritime organizations can apply various protection technologies and tools. However, the employees accessing those networks bring a diverse range of personal experience, cybersecurity education, knowledge, and behavior, and thus present cyber risk. Employees can introduce cyber risk via negligence, such as unknowingly violating security policies or malicious intentions, such as stealing organizational data. These vulnerabilities (known as insider threats) require that all staff, including senior leaders, receive cyber risk awareness training (see Section 5.2.1).

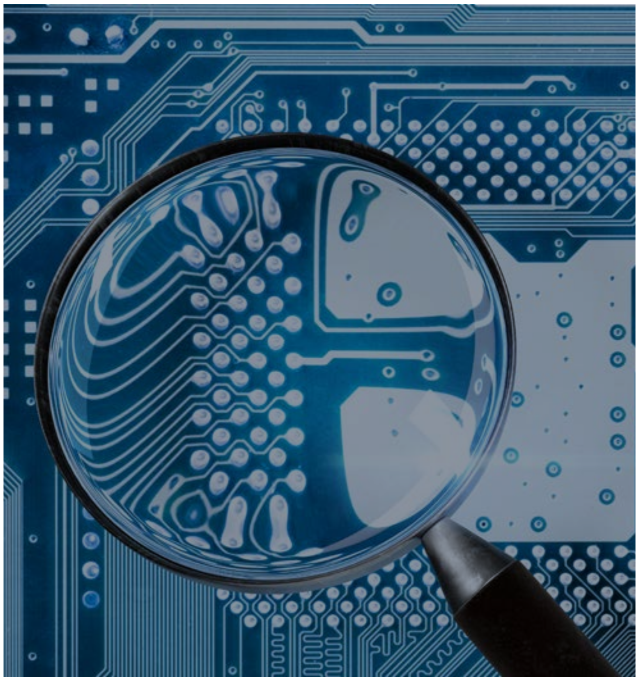


2.2.3 Port-ship interface

As part of their operational circumstances, maritime organizations face unique vulnerabilities due to the ships they service, which are potential conduits or carriers of cyber risk. This is a result of several factors specific to ships, including that ships are multi-national entities, often relatively lightly governed, and very mobile. Due to this, when moored in port, ships potentially bring many of the security risks from the previous ports they have visited. These risks can include:

- Possible infection of ship systems, such as navigation systems, or the use of ship systems to convey cyber threats from previous port calls. Ship systems can be infected through the inadvertent introduction of viruses and other cyber threats by crewmembers with poor cybersecurity practices, such as opening malware-infected emails or using infected USB-enabled devices.
- Equipment on the vessel designed to collect and enter port or government information systems as a form of espionage.

Furthermore, shore-side maritime organizations are becomingly increasingly integrated with ships, as ships and ports often use digital communications to exchange information. Due to this integration, maritime organizations should be aware of the ways that ships may serve as carriers of cyber threats against other maritime organizations. One notable example is a cyber threat campaign known as “Daily Show.” This attack began as a phishing attack (see Section 5.2.4) against the shipmaster on a tanker. The malware has since infected vessels, port facilities oil/gas facilities, manufacturing, customs agencies, logistics companies, and banks across the world, including locations in Mexico and Panama[9].



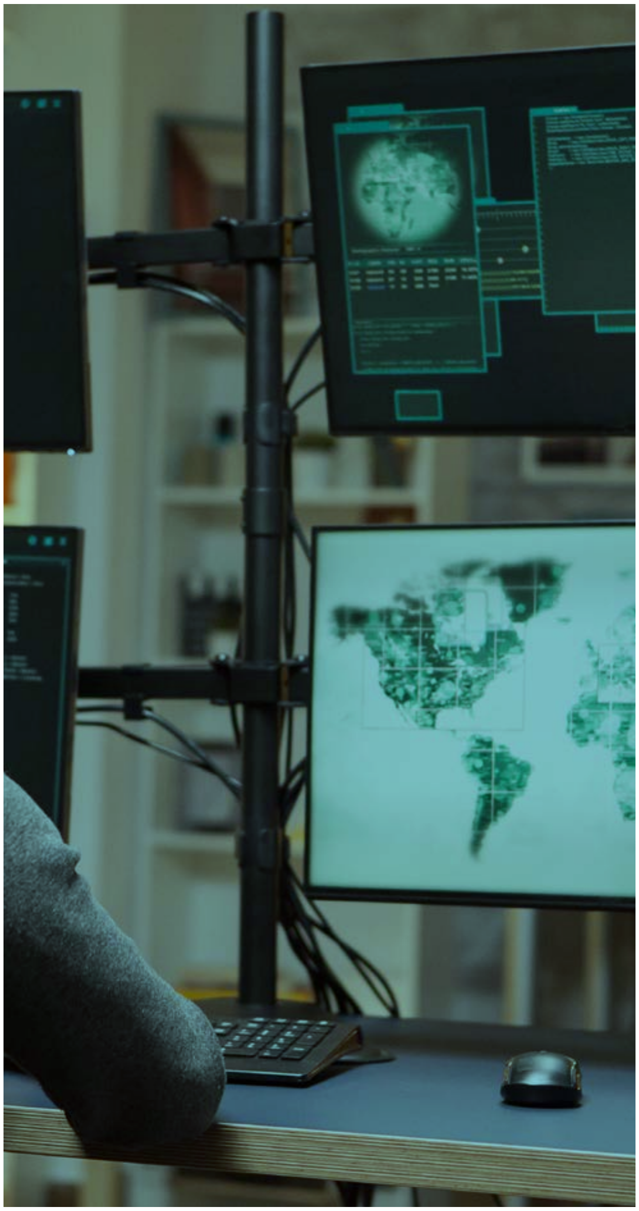
2.2.4 Cyber-physical intersection

Maritime organizations have been evolving from operations carried out manually or with non-digital equipment to now performing an array of port services with varying levels of integrated, digital, and automated processes and technologies. One factor driving both the evolution and complexity of cyber threats is the connectivity among the following systems:

- IT-based systems, such as access control and ERP applications,
- Domain awareness-oriented systems, such as integrated security monitoring systems, including video, RADAR, and Automatic Identification Systems (AIS), and
- OT-based systems, such as ICS, SCADA-enabled systems, cargo-handling systems, bulk liquid transfer storage and distribution, and environmental sensors, etc.

As best practices, these systems are typically segregated. However, many maritime organizations continue to connect IT-enabled networks supporting business or security systems to control system networks[10].As more maritime organizations connect these systems to networks, and further seek to adopt IoT-based technologies, new vulnerabilities emerge that threat actors can exploit. This is particularly the case for IT networks that connect to SCADA-enabled and ICS systems involved in cargo handling, fuel storage transfer, and building management systems. For instance, cyber threat actors could use digital controls to manipulate physical systems, such as damaging or corrupting a crane's operating system, rendering it inoperable. In the maritime context, this could involve compromised programmable logic controllers that can over-pressurize bulk liquid pipeline infrastructure, resulting in a catastrophic failure that could jeopardize the health and safety of personnel, or impact an entire port community[11].

Cyber threat actors have capitalized on this IT/OT convergence in several large-scale attacks on numerous private-sector organizations. One in particular included pirates who accessed a shipping company's shore-based business systems to support advance planning for an attack on a vessel. The attackers subsequently stopped the vessel at sea, boarded, identified their targeted cargo, located it on the vessel, then escaped with the cargo without further incident[12]. For additional examples of the physical manifestation of cyber attacks, see the NotPetya case study in Section 2.3.2.



2.3 Cybersecurity threats

2.3.1 Types of cyber threat actors

Maritime organizations face threats from a wide variety of cyber threat actors:

Competitors:

Unethical competitors seeking to exploit cyber vulnerabilities may hire cyber attackers to target payment data, cargo movement and position data, contracts, confidential client information, merger and acquisition strategies and activities, employee personal information, and other confidential information. This information can provide insight into the organization's operations and decision-making processes, among other things, offering potential advantages to unethical competitors.

Organized crime:

Maritime-based transnational organized crime activity continues to be a topic of concern to international bodies[14]. Criminal groups have successfully breached networks and systems at ports (see Section 2.3.2.1). By gaining access to cargo management and logistics systems, organized criminals can access, view, and manipulate sensitive cargo information, allowing them to reduce the risk of customs inspection on a given shipment or even steal entire containers altogether.

MARITIME ORGANIZATIONS FACE THREATS FROM A WIDE VARIETY OF CYBER THREAT ACTORS

States:

Cyber attacks are becoming a weapon for governments seeking to defend national sovereignty and project national power. State-sponsored attacks can have physical, economic, and security consequences. Critical infrastructure is known to contain sensitive data and to be crucial to economies, maritime organizations such as ports have been targets of nation-state-sponsored cyber attacks[13].

Terrorists:

While the maritime industry has taken significant steps to harden its operations against the threat of physical terrorist attacks to facilities and other critical infrastructure, maritime organizations remain vulnerable to the emerging threat from cyber-terrorism. Key ports, or other critical maritime infrastructure such as the Panama Canal, could be attractive targets for terrorists in the Western Hemisphere.

Insider threats:

Maritime organizations face cybersecurity risks from current employees, former employees, contractors, partners, and vendors. These threats arise from both deliberate and unintentional actions. Intentional insider threats can be from a disgruntled former or current employee who is able to use unrevoked credentials. Employees might also be susceptible to bribery or blackmail by third parties into revealing sensitive information, inserting malicious programs, or even reconfiguring IT/OT protocols, processes, and configurations. Insiders can also inadvertently download malicious software from fake emails or infected websites.

Hackers and hacktivists:

Individuals or small groups with specialized knowledge, unique skillsets, and experience can facilitate the cyber theft of money or goods that they can sell. Hackers sometimes contract their services to other cyber threat actors, such as organized criminal groups, governments, or even private companies seeking a competitive advantage. Some hackers are motivated more by ideology than financial gain. These individuals are referred to as "hacktivists," and they use cyber means to advance political agendas or causes, either independently or through a larger organization.

2.3.2 Case studies

Numerous successful cyber attacks have occurred on maritime organizations and their community members in recent years. The case studies in this section illustrate the different types of attacks that maritime organizations could face: attacks aimed at an entire port community, attacks that seek to maximize destruction, and attacks that are opportunistic attempts at financial gain.

2.3.2.1 Port community attacks

From 2011 through 2013, press reports indicate that a Netherlands-based organized crime group recruited hackers to breach Port of Antwerp IT systems that controlled the movement and location of containers[15]. Attackers penetrated physical security boundaries through physical intimidation of terminal facility employees. Once attackers gained physical access to administrative offices, they attached keyloggers to network devices to gain visibility into systems with critical data. They did this to hide cocaine and heroin among legitimate cargos, including containers of timber and bananas shipped from countries in South America[16]. With the hackers' assistance, the criminals accessed the release codes for targeted containers and gained advance knowledge of when and where to send a truck to intercept a container before the legitimate owner arrived.

This attack illustrates how maritime organizations, including ships, terminal operators, and ports, do not operate in isolation. Instead, they operate within the same community in which they regularly exchange and store data from a wide variety of groups, including shipping lines, carriers' agents, terminal operators, freight forwarders, road haulage, train operators, border control and inspection, port state control, and customs authorities[17]. The cyber attack on the Port of Antwerp, which was the result of coordination and collaboration between different types of actors (organized criminals and hackers) who threaten maritime organizations, put at risk data from all members of that port community.

2.3.2.2 Reports of State attacks

One example of a significant cybersecurity attack on ports that affected the Western Hemisphere region is the so-called "NotPetya" case. In June 2017, government[18,19,20] and media[21] reports indicate that a wave of damaging cyber attacks spread around the world, delivering a piece of wiper malware called "NotPetya." Eventually it affected the global operations of A.P. Moller-Maersk, the world's largest container ship operator[22] and among the largest five port terminal operators[23]. Computers were infected with NotPetya malware and affected operations in 17 port terminals that Maersk operates, including terminals in Callao (Peru), Elizabeth, New Jersey (USA), Itajai (Brazil), Los Angeles (USA), and Buenos Aires (Argentina). Maersk was forced to halt operations as the malware spread through critical IT systems and, in order to recover, had to overhaul nearly all of its IT infrastructure[24]. This attack had effects throughout Maersk's customer base, including triggering cargo delays for many customers[25]. Speaking at the World Economic Forum in January 2017, Maersk's Chairman, Jim Hagemann Snabe, shared that Maersk reinstalled its entire IT infrastructure and its resulting financial losses up to 300 million USD[26].

Although many initially believed that NotPetya was ransomware, and that the attackers were seeking financial gain from the attack, the malware's goal may have been focused on destruction[27]. Known as wiper malware, NotPetya encrypted key parts of infected computers, but no key existed to reverse the encryption. Governments in many affected countries, including the United States[28] and United Kingdom[29],and intergovernmental organization such as the North Atlantic Treaty Organization[30],announced that a state actor was behind NotPetya. While this type of data destruction was not intended specifically for Maersk, or any other maritime organization, NotPetya was a reminder that maritime organizations that operate in the modern, digital world can fall victim to these types of cyber attacks.

2.3.2.3 Opportunistic attacks

In addition to targeted attacks (Antwerp) and large-scale destructive attacks (NotPetya), maritime organizations should also be wary of less coordinated but still disruptive opportunistic attacks that occur often. These opportunistic attacks take advantage of a vulnerable target that the attacker had not previously identified. For example, a number of maritime organizations have suffered ransomware attacks, which is a common opportunistic attack[31]:

- In 2018, the Port of San Diego (United States) was the victim of a ransomware attack against more than 200 public entities and hospitals[32].

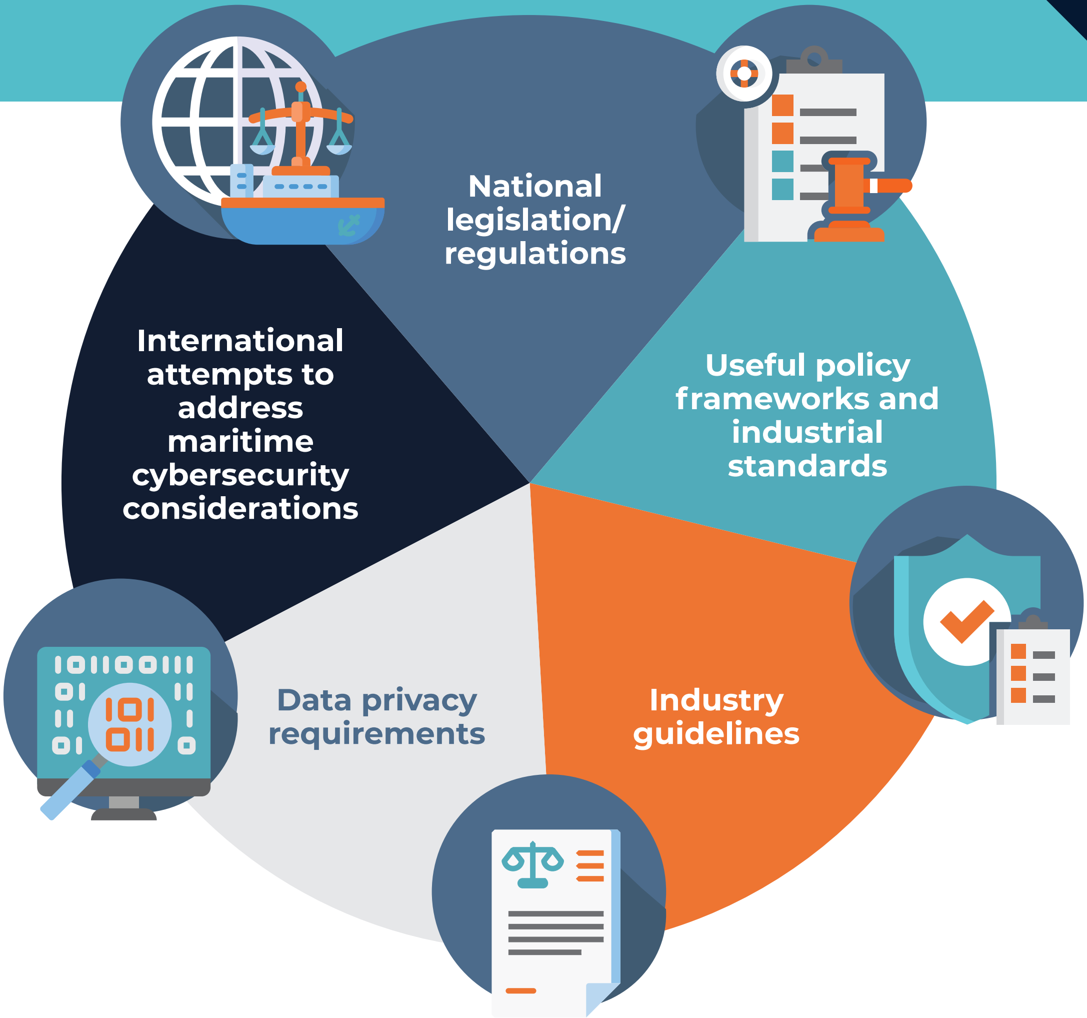
- In 2018, the Port of Barcelona (Spain) suffered a ransomware attack that affected some of its servers and systems[33].

- In 2018, the shipping line Cosco suffered a ransomware attack that affected its communications systems in the United States, Canada, and South America[34].

- In 2020, the logistics company Toll Group suffered a ransomware attack that affected many of its IT systems[35].

These maritime organizations were not specifically targeted in the way that the Port of Antwerp was in the case study in Section 2.3.2.1. Instead, they happened to have a weakness or vulnerability that attackers were targeting as part of broader campaigns and became victims to these less impactful but still damaging attacks.

3.0 REGULATIONS AND GUIDELINES


National legislation/ regulations
Useful policy frameworks and industrial standards
Industry guidelines
Data privacy requirements
International attempts to address maritime cybersecurity considerations

To prevent the sorts of attacks illustrated above, States, international organizations, and private entities are developing rules on how to manage cyber risk, including rules to guide how sensitive electronic information is managed and exchanged, personal information is secured, cyber breaches are reported, and to reduce other vulnerabilities. This section discusses how the International Maritime Organization (IMO)[36],other multilateral bodies, and states are developing those rules relevant to cybersecurity that are either specific to or will affect the maritime industry.

3.1 International attempts to address maritime cybersecurity considerations

3.1.1 IMO and shipping

The IMO, which is the leading international maritime organization, has only recently begun to address cybersecurity considerations in the maritime area with any level of specificity. In 2017, the IMO passed a resolution and released specific guidance addressing vessel cybersecurity[37]. This resolution requires vessel owners and managers to incorporate cyber risk management into their safety management systems by a certain date for each vessel. His Resolution encourages national authorities to verify compliance with this requirement.

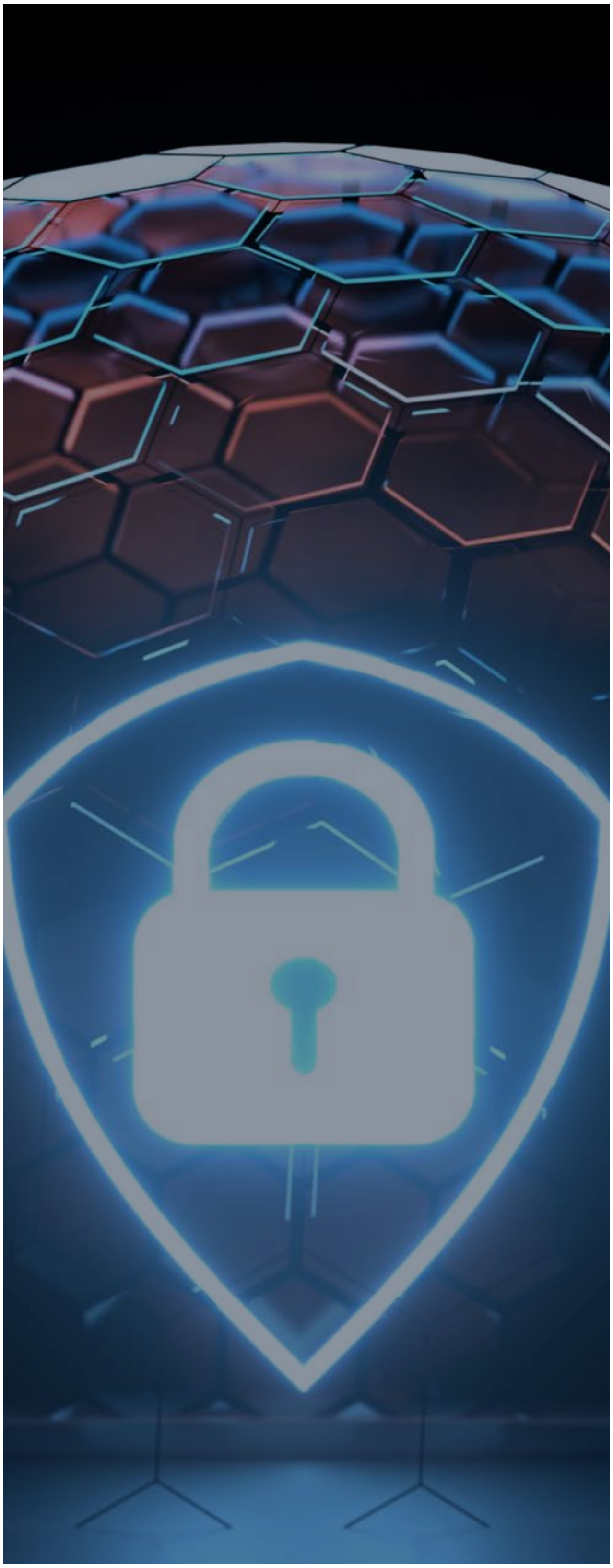
That same year, the IMO supplemented this Resolution with its *Guidelines on Maritime Cyber Risk Management*[38]. The Guidelines provide high-level recommendations on maritime cyber risk management. The Guidelines recognize that cyber technologies are essential to the operation and management of the systems that are critical to the safety and security of shipping and protection of the marine environment and further acknowledge that maritime organizations are vulnerable to cyber risk and therefore need to address how their systems are accessed, interconnected, and networked. These Guidelines closely align with similar guidelines adopted by the United States called the "National Institute of Standards and Technology Cybersecurity Framework" (NIST CSF) which are discussed in Section 3.3.

3.1.2 IMO and ports

To date the IMO has not yet adopted measures specifically focused on cybersecurity in port facilities (as opposed to the measures above which focused on vessels). However, in June 2020 the IMO issued a circular endorsing the industry call to action led by the International Association of Ports and Harbors to drive the acceleration of digitalization of maritime and logistics, including the need to address cyber risks in ports.

Port authorities, however, are under some obligation to address cybersecurity, even in the absence of a specific IMO resolution on the topic. For example, port facilities that are subject to the International Ship and Port Facility Security (ISPS) Code should account for cyber threats as part of their compliance with the ISPS Code. The ISPS Code is part of the Safety of Life at Sea (SOLAS) Convention, which provides for minimum security arrangements for ships, ports, and government agencies.

To comply with ISPS regulations, a port facility must undertake a port facility security assessment (PFSAs), develop a port facility security plan (PFSP), appoint a port facility security officer (PFSO), and invest in certain security equipment. PFSAs are required to include the identification of possible threats to assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures. Cyber threats are increasingly prevalent, and therefore identifying and including cybersecurity considerations in a PFSA would be an ideal way for maritime organizations to begin addressing these crucial issues. This, along with the development of national cybersecurity strategies, are practical avenues for states to develop a legal and practical framework to confront these challenges.



3.2 National legislation / regulations

Minimal maritime-specific national legislation about cybersecurity currently exists, including in the Western Hemisphere. Nonetheless, ports and other maritime infrastructure are covered under some national cybersecurity strategies and general national and multilateral cybersecurity legislation.

3.2.1 National cybersecurity strategies

By the end of 2020, a total of thirteen (13) countries throughout the Western Hemisphere have developed national cybersecurity strategies and seven (7) are currently under development with support from the OAS/CICTE[39].Cybersecurity strategies specifically define cyber protection of critical infrastructures, including ports, as a core objective of these strategies. Due to their critical role in modern economies, ports are widely considered to be core infrastructure. Accordingly, ports should ensure that their cybersecurity strategies align with their roles and responsibilities established in relevant national cybersecurity strategies.

3.2.2 National and supranational legislation and multilateral regulation

Several States and multilateral bodies have directives and other guidance focused on ports and their cybersecurity responsibilities as critical infrastructures. The directives and guidance highlighted below, while mainly focused on the ports within each entity's jurisdiction, are still useful for ports outside of their jurisdiction. These include:

- **United States Navigation and Vessel Inspection Circular 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act Regulated Facilities.** In 2020, the United States released the Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at Maritime transportation Security Act (MTSA) Regulated Facilities, which provides guidance to facility owners and operators about complying with the requirements to assess, document, and address computer systems and network vulnerabilities. In NVIC 01-20, the United States Coast Guard (USCG) takes the position that port facility owners and operators are required, under the MTSA of 2002, which implemented the ISPS Code in the United States, to address cybersecurity vulnerabilities and ensure the cybersecurity of their facilities. The United States has announced that, beginning on October 1, 2021, port facility owners and operators should submit cybersecurity amendments to their MTSA-required assessments and plans during audits. NVIC 01-20 provides guidance on how port facility owners and operators can meet those requirements but does not create any new obligations or change requirements found in existing regulations[40]. In addition, in December 2020, the United States released a National Maritime Cybersecurity Plan, which will require the USCG to develop a framework for port cybersecurity assessments[41].

- **European Union Directive on Security of Network and Information Systems.** In 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (NIS Directive), which assists operators of critical infrastructure

in creating cybersecurity programs that can appropriately prevent, detect, notify authorities of, and respond to security incidents. The NIS Directive classifies managing bodies of ports, including their port facilities, as well as entities operating works and equipment contained within ports, as Operators of Essential Services. Therefore, as Operators of Essential Services, these organizations are subject to the NIS Directive's requirements, including the conduct of risk assessments that cover, among other things, the security, integrity, and resilience of NIS[42].

- **Singapore Cybersecurity Act.** In 2019, Singapore passed the Singapore Cybersecurity Act, which establishes a legal framework for the oversight and maintenance of cybersecurity in Singapore. This Act requires that organizations in critical information infrastructure sectors prevent, manage, and respond to cybersecurity threats and incidents; protect critical information infrastructures, and share critical information infrastructure information with the Cyber Security Agency of Singapore in the event of a cyber attack. Maritime transport infrastructure is included in the definition of critical information infrastructure.

3.3 Useful policy frameworks and industrial standards

As noted above, there are few national cybersecurity legislative frameworks in place and few multilateral requirements to address maritime cybersecurity threats. Having said that, there are other existing references that can help maritime organizations address these issues and inform the development of their cybersecurity capabilities. The standards and frameworks discussed in this section are either for critical infrastructure generally (Sections 3.3.1, 3.3.2, and 3.3.3) or maritime infrastructure specifically (Sections 3.4.1 and 3.4.2)[43].

3.3.1 United States National Institute of Standards and Technology Cybersecurity Framework

The NIST CSF was among the first policy frameworks for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks[44,45]. The NIST CSF offers a roadmap for organizations, such as maritime facilities, seeking to identify vulnerabilities, threats, and dependencies, as well as implement best practices for cyber risk management[46].The NIST CSF enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. Since its launch, it has been translated into multiple languages, including Spanish and Portuguese, and has been adopted by numerous countries, such as Italy, Japan, Saudi Arabia, Switzerland, and Uruguay[47].

Both the IMO's Guidelines on Maritime Cyber Risk Management and the USCG NVIC 01-20 are based on the NIST CSF framework. The NIST CSF framework consists of five functional areas for managing cyber risk across an organization as part of a coordinated plan: Identify, Protect, Detect, Respond, and Recover.

NIST Framework

1. Identify

Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to maritime business and facility operations.

2. Protect

Implement risk control processes and measures (including technical measures) and contingency planning to protect against a cyber event and ensure continuity of maritime administrative and operational activities.

3. Detect

Develop and implement activities to detect a cyber event in a timely manner, communicate incidents to stakeholders across administrative and operational environments, and ensure timely communication to port and cargo community stakeholders, where appropriate.

4. Respond

Develop and implement activities and plans for resilience and systems restoration when cyber events impair maritime operations or services.

5. Recover

Identify measures to back up and restore systems necessary for maritime operations affected by a cyber event, including coordinate and working with external stakeholders, as necessary.

3.3.2 International Organization for Standardization 27000 and 28000 standards

The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) family of standards is designed to help secure information assets, which include intellectual property, sensitive employee or customer data, and financial information across a number of industries. While there are numerous standards in the 27000 series, the best known is 27001, which offers requirements for an Information Security Management System (ISMS). An ISMS is a management framework used to identify and assess information risk and adapt and evolve to meet changes in cyber threats and vulnerabilities.

In addition to ISO 27001, ISO 28000:2007 provides specifications for security management systems for the supply chain, including information security and security assurance. This standard is useful for organizations of all sizes and ranges of IT/OT complexity, which can be beneficial to maritime organizations, whose size and IT/OT complexity can vary. This standard can be particularly useful to maritime organizations whose objectives include ensuring internal compliance with defined security management objectives and to measuring organizational progress against best practice benchmarks.

3.3.3 CIS Controls

The Center for Information Security (CIS) Critical Security Controls for Effective Cyber Defense, known as the CIS Controls, are a set of best practices that organizations can implement to block or mitigate known attacks. These Controls were originally developed by the SANS Institute with contributions from United States Government agencies and commercial experts. The Controls are particularly useful because they are continuously updated and informed by attack-side lessons learned.

3.4 Industry guidelines

3.4.1 Port Cybersecurity: ENISA Good Practices for Cybersecurity in the Maritime Sector

In addition to the IMO and USCG guidance based on NIST CSF, the European Union (EU) has developed a best practice guide for port-sector Chief Information Officers (CIO) and Chief Information Security Officers (CISO). This Guide identifies emerging challenges related to IT and OT in the port sector, defines port cybersecurity threats, and recommend e security measures that ports should implement. This Guide identifies the following best practices:

- Define clear governance around cybersecurity, involving all stakeholders involved in port operations,
- Raise awareness of cybersecurity matters at port level and infuse a cybersecurity culture,
- Enforce the technical cybersecurity basics,
- Consider security by design in applications, and
- Enforce detection and response capabilities at the port level.

3.4.2 United Kingdom (Good Practice Guide: Cyber Security for Ports and Port Systems)

In 2020, the United Kingdom Department for Transport published an updated iteration of its Good Practice Guide: Cyber Security for Ports and Port Systems (originally published in 2016). It provided actionable advice on developing a cybersecurity assessment and plan for important assets; handling security breaches; and ensuring the use of correct governance structures, roles, responsibilities, and processes. This Guide includes information about developing a cybersecurity assessment, developing a cybersecurity plan, and establishing cybersecurity governance and management within a port facility. This level of detailed is intended for port security practitioners rather than executives who oversee port security at a high level.

3.5 Data privacy requirements

Data protection laws are growing both in number and in breadth across the Western Hemisphere. It is important for a maritime organization to understand (1) the data protection legal framework in the country in which it operates and (2) if the data it processes is subject to data protection laws in other countries.

A number of states in Latin America have adopted stringent data protection laws along the lines of the influential EU on General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. One example of a stringent data protection law in the Western Hemisphere is Brazil's General Data Protection Law, which was passed on July 9, 2019, and closely aligns with many of the GDPR provisions, including data subject rights, requirements for data protection officers, and the bases upon which personal data can be processed[48]. Argentina has had a Personal Data Protection Law in place since 2000, but its Congress has debated a replacement bill that would closely align with GDPR, including granting citizens the right to access a copy of the personal data processors hold and the right to have personal data deleted once processing is complete. Panama, for its part, enacted a Data Protection Law in 2019, which will go into effect in 2021 that recognizes rights similar to those set out in the GDPR, including the right to erasure and to data portability.

Although the EU GDPR is EU-based and applies to entities that operate in the EU, it also applies to any entity outside the EU that handles the data of EU residents, regardless of where the data is processed[49].Significantly, where the rights of EU citizens are affected, the GDPR mandates cyber breach notification to the affected parties, and, even more, establishes stringent fines that can total the greater of €20 million or four percent of an organization's annual turnover[50].

Laws governing data protection and privacy – the relationship between an organization's collection and use of data and the rights of citizens to control how their information is collected and used – have become more widespread in the Western Hemisphere in recent years. Because of increased legal and policy requirements placed on the security of personal information, it is all the more important for maritime organizations to adopt policies to secure information effectively.

4.0 INITIAL STEPS FOR DEVELOPING ORGANIZATIONAL CYBERSECURITY CAPABILITIES

Managing cyber risk and implementing a successful cybersecurity program spans nearly all aspects of a maritime organization. Thus, responsibility for effective cyber risk management and cybersecurity begins at the top of a maritime organization. A maritime organization should:

1. Establish who within the organization is responsible for overseeing all cyber risk management and cybersecurity activities,

2. Define the internal personnel and external parties who are involved in the organization's cyber risk management and cybersecurity activities,

3. Create a steering committee to formally coordinate and manage all cyber risk management initiatives,

4. Perform an initial baseline assessment of the organization's overall cybersecurity capabilities, and

5. Develop a cyber risk management strategy and implement a cyber risk management plan.

4.1 Establish oversight

Evaluating and managing organizational cyber risk is still a relatively new concept for maritime organizations. It is critical that the appropriate people within an organization perform the overarching cyber risk evaluation and management. Oversight of cyber risk management activities should be the responsibility of the owners, board members, and executives of an organization. Owners and board members are responsible for evaluating cyber risk to invested capital and protecting investor or taxpayer equity; executives are responsible for evaluating cyber risk to the organization's financial performance and operational viability. As part of this evaluation, owners, board members, and executives should ensure that the maritime organization properly defines its cyber stakeholders and establishes a cybersecurity steering committee (CSC), as described in the following subsections.

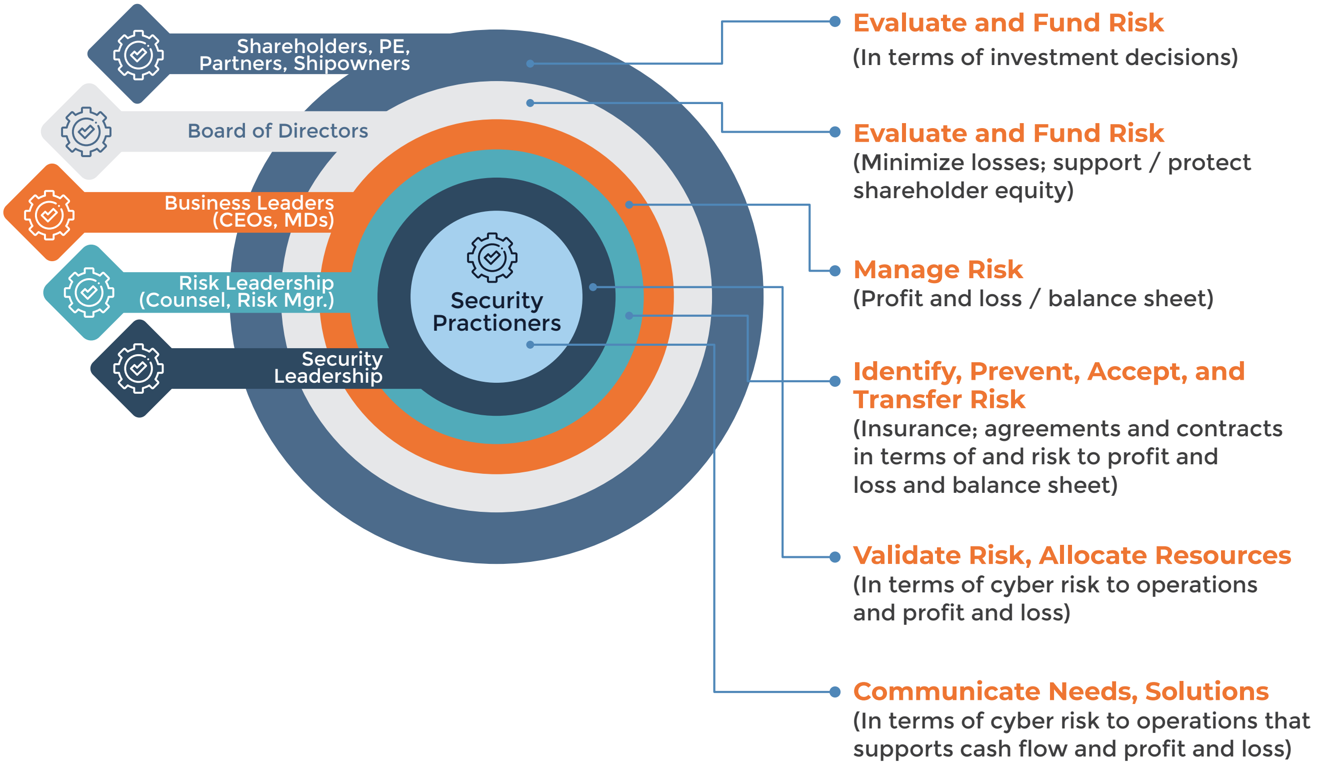
4.2 Define cyber stakeholders

One of the most important initial steps a maritime organization can take is to define its cyber stakeholders. Although no two maritime organizations in the world are alike, each shares a relatively common universe of key stakeholders. In most cases, this includes representatives from both the government and commercial sector. The government side includes port state control/contracting government authorities, port authorities, customs and immigration, border control, national/local law enforcement, military, and other government agencies, including environmental, tax, health, and safety. The commercial side includes a wide range of cargo terminal operators (regulated and unregulated), shipping companies, shipping agents, logistics providers, freight forwarders, rail and road operators, warehouse operators, ships chandlers, stevedoring companies, ship repair and maintenance companies, utility companies, oil/gas and related companies, telecommunications companies, and assorted specialized service/consulting firms.

Cyber stakeholders within a maritime organization encompass all administrative and operations employees who access digital assets in order to create, access, process, store, or transmit electronic data. This also includes boards of directors, investors, commissioners, partners, vendors, customers, all government stakeholders, and other individuals who are involved in such data exchanges, such as:

- Chief Operating Officers,
- Chief Technology Officers,
- Chief Security Officers,
- Port Facility Security Officers, and
- Directors of departments such as cargo operations, contracts and vendor management, IT, legal, health and safety, and training.

Even more, it also extends beyond these immediate stakeholders to their personal relationships, who often communicate with, transmit data to, or receive information from the maritime organization stakeholders.


Shareholders, PE, Partners, Shipowners
Board of Directors
Business Leaders (CEOs, MDs)
Risk Leadership (Counsel, Risk Mgr.)
Security Leadership
Security Practioners
Evaluate and Fund Risk
(In terms of investment decisions)
Evaluate and Fund Risk
(Minimize losses; support / protect shareholder equity)
Manage Risk
(Profit and loss / balance sheet)
Identify, Prevent, Accept, and Transfer Risk
(Insurance; agreements and contracts in terms of and risk to profit and loss and balance sheet)
Validate Risk, Allocate Resources
(In terms of cyber risk to operations and profit and loss)
Communicate Needs, Solutions
(In terms of cyber risk to operations that supports cash flow and profit and loss)

4.3 Create a cybersecurity steering committee

Once the maritime organization has defined its cyber stakeholders, it should establish a CSC. The role of the CSC is to oversee and coordinate organization-wide initiatives intended to reduce cyber risk. The CSC should help lead the organization's cyber risk management strategy, ensure coordination in its implementation, consolidate authority, reduce the potential for duplication in security spending, control and oversee complex investments and/or infrastructures, streamline cross-functional communications, and drive organizational cybersecurity cultural change. The CSC should be responsible for continuously engaging on the identification, assessment, and mitigation of vulnerabilities; responding to and recovering from incidents; and drafting, implementing, and updating policies and procedures. Establishing a CSC enables the organization to optimize budgeting and procurement activities, obtain and drive consensus, assign authorities and institute accountability, and serves as the primary driver information sharing and cross-functional engagement.

The CSC should include senior-level stakeholders from across all operational functions of the maritime organization. A multi-disciplinary team with a variety of perspectives, knowledge, and experience will be best able to characterize vulnerabilities, recognize consequences, and identify solutions. Ideally, a maritime organization's team will include representatives from security, engineering and operations, IT, industrial health and safety, training, emergency management, administration, finance, legal, human resources, and risk management/compliance, among others. In some cases, representatives from critical partners, such as a port facility tenant or outsourced service provider (such as IT or security), may also be involved.

4.3.1 Strategies for driving change

A World Economic Forum study in 2014 found that the single greatest driver of organizational cybersecurity capability (and thus resilience) was executive engagement. This was validated regardless of organizational size, sector, and allocated resources[51]. Thus, in addition to defining stakeholders and establishing a CSC, maritime organization leaders should be actively involved in their organizations' cyber risk management activities. Important considerations for maritime organization leaders include:

- **Engaging in cyber risk management decision-making processes.** Maritime leaders can help their organizations determine what is at cyber risk, organizational cyber risk tolerances, and the organization's cyber risk management priorities, considering tradeoffs among risk acceptance, avoidance, mitigation, and transfer (insurance).

- **Driving cyber risk awareness and engagement across all organizational functional areas.** Maritime leaders can ensure that all functional areas of the organization, including operations, legal, contracts, procurement, sales/marketing, public relations, administration, and finance, are aware of and engaged in cyber risk management activities.

- **Changing organizational behaviors.** Maritime leaders can demonstrate the importance of cyber-aware behavior by highlighting the importance of cyber awareness training and cyber awareness campaigns. For example, they can emphasize the importance of cyber-responsible email use.

- **Implementing governance and accountability.** Maritime leaders can actively support efforts to formally include cybersecurity responsibilities in all roles, define appropriate authorities, and institute defined reporting procedures to track progress against business objectives.

- **Budgeting for sustained cyber risk management.** Many organizations include their security budgets into other cost centers[52]. Maritime leaders can establish dedicated budgets for cyber risk management, including both capital expenditures and recurring operational expenditures.

4.4 Organization-wide baseline capability assessment

After defining its universe of cyber stakeholders and establishing a CSC, it is important for maritime organizations to understand their existing cyber risk management capabilities. This understanding will enable a considered approach to determine appropriate steps to improve current cyber risk management capabilities. To gain this understanding, maritime organizations should perform an organization-wide baseline cybersecurity capability assessment. This assessment will help maritime organizations understand their ability to manage and mitigate cyber risk and determine the steps required to implement improvements or measure progress over time.

Conducting a cybersecurity capability assessment will enable maritime organizations to review the processes, personnel, and technologies that comprise its cyber risk management and cybersecurity posture. By performing this assessment, maritime organizations will be better able to identify and analyze cybersecurity capability gaps and understand the most effective and efficient allocation of resources for enhancing its existing cybersecurity capabilities. This assessment should cover topics such as:

- Governance framework, including the maritime organization's leadership engagement, cyber risk management policies, and cyber threat reporting.

- Technological footprint, including all corporate networks across headquarters, branch offices, satellite facilities, and subsidiaries/joint ventures, as well as all network and digitally enabled platforms, critical control systems, and other operational technologies that support day-to-day operations, such as cargo handling, fuel storage and transport, and warehousing and logistics support.

- Critical partner and supply chain relationships and dependencies, including vendor management programs, incorporation of cyber incident notification requirements, and policies for sharing cyber information with important third parties.

- Incident response practices, including documented plans, relationships with third parties who will assist with incident response, and training, drills, and exercises.

A maritime organization's understanding of its current cybersecurity capabilities and gaps will inform the development of a cybersecurity risk management strategy and for implementing and sustaining the supporting plan over time. This strategy and implementing plan are discussed in the next section.

4.5 Cybersecurity strategy and implementing plan

After performing its initial cybersecurity capability assessment, a maritime organization can begin to develop its cybersecurity strategy and implementing plan.

4.5.1 Cybersecurity strategy

A cybersecurity strategy contains goals for maturing internal cybersecurity capabilities across both administrative and operational environments, and an overview of initiatives that advance organization-wide cybersecurity, such as investment planning for technology upgrades and employee training initiatives. A cybersecurity strategy should also incorporate regulatory requirements, where appropriate (see Section 3.0).

It is essential that the cybersecurity strategy align with the maritime organization's overall operational strategy. Maritime organizations should specifically consider its performance objectives that require complex OT-enabled activities, such as terminal operations, cargo handling, fuel storage and transport, and warehousing and logistics support. Important considerations include:

- **Understanding what the organization should protect.** This should include critical assets and data across all administrative and operational environments. For example, a container port might prioritize its ship-to-shore cranes and system that manages yard operations, while a liquid bulk terminal might prioritize storage tanks and pipelines and the systems that operate those assets. Maritime organizations should also determine what critical information resides in their systems, such as crew or passenger data and commercially sensitive data.

- **Understanding the organization's risk appetite.** This will vary depending on factors such as a maritime organization's industry, size, objectives, and financial situation.

- **Understanding the organization's threat landscape.** This includes understanding a maritime organization's customers, products, competitors, and potential attacker motivations. Identifying what benefits an attacker could derive from a cyber attack on a specific maritime organization is also important (see Section 2.3.2 for examples of cyber attacks on maritime organizations).

4.5.2 Cybersecurity plan

Once a maritime organization has developed its cybersecurity strategy, it can then craft a plan for implementing that cybersecurity strategy. Developing an implementation plan should include at least the following steps:

- **Select a framework around which to build a cybersecurity plan.** Options include the frameworks described in Section 3.3, including NIST CSF, ISO/IEC 27001, and CIS Controls. These frameworks are designed to improve cybersecurity risk management in organizations in any sector or community and are applicable to maritime organizations. These frameworks enable organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.

- **Identify all hardware, software, equipment, platforms, users, and key dependencies**. Assets specific to maritime organizations can include systems for cargo management, terminal operations, security monitoring, vessel traffic management, emergency management, industrial controls, communications, fuel transfer/storage, and environmental monitoring.

- **Understand consequences to critical assets of cyber events.** Due to the interconnectedness of maritime organizations specifically and the maritime industry generally, cyber events in maritime organizations can cross systems and operational areas. For instance, a cyber event in a port's ERP could migrate to a connected TOS and then migrate to a shipping line's system that connects to the TOS, and vice versa.

- **Plan for the provision of cyber awareness training to all personnel**. Because the vast majority of data breaches are caused by human error, people are often the primary targets of cyber attacks[53]. Accordingly, any cybersecurity plan should account for the need to continuously train all personnel on cyber risk awareness (see Section 5.2.1).

- **Continuously re-assess, test, and use feedback loops.** Continuous reassessment of the cybersecurity plan will enable a maritime organization to refine its cybersecurity plan to align with evolving regulations and standards, responses to and recovery from incidents, and results from training and exercises. This will enable the organization to continue to improve its overall cybersecurity capability maturity and ability to manage and mitigate cyber risk.

5.0 BEST PRACTICES

5.1 Governance/policy best practices

As discussed in the cybersecurity strategy and plan in Section 4.3, all maritime organizations should develop and maintain a set of clearly articulated policies to safeguard sensitive data, protect their reputation, and encourage the development of a cyber-aware culture. Below is a comprehensive summary of the elements that should be considered in formulating such a strategy and plan; these guidelines have application to maritime facilities throughout the Western Hemisphere.

5.1.1 Data security

Maritime organizations generate, receive, process, store, and transmit a significant amount of information, including port community stakeholder, customer, and partner information; banking and payment information; personal records; contract details; cargo and manifest data; and security system data. A maritime organization should understand what critical data it has, know where that critical data is located, and ensure that the critical data is protected. As mentioned in Section 2.1.2, maritime organizations should take steps to protect the confidentiality, integrity, and availability of their data and information, as well as comply with relevant laws on data protection:

- **Confidentiality:** Maritime organizations should restrict data and information access only to those with a defined responsibility related to the data and information or with another defined need for such access. Threats to confidentiality can come from both external and internal actors seeking to access, steal, or inappropriately use sensitive information.

- **Integrity:** Maritime organizations should preserve the accuracy of their data and information. This includes protecting data from unauthorized modification or deletion and building capacity to restore accurate data when data integrity is lost.

- **Availability:** Maritime organizations should ensure that data and information can be retrieved when needed. This includes protecting data against loss, destruction, and denial, in particular to data that is sensitive or critical to operations.

Steps to preserve data and information confidentiality, integrity, and availability include:

- **Inventory and classify critical data.** This should include both critical administrative and operational data. For maritime organizations, critical administrative data can include customer information, payment information, employee information, and intellectual property. Critical operational data can include financial records, cargo characteristics, vessel loading data, and passenger manifests. Maritime organizations should know where both types of critical data are located on their networks and have a documented accounting of those locations. Finally, maritime organizations should consider developing and publishing on its website a privacy policy that states how it collects, handles, and processes data of its customers, partners, vendors, and other third parties.

- **Control access to data.** Maritime organizations should control access to data according to the data's sensitivity. Once the data has been classified, a maritime organization can develop access privileges and rights based on roles and responsibilities. In general, certain information should only be accessed by individuals who have an explicit need to do so. For instance, while a terminal operations supervisor might require access to cargo data, a human resources manager should not receive such access.

- **Protect data.** In addition to the administrative controls and procedures that regulate access rights, technical safeguards are also essential for protecting data. Two key mechanisms for data protection are the user identification/password combination and encryption. Maritime organizations should strongly consider encrypting critical administrative and operational data.

- **Back up data.** If a maritime organization's data is compromised, stolen, or destroyed, or even accidentally erased, a backup copy will help a maritime organization recover and return to normal operations. Maritime organizations should develop a backup policy that identifies the data that requires backup, defines the frequency of backup, and identifies where backups are stored. All maritime organizations, but in particular those in a geographic region prone to natural disasters, should consider backing up data to a remote, secure data center.

- **Plan for data loss.** Maritime organizations should have contingency plans that they update periodically to plan for the unexpected loss, disruption, or destruction of critical data. Contingency plans should include processes for incident reporting; alerting customers, employees, and others whose data might be affected by a breach; and how the organization will conduct critical operations, such as cargo handling and fuel storage and transportation, when temporarily unable to access critical data.

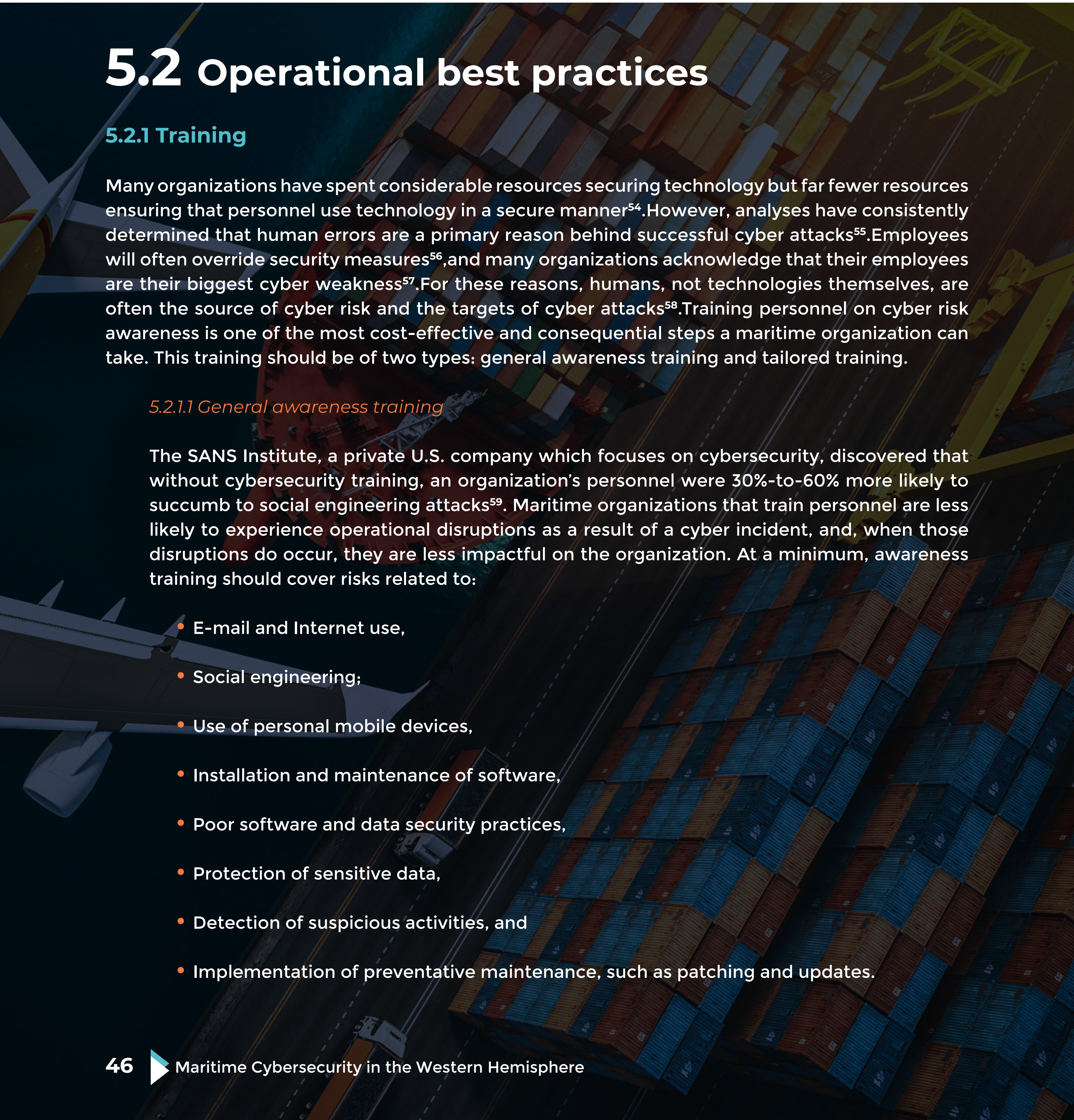
5.1.2 Technology policies

In addition to handling a considerable amount of data, maritime organizations use a significant number of technologies in their operations. Accordingly, they should establish clear policies governing their personnel's use of technology. Key policies include:

- **Acceptable use policy.** Maritime organizations should establish a policy that defines the practices and restrictions that users must agree to in order to access organizational networks and the Internet on organizational assets. This policy should allow personnel the necessary flexibility to perform their assigned duties while still defining rules of conduct for online behavior and establishing boundaries to protect the organization. With the growing use of mobile devices in maritime organizations, including cellular phones, tablets, and RFID scanners, maritime organizations should consider establishing a policy specific to the acceptable use of mobile devices.

- **Personal device policy.** Some maritime organizations, particularly medium and small maritime organizations, might allow personnel to use their personal devices for their assigned duties. While this enables the organization to save on purchasing and replacing technology, it also creates security risks. Maritime organizations that allow personnel to use their personal devices for their assigned duties should have a personal device policy that establishes minimum required security controls, ownership of data, and organizational rights for altering the device and remote wiping of data.

- **Social media policy.** Social media can be useful for maritime organizations that want to promote their activities and communicate with clients, partners, and vendors. However, because cyber attackers frequently use social media outlets to obtain information that can inform social engineering efforts, maritime organizations should develop a social media policy. The policy should include guidance about when staff may reveal organization-specific information or activities on social media, rules of behavior for staff using social media for personal reasons, and guidance regarding the use of unique passwords for organizational social media accounts.



5.2 Operational best practices

5.2.1 Training

Many organizations have spent considerable resources securing technology but far fewer resources ensuring that personnel use technology in a secure manner[54].However, analyses have consistently determined that human errors are a primary reason behind successful cyber attacks[55].Employees will often override security measures[56],and many organizations acknowledge that their employees are their biggest cyber weakness[57].For these reasons, humans, not technologies themselves, are often the source of cyber risk and the targets of cyber attacks[58].Training personnel on cyber risk awareness is one of the most cost-effective and consequential steps a maritime organization can take. This training should be of two types: general awareness training and tailored training.

5.2.1.1 General awareness training

The SANS Institute, a private U.S. company which focuses on cybersecurity, discovered that without cybersecurity training, an organization's personnel were 30%-to-60% more likely to succumb to social engineering attacks[59]. Maritime organizations that train personnel are less likely to experience operational disruptions as a result of a cyber incident, and, when those disruptions do occur, they are less impactful on the organization. At a minimum, awareness training should cover risks related to:

- E-mail and Internet use,
- Social engineering;
- Use of personal mobile devices,
- Installation and maintenance of software,
- Poor software and data security practices,
- Protection of sensitive data,
- Detection of suspicious activities, and
- Implementation of preventative maintenance, such as patching and updates.

In addition, maritime organizations' general cyber awareness training program should consider the following:

- **Require training for all personnel.** Maritime organizations should require training for all personnel, including all senior executives, board members, administrative staff, terminal and other operations staff, vendors working onsite, and any other external stakeholders accessing the organization's IT or OT systems. Due to the variety of different IT and OT systems administrative and operations personnel will use as part of their duties, maritime organizations should consider tailoring this awareness training to their specific operating environments.

- **Use a variety of training techniques.** Maritime organizations should remember that different personnel learn in different ways. Hence, organizations should implement several techniques should be implemented such as classroom-style training sessions, security awareness websites, helpful hints via e-mail, and posters. These techniques can help personnel understand organizational security directives, policies, procedures, and best practices.

- **Ensure that training is recurring.** Due to cyber threats constant evolution as attackers devise new methodologies, modify tools, and design tactics to compromise secure networks, cybersecurity awareness training should not be a check-the-box, annual exercise. Training should be both relevant and recurring for all maritime personnel. This will help the organization establish and sustain a stronger defense against known and emerging cyber threats.

5.2.1.2 Tailored training

In addition to general cyber awareness training for all staff, it is important that technical staff receives cyber-focused training that is specific to the maritime organization's characteristics and environment. While the type of training will vary by the environment as well as individual technical staff members' skills, maritime organizations should consider ensuring that the training includes:

- Special consideration for the organization's most important systems and networks. This should include systems involved in critical operations, like cargo handling, and in critical administrative tasks, like handling sensitive client data.

- Understanding IT-OT convergence and complexities particular to the maritime organization. Maritime organizations are increasingly integrating their IT systems and OT systems, and technical staff should understand where that integration occurs and be prepared to take steps to mitigate the cyber risks related to that interconnection.

- Updated to reflect the evolving cyber threat environment relevant to maritime organizations. Cyber threats are constantly evolving, and technical staff should receive training regarding threats and vulnerabilities based on cyber threat intelligence and related information (see Sections 5.2.6 and 5.2.7).

- Information relevant to port facility security officers and other security personnel. PFSO and other security personnel should receive training about the ways that digital security assets and platforms, such as networked closed-circuit television and card access systems, may be connected to other organizational assets and the risks those connections pose. They should also understand the need to physically secure areas with important digital assets, such as server rooms.

5.2.2 Managing cyber-physical access control

Attackers can exploit a weakness in one area of an organization's security posture to gain legitimate access to another area, such as in the Port of Antwerp attack (see Section 2.3.2.1). Due to this integrated nature of cyber and physical risk, it is critical that maritime organizations consider an integrated approach to planning and implementing digitalized security for their operating environments. Maritime organizations should carefully assess their security capabilities, processes, and internal operations for potential weaknesses and seek to understand how a weakness in one area of the operation might serve as an entry point and subsequent stepping-stone to more sensitive areas. Maritime organizations should consider:

- **Ensure network segmentation.** Network segmentation best practices suggest that IT- and OT-based systems be kept separate. Efficiency gains can at times outweigh this consideration, but maritime organizations should analyze the risks in linking IT-enabled security systems with critical OT-enabled systems.
- **Invest in integrated security.** These investments in integrated security should align with compliance needs, such as those required by the ISPS Code (see next bullet), as well as accommodate the maritime industry's ongoing technological evolution.
- **Update existing PFSPs.** Maritime organizations subject to ISPS Code requirements must update their existing PFSPs if they deploy new integrated cyber-physical capabilities that result in material changes to the PFSP.
- **Managing access to assets.** Gaining physical access to areas with important digital assets, such as server rooms, allows logical access to a digital asset. Maritime organizations should physically secure sensitive and restricted areas or tangible assets to limit that access.

5.2.3 Email security

Email is a critical tool for a maritime organization's daily functions. Although there are inherent risks to using email, the benefits far outweigh the negative potential consequences. Nevertheless, to protect data, maritime organizations should draft basic policies, apply necessary tools, and implement appropriate controls to support email use. To ensure the proper and safe use of email, maritime organizations should consider:

- **Create an email usage policy.** An effective email usage policy can encourage positive, productive communications while protecting the organization from cybersecurity breaches. This policy should clearly define appropriate usage parameters and expectations for all staff, including reminders that users should:

  - Be suspicious of messages from unknown senders,

  - Never open attachments from unknown senders,

  - Never click on links in emails, and

  - Verify authenticity of requests for sensitive information before sending such information.

  This is of particular use for maritime organizations whose staff operate in many different languages, including languages of which they are not native speakers.

- **Create an email retention policy.** All emails sent from organization email addresses should be the organization's property. These emails often include information that is valuable to and about the organization. Accordingly, maritime organizations should consider how they manage and store emails on internal systems and their backup and data recovery. Maritime organizations should also consider legal and regulatory requirements, such as those related to data privacy (discussed in Section 3.4).

- **Implement anti-spam measures.** Email has become an effective means for deploying a cyber attack, with over 90 percent of all attacks on enterprise networks resulting from successful phishing or spear phishing[60]. Spam email filtering is an import element of an email security strategy, and maritime organizations, many of which conduct critical business via email, should enable automatic updates to their email applications, email filters, and anti-virus software. Specifically, three increasingly important anti-spam measures are designed to enhance fidelity and trust between senders and recipients include: Sender Policy Framework (SPF), email signing (also referred to as DomainKeys Identified Mail, or DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which uses both SPF and DKIM. As a best practice, administrators should at least set up SPF and DKIM to improve email delivery and establish higher assurance communications. Although less widely adopted, maritime organizations with SPF and DKIM in place can consider implementing DMARC.

- **Train staff on safe email use.** Most staff in maritime organizations will use email as a means of communication for business purposes. Maritime organizations should regularly train staff on safe email use and how to identify potential cyber risks, inappropriate use, and know whom to contact in the event of an incident. This training should align with the email usage policy discussed in this section.

5.2.4 Protecting against social engineering

Many email attacks involve tricking unsuspecting persons into bypassing normal security controls and divulging sensitive or confidential information or unwittingly providing access to organization networks. This is called social engineering, which can take many forms, including:

- **Phishing:** a form of communication that appears to originate from either a legitimate or from a trusted source but is instead a customized deception intended to convince the recipient into clicking on an embedded hyperlink or opening or downloading an attached file.

- **Spear-phishing:** a type of phishing that is customized specifically for the intended recipient, usually by using specific commercial brands or incorporating affinity groups or social causes in which the target maintains loyalty or sympathy.

- **Business email compromise:** the use of email fraud to attack an organization and achieve specific outcomes that negatively affect that organization.

- **Pretexting:** a phishing attack in which the attacker poses as a trusted agent with perceived authorities or responsibilities.

- **Whaling:** a type of spear-phishing attack carried out against senior-level executives, key decision makers, board members, or commissioners.

- **Tailgating:** a situation when an unauthorized person follows an authorized person into a secure location, such as a restricted area within a terminal facility, to obtain physical access to operational technologies (such as cranes, cargo loading operations, fuel/bunkering controls), information-based systems (such as security operations and vessel traffic monitoring and information systems), or protected property (such as cargo warehouses).

- **Vishing:** a combination of voice and phishing, in which the attacker uses the telephone to gain access to sensitive information or systems.

- **Baiting:** a form of leaving removable media devices in heavily trafficked areas of a targeted organization or conference so that a user will later insert it into a workstation, unknowingly installing malware on the system and network.

- **Email spoofing:** an electronic counterfeit in which the email address in the "From" field is not from the actual sender.

- **Water-holing:** a strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware.

Social engineering exploits the victim's desire to trust or be helpful and deceives the victim into revealing information or providing network or system access that the victim would not otherwise do. Social engineers take advantage of human tendencies, such as returning favors, socially conforming, obeying authority[61].To protect against social engineering, maritime organizations should:

- **Train staff** to be aware of common types of social engineering attacks, the type of information they send over email or the telephone, and being sensitive to communications with a sense of pressure or urgency,

- Have a **suspicious activity reporting policy** and a mechanism for reporting suspicious activity, such as a phone hotline and dedicated email address to which personnel can forward suspected social engineering emails,

- Perform **social engineering tests** to assess and review the effectiveness of social engineering training,

- Use **reputable anti-virus software**, and

- Perform **regular email backup**.

5.2.5 Access control

Maritime organizations interact with a diverse range of employees, contractors, partners, and customers. To ensure the confidentiality, integrity, and availability of their data, maritime organizations should establish digital access control policies that define who can and cannot access certain assets and data (see Section 5.2.2 for a description of cyber-physical access control). These policies should include authentication, which is the confirmation that a user is who he or she claims to be, and authorization, which is the level of access a user is granted. These policies should consider:

- **Identity and password management,** including enforcing unique identification credentials for each user, requiring users to change their passwords at the first logon and thereafter to regularly change passwords and maintaining a record of previously used passwords to prevent re-use.

- **Two-factor authentication,** which involves granting access to a user only after the user has presented two pieces of information in combination, such as a password and a one-time code sent to an authentication application (recommended) or via Short Message Service (SMS) to that user's cell phone.

- **Technical steps,** including logging all transactions, requiring digital signature use, filtering all outgoing traffic to prevent spoofing and routing of all traffic for Internet access services through a limited number of controlled security gateways.

- **Different privileges for different users,** including clearly defined user roles and access privileges and limitations on privileges for certain users.

5.2.6 Cyber threat information collection and analysis

Maritime organizations should collect and analyze information about cyber threats and share information about threats and successful attacks.

Maritime organizations can be attractive targets for cyber attackers due to the extensive amount of data and information that they create, access, process, store, or transmit. As a result, it is important that maritime organizations have access to information about cyber threats and threat actors to better prepare themselves and others to mitigate potential cyber attacks. Cyber threat intelligence can include open-source intelligence, social media intelligence, human intelligence, technical intelligence, and intelligence from the deep or dark web. To ensure that they collect and analyze cyber threat information, maritime organizations should consider:

- **Employing external real-time monitoring services for potential vulnerabilities and threats.** Numerous commercial monitoring services are available to maritime organizations. These monitoring services can identify potential cyber threats, such as new malware and newly identified software vulnerabilities, within maritime organizations' environments. This visibility is important in efforts to prevent cyber attacks before they occur.
- **Seeking actionable information from cyber threat intelligence providers.** This information should include real-time insights into which common IT/OT technologies are of interest to threat actors and potential remediation recommendations, such as patching and upgrades, to avoid being a target for cyber attacks, preventing cyber attacks, and minimizing the effects of cyber attacks when they do occur. The Maritime Transportation Systems Information Sharing and Analysis Center (MTS-ISAC) (https://www.mtsisac.org) could be an ideal industry-specific mechanism for maritime organizations.

5.2.7 Information sharing

When a cyber incident occurs, sharing information about it internally with organizational personnel, as well as externally with public and/or private sector partners, can help a maritime organization elevate its level of cyber readiness and more proactively anticipate cyber risks and subsequent cyber breach mitigation.

Internal information sharing

Maritime organizations should establish guidance for how it communicates information about cyber threats to all members of the entire organization. That guidance should:

- Identify who in the organization is responsible for coordinating cyber information-sharing activities, including threat information and alert notifications.

- Document the processes for communications protocols.

- Define specific protocols for sharing sensitive information, which includes data classification and escalation and alerting criteria.

- Establish information-sharing criteria to characterize, classify, and prioritize the analysis and sharing of specific data, including personnel information or cargo information, on a need-to-know basis.

External information sharing

Maritime organizations should establish guidance for communicating cyber information to stakeholders outside of the organization. That guidance should identify who in the organization is responsible for sharing cyber information with external parties with whom the organization is required to share information and external parties with whom the organization should or might want to share information. External parties with whom the organization might be required to share information could include port state officials and other national bodies, which varies among countries. The organization might decide to share cyber information with other external parties, such as the MTS-ISAC; local security operations centers; and, when appropriate, bodies that support cyber incident response and recovery efforts within that country, such as national Computer Emergency Response Teams (CERT)[62]. Finally, it is important for maritime organizations to establish official information-exchange protocols, such as non-disclosure agreements and memoranda of understanding, and secure communication channels with its information-sharing partners.

5.2.8 Network security, vulnerability management, and situational awareness

Most maritime organizations manage complex, integrated IT/OT environments. Their IT environments are service-focused, support almost every aspect of an organization, including internal business processes and communications, as well as OT-based activities. Therefore, it is important that maritime organizations consider:

- **Understanding threats and vulnerabilities.** Vulnerability and threat management is about both the application of technology and continuous engagement and monitoring. As with any organization, maritime organizations should use firewalls, intrusion detection systems, and intrusion prevention systems as the foundational technical elements for protecting their operating environments. They should also conduct penetration tests to ascertain where the organization might have perimeter gaps or vulnerabilities. Finally, they should consider employing a security information and event management system for an effective overview and real-time correlation capacity of possible events and threats that could affect the platforms.

- **Application security.** As maritime organizations adopt new applications, and in particular mobile applications, it is important to ensure application security. This includes understanding what data reside or could reside in those applications, establishing an effective application lifecycle process, and scanning and testing before and after deployment.

- **Patch management.** Patching is the process of implementing fixes for vulnerabilities in software and applications. Due to the fact that patching occurs for nearly all digitally enabled assets and systems, the number of patches an organization needs to implement can be significant. As such, maritime organizations that employ a large number of IT/OT systems should implement a disciplined process for determining patch management requirements and ensuring that needed patches are installed and implemented. Patch management should be part of a continuous process designed to reduce vulnerabilities.

- **Cloud security.** Cloud connectivity provides a platform for automation[63], operating systems that support IoT platforms[64], collaborative planning, and real-time information sharing[65], which can produce significant operational efficiency gains. Before employing any cloud-based services, maritime organizations should consider its cloud-based risk appetite, ensure it manages access to cloud environments with enhanced security measures such as two-factor authentication, and incorporate minimum-security requirements into cloud service contracts.

- **Mobile security.** The increased use of mobile technologies in maritime organizations, such as cell phones, tablets, and RFID scanners, allows cyber attackers an additional entry point through which to access assets and systems. Accordingly, endpoint security now involves those smartphones, tablets, and mobile handheld devices (such as RFID scanners) in addition to computers, servers, and connected systems. To account for this evolution, maritime organizations should consider implementing mobile security software, applying encryption to data on mobile devices, and establishing a reporting procedure for lost or stolen mobile devices. In addition, maritime organizations that permit the use of personal devices should consider a personal device policy (see Section 5.1.2), whitelisting approved applications for accessing organizational data, and minimum security configurations and standards for mobile devices.

- **Storage and data loss prevention.** As most maritime organizations will suffer successful cyber attacks, they should ensure that their data are stored and backed up appropriately and that critical IT and OT systems can be restored quickly. For restoring data, this could include backing up all critical data, testing backups, ensuring that backups are stored at remote facilities (particularly important for maritime organizations in regions prone to natural disasters), and encrypting all data in transit as well as stored data. For restoring systems, this could include establishing redundancies for critical systems, training staff to engage in manual systems, and performing regular exercises of recovery plans.

5.2.9 Supply chain and third-party management

Maritime organizations are key players in the complex global logistics environment and rely on digitally enabled and increasingly integrated systems that exchange data with a large number of external parties. The integration of this wide variety of systems means that cyber attackers can compromise customers', partners', and vendors' systems in order to exploit a maritime organization's data for illicit purposes. This reinforces the need for maritime organizations to ensure that their customers, vendors, and other third parties with whom they exchange information take appropriate measures to minimize their vulnerability to cyber attacks. To manage this supply chain and third-party cyber risk maritime organizations should consider the following measures:

- **Understand data flows to and from third parties.** Maritime organizations should understand what data they transmit to and receive from which third parties. In particular, maritime organizations should identify the sensitive data, such as confidential contract details, sensitive security information, cargo data, and personnel information that it exchanges with parties (see Section 5.1.1).

- **Implement a third-party management program.** This should include defining roles and responsibilities for personnel working with third parties. The program should also include a policy for managing important third parties that details third-party classification, who within the organization is responsible for managing each third party, and a tiered ranking of security controls for each third party. In addition, this program should define security questions and risk assessment controls for supply chain vendor evaluation.

- **Review and update procurement contracts.** These contracts should include clauses defining cybersecurity standards and measures, including governance, physical security, personnel security, information security, risk management plans, processes and procedures, quality control, and cyber breach response requirements. Maritime organizations should also consider clauses, such as indemnification and a requirement for cyber liability coverage, that reduce the maritime organization's financial risk if a vendor's practices result in a cyber incident.

- **Define training requirements for third parties.** All third parties, including vendors and contractors, should complete cyber training prior to arriving at the organization's facilities, in particular if the third-party personnel will access a critical digitally enabled asset or any key IT/OT asset connected to a network.

5.3 Cyber incident response preparation

In the modern, digital world, it is almost a certainty that a maritime organization will suffer a cyber attack that can disrupt or degrade operations such as cargo handling, damage equipment and assets such as cranes and TOS, and harm reputations. Due to the potential for significant tangible and intangible costs, maritime organizations should be prepared to respond to, recover from, and remediate cyber attacks. To establish and maintain this capability, maritime organizations should consider creating (or updating) the following[66]:

- A cyber incident response plan, which describes how to prepare for, detect, and respond to cyber incidents. This can be incorporated as a supplement to the organization's existing, non-cyber-specific incident response plan.

- A continuity of operations plan, which often includes a business continuity plan and discusses how the organization can maintain services during and immediately after an incident

- Disaster recovery plan, which focuses on transitioning from alternative processes back to regular processes after an incident is resolved.

5.3.1 Create an incident response plan

The maritime organization should have a cyber incident response plan. Effective cyber response plans help to contain the impact of an incident, identify and analyze the incident in order to put in place necessary countermeasures, restore normal functions of the affected system(s), and prevent the recurrence of similar or identical attacks. A maritime organization's cyber incident response plan should account for the following:

- Organize a cyber incident response team. This should include personnel who can restore system operations, investigate the reasons for a network compromise or other cyber incident, and take corrective measures to mitigate the risk that a similar attack could occur again. Importantly, this should also include operational personnel, such as those involved in terminal operations, who can assist with the implementation of contingency plans for when cyber attacks disrupt critical OT systems, such as cranes and pipelines.

- Define communication protocols to identify an incident. This should define alerting and escalation procedures, which can be supported by an internal help desk or ticket management system so that the organization can identify, triage, and escalate potential incidents. These protocols should account for the criticality of certain assets and systems, such as cargo handling and fuel handling and storage, and ensure that potential incidents involving critical systems are escalated quickly.

- Define lines of communication among responding personnel and with the public. This should include identification of the person responsible for making real-time decisions during the incident response. For external communications, the plan should identify external parties with whom the organization is required to communicate (such as port state control officials and National Response Teams) and external parties with whom the organization should communicate (such as customers and the press) and how the organization will communicate with those parties.

- Identify external resources important to a cyber incident response. External resources such as forensic analysis, legal counsel, and public relations specialists should be involved in most cyber incident response actions. Identifying those resources in a plan in advance of an incident enables the organization to call on those resources as quickly as possible after an incident (see Section 5.3.3).

- Require periodic testing and exercises. Testing and exercising cyber incident response plans ensure that personnel are familiar with the actions they will take in the aftermath of a cyber incident response and that the organization can identify any cyber incident response gaps before an incident occurs. It is important to update a cyber incident response plan based on lessons learned from drills and exercises. For maritime organizations that must comply with the ISPS Code, incident response plan testing can occur as part of ISPS Code-mandated drills and exercises.

- Establish response and recovery actions. These should include:

    - An initial assessment of the breach, identifying which IT/OT assets, systems, and/or data are affected; an evaluation of the effects on data integrity; and a determination of threat persistence and, if so, which other assets and systems may be at risk.

    - Mitigation activities, including cleaning, recovering, and restoring affected assets and systems; recovering and restoring data by removing threats and correcting software compromises; and restoring operational services as soon as possible.

    - Post-incident analysis, including investigating the cause of the incident; determining the operational impact to the affected IT/OT assets and systems; understanding financial, regulatory, legal, and reputational consequences; and developing a set of lessons learned.

5.3.2 Continuity of operations and disaster recovery planning

In the immediate aftermath of a cyber incident, it is important to have plans to maintain minimally acceptable level of services and functions (continuity of operations), and then to restore normal services and functions (disaster recovery) as soon as possible. Continuity of operations plans often (but not always) assume the form of a business continuity plan. Cybersecurity considerations for continuity of operations can include:

- Defined authorities, processes, procedures, and resources required for the organization to recover from a cyber incident, including emergency operations locations, data backup sources, and emergency IT administration rights.

- Identified requirements for sustaining minimum IT/OT-based operations during and after a cyber incident.

- Determinations of what IT/OT assets and systems should be prioritized for restoration during and after a cyber incident.

Disaster recovery plans focus on how the organization can return to normal operations as quickly as possible following a cyber incident. In disaster recovery plans maritime organizations should:

- Understand what data the organization has, where the organization stores the data, and how critical the data is to the organization's operations.

- Develop a prioritized inventory of IT/OT assets and systems.

- Establish recovery time objectives and recovery point objectives for critical systems and services, such as cargo handling and fuel storage and transfer.

- Define procedures to protect sensitive data during the recovery process.

5.3.3 Develop relationships with third parties who will assist with incident response and recovery

Very few organizations can adequately respond to and recover from a cyber incident without external assistance. As part of their cyber incident response and recovery planning, maritime organizations should identify external parties who might need to assist with cyber incident response and recovery activities. These can include:

- **Forensic analysts.** Experts with specialized skills in cyber technical analysis can be critical to effective cyber incident investigation and remediation. Commercial providers of these skills increasingly offer zero-down retainers that will provide maritime organizations with cost-effective access to this expertise.

- **Legal counsel.** A cyber incident can affect compliance with national and local laws, including data privacy laws (see Section 4.4), and have legal consequences, including potential legal liability. Specialized legal counsel with specific knowledge should be available to assist with cyber incident response.

- **Public relations specialists.** Most cyber incidents affect external parties. Thus, communications and public relations experts can help maritime organizations ensure that their wide array of stakeholders, including customers, partners, vendors, regulators, and members of the general public, are appropriately informed of cyber incident information.

- **Insurance.** Transferring some cyber risk through insurance is an increasingly common risk mitigation tool[67].Maritime organizations should consider their most likely cyber loss scenarios, such as the compromise of sensitive customer information or disruption to cargo-handling operations. Taking into consideration those scenarios, questions to consider include:

  - Do current policies cover the loss scenarios?

  - If there are gaps/exclusions, what are they?

  - Are all cyber coverages affirmative? Are any of them silent?

  - How would existing policies respond to a cyber incident?

  - Does the insurer offer all the appropriate coverage the organization required?

5.3.4 Perform cyber breach incident response drills and exercises

When cyber incidents do occur, maritime organizations need to be able to implement their cyber incident response, continuity, and disaster response plans as quickly and effectively as possible. Conducting periodic training, drills, and exercises enable maritime organizations to implement those plans effectively and identify gaps in plans before incidents occur.

- **Training.** A maritime organization's personnel who will participate in the response to a cyber incident should be trained in the topic, including understanding processes for recovery procedures, methods for data protection during a cyber incident, and meeting recovery time objectives. These personnel could be from departments as varied as IT, security, and operations.

- **Drills.** Cyber incident response drills enable a cyber incident response team to practice aspects of the response plan. Drills are an effective mechanism for identifying technical gaps or weaknesses and providing opportunities to remediate those gaps and weaknesses.

- **Exercises.** Exercises help test general awareness, validate plans and processes, and assess existing systems and protocols for incident response and recovery. A tabletop exercise simulates a cyber incident and allows participants to gather to discuss simulated procedures and become familiar with various threat scenarios. Exercise scenarios can begin with a cyber incident or include cyber-specific injects to which participants respond. Participants should include members of a maritime organization's cyber incident response team, with particular focus on representation from the organization's various IT and OT environments.

6.0
CONCLUSION

Maritime transport is crucial to global economic activity and growth. The maritime industry's adoption of digital technologies is likely to continue, and this increase in maritime digitalization and automation brings a corresponding increase in maritime cyber risk, including in the Western Hemisphere. As a consequence of their growing IT and OT complexity, maritime organizations are vulnerable to cyber threats for many reasons, including the fact that they handle a vast amount of commercial data and, as recent incidents indicate, they have become attractive targets for cyber attackers. Yet limited information is available on the scope and consequences of such attacks since private sector actors are often reluctant to highlight vulnerabilities publicly.

Further, the regulation of cyber risk management is in its inception and still evolving both in international bodies and national legislation. Although binding rules could become more prevalent in the future, there are standards, frameworks, and guidance that maritime organization can use as a basis for steps to organize, evaluate, manage, and measure their cyber risk, cybersecurity capabilities, and organizational cyber resilience. To do so, maritime organizations can:

- **Base their cybersecurity strategies and implementation plans upon existing frameworks and standards for critical infrastructure cybersecurity,**
- **Develop key governance and policy documents to guide their organizations and staffs in using systems and data securely,**
- **Employ operational best practices to minimize the cyber risk to their systems and data,**
- **Plan on responding to, recovering from, and remediating cyber attacks when they do occur, and**
- **Share information internally and externally about cyber threats, vulnerabilities, and attacks.**

In the modern, digital world in which maritime organizations operate, cyber risk will be an ongoing challenge. However, is one that maritime organizations that take a considered approach will be able to manage even as international standards and frameworks in this area continue to develop.

REFERENCES

1. The maritime domain is defined as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances.

2. International Maritime Organization. 5 June 2020. Circular Letter. Coronavirus (COVID-19) – Accelerating digitalization of maritime trade and logistics – A call to action. See: http://www.imo.org/en/MediaCentre/HotTopics/Documents/COVID%20CL%204204%20adds/Circular%20Letter%20No.4204-Add.20%20-%20Coronavirus%20(Covid-19)%20-%20Accelerating%20Digitalization%20Of%20Maritime%20Trade.pdf

3. In 2004, OAS member states emphasized the importance of developing a comprehensive strategy for protecting information infrastructure. In 2015, OAS member states issued a declaration on the “Protection of Critical Infrastructure from Emerging Threats” and a “Report on Cybersecurity and Critical Infrastructure in the Americas,” which highlights how governments in the region will need to work with those responsible for critical infrastructure in protecting against attacks on crucial sectors. See: https://documents.trendmicro.com/assets/wp/2015-OAS-TrendMicro-Report-on-Cybersecurity-and-Critical-Infrastructure-in-the-Americas.pdf?_ga=2.70956752.1795230221.1609171841-1428500618.1597249018. Further, in 2018, the OAS, in collaboration with the Microsoft Corporation, issued a report noting the increasing efforts of OAS member states to address cybersecurity concerns with respect to their critical infrastructure. See: https://www.oas.org/es/sms/cicte/cipreport.pdf.

4. Pre-COVID-19 pandemic

5. UNECE. Trade facilitation implementation guide. Port Community Systems. See: http://tfig.unece.org/contents/port-community-systems.htm

6. More information on https://csirtamericas.org/

7. Fintech News. 20 August 2020. “The 2020 cybersecurity stats you need to know.” See: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/

8. The Maritime Executive. 23 June 2020. “Report: Maritime Cyberattacks Have Quadrupled Since February.” See: https://www.maritime-executive.com/article/report-maritime-cyberattacks-have-quadrupled-since-february

9. Hall, Chris. Wapack Labs, Inc. 14 June 2015. “The Daily Show Agenda,” presented at the First Berlin Conference. See: https://www.first.org/resources/papers/conf2015/first_2015_-_hall-_chris_-_daily_show_agenda_20150618_fw.pdf

10. National Infrastructure Advisory Council, Physical/Cyber Convergence Working Group. 16 January 2007. “Final Report and Recommendations by the Council.” See: https://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport.pdf

11. A notable example of cyber attacks with physical consequences was the Stuxnet attack. Stuxnet is a computer worm that was originally designed to target Iran’s nuclear facilities and has since mutated to other industrial and energy producing facilities. The original attack targeted Siemens programmable logic controllers used to automate centrifuges that supported uranium enrichment. It was conveyed across the facility’s unconnected networks (known as an “air gap”) via USB devices and spread through Microsoft Windows computers. Once the worm identified the targeted equipment, it then sent damage-inducing commands to the electro-mechanical equipment, causing the nuclear centrifuges to spin out of control and tear themselves apart. During the attack the worm sent false information to the main controller, thus misleading engineers into a false sense of security that anything was wrong. See: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

12. Verizon Data Breach Digest. 2015. See: https://www.darkreading.com/operations/pirates-ships-and-a-hacked-cms--inside-verizons-breach-investigations/d/d-id/1324474

13. Council on Foreign Relations. “Disruption of operations at Shahid Rajaee Port.” May 2020. See: https://www.cfr.org/cyber-operations/disruption-operations-shahid-rajaee-port

14. United Nations Office on Drugs and Crime. “Combating Transnational Organized Crime Committed at Sea.” Issue Paper. 2013. https://www.unodc.org/documents/organized-crime/GPTOC/Issue_Paper_-_TOC_at_Sea.pdf

15. Riley, Michael and Jordan Robertson. “The Mob’s IT Department.” BusinessWeek. July 2015. See: https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/

[16] Ibid.

[17] IMO. “Just in Time Arrival Guide.” Page xiii. August 2020. See: https://wwwcdn.imo.org/localresources/en/OurWork/PartnershipsProjects/Documents/GIA-just-in-time-hires.pdf

[18] United States Cybersecurity and Infrastructure Agency: https://us-cert.cisa.gov/ncas/alerts/TA17-181A

[19] United Kingdom National Cyber Security Centre: https://www.ncsc.gov.uk/report/weekly-threat-report-28th-july-2017

[20] Australia Minister for Law Enforcement and Cyber Security: https://www.dfat.gov.au/sites/default/files/australia-attributes-notpetya-malware-to-russia.pdf

[21] “Global ransomware attack causes turmoil.” British Broadcasting Corporation. 28 June 2017. See: https://www.bbc.com/news/technology-40416611

[22] Ship Technology. “The ten biggest shipping companies in 2020.” 19 October 2020. See: https://www.ship-technology.com/features/the-ten-biggest-shipping-companies-in-2020/

[23] Lloyd’s List. “Top 10 box port operators.” 1 December 2019. See: https://lloydslist.maritimeintelligence.informa.com/LL1130163/Top-10-box-port-operators-2019

[24] Osborne, Charlie. “NotPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs.” ZDNet. 26 January 2018. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/.

[25] Morley, Hugh R. “US ports building up cyber attack defenses.” Journal of Commerce. 15 December 2017. See: https://www.joc.com/technology/ports-say-they-take-cyberattacks-seriously_20171215.html

[26] Remarks during “Securing a Common Future in Cyberspace.” World Economic Forum. 24 January 2018. See: https://www.youtube.com/watch?v=Tqe3K3D7TnI&feature=emb_logo.

[27] Arghire, Ionut. “NotPetya – Destructive Wiper Disguised as Ransomware.” Security Week. 29 June 2017. See: https://www.securityweek.com/notpetya-destructive-wiper-disguised-ransomware

[28] “Treasury Sanctions Russian Federal Security Service Enablers.” Press Release. United States Department of Treasury. 11 June 2018. See: https://home.treasury.gov/news/press-releases/sm0410

[29] “Russian Military ‘Almost Certainly’ Responsible for Destructive 2017 Cyber Attack.” Press Release. United Kingdom National Cyber Security Centre. 14 February 2018. See: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

[30] Graham, Luke. “NATO-Think-Tank Says a ‘State Actor’ Was Behind the Massive Ransomware Attack and Could Trigger Military Response.” CNBC. 30 June 2017. See: https://www.cnbc.com/2017/06/30/petya-ransomware-attack-nato-says-state-actor-to-blame.html

[31] “Ransomware: Facts, Threats, and Countermeasures.” Blog Post. Center for Internet Security. https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/

[32] “Senzee, Thom. “What Happened in Ransomware Attack on Port of San Diego.” San Diego Reader. 10 April 2019. See: https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/

[33] ““Port of Barcelona Suffers a Cyberattack That Impacted Many of Its Servers.” Cyware. 24 September 2018. See: https://cyware.com/news/port-of-barcelona-suffers-a-cyberattack-that-impacted-many-of-its-servers-5f22c204

[34] Mongelluzzo, Bill. “Cosco’s Pre-Cyber Attack Efforts Protected Network.” 30 July 2018. Journal of Commerce. See: https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html

[35] Osborne, Charlie. “Logistics Giant Toll Group Hit by Ransomware for the Second Time in Three Months.” ZDNet. 6 May 2020. See: https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/

[36] The IMO is a specialized agency of the United Nations (UN) composed of over 170 states in the world that is the global standard-setting authority for the safety, security, and environmental performance of shipping.

[37] IMO. Resolution MSC.428(98). Adopted 16 June 2017. See: http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-%28MSC%29/Documents/MSC.428%2898%29.pdf

[38] “Guidelines on Maritime Cyber Risk Management.” IMO. 5 July 2017. See: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf http://www.imo.org/en/OurWork/Facilitation/docs/FAL%20related%20nonmandatory%20instruments/MSC-FAL.1-Circ.3.pdf

[39] The report “CYBERSECURITY: RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN“ (2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean | Publications (iadb.org)) , a joint work between OAS and IDB, provides information about the maturity level of cybersecurity and a detailed description of national capacities of the countries of Latin America and the Caribbean (LAC) to combat cyberterrorism and ensure safer access to the internet in the region. The study analyzes the cyber maturity of each country in the five dimensions identified in the Cybersecurity Capacity Maturity Model for Nations (CMM): (i) Cybersecurity Policy and Strategy; (ii) Cyberculture and Society; (iii) Cybersecurity Education, Training, and Skills; (iv) Legal and Regulatory Frameworks; and (v) Standards, Organizations, and Technologies.

[40] United States Coast Guard Navigation and Vessel Inspection Circular No. 01-20. 26 February 2020. See: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023.

[41] United States National Maritime Cybersecurity Plan. December 2020. See: https://www.whitehouse.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf

[42] Directive (EU) 2016/1147, Paragraph 13. 6 July 2016. See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[43] Although this document is not intended to address cyber risks specific to vessel operations, the BIMCO Guidelines on Cyber Security Onboard Ships is a useful resource for learning more about standards for vessel cybersecurity. See: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[44] Originally published in 2014, the NIST CSF has since been revised, relying on eight public workshops, multiple comment periods, and inputs from thousands of experts and representatives from many industry sectors.

[45] See https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework(CSF)-ENG.pdf for the Organization of American States Inter-American Committee against Terrorism’s overview of the NIST CSF.

[46] The report “NIST CYBERSECURITY FRAMEWORK: A comprehensive approach to cybersecurity,” published by CICTE/OAS, is a point of reference regarding implementation of the NIST Framework in the Western Hemisphere. See: https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework(CSF)-ENG.pdf.

[47] NIST Cybersecurity Framework International Resources. See: https://www.nist.gov/cyberframework/international-resources.

[48] “Latin America steps up data privacy legislative and enforcement efforts.” Holland & Knight General Data Review. 7 May 2019. See: https://www.hklaw.com/-/media/files/insights/publications/2019/04/latinamericastepsupdataprivacylegislativeandenforcementefforts.pdf?la=en

[49] European Commission, What Does the General Data Protection Regulation (GDPR) Govern? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

[50] European Parliament and Council of European Union (2016) Regulation (EU) 2016/679, Article 83. See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[51] “Risk and Responsibility in a Hyperconnected World.” World Economic Forum. January 2014. See: http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

52. Filkins, Barbara. "IT Security Spending Trends," SANS Institute. February 2016. See: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

53. Kulesa, Patrick. "Driving a cyber-savvy culture to combat cyber threats." Willis Towers Watson. 2017. See: https://www.willistowerswatson.com/-/media/WTW/Insights/2017/07/decode-cyber-cyber-savvy-culture.pdf?modified=20170724185825

54. SANS Institute. "The Rising Era of Awareness Training." 2019. See: https://www.knowbe4.com/hubfs/SANS-Security-Awareness-Report-2019.pdf

55."Effective Cybersecurity Strategy Rests on People, Not Just Technology." Insurance Journal. 1 March 2017. See: https://www.insurancejournal.com/news/national/2017/03/01/443270.htm

56.Bhargava, Rishi. "Human Error, We Meet Again." Security Magazine. 6 December 2018. See: https://www.securitymagazine.com/articles/89664-human-error-we-meet-again

57. "The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable From Within." Blog Post. Kaspersky. See: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

58.Ibid.

59. Lance Spitzner, "Securing the Human." Presentation. SANS Institute. 2013. See: https://www.itpss.com/pdf/STH-Presentation-HumanMetrics.pdf

60. "Improving Your Security Awareness Campaigns: Examples from Behavioral Science." Security Intelligence. June 2015. See: https://securityintelligence.com/improving-your-security-awareness-campaigns-examples-from-behavioral-science/

61. Cialdini, Robert. Influence: the Psychology of Persuasion. 1984.

62. FIRST is a global registry of CERTs/CSIRTS where a reader can go to in order to identify their national bodies. See: https://www.first.org/members/teams/. For Western Hemisphere-specific information, please see: https://the-gfce.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/

63. Olujide, Akintola. "Ports in the Cloud: the Next Step in Automation?" Port Technology. 9 November 2018. See: https://www.porttechnology.org/news/ports_in_the_cloud_the_next_step_in_automation/

64. "The Internet of Things in Transportation – Port of Hamburg Case Study." SIA Partners. 30 September 2016. See: https://www.sia-partners.com/en/news-and-publications/from-our-experts/internet-things-transportation-port-hamburg-case-study

65. Olujide, Akintola. "Ports in the Cloud: the Next Step in Automation?" Port Technology. 9 November 2018. See: https://www.porttechnology.org/news/ports_in_the_cloud_the_next_step_in_automation/

66. There are a wide variety of reference documents organizations can use to guide their development of response and recovery plans, such as the United States National Institute of Standards and Technology's Computer Security Incident Handling Guide (see: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) and the European Union Agency for Good Practice Guide on Incident Management (see: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management).

67. Abraham, Ben. "New Customised Cyber Insurance Product for Shipowners." Seatrade Maritime News. 28 April 2020. See: https://www.seatrade-maritime.com/finance-insurance/new-customised-cyber-insurance-product-shipowners

MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

OAS | More rights for more people

ISBN 978-0-8270-7241-1