IAPH Cybersecurity Guidelines for Ports and Port Facilities

Version 1.0

IAPH
International Association of Ports and Harbors

WPSP
WORLD PORTS SUSTAINABILITY PROGRAM

TABLE OF CONTENTS

Table of Contents 1
List of Figures 3
AcknowledgEments 5
Abbreviations and Acronyms 6
Foreword 7
Executive Summary 8
1. Introduction 9
2. The Business of Managing Risk 12
2.1 Developing the business case for cybersecurity 12
2.1.1 Determine business impact 13
2.1.2 Develop realistic loss scenarios 13
2.2 Establishing a common language 14
2.2.1 Language and stakeholder responsibility 14
2.2.2 The importance of shared common terms 14
2.2.3 Managing cyber risk in financial context 15
2.3 Other key business considerations 15
2.3.1 Risk transfer 15
2.3.2 Budgeting and the challenge of “ROI” 16
2.4 Organizing for managing cyber risk 17
2.4.1 Identifying cyber stakeholders in the port environment 17
2.4.2 Duties, responsibilities and authorities 17
2.4.3 Establishing oversight responsibility for managing cyber risk 18
2.4.4 The role of the Board in managing cyber risk 18
2.4.5 Driving cybersecurity across the organization: the cybersecurity steering committee 18
2.5 Leadership strategies for driving change 19
3. Cybersecurity and Risk Management 21
3.1 Cyber risk in the maritime industry 21
3.2 Defining cybersecurity 22
3.3 What is at risk: data confidentiality, integrity and availability 23
3.4 Governance 24
3.5 Developing a cyber risk management strategy and plan 24
3.5.1 Achieving defense-in-depth via the three lines of defense model 25
3.5.2 Defense-in-depth strategy based on a zero trust framework 26
3.6 Understanding the “cyber-physical” intersection 26
4. Maritime Cyber Threats and Consequences 29
4.1 Understanding the 21st Century cyber threat landscape 29
4.2 Understanding the potential physical impacts of a cyber attack 31
4.3 Understanding the potential non-physical impacts of a cyber-attack 32
5. The Organization’s Cyber Ecosystem 34
5.1 Identify, inventory and classify critical activities and stakeholders 34
5.2 Identify, inventory and classify critical assets 35
6. Assessing for Risk and Vulnerabilities 37
6.1 Assess for vulnerabilities 37
6.2 Assess for impact 37
6.3 Assess for risk 37
6.4 Risk identification 38
6.4.1 Asset identification 38

6.4.2 Understanding data as an asset 38
6.5 Risk evaluation 40
6.6 Risk tolerance 41
7. Protection, Detection and Mitigation Measures 42
7.1 Protection measures 42
7.2 Detection measures 44
7.3 Mitigation measures 46
8. Information Sharing, Communications and Coordination 48
8.1 Information sharing, communication and coordination 48
8.2 Why share cybersecurity information? 48
8.3 Information sharing basics 49
8.4 Establishing a strong cybersecurity information sharing program 50
9. Training 52
9.1 The importance of establishing organizational cyber awareness 52
9.1.1 The Human as a risk 52
9.1.2 Recognizing the Human as the first line of defense 52
9.2 Training is an integral part of a cyber risk management program 53
9.2.1. Workforce development and management 53
9.2.2 General awareness training 54
9.2.3 Technical cybersecurity training 54
9.2.4. Training implementation 54
9.2.5 Training as a means for driving continuous improvement 55
10. Incident Response and Recovery 57
10.1 Incident response planning and preparation 57
10.2 Key components of cybersecurity incident response and implementation steps 58
10.3 Detection and analysis 60
10.4 Containment and recovery 61
10.5 Containment and eradication 62
10.6 Post incident recovery 62
10.7 Develop lessons-learned with relevant stakeholders 62
11. Continuous Improvement and Cybersecurity Maturity 64
11.1 Why cybersecurity is not just for the “IT department” 64
11.2 How cybersecurity capability drives cyber resilience 64
11.3 Leadership strategies for driving cyber resilience 66
12. Annexes – Port Facility Cybersecurity Assessment and Plan Templates 68
12.1 Introduction 68
12.2 Port and Port Facility Cybersecurity Assessment Template 68
12.3 Port and Port Facility Cybersecurity Plan Template 70
Glossary of terms 73

LIST OF FIGURES

Figure 1 - What is Cybersecurity? 22
Figure 2 - CIA-triad........ 23
Figure 3 - ICAS 3LoD model 25
Figure 4 - Layers of Defense 26
Figure 5 - Seafarer as a cyber threat vector 29
Figure 6 - General attacker types 30
Figure 7 - Challenges likely to be exploited by cyber threat actors 31
Figure 8 - Design of risk scenario 39
Figure 9 - Risk matrix for determining risk level for individual risk scenario 40
Figure 10 - Sample risk tolerance........ 41
Figure 11 - Example of protection measures........ 44
Figure 12 - Cyber-attack classification........ 46
Figure 13 - Cyber information sharing benefits 48
Figure 14 - Cyber information sharing model for ports and port facilities........ 50
Figure 15 - Types of human errors 52
Figure 16 - Individuals subject to cyber awareness training........ 53
Figure 17 - Types of cyber incidents 57
Figure 18 - BCPs share four general components........ 61
Figure 19 - Building cyber resilience 65

IAPH Head Office
7th Floor, South Tower New Pier Takeshiba
1-16-1 Kaigan, Minato-ku, Tokyo 105-0022
Japan
Tel: +81 3 5403 2770
Fax: +81 3 5403 7651
E-mail:info@iaphworldports.org

The information provided in this publication has been created by the International Association of Ports and Harbors (IAPH) for the purpose of providing the international port industry with a set of cybersecurity guidelines. These guidelines should be considered as additional guidelines to instruments promulgated by the International Maritime Organization (IMO) and especially to supplement maritime industry guidelines consistent with MSC-FAL.1/Circ. 3, 5 July 2017.

The IAPH Cybersecurity Guidelines provided herein are based on successes achieved by ports and port facilities from around the world and are designed to assist executives in the port industry in their effort to foster greater collaboration within their organizations, as well as more broadly with their local, regional, national, and international partners and stakeholders.

This work is a product of the staff and the membership of IAPH, together with contributions from the staff of the World Bank.

Rights and Permissions

Terms of use

The advice in this publication is intended purely as guidance to be used at the user's own risk. No warranties or representations are given, nor is any duty of care or responsibility accepted by the authors, their membership or employees of any person, firm, corporation or organization (who or which has been in any way concerned with the furnishing of information or data, or the compilation or any translation, publishing, or supply of this publication) for the accuracy of any information or advice given in this publication; or any omission from the guidelines or for any consequence whatsoever resulting directly or indirectly from compliance with adoption of or reliance on guidance contained in this publication, even if caused by a failure to exercise reasonable care on the part of any of the aforementioned parties.

ACKNOWLEDGEMENTS

This technical report was prepared by a joint team of representatives from the members of the International Association of Ports and Harbors (IAPH) and the World Bank.

The IAPH team was led by Dr. Patrick Verhoeven, Managing Director Policy and Strategy and Pascal Ollivier, Chairman of IAPH Data Collaboration Committee and President of Maritime Street, and composed of Frans van Zoelen, Special Projects—Head Legal Emeritus, Port of Rotterdam Authority, Legal Counselor of IAPH and Chairman of IAPH Legal Committee; Max Bobys, Vice-President, HudsonCyber; Andrew Baskin, Vice President, HudsonAnalytix; Lance Kaneshiro, Chief Information Officer, Port of Los Angeles; Chin Beng Ong, Chief Information Security Officer, Maritime and Port Authority of Singapore; Adeline Tiang, Assistant Vice President , Group Cybersecurity , PSA International , Singapore; Mohamed Absar, Head of Projects and Solutions, DP World ; Gadi Benmoshe, Chief Information Officer, Israel Ports Company; Dr. Phanthian Zuesongdham, Head of Division Port Process Solution, Hamburg Port Authority; Lars Wentorp, Chief Information Officer, Hamburg Port Authority; Dr Quang-Vu Pham, Head of Data Privacy and Information Security, Hamburg Port Authority; Machiel Noijen, Strategic Policy Advisor, Harbour Master Division, Port of Amsterdam Authority; Peter Alkema, Strategic Policy Advisor Harbour Master Division, Port of Amsterdam Authority; Mark de Pater, Chief Information Security Officer, Port of Rotterdam Authority; Yannick Herrebaut, Chief Information Security Officer, Port of Antwerp; Jerome Besancenot, Digital Transition Project Director, HAROPA Port; Francis Donkoh, Chief Information Officer Ghana Ports and Harbours Authority; and Scott Dickerson, Executive Director, Maritime Transportation System, Information Sharing and Analysis Center.

The World Bank team consisted of Hagai Mei Zahav, Cyber Specialist, Digital Development, The World Bank, Richard Martin Humphreys, Global Lead for Transport Connectivity and Regional Integration, and Lead Transport Economist, ITRGK, and Ninan Oommen Biju, Senior Port and Maritime Transport Specialist, IEAT.

The lead authors thank the following for their substantive contributions to the preparation of this report: Dr. Antonis Michail, Technical Director of IAPH, and Victor Shieh, Communications Director of IAPH.

The team as a whole extends its special thanks to Mr. Santiago Garcia-Milà, President of IAPH and Deputy General Manager of the Port of Barcelona, for his leadership of IAPH and in particular his unwavering support of the Data Collaboration Committee taking the initiative to launch these Cybersecurity Guidelines for Ports and Port Facilities.

ABBREVIATIONS AND ACRONYMS

TERMINOLOGY	ABBREVIATION / ACRONYM
Advanced Persistent Threats	APT
Artificial Intelligence	AI
Automatic Identification System	AIS
Business Impact Analysis	BIA
Business Continuity Plan	BCP
Computer Emergency Response Team	CERT
Computer Security Incident Response Team	CSIRT
Chief Information Officer	CIO
Chief Information Security Officer	CISO
Commercial-off-the-Shelf	COTS
Control Objectives for Information Related Technologies	COBIT
Critical Information Infrastructure	CII
Cyber Threat Intelligence	CTI
Cybersecurity Incident Response Team	CSIRT
DHS Cybersecurity and Infrastructure Security Agency	CISA
Electronic Data Interchange	EDI
European Union Agency for Cybersecurity	ENISA
Incident Response Plan	IRP
Indicator of Compromise	IoC
Industrial Control Systems	ICS
Industrial Internet of Things	IIoT
Information Technology	IT
Information Technology Infrastructure Library	ITIL
International Maritime Organization	IMO
International Organization for Standardization	ISO
International Ship and Port Security Code	ISPS Code
International Society of Automation	ISA
Internet of Things	IoT
Intrusion Detection System / Intrusion Protection System	IDS/IPS
Maritime Single Window	MSW
Non-Governmental Organization	NGO
Open Source Intelligence	OSINT
Operational Technology	OT
Port Community System	PCS
Programmable Logic Controller	PLC
Recovery Point Objective	RPO
Recovery Time Objective	RTO
Security Information and Event Management	SIEM
Security Operations Center	SOC
Skill, knowledge and ability	SKA
Supervisory Control and Data Acquisition	SCADA
Table-Top Exercise	TTX
Tactics, Techniques and Procedures	TTPs
Terminal Operating System	TOS
U.S. Department of Homeland Security	DHS
U.S. National Institute of Standards and Technology	NIST
Vessel Traffic Service / Vessel Traffic Management System	VTS / VTMS

FOREWORD

The International Association of Ports and Harbors (IAPH) is a non-profit-making global alliance of 170 ports and 140 port-related organizations covering 90 countries and with consultative NGO status with several United Nations agencies, including the International Maritime Organization (IMO).

Through its knowledge base and access to regulatory bodies, IAPH aims to accelerate digitalization and assist in improving overall resilience of its member ports in a constantly changing world.

The COVID19 pandemic has proven to be the pivotal moment for ports in moving away from manual, paper-based processes to digital exchanges of information. The virus has drastically impacted person-to-person contact between ship and shore, and obliged rapid adoption of safety-related digital solutions for cargo and people movements to and from the port gates, in the offices, on the quayside, alongside vessel berths and beyond the pilot station. However, this has also increased the vulnerability of ports, some of whom have been subjected to highly effective cyber-attacks.

In a call to action to accelerate the pace of digitalization to cope with a post-COVID19 “new normal” endorsed by the entire maritime industry, IAPH set out a nine-point plan, which includes:

> *To review existing IMO guidance on Maritime Cyber Risk Management on its ability to address cyber risks in ports, developing additional guidance where needed.*

This first edition of IAPH Cybersecurity Guidelines for Ports and Port Authorities serves this purpose. It also serves as a crucial, neutral document **for senior executive decision makers at ports** who need to be neither technical nor savvy in the latest cyber trends, but who have to find answers to the following questions to safeguard the business viability of their organization:

- *How can I establish the true financial, commercial & operational impact of a cyber-attack?*
- *How ready is my organization to prevent, stop and recover from a cyber-attack?*
- *What do I need in terms of resources to effectively manage the risk of a cyber-attack?*

This document will evolve to meet the challenge of answering these questions, provided by the port industry’s leading experts on this critical subject.

Dr. Patrick Verhoeven
Managing Director, Policy and Strategy
IAPH

EXECUTIVE SUMMARY

Ports and port facility stakeholders from around the world are reporting measurable increases in cyber-threat activities, particularly since the outbreak of the COVID-19 pandemic. Between February and May of 2020 alone, the maritime industry overall suffered a fourfold increase in cyber-attacks and those attacks against OT systems specifically increased by 900 percent since 2017. The risk of a cyber-attack has become the top risk for port authorities and the wider port community.

The accelerated pace of digitalization in port and port facilities only intensifies the urgency for executives to focus on organizational cyber resilience in order to safeguard the integrity and availability of critical data, ensure service delivery and protect maritime infrastructure. Doing so will increase the overall cybersecurity capabilities of the global maritime supply chain.

The IAPH Cybersecurity Guidelines are developed to support the global port and port facility community in a manner consistent with IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3, 5 July 2017). It is intended for use by the Chief Executive Officer and C-suite executives to recognize the importance of managing cyber risk and to instill an understanding that it is a responsibility that starts at the top of their organization, despite the digital divide among the ports, worldwide.

The guidelines are mainly focused on developing the business case for the executive committee to determine "*how much enough is enough*?" as reasonable level of investment in cyber risk management and to gain insights into how a cyber event could impact a port or port facility's ability to function, along with the cost of disruption.

These guidelines also address the need for executives to develop a cyber risk management strategy and plan to achieve and sustain a defense-in-depth posture, provide key insights into the 21st Century cyber threat landscape, and include insights into the impacts of cyber-attacks against integrated port systems. Specific considerations address organizational structures, the identification of key stakeholders, reporting mechanisms, data flow and network mapping, characterizations of critical activities that are performed, and the identification and analysis of critical data, systems, assets, and infrastructures.

The guidelines illustrate how executives should consider cyber risk in the context of their own operations, irrespective of where they might reside within the digital divide. Insights are provided for executives in how to assess risk and vulnerabilities in their port operations and how to adopt a holistic approach that will enable them to organize and manage their cybersecurity program by implementing customized cybersecurity protection, detection, and mitigation measures. Best practices for why cybersecurity information sharing, communication and coordination are key to reducing cybersecurity risks are also provided. General recommendations are provided throughout.

Equally important, is the establishment of an organizational cyber awareness to address the human as the pivotal element. Therefore, general and technical training is highlighted, and which accomplishes the design and the implementation of the emergency management plan vital for maritime organizations to respond quickly and effectively to improve the resiliency of port and port facilities, as well as the broader port ecosystem.

Since cybersecurity represents a collective responsibility – that it is not solely limited to the IT department – the guidelines demonstrate how cybersecurity capability can drive cyber resilience. It is essential that C-suite executives take the lead in allocating resources to deal with cyber security, actively managing governance and building an organizational culture to support cybersecurity operations, and developing leadership strategies for driving cyber resilience including the creation of a port ecosystem cybersecurity workforce.

Finally, the guidelines provide the designated cybersecurity lead with practical assistance in developing their port and port facility security assessment and plans.

1. INTRODUCTION

The maritime industry and cyber risk

The global maritime transportation industry and the integrated multimodal supply chain networks it supports, benefits greatly from the myriad digital solutions introduced by the Fourth Industrial Revolution[1]. Digitalization and the integration of automation and machine learning solutions rely on increased connectivity between networked information technology (IT) and operational technology (OT) systems of individual entities and on the extraordinary volumes of data created, processed, exchanged, and stored. Such advances increase maritime transportation system efficiencies, resulting in year-on-year progress that delivers both qualitative and quantitative improvements to consumers and producers in order to respond in real-time to business requirements.

To remain competitive in supporting their customers and their regional and national economies, ports and port facilities must adapt to the demands of the increasingly digitalized global market. As digitalization accelerates, the global cyberspace[2] within which ports and port facilities operate, evolves. Over time, economic inequalities, the speed of infrastructure investment, the pace (and willingness) of technological adoption, and even geographic circumstances open technological rifts – albeit "digital divides" – between ports and port facilities. Inevitably, these digital divides grow, exacerbating the deficiencies of some ports and port facilities while highlighting the competitive advantages of others.

Regardless of the level of digital adoption at a port or port facility may be, the unavoidable handmaiden to digitalization is cyber risk. No port or port facility is immune to it. Given that the majority of cyber-attacks involve people and fragmented system landscapes, every port and port facility is at risk. Moreover, the inequalities of the digital divide and the burdensome role the maritime industry plays at the center of global trade and information exchange underscores the shared nature of cyber risk within the global port and port facility community.

Effective management of cyber risk is critical to the proper functioning of a diverse maritime community where stakeholders from the port authority, ship operators, port facilities, maritime agencies, customs, and law enforcement are all interconnected.
Port and port facility leaders must recognize that cyber threats are not bound by any border, port perimeter, or even logistical supply-chain where every link is critical. Cyber threats can jeopardize an entire port or port facility's operations and are proliferating at an ever-increasing pace. With the evolution and introduction of new IT and OT technologies, automated systems, and integrated processes that rely on key cloud-service providers, **port leaders must recognize the importance of managing cyber risk and understand that it is a responsibility that begins at the top.**

A growing body of evidence underscores the increasing success cyber-attackers have had targeting the maritime industry. For example, between February and May of 2020 the maritime industry in

[1] *The Fourth Industrial Revolution* collectively represents the global trend towards automation and data exchanges spanning manufacturing, industrial systems, and infrastructure processes which include cyber-physical systems, Internet and Industrial Internet of Things, cloud computing, machine learning, machine to machine communications, and artificial intelligence.

[2] *Cyberspace* can be defined in many ways. At its simplest, it represents the totality of all digitally interconnected technology. A more expansive view accommodates the totality of all social interactions and communications facilitated by the computational medium of the Internet and all Internet-enabled interconnected IT based networks and supporting infrastructure.

general suffered a fourfold increase in cyber-attacks[3] and those attacks against OT systems specifically increased by 900 percent over the last three years.[4] Ports and port facility stakeholders from around the world are reporting measurable increases in cyber-threat activities, and the Maritime Transportation System Information Sharing and Analysis Center's (MTS-ISAC) 2021 Annual Report[5] highlighted some of the most commonly reported attack techniques. Maritime organizations are commonly seeing phishing attacks as the primary means for attackers to compromise accounts, redirect legitimate payments, or otherwise facilitate their activities. In addition, scanning of public Internet-facing infrastructure for unpatched systems and vulnerabilities also is common.

As ports and port facilities enable global trade, they should be recognized as critical information infrastructure (CII)[6]. **The consequences of compromised port and/or port facilities' digital processes could result in operational disruption, affecting customers, port authorities, port community systems, and related port services.** In addition, cyber-attacks exposing sensitive data to unauthorized access, manipulation or exfiltration can further undermine the integrity of the maritime supply chain.

Background

In June 2020 the IAPH, in collaboration with the International Cargo Handling Coordination Association (ICHCA) and the TT Club published the *Port Community Cybersecurity Note*[7]. This report advocated the need for accelerating the digitalization of capabilities within port and port facilities, worldwide. However, for the reasons described above, such advocacy for digitalization also warrants parallel investments in cybersecurity capabilities.

In January 2021 the IAPH and the World Bank published a joint report[8] titled "*Accelerating Digitalization Critical Actions to Strengthen the Resilience of the Maritime Supply Chain*", which focused on port digitalization. This report also raised awareness regarding cyber risk in the context of digitalization. Building on previous work with its partners, the IAPH has developed this first version of its *Guidelines for Cybersecurity at Ports and Port Facilities*[9] (hereafter referred to as the "IAPH Cyber Guidelines").

The IAPH Cyber Guidelines were developed to specifically support the global port and port facility community in a manner consistent with IMO's *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3, 5 July 2017[10]). The IMO guidelines offer non-prescriptive guidance on maritime cyber

[3] https://www.captiveinternational.com/news/maritime-businesses-see-fourfold-increase-in-cyber-attacks-since-february-astaara-3568

[4] https://www.professionalmariner.com/naval-dome-maritime-cyberattacks-up-900-percent-in-three-years/

[5] https://www.mtsisac.org/post/2020-mts-isac-annual-report

[6] Under EU Directive 2016/1148 (NIS Directive) ports are considered as CII for water transport and further classifies them as *Operators of Essential Services*. As cyber resilience of port and port facility ecosystems is critical to supporting the global maritime industry CII protection is central to various port-specific cyber security initiatives, such as Singapore's Cybersecurity Strategy, the European Union's Agency for Cybersecurity (ENISA) and the U.S. Government's National Maritime Cybersecurity Plan.

[7] https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

[8] https://sustainableworldports.org/wp-content/uploads/World-Bank-IAPH-joint-paper-accelerating-digitalization.pdf

[9] *This publication is not intended to provide a basis for, and should not be interpreted as, calling for external auditing or vetting the individual organization's approach to cyber risk management.*

[10] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

risk management to improve the cybersecurity resilience of the shipping industry in the face of current and emerging cyber threats.

Intended audience

These IAPH Cyber Guidelines are intended for use by the Managing Director, CEO, C-suite executives, and all senior managers responsible for ports and port facilities spanning the global port community.

This document provides an overview of all relevant topics necessary to strengthen the cyber security of critical IT/OT based equipment, networks, applications, systems, and infrastructure supporting the full spectrum of port and port facility administrative and operational environments.

The IAPH Cyber Guidelines also acknowledge the uniqueness of a port or port facility’s digital ecosystem vis-à-vis its position within the port community in which it resides where digital technologies are increasingly deployed and integrated. Collaboration among ports and port facilities and port community stakeholders is not only encouraged but is necessary to drive awareness and elevate the cyber resilience across the maritime supply chain locally, regionally and globally.

This document further recognizes that the digitalization of ports and port facilities represents a business challenge and is not limited to IT staff. Fostering a cyber-resilient culture requires behavioral changes and critical understanding of the consequences of individuals’ actions that lead to cyber threats. Port and port facility leaders must understand the interrelationships and interdependencies that exist between maritime entities and recognize the necessity to analyze them, the need for internal and external collaboration and information sharing, and the recognition for disciplined change management.

Ultimately, these guidelines are to assist port and port facility leadership teams to collectively commit, achieve consensus, internal commitment, and to postulate that the implementation of these guidelines indeed is an orchestrated effort of all disciplines under the considered support of the highest authority of the entity concerned. Whilst at the same time there is a very real need for implementation into actual work streams in order to successfully accomplish efficient, cyber-secured operations.

2. THE BUSINESS OF MANAGING RISK

Since they reside at the nexus of global trade, cyber-attacks against ports and port facilities can be both disruptive and costly. While intellectual, financial, and/or personal data can be compromised and exploited, operational disruptions can swiftly cascade, resulting in widespread economic and even political consequences. As port and port facilities adopt new technologies, such as automation platforms and integrated, cloud-enabled IT/OT/IIoT systems, **port leaders should acknowledge cyber risk management as a top-level responsibility, recognizing it as a competitive and operational imperative.**

With the large exposure to risks, port and port facility executives contend with questions such as: "*How much investment is enough?*" and "*What is my return on investment?*" are common. Examples of such rationales include:

- ***The competitive imperative.*** Trade-offs are always made weighing security (which introduces inefficiencies) against operations (which seeks efficiency). As a result, executives whose risk calculus is too often focused on IT unintentionally accept some Operational Technology (OT) cyber exposures.
- ***Cyber risk is pervasive*.** Cyber risk factors touch every aspect of the organization including administration and operations. The perceived all-embracing nature of cyber risk may appear overwhelming and perhaps even insurmountable. Such views inhibit proactive efforts to invest in key resources (people, processes, tools, and funds).
- ***Cyber risk is difficult to quantify***. While there are numerous tools and methods that attempt to quantify value-at-cyber-risk, no common standard exists. Developing loss scenarios to support cyber risk quantification entails collaboration, assumptions, and subjective analysis.
- ***Difficult to change behavior and culture – Nothing's happened so why change?*** This is one of the greatest challenges for most organizations. How do you prevent staff from opening phishing emails with embedded links to malware-infected sites or from downloading malware-infected attachments? How do you mitigate social media exploitation while protecting privacy and data? How do you incentivize the sharing of critical cyber threat information?

Such justifications reveal a common perception plaguing executive suites – that investments in cybersecurity are often considered a cost center rather than as an enabler of port operations. The answers to such questions, however, can be found when decision-makers employ a common language and frame them in the context of finance.

2.1 Developing the business case for cybersecurity

In order to determine reasonable levels of investment in cyber risk management, executives must first understand how a cyber event could impact their organization's ability to function and the potential costs of disruption as well as impacting business opportunities. This involves determining actual business impact, which can be achieved through a business impact analysis (BIA) and the development of realistic cyber loss scenarios. A BIA is a methodology for profiling the conceivable consequences of disruptions to the organization through its operational processes, systems, applications, platforms, and/or equipment. Performing a BIA enables executives to identify and analyze critical business and operational functions and key assets and systems, as well as to anticipate the potential consequences of a disruptive event.

2.1.1 Determine business impact

Effective BIAs entail cross-functional collaboration to enable different stakeholders from across the port or port facility to explain how an unexpected event might affect their business activities and/or operational functions. These insights will help prioritize specific functions and, when *Recovery Point Objectives* (RPO) and *Recovery Time Objectives* (RTO)[11] identified, help executives better understand such operational functions might be impacted by a cyber-attack. A BIA will characterize the operational and financial impacts resulting from the disruption of business functions and operational processes. Impacts for ports and port facilities to consider may include:

- Interruption/loss of access to critical systems or infrastructure (e.g. automated port gates, cargo loading, terminal operations, traffic management) resulting in logistical delays.
- Lost or delayed sales and income.
- Health, safety and environmental impacts.
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, legal fees, etc.).
- Fines incurred due to regulatory violations.
- Contractual penalties or loss of contractual bonuses.
- Customer dissatisfaction or defection / reputational harm.

2.1.2 Develop realistic loss scenarios

By calculating costs for various loss scenarios, port or port facility executives can gain critical insights into which assets, data, applications, processes, systems, or infrastructure might trigger the costliest or most disruptive consequences, if compromised. While it is difficult to model reputational and legal financial consequences, the value of cyber loss scenario analysis can deliver additional benefits in business continuity and disaster recovery planning (Section 7) by the way it:

- **Facilitates collaboration** among different stakeholders from across the organization (e.g. IT, security, operations, legal, security, finance and administration, health and safety).
- Forces contributors to recognize that cyber threats can impact every aspect of the organization’s ecosystem, including clients and external port/cargo community partners.
- **Supports evaluations** of controls, processes and tools in the context of real-world situations.
- **Educates participants in potential *value-at-risk*** associated with the organization’s investments (or non-investment) in the resources required for cyber defense.
- **Helps prioritize investments** based on analysis of business impacts.
- Informs cyber insurance (Section 2.4.1).

Developing cyber-specific and cyber-physical loss scenarios facilitate the BIA process for ports and port facilities. Loss scenarios illustrate how a cyber incident can result in a calculable financial loss. Examples include the loss of access to terminal operating systems, cargo handling equipment, gate access controls, hand-held scanning devices (including RFID), power generation and distribution infrastructure, bulk liquid storage and transmission, communications, Vessel Traffic Management Systems, and office-networked computers. Compromised assets or people in office environments can

[11] ***RPOs*** describe the time duration of a disruption before the quantity of data lost during that period exceeds the organization’s maximum allowable threshold or “tolerance.” ***RTOs*** define the duration of time and a stated service level within which the business process, asset or system should be restored after an event occurs in order to avoid unacceptable consequences. The RTO answers the question: “How much time did it take to recover after notification of disruption?“

also result in financial losses due to attacks against data integrity, such as fraudulent email spoofing, manipulation of manifest data, and man-in-the middle attacks redirecting payments.

Cyber loss scenarios can be developed with the following considerations (Section 6.5):

- ***Scenario Definition*** – Develop scenarios around historical events or hypothetical conditions, soliciting stakeholder teamwork. Consider real-world events to inform on the design of scenarios by modifying the experiences of others to the organization's profile and specific capabilities.
- ***Scenario Probability*** – Estimating the likelihood of a cyber-induced incident should involve key stakeholders from all operational areas. Using past incidents and/or current cyber threat trends as guidance, and applying a consistent methodology, characterize the likelihood of each.
- ***Focus on the Unexpected*** – Do not limit the focus on what would be considered unexpected, severe, and acutely disruptive rather than on expected losses, which may be due to normal attrition or losses associated with the cost of doing business.
- ***Develop a Realistic Story*** – Scenarios should be high-impact but realistic. Consider malicious hackers, competitors, disgruntled insiders with administrative privileges, accidental events caused by employees, or vendor-triggered events due to compromised patching.
- ***Define the Outcomes*** – Once a scenario is defined, the potential outcomes should be varied and clearly defined, with cost estimates attributed to each outcome. Examples include: operational delays, loss of revenue, incident response and mitigation efforts, legal costs, and fines.
- ***Define What Is in Place*** – Identify existing controls and systems and analyze how each could be used to prevent, detect, and respond to scenario conditions. Also, justify how effective each of them is. Consider: How do the controls and systems affect one another? Do dependencies exist? What is the probability of their failures?
- ***Define the Frequency*** – Estimate event frequency, which should be the result of a cooperative efforts among stakeholders responsible for various operational areas.
- ***Define Outcome Severity*** – Characterize and define the severity of each outcome.
- ***Quantify All Outcomes*** – Define and assign financial values of losses related to assets, systems, equipment, infrastructure, cost for recovery or – if needed – replacement, costs of third-party services rendered, lost revenue, etc.
- ***Adjust for Bias*** – It is human nature for people to have an optimistic bias of their perceptions of personal knowledge, skills, competency, and overall ability to succeed. To avert bias, base loss scenarios on a hypothetical entity that mirrors the organization. Ask different groups of people in the organization as well as relevant stakeholder entities for their subjective judgements.

2.2 Establishing a common language

2.2.1 Language and stakeholder responsibility

Port and port facility leadership teams also face the challenge of *language and communication.* **Successful cyber risk management *begins with* and *depends on* a common understanding of terms, financial grounding, and recognition of shared responsibility.**

2.2.2 The importance of shared common terms

In response to cyber threats, port and port facility executives often deploy resources – their people, processes, tools, and funding – in a reactive manner informed by varying assumptions and inconsistent terminologies. Terms common to some can have different meanings depending on the context of the organization's specific operating environment and the roles, responsibilities, and experiences of staff. For example, a cyber "incident" for one organization may imply a range of possible events, while within another the term may indicate a narrower meaning.

Significantly, inconsistent terms can create confusion, such as undisciplined escalation, ad hoc alerting, and irregular reporting that can jeopardize operations and service delivery, or, more broadly, place port community partners at risk. This can frustrate key stakeholders and business partners and produce conditions that allow cyber risks to cascade and impact additional stakeholders.

The first step in instituting a common language requires establishing a common vocabulary. Port and port facility stakeholders should agree on the terminology to be used within the organization, which should be used to facilitate clear, unambiguous communications across different internal stakeholder groups. This will improve the clarity of cyber communications at organizational and community levels and reduce the likelihood of misunderstandings and/or miscommunications. A *Glossary of Terms* is included to assist stakeholders in this process.

2.2.3 Managing cyber risk in financial context

In addition to establishing a common vocabulary, cyber risk discussions should be grounded in *financial* context. Doing so transforms the cyber risk management discussion into the structural conceptions and readily-recognized financial management metrics of *business*. **Establishing the *cyber-risk-to-money* intersection across all areas of a port or port facility will offer a means of measurement to inform on investment decisions concerning resource identification, allocation, and prioritization.**

Loss scenario analysis supports this process by illuminating the risks in financial terms. However, it only represents the first part of the cyber-risk-to-money concept. **Using loss scenario outputs, stakeholders can then determine how to best prioritize the appropriation of available resources – its people, processes, tools and funding, which represent a cost – by effectively comparing the cost of the risk (e.g. loss scenarios) against the cost of the resources.** Financially grounding the cyber risk management discussion empowers executives and key decision-makers with the commercial context and the operational insights necessary to make informed judgments in a consistent manner regarding investment planning and resource allocation.

2.3 Other key business considerations

2.3.1 Risk transfer

Cyber threat actors are relentless, creative, persistent, and highly motivated. Insufficiently mitigated risks leave organizations exposed to potential losses, first- and third-party liability, fines, and a host of cascading costs related to mitigation, response, and recovery efforts. It is important to recognize that cyber risks are constantly evolving, and cannot be totally eliminated. But cyber risk can be mitigated, accepted, avoided, or transferred (Section 7).

Transferring some cyber risk through insurance offers port and port facility leaders an additional risk mitigation strategy because cyber insurance can help cover response and recovery costs in the event of a cyber-attack. As the technological sophistication of port operations intensifies, and as automation and IT/OT/IIoT infrastructure evolves, port and port facilities investing in cyber risk management may wish to consider engaging their insurance brokers to discuss cybersecurity insurance options.

However, port and port facility executives should approach cybersecurity insurance cautiously and in collaboration with legal counsel to craft policies appropriate to the organization's risk. Cyber cover does not release an organization from the responsibility of managing their cyber risks, but rather requires the port or port facility to sustain a cybersecurity program that fosters continuous improvement.

To prepare for cyber insurance, a good first step is to evaluate the organization's overall cybersecurity capabilities and risk exposure. To accomplish this, first the organization should review current insurance policies to see how they might perform against a set of realistic loss scenarios. Next, it should identify and characterize current organizational cybersecurity capabilities spanning all functional areas. Then, it needs to consider implementing a cybersecurity maturity-based approach, as discussed in Section 11, which many underwriters use to craft policies and pricing thresholds in lieu of cyber-related actuarial histories.

2.3.2 Budgeting and the challenge of "ROI"

Cybersecurity investments require budget decisions, and the question of "*How much is enough?"* should be considered when implementing a cybersecurity program. Decision makers with profit and loss responsibilities scrutinize security investments because of the difficulty in forecasting return-on-investment (ROI). Typically, security investments are measured against the potential for losses based on "what-if" scenarios affecting an organization's reputation, first- and third-party liability claims, lost revenue, regulatory fines, etc. Unlike investments in physical security equipment and systems, such as networked video or access control systems, investments in cybersecurity have been slow to take hold because their perceived benefits may seem less obvious to uninformed security practitioners. Some organizations might also assess what contracts and business opportunities may be available to them if they meet certain cybersecurity requirements that some stakeholders are requiring in their contracts.

Organizations across all industries are increasingly recognizing that a dedicated cybersecurity budget is critical to cyber risk management. As ports and port facilities seek to better understand and effectively address cyber threats, one of the first steps taken must be to establish a dedicated, sustainable operating budget for supporting cyber risk management activities.

With the exception of a few leading port and port facilities, investments into cyber defense and risk management have been underfunded, *ad hoc* in execution, and reactionary. Unfocused investments leave ports exposed to asymmetrical cyber-attack and exploitation.

While many executives may presume that cyber threats can be addressed by increasing IT budgets, they are most effective when organized in a coordinated fashion under a cybersecurity program. **Cybersecurity budgets should address cyber risk management across all operational areas of the business**, including IT, operations, security, training, physical security, health and safety, administration, and incident response. In this context, the understanding of the distinction between Information Technology (IT) and Operation Technology (OT) is crucial. IT relates to hardware and software products which lay the foundation of your information system like server, cloud-service, communication network components, administration system, business software, etc. OT, on the other hand, relates to hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events[12].
In addition, port commissioners and boards of directors and executives – especially those overseeing publicly traded companies – face obligations and fiduciary responsibilities for allocating the funding necessary to execute an enterprise-wide cyber risk management program. For privately-owned

[12] See https://en.wikipedia.org/wiki/Operational_technology

organizations the responsibilities are less clear, but these guidelines can help stakeholders set common standards of care.

2.4 Organizing for managing cyber risk

A World Economic Forum study discovered that the single greatest driver of organizational cybersecurity capability (and thus resilience) was executive engagement. This was found to be true regardless of an organization's size, sector and resource availability.[13]

Although the digital divide can be characterized by resource availability separating ports and port facilities, the term can also be applied to describing the perceptions of cybersecurity – namely, *what is it, who is responsible?* – separating decision-makers within the same organization. In this sense, the digital divide poses less of an economic challenge distinguishing the capabilities of ports and port facilities from one another, than an intellectual one dividing key decision-makers within the same organization. Therefore, **before technical resources are engaged, port or port facility executives should first organize to manage the cybersecurity challenge.** This involves identifying key staff, assigning duties and defining responsibilities, consolidating oversight and reporting protocols, and implementing a working group.

2.4.1 Identifying cyber stakeholders in the port environment

Port and port facility cyber stakeholders include all administrative and operations staff who access digital assets to create, access, process, store, or transmit electronic data, internally or externally, to government and commercial third parties. While this includes a diverse range of internal stakeholders, it should also be expanded to include external stakeholders, such as key vendors and/or partners who access the port or port facility's digital assets and infrastructure, and who rely on the confidentiality, integrity and availability of data. Since the stakeholders may change over time depending on the dynamics of port ecosystem, a regular review of these stakeholders should be conducted accordingly.

2.4.2 Duties, responsibilities and authorities

In both daily operations and crisis situations, **clear roles, responsibilities, and role-based authorities are essential to effective cyber risk management.** This begins with identifying and defining appropriate stakeholder roles and responsibilities for accessing and overseeing activities involving digitally connected assets and infrastructures. Stakeholders must then be identified for these positions and assigned with the suitable responsibilities and granted the requisite authorities to effectively perform their cyber risk management functions. Critically, and as discussed in Section 9, authorities should be assigned to stakeholders with the necessary knowledge, skills, and/or abilities (KSAs).

Specific responsibilities include, among others, ensuring that cybersecurity capabilities, technical controls, procedures, and processes are properly employed and sustained across all operating environments. For example, the physical security of critical hardware (e.g., servers in restricted areas) should be monitored, and, with it, defined duties assigned in order for this activity to be sufficiently completed and audited. Assignment of duties, responsibilities, and role-based authorities is not a one-time activity. Organizations should regularly review roles, responsibilities, and authorities to ensure that they remain appropriate and relevant and continue to support the mission of the business.

[13] See: http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

2.4.3 Establishing oversight responsibility for managing cyber risk

While a port or port facility's cyber risk management success requires collective effort, the organization should define *who* has overall oversight of the program. Owners, shareholders, and institutional investors (e.g., private equity) evaluate cyber risk in terms of risk to investments. However, operational cyber risk management oversight lies with those individuals who have ultimate responsibility for the governance of the port authority or port facility. This is the CEO, Managing Director, or other designee, and their responsibility includes Board-level reporting.

To implement oversight and accountability, and to manage its organizational cyber risk, the organization should also identify and appoint a named Chief Information Security Officer (CISO), or assign the duties of a CISO to a Chief Information Officer (CIO) or similar. The CISO directs the cybersecurity program and their role includes but is not limited to the implementation and sustainment of cybersecurity plans, policies, procedures and controls; technical operations; and internal/external communications. While the role of the CISO reports directly to the CEO or Managing Director, they should also be endowed with "dotted line" access to the Board.

2.4.4 The role of the Board in managing cyber risk

Cyber risk has evolved into one of the most important topics in today's boardroom discussions. **A primary responsibility of the Board is to institute cyber risk oversight, which can be enforced via an audit mechanism (e.g. audit committee) to monitor the policies supporting the port or port facility's cyber risk management program.** For example, on a quarterly basis as a minimum, boards should expect senior management status reports of the organization's cybersecurity program. In most cases, a port or port facility's Board members are not cybersecurity experts. To be effective, Boards should be informed of cyber risks, incidents (including results), and options for risk treatment, acceptance, transfer.

To support decision-making for adequate investment planning and resource allocation, the reporting language should be based on a shared terminology, utilization of key performance indicators, and include financial grounding. While this is the responsibility of CISOs or CIOS in the largest organizations, smaller organizations might assign such responsibilities to IT or operations staff. One trending, cost-effective option is the outsourcing of the CISO role to third-party advisors who are engaged (e.g. part- time) to support Board-led cybersecurity efforts. To be effective, Boards should:

- Be prepared to engage external expertise for understanding cyber risk (if not, seek training).
- Review mechanisms to oversee cyber risk management activities.
- Review resource development and allocation decisions.
- Have a process for reviewing insurance policies to ensure that cyber risk factors are addressed.
- Appoint an individual responsible for implementing the cyber risk management program and who directly reports to the Board at least quarterly.
- Have a process for managing its cyber reputation and addressing public exposures.
- Support organization-wide education/awareness campaign addressing cybersecurity.

2.4.5 Driving cybersecurity across the organization: the cybersecurity steering committee

One cost-effective approach a port or port facility can take is to establish a dedicated internal cybersecurity steering committee. Establishing one can become a key tool in the organization's efforts to assume responsibility for overall cyber strategy, ensure coordination in its implementation, reduce the potential for duplication in security spending, consolidate lines of reporting, control and oversight of complex investments and/or infrastructures, streamline communications, and drive cultural change.

The role of cybersecurity steering committee is to take ownership of and coordinate port/port facility-wide initiatives intended to reduce cyber risk. Under the direction of the CISO or CIO it enables the organization to optimize budgeting and procurement, drive consensus, assign authorities and institute accountability, and serve as the primary driver for information sharing and cross-functional engagement among port/port facility stakeholders. Effective steering committees should:

- ***Implement a charter*** that includes a statement of executive acceptance.
- ***Define authorities and responsibilities.***
- ***Assume ownership*** of the organization's strategy, plan and governance activities.
- ***Coordinate*** organization level communications, including pre-/post-incident response.
- ***Govern information-sharing*** protocols.

Further crucial roles in the Cybersecurity Governance should also include:

- **Designated Cybersecurity Lead** – a managerial role to understand, specify cyber risks and provides inputs for the cyber strategy and plan as well as coordinate the measures at the operational level of cybersecurity-related actions.

2.5 Leadership strategies for driving change

Cyber risk management only succeeds with the active executive engagement and oversight. Effective leaders proactively implement cybersecurity capabilities that are both multi-disciplined and engage all functional areas. The following strategies can help executives drive their organizations forward:

- **Facilitate and engage in the decision-making process**. Participate in the development, analysis, and determination of operational risk appetites. Consider: What is at risk? What is and is not acceptable to be at risk? What are the trade-offs regarding risk exposure, acceptance, avoidance, mitigation, and transfer? What are the priorities? Who should participate?
- **Actively drive cyber risk awareness and engagement across all functional areas**. Every individual is a potential target for cyber threat actors. Engaging personnel from all functional areas, including operations, legal, contracts, procurement, sales/marketing, public relations, and administration and finance, is critical. An additional option is to integrate key influencers in the organization who help promote or educate personnel on the cyber risk awareness at the department or local operational level. Incorporating cybersecurity considerations into contracts and service agreements is important. Fostering collaboration through the employment of internal working groups with operational overlap is encouraged.
- **Change behaviors**. Since change is never easy, organizations should begin with simple steps. Sponsor regular cyber awareness training and implement an email awareness campaign highlighting the vulnerabilities associated with email or use gamification for cyber risk training as an alternative way to attract interest of people. Do not limit the tasks and responsibilities to IT or Security personnel. Include cybersecurity responsibilities, metrics and incentives in performance reviews across the organization. Taking into account the communication culture, **initiatives that are suited and can be adapted should be made that can be measured on their effectivity.**

- **Dynamic focus**. Recognizing the ever-changing nature of the cyber threat landscape, cyber risk management efforts should continuously re-assess, which should also take into consideration the organization's cyber risk profile from an attacker's perspective.
- **Implement governance and accountability**. Humans naturally seek shortcuts. Some will actively circumvent cybersecurity policies and controls no matter how rigorous. Consider formalizing cybersecurity responsibilities in all roles, defining appropriate authorities, and reinforcing them with reporting procedures to enable monitoring against defined objectives. Enforce policies and commitments and hold people accountable.
- **Accountability**. Legal specialists should be actively and regularly involved in pre-breach planning activities to ensure that the organization can adequately respond to and recover from a cyber- attack that may involve risks to first and third parties.

3. CYBERSECURITY AND RISK MANAGEMENT

3.1 Cyber risk in the maritime industry

According to the IMO, maritime cyber risk refers to *a measure of the extent to which an asset, system, application, or connected infrastructure could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised*[14].

The IMO further defines cyber risk management as the *process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders*.

Many integrated IT, OT, and IIoT platforms in the maritime sector continue to rely on legacy technologies and systems that were not originally designed to meet robust cybersecurity requirements. Ports and port facilities implementing operational efficiencies has resulted in stand-alone applications and platforms, networked OT-enabled equipment and infrastructure being integrated with Wi-Fi networks, and with them being connected to the Internet via administrative systems. While some efforts have been carefully planned, others are the result of ad hoc efforts driven by business needs.

While integrated IT, OT, and IIoT platforms deliver measurable efficiencies, they also introduce new cybersecurity vulnerabilities in previously unforeseen ways. Some companies opt to not integrate these systems (IT, OT en IIOT) into their network, while others integrate these into a seamless network. The risks involved within the integration of these systems need to assessed before the integration is made.
The extent of ad hoc integration is so widespread across the global port and port facility community that it is not unusual to discover unknown IT and OT network connections that leave their organizations vulnerable to cyber-attack.

The reality of today's connected global economy is that maritime operations rely on Internet connectivity, and the growing dependence on vendors accessing networked assets, cloud-based service providers and networked supply chains which only underscore the potential of cascading cyber risk. While cyber-attacks against maritime stakeholders occur daily, two notable port / port facility victims include:

- **A.P. Moller-Maersk.** Originating in the Ukraine and masquerading as ransomware in 2017, the NotPetya malware spread around the world so swiftly via Internet connections that organizations spanning a variety of industries were indiscriminately attacked and successfully breached. The impact was swift and severe, and the impact on the Danish shipping company A.P. Moller-Maersk was global. Public disclosures indicated the attack disrupted 17 container terminals around the world, disrupted global operations, and forced stakeholders to revert to manual processes for managing and tracking shipments. Truck backlogs grew by the thousands.

[14] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx#:~:text=Maritime%20cyber%20risk%20refers%20to,being%20corrupted%2C%20lost%20or%20compromised

- **The Port of Shahid Rajaee.** In May 2020 the Port of Shahid Rajaee in Iran suffered a cyber-attack that resulted in a cascading series of disruptive actions.[15] The attack resulted in the shutdown of the port's computer systems controlling the flow of vessels, vehicles and goods. Cargo loading and unloading activities came to a standstill, traffic jams grew outside the port, and vessels were unable to berth. Port authority stakeholders were forced to revert to manual loading and unloading processes, severely impacting efficiency.

These events serve as continual wake-up calls to ports and port facility executives. Regardless of whether a cyber-attack is targeting a victim on the other side of the world, the integrated nature of the global maritime economy leaves all ports and port facilities on both sides of the digital divide vulnerable to attack and operational disruptions of the global maritime transportation system.

3.2 Defining cybersecurity

What is Cybersecurity?

Cybersecurity refers to the protection of IT, OT and IIoT systems (hardware, software and associated infrastructure), networks and the data on them, and the services they provide, from unauthorized access, harm, misuse or destruction. This includes harm caused by either intentional or unintentional causes. Further, it supports the preservation of information confidentiality, integrity and availability, and includes the additional attributes of authenticity, accountability, non-repudiation, and reliability. Where cyber-physical environments intersect, its purpose is to prevent unwanted physical actions from occurring. Cybersecurity best practices address people, process and technology controls to allow for improved organizational resiliency from cyber attacks, by supporting protection, detection, response and recovery activities.

—The *Cyber Security Body of Knowledge*, V1.0, 31 October 2019; See: https://www.cybok.org

Figure 1 - What is Cybersecurity?

[15] https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/

3.3 What is at risk: data confidentiality, integrity and availability

A risk is a situation in which a threat exploits a vulnerability, which can negatively impact data, system or network *Availability, Integrity* and *Confidentiality*, typically referred to as the "CIA-triad"[16] . To protect the hyper-connected global maritime supply chain, which depends on the efficient and trustworthy exchange of data as well as OT systems that allow for efficient operations, **ports and port facilities should seek to manage cyber risks within their defined acceptable limits**.

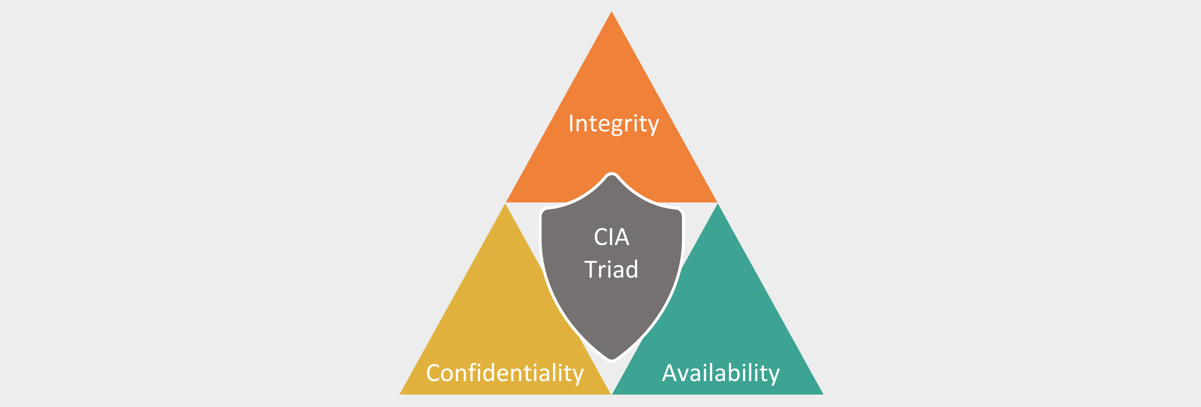


Figure 2 - CIA-triad

- ***Confidentiality:*** Ensures that information or systems are only accessible to authorized users. In guarding its data confidentiality, a port or port facility may group information according to sensitivity and restricted access, both digitally and physically. Tactics for ensuring confidentiality include file permissions, encryption and access control lists.
- ***Integrity:*** Integrity refers to preserving information or system accuracy; it is about the protection of data from unauthorized modification or deletion. Integrity violations can undermine confidence that data about goods, customers or finances is no longer reliable. Ports and port facilities may use version control or system backups to ensure unauthorized changes to data can be reverted.
- ***Availability:*** Availability represents the certainty that users of a digital system or information can make use of it when needed. Cyber threats targeting availability can cause critical system outages, to include terminal operating systems, Wi-Fi and RFID-enabled operations, office-based ERP systems, and network enabled communications, such as IP based telephones. To protect availability, ports and port facilities may have a number of redundancies in place (systems, communications and even data backups) as well as protections against denial of service attacks.

The CIA-Triad is widely used to guide information security policy development. For ports and port facilities, it offers important considerations for the steps that can be taken to improve cyber resiliency.

[16] Sometimes also referred to as the "AIC Triad" to avoid confusion with the U.S. Central Intelligence Agency.

3.4 Governance

Executive buy-in regarding the implementation of cyber risk management policies and a related governance framework is required for any port or port facility seeking to become cyber resilient. Strong cyber risk management policies implemented under an effective governance framework can make a maritime organization's IT services more efficient and OT enabled operations more productive.

When introducing cyber risk management policies within the organization, it is critical for executives to align them with defined operational objectives. Too often, key functional areas operate in isolation – with IT staff focusing on IT matters; operations staff focusing on cargo operations; security staff focusing on security; and so on. Under an integrated cyber governance framework, which can be coordinated under the cybersecurity steering committee (Section 2.4.5), plans and policy documents should be regularly reviewed and updated as organizational structures evolve, authorities are adjusted, new technologies and/or processes are adopted, and threats and vulnerabilities change. More importantly, the essentials of these documents should be translated in comprehensive messages for an organizational-wide communication.

To support the organization's cyber risk governance efforts, the following cyber risk management activities should be considered, which are covered throughout this guide:

- The identification of critical assets and networks, including IT, OT and IIoT environments.
- An analysis of threats to critical assets and vulnerabilities.
- An understanding of the implications of a cyber incident, including costs of loss or replacement.
- Determining the risk tolerances.
- An assessment of business / operational needs and related risks.
- The prioritization of security-related projects, and create a plan based on your risk exposure.
- Determining where your data resides.
- Implementing a standardized means for analyzing, measuring, and reporting risk profiles.
- Defining an appropriate set of risk mitigation measures with interval revision.

3.5 Developing a cyber risk management strategy and plan

Developing a cyber risk management strategy and plan takes time and planning, and their implementation requires the participation of executive leadership, as outlined in Section 2. It is essential the cyber risk management strategy aligns with the organization's overall operational strategy. Careful considerations should be given to the specific business requirements supported by administrative activities and performance objectives supported by complex OT enabled environments.

A cybersecurity strategy should include goals for maturing cybersecurity capabilities across all operating environments. The strategy document needs to be sufficiently high-level and flexible to accommodate both technological and threat actor changes. As needed, regulatory requirements should be acknowledged and incorporated into the strategy. Once the strategy is established, a cyber risk management program can then be implemented.

A cybersecurity plan acknowledges and addresses identified threats and vulnerabilities, such as un-segmented networks; unmanaged third-party risks (e.g. vendors, berthed vessels); risks posed by insider threats; and the myriad cyber threats outlined in Section 6. The plan should incorporate feedback loop mechanisms to be effective, remain relevant and ensure sustainability.

To develop the strategy and plan, the organization should seek to understand its specific risks through the application of risk assessments (Section 8).

While there is no single correct cyber risk management strategy that applies uniformly to all ports and port facilities, specific considerations include:

- Identify and incorporate cybersecurity controls from an identified cybersecurity framework, such as those from the International Organization for Standardization (ISO), U.S. National Institute of Standards and Technology (NIST), and the International Society of Automation (ISA). Several frameworks are available that can be leveraged to blend cybersecurity controls for complex IT, OT and IIoT port environments and it is important that executive leadership is included in the framework selection process.
- Adopt a defense-in-depth approach, such as the "three lines of defense" model.

3.5.1 Achieving defense-in-depth via the three lines of defense model

Defense-in-depth leverages the implementation of multiple layers of security controls across a networked operating environment dependent on IT systems. Defense-in-depth is achieved through the layering of various security controls in a manner that delivers security redundancy. These controls cover distinct areas, including physical (e.g. perimeter security, CCTV), technical (e.g. hardware and software such as encryption, 2-factor authentication) and administrative (e.g. policies and procedures).

The first line of defense is responsible for implementing the security controls and measures based on the cybersecurity principals and best practices outlined in the risk management framework adopted by the organization. For example, these can include parameters users must adhere to when setting passwords. The Designated Cybersecurity Lead ensures that users follow established protocols in accordance with the cybersecurity policy.

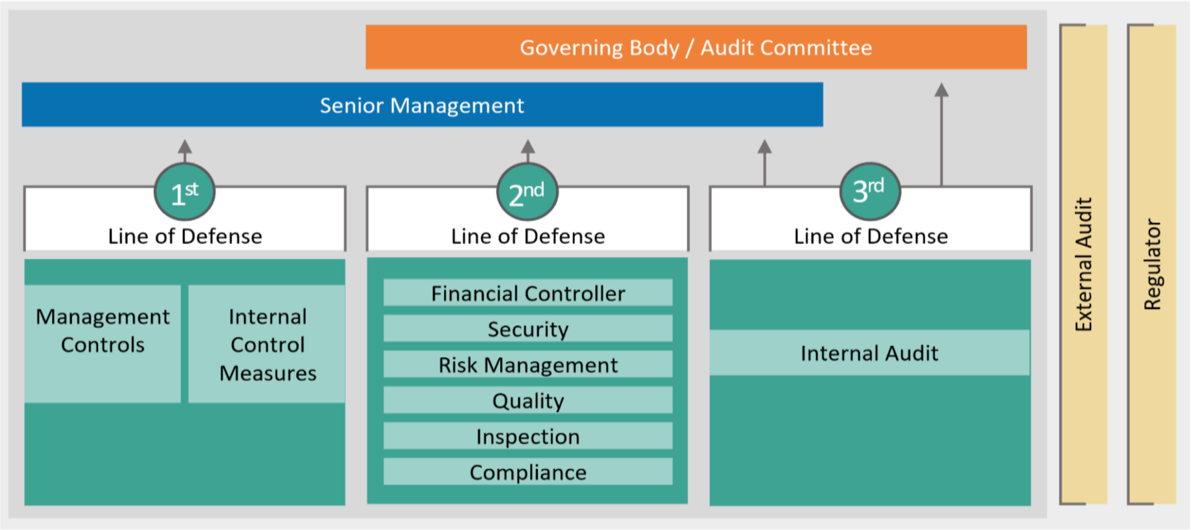


Figure 3 - ICAS 3LoD model

The second line of defense leverages best practices that support risk management and compliance-based activities. These are intended to develop, facilitate and monitor for effectiveness the first line-of-defense controls. While these may vary across ports and port facilities, an organization may have multiple compliance functions spanning security (e.g. ISPS Code), data confidentiality (e.g. GDPR), financial (e.g. PCI-DSS), and supply chain (e.g. WCO).

The third line of defense is the internal audit department that may check with the 2nd line depending on the guidelines (in accordance with the risk tolerance, etc.) and if these are implemented by the first line. This third line may be optional for smaller organizations which lack an internal audit department. In adopting this model stakeholder areas of responsibility can be clearly defined.

3.5.2 Defense-in-depth strategy based on a zero trust framework

Defense-in-depth best practices are based on the principle of creating multiple layers of defense to make it more difficult for an attacker to succeed. Such layers provide multiple opportunities for the organization to protect, detect, and respond to an attack. When one defensive layer fails or is overcome by an attacker, the remaining layers ensure the organization can still halt the attack. For example, the firewall and perimeter IDS/IPS provides one layer of defense for an organization, as the firewall prohibits certain access and ensures communication is monitored. In the event an attacker successfully breaches the firewall and IDS/IPS, a second layer of defense, such as an endpoint protection capability, provides another obstacle for the attacker to overcome.

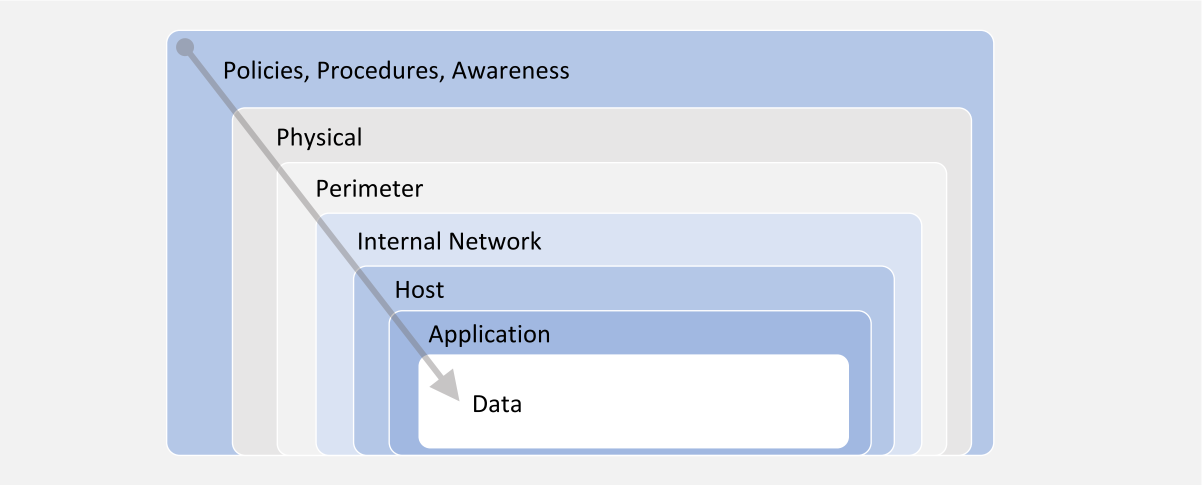


Figure 4 - Layers of Defense

3.6 Understanding the “cyber-physical” intersection

OT systems are defined as hardware and software that directly changes, monitors and controls physical devices, industrial equipment, assets, processes, and events. An example of OT is Supervisory Control and Data Acquisition (SCADA), which collects and analyzes data in real time for the purpose of monitoring control systems in plant, machinery and infrastructure systems. Many OT systems depend on Programmable Logic Controllers (PLCs) that receive data from sensors, process data, and perform specific tasks based on pre-defined protocols. Industrial Control Systems (ICS), which are frequently managed by SCADA systems, represent another type of OT that control and monitor processes, such as conveyor belt systems. Increasingly, OT systems are being connected, managed and monitored remotely via the Internet with IIoT systems also connected into these networks. With increasing frequency, new ICS technologies share common TCP/IP protocols[17], enable every greater connectivity.

IT systems refer to computer-based technologies, which include software, hardware, communications technologies, and related information processing services. IT systems have expanded into the OT world by providing port and port facility staff with real-time insights into the condition of OT systems and infrastructures. What distinguishes OT from IT systems is that OT devices control *physical* systems. IT systems *manage the systems that manage data.*

Regarding cybersecurity OT and IT systems are different

OT and IT systems are different, especially in attack outcomes. **A successful cyber-attack against an IT asset, such as an application server on an administrative network, could result in data theft, while an attack on OT systems could lead to injury or loss of life, damage to the asset, or environmental harm.**

One factor driving both the evolution and complexity of cyber risk to ports and port facilities is the convergence of and connectivity among IT systems (i.e. access control, enterprise resource planning applications, etc.), domain awareness systems (i.e. video, RADAR, AIS, etc.) and OT systems (ICS, SCADA-enabled systems fuel storage and distribution, gantry cranes, etc.). As more and more ports and port facilities connect their OT systems to IT networks, and further adopt and employ IoT/IIoT technologies, and by implication, to the wider worldwide web, new vulnerabilities emerge that threat actors can exploit.

Historically, critical mission-specific platforms and networks were segregated and not physically connected. This segregation or separation helped insulate control systems from changing cyber threats. It was thought that cyber attackers could not cross this physical divide until *Stuxnet*[18] dispelled the myth. As more systems became network-enabled, previously stand-alone IT and OT networks were connected – often on an ad hoc basis whereby security was not factored in. Today, in spite of network segmentation best practices, many maritime stakeholders continue to connect IT-enabled networks supporting business or security systems to control system networks using flat network designs.[19]

Over time, cyber threat actors have capitalized on IT-OT convergence. With the rise of automation platforms in cargo operations, the trend continues. And with IoT systems, which are too often designed with little to no security in mind, the foundations are being rapidly laid for an ever-more complex, more dynamic cyber risk landscape that most ports and port facilities are ill prepared for.

Contextualizing IT vs. OT security via the CIA-Triad

[17] TCP/IP (The Transmission Control Protocol/Internet Protocol) is a standard defining how devices (thus systems) and applications transmit data between them and enables communication exchange over networks and the Internet.

[18] Launched in 2009, *Stuxnet* is a computer worm that was originally designed to target Iran's nuclear facilities. The original attack targeted Siemens programmable logic controllers (PLCs) used to automate centrifuges that supported uranium enrichment. It crossed the facility's air gap via USB sticks and spread through Microsoft Windows computers. Once the worm identified the targeted equipment, it then sent damage-inducing commands to the electro-mechanical equipment. During the attack, the worm sent false information to the main controller, thus misleading engineers into a false sense of security while it damaged the centrifuges.

[19] Physical/Cyber Convergence Working Group, "Final Report and Recommendations by the Council," National Infrastructure Advisory Council, Jan. 16, 2007, https://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport.pdf

One way to distinguish between IT-based security and OT-based security is to view it through the 'lens' of the CIA-Triad. The CIA-Triad is designed to offer insight to an organization based on data confidentiality, integrity and availability – effectively the IT benchmark. The OT benchmark, however, is *control, availability, integrity,* and *confidentiality* (CAIC). The main difference between CIA and CAIC is that the latter focuses more on safety and control rather than data protection.

Securing OT systems and networks requires a strong CAIC design-based approach. When securing OT systems the foremost objectives are to ensure system availability, system safety and that system controls are properly functioning and not subject to cyber-attack. OT security measures should be included in the daily, first line of defense procedures.

4. MARITIME CYBER THREATS AND CONSEQUENCES

4.1 Understanding the 21st Century cyber threat landscape

Ports and port facilities play a central role in supporting national economies. Faced with the increasing complexity of maritime transportation supply chains, a key factor in maintaining competitiveness rests on the abilities of a maritime organization’s IT and OT infrastructure to not only accommodate new automation and IT, OT and IIoT systems, but also to process fast-growing data sets enabling the movement of goods, passengers and ships. Systems, applications, and data must be kept available and their integrity maintained. These factors make the maritime sector attractive to cyber threat actors.

As ports and port facilities adopt automation enabled by IT, OT and IIoT systems, which deliver measurable savings and operational efficiencies, new vulnerabilities are emerging that can be exploited by threat actors. Data processing activities are largely based on electronic data interchange (EDI) and in many environments are processed through Port Community Systems (PCS). With data transaction volumes measuring in the millions, the adoption of Big Data analytical solutions, automation, and artificial intelligence (AI) technologies will increasingly be leveraged by organizations seeking operational agility. Couple these capabilities with autonomous and wireless, networked-enabled vehicles as well as IoT/IIoT enabled sensor systems, and the operational complexity widens, presenting opportunities for cyber threat actors to exploit vulnerabilities or poorly-secured environments.

Seafarer as a Cyber Threat Vector

Modern mariners often travel today with multiple, personal IT devices (i.e. laptops, tablets and phones), They often connect to a variety of networks while making purchases or communicating with family and friends during shore leave in port areas. Back onboard, connecting these systems to the vessel network may introduce malware into the environment, even if it is simply connected to charge the device. Even when seafarers engage in good cybersecurity practices, many may be dependent on legacy operating systems that have not been properly patched or updated, or are no longer supported by the manufacturer. Use of such systems, including the almost endemic use of mobile storage devices (e.g. ‘thumb drives’) on the vessels serve as vectors for malware to access ship’s critical systems, and through them, to ports through the exchange of information or connected systems. Cybersecurity awareness and education programs are now a critical element for companies to reduce the potential risks mariners can pose, albeit perhaps unintentionally, to critical systems and data.

Figure 5 - Seafarer as a cyber threat vector

Cyber threat actors targeting multiple critical infrastructure sectors, including maritime, are not constrained by geography or language. *Any* networked environment, including those found in every port or port facility in the world, could be vulnerable to cyber-attack, compromise and exploitation. Unique to port operations, for example, vessels represent potential conduits of cyber risk to the ports they visit, the companies managing them and the supply chain they support. Ships can be risky if their shipboard environments are lightly governed and have little to no oversight. When moored, a ship can potentially introduce cyber risks to a port facility through ship-shore connections.

The primary motivation of most cyber threat actors is financial gain. The latest trend is the increasing use of ransomware attacks propagated via phishing mails. **Cyber criminals will continue to evolve**

their tactics, techniques, and procedures (TTPs) over time, which requires cybersecurity professionals to also adjust their defensive tactics, but cyber attacker motivations and objectives remain consistent.

Other motivations for threat actors include ideology (Hacktivism) and cyber espionage (nation-state actors). Insider threats include potential employees -looking to take action against an organization or individual. Again, the specific TTPs used by attackers are constantly evolving, with specific campaigns and efforts sometimes running for a period of weeks to even sometimes years. Section 8 outlines how cyber threat information sharing can enable maritime organizations to maintain awareness of the latest threats.

GROUP	MOTIVATIONS	OBJECTIVES
Nation States / State Sponsored Organizations (Advanced Persistent Threats)	▪ Political gain ▪ Financial gain ▪ Espionage (including commercial & industrial) ▪ Commercial gain ▪ Smuggling	▪ Gaining data, intelligence and information ▪ Disruption to economies and critical national infrastructure ▪ Providing advantage to their national commercial enterprises in the marketplace ▪ Financial / economic to offset sanctions
Criminals	▪ Financial gain ▪ Commercial / industrial espionage ▪ Fraud ▪ Smuggling ▪ Bribery	▪ Selling stolen data ▪ Ransoming stolen data ▪ Ransoming system operability ▪ Arranging fraudulent or illegal transportation or smuggling of cargo and/or people ▪ Gathering intelligence for more sophisticated crimes, exact cargo location, ship transportation and handling plans, etc.
Insiders	▪ Revenge ▪ Unintentional	▪ Seek payback for perceived harm ▪ Perform duties (accidental risk)
Activists	▪ Reputational damage ▪ Disruption of operations	▪ Destruction or unnoticed changing of data ▪ Publication of sensitive data ▪ Media attention ▪ Denial of service (DoS)
Opportunists	▪ The challenge	▪ Getting through cyber security defences ▪ Self-fulfilling, adventure ▪ Financial and reputational gain
Terrorists	▪ Ideological ▪ Political	▪ Disruption or destruction ▪ Media attention ▪ Influence political agendas ▪ Financial gain to support their activities

Figure 6 - General attacker types

When evaluating risk to their organization, ports and port facility leaders should seek to identify relevant threat actor profiles and anticipate their motivations and objectives. This allows for an improved ability to develop cybersecurity strategies that can evolve to counter the tactics employed by threat actors. These strategies can be supported through information sharing mechanisms described in Section 8.

4.2 Understanding the potential physical impacts of a cyber attack

A cyber-attack against port critical infrastructure represents a risk not only for the organizations responsible for such assets, but also for their partners, suppliers, customers and all companies and individuals potentially affected. Cyber-physical attacks against critical port systems could target IT, OT, and/or IIoT systems that manage or are connected to a wide range of equipment, such as terminal operating systems, cranes, gate systems, locks or bridges, camera systems, fuel systems, electric power systems, traffic management system, or any other system supporting daily port operations.

Challenges Likely to be Exploited by Cyber Threat Actors Targeting the Maritime Industry

- **Labor costs and skills shortage.** As digitalization across the maritime sector accelerates, the skills necessary for supporting and securing complex systems will increase in value and demand. Labor shortages may arise, which will further pressure organizations and provide opportunities for attackers to identify insecure systems.
- **Weaknesses in IT/OT/IIoT security architecture.** Port architectures are evolving to support increased sharing of digital data, particularly for use in real-time supply chain operations. Monitoring, reporting and new port business processes, such as the digital twin, require open communication flows between IT, OT and IIoT technologies. As a result, vulnerable designs can lead to new critical breaches.
- **Insecure software development.** Attackers will continue to exploit software vulnerabilities, whether commercial-off-the-shelf (COTS) or in-house developed software. This could be via regularly published commercial software vulnerabilities, or less well-known vulnerabilities in custom software.
- **Undisciplined lifecycle support / change management.** Unfortunately, when key systems are temporarily taken offline to perform maintenance or apply security patches, updates or upgrades, operations are temporarily suspended impacting port operations. As a result, updates are often postponed, leaving critical IT/OT/IIoT systems vulnerable to attack.
- **Integrated one-to-many relationships.** The maritime sector is supported by a number of commonly used applications. For example, the global expansion of Maritime Single Windows (MSW) can potentially act as force multipliers for threat actors seeking to exploit access to integrated electronic platforms.

Figure 7 - Challenges likely to be exploited by cyber threat actors

The physical consequences of a cyber-attack could prove to be wide ranging and could severely impact port and/or port facility activity, along with their dependent supply chains, lasting days or even weeks.

Although IT, OT, and IIoT integration is well intentioned, a cyber-attack against integrated systems could result in a major security and/or environmental incident. Examples of physical-cyber-attack impacts include:

- A compromised lock system could result in a major safety incident if water level controls are manipulated. For example, draining a tidal basin could jeopardize water pressure supporting the balance of a quay, resulting in safety concerns and a seriously damaged port.
- A bridge could be maneuvered when a ship or barge sails under it, triggering a collision.
- Unauthorized and/or unmonitored maintenance on equipment, systems or infrastructure (e.g. ship-shore, gantry crane, straddle carrier, conveyors) could generate vulnerabilities that threaten safety or the environment.

- Aides to navigation could be compromised (e.g. altering signal colors) or damaged, which could affect vessel traffic and safety.
- RADAR and AIS systems could be compromised whereby bathymetric and/or ship channel information is compromised, which could lead to vessel groundings.
- Compromised PLC controllers could result in over-pressurization of bulk liquid pipeline infrastructure, which could increase the risk of explosions.
- Compromised container monitoring systems (e.g. Smart Container) can result in illicit data manipulation, which can hamper tracking the locations of hazardous cargos or change of cargo details, resulting in increased risk to the environment and safety or allow for the unauthorized release of people, cargo, vessel release, or intermodal cargo transfer to facilitate smuggling activities.
- Compromised EDI files regarding loading plans could undermine container weight distributions, undermining ship load balance. Improper loading can undermine vessel seaworthiness, placing at risk the vessel, the environment and seafarer safety.
- Compromised vessel, cargo or custom clearances could result in port congestion and might compromise supply chain activity, resulting in local, regional and/or national economic losses.

4.3 Understanding the potential non-physical impacts of a cyber-attack

Examples of non-physical impacts can be characterized following the CIA-Triad model (Section 3.3).

Confidentiality
Port and port facilities create, process, receive, manage, store, and transfer large data volumes, which includes but is not limited to payment transactions, service activities, manifest data and banking details. Cyber threat actors might use any of this data for illicit gain that could impact organizational:

- ***Reputation***, by publicly releasing proof of the attack or a range of sensitive information.
- ***Competitiveness,*** by selling information to a competitor.
- ***Regulatory compliance,*** in the event the attacker publishes/sells part/all of the data and it contains sensitive information, the organization might be found guilty of violating privacy laws, such as, for example, the European Union's General Data Protection Regulation (GDPR).

Integrity
Most billing procedures are performed digitally and automatically. A cyber threat actor might alter information, which could impact the port or port facility's:

- ***Revenue***
  - Changing data to reduce charges to customers.
  - Changing data to increase payments to suppliers.
  - Changing data to transfer funds to the attacker's bank account.
  - Impersonate a C-level executive to give orders to an employee to transfer funds to the attacker's bank account.
- ***Regulatory compliance***
  - Changing data, such as emissions information, to indicate a regulatory issue or false formality reporting (customs, health, agriculture, etc.).
- ***Security***
  - Altering account data to hide unauthorized activity or compromise of systems.
  - Create falsified credentials or unauthorized accounts.

Availability
By undermining data or system availability, cyber threat actors can create impacts such as:

- Nullifying compliance with National Maritime Single Window (if administrative data cannot be exchanged anymore).
- Delaying or disrupt exchanging the operational data for traffic coordination, loading, or other operational processes.
- Delaying work efforts related to electronic Information for statistics and data analysis for marketing, customer service or other business operations.
- Providing historical data required for vessel accident investigations.
- Delaying submission of documents required by declarants (clearances, bills…).
- Undermining the ability for stakeholders to process orders, track cargo, etc.
- Effectuating an operational service outage resulting in a work stoppage.

5. THE ORGANIZATION'S CYBER ECOSYSTEM

5.1 Identify, inventory and classify critical activities and stakeholders

Every port and port facility is unique. One of the key challenges leaders face in their efforts to manage their cyber risk is the distinctive complexity of the integrated IT/OT/IIoT operations that is specific to their business and industrial port processes**. In order to manage their cyber risk port and port facility leaders must first understand what are the most critical operational activities, and who are the individual stakeholders supporting them.**

5.1.1 Critical activities

While the range of activities occurring in ports is diverse and unique to each operational environment, a common set of critical activities can be identified. Port and port facility infrastructure is comprised of any variation of administration buildings, cargo loading and distribution infrastructure, warehouses, storage areas and facilities, bulk liquid pipelines, and related utilities (water, electric, etc.). Port authorities often entrust the management of specific areas to commercial terminal operators, which assume responsibility for overseeing, operating and maintaining specific infrastructure (cranes, silos, specific fences, control facilities, passenger terminals, etc.). In addition, ports often furnish key services, provide security controls, and facilitate inspections of vessels, goods, passengers and port operations.

In addition, PCS environments support port operations by integrating and streamlining information exchange and critical service coordination activities among participating port entities.

A port or port facility can categorize key activities by core services, and their supporting critical information infrastructures, provided by:

- **Activities linked to sea freight and hinterland transport** (container, general cargo, bulk liquid or dry, etc.) with dedicated infrastructure and services to accommodate cargo ships and manage related operations (e.g. unloading and loading, storage, customs inspection, sanitary controls, etc.).
- **Activities related to the transport of passengers and vehicles** with infrastructure and dedicated services to accommodate passengers and vehicles onboard vessels and related operations related to managers (e.g. passenger bridges, parking, restaurants and bars, border control, etc.). This can also include Roll-on / Roll-off (RoRo) vessels.
- **Fishing related activities** with dedicated infrastructure and services to accommodate fishing vessels and manage related operations (e.g. unloading / loading of fish, inspection of fish, refrigerated storage of fish, etc.).
- **Activities related to traffic coordination** with dedicated infrastructure, technical equipment (video detection camera, AIS Station, traffic light or signal, etc.) and services to ensure safe and secure traffic management within the port area on the waterway as well as on land infrastructure.
- **Industrial activitie**s where operations are linked to port logistics, such as plants where products are routed from the port area for processing (refinery, petrochemicals, energy, etc.). Although such sites are often designated restricted areas, they are increasingly cyber interconnected.

5.1.2 Critical stakeholders

After identifying the critical activities in 5.1.1, ports and port facilities should also identify the corresponding critical port, maritime and industrial stakeholders. The stakeholder landscape involved in port activities and business processes (depending on the size, scope and complexity of the operating environment), can be extensive. This can reach several hundred or thousands of different processes in large ports). It is crucial to involve all identified stakeholders in the cybersecurity initiative, and these can include:

- **Ocean transportation:** shipping companies, shipowners, ship management companies, crew manning agencies, shipmasters.
- **Port service providers:** tug operators, pilots, linemen, waste collectors, chandlering services.
- **Authorities:** Maritime administration, customs, immigration, police, military, navy, coast guard, health authority, port administration authorities, agriculture, veterinary, port state control, statistics, and trade administrations.
- **Supply chain:** cargo agents, warehouse operators, freight forwarders, truckers, train operators, barge operators.
- **Industrial:** automotive, energy, chemicals, petrochemicals, aeronautics sectors, energy providers such as high voltage electricity, oil/gas, industrial water, steam, waste treatment companies.
- **Terminal operators:** stevedore, cruise terminal operators, bulk and liquid terminal operators, chemical terminal operators, ferries, roll on/roll of, clinker operator, refer operators.
- **PCS operators:** PCS management companies.
- **Cross-sector stakeholders:** essential service providers supporting primary port stakeholders.

5.2 Identify, inventory and classify critical assets

The complexity and diversity of port and port facility ecosystems and the uniqueness of each port is reflected in its specific deployment of IT/OT/IIoT systems. **To accurately identify cyber threats to a port or port facility ecosystem, it is essential to identify the ecosystem's digitally enabled systems, assets and infrastructures. Stakeholders should collaboratively create an inventory** of key port systems, data flows and interactions with external system dependencies identified in order to develop a baseline.[20]

Port operating systems interact with a wide range of automated technologies, such as machine-to-machine (via EDI) and/or manual interfaces (web interfaces, smartphone, emails, paper or fax). The data exchanged can be classified as follows:

- Mandatory declarations, such as electronic reports required to be submitted by shipping companies, freight forwarders or other stakeholders to port or other authorities, in accordance with international and national regulations.
- Control and authorization granted by the authorities to the commercial stakeholders such as port, vessels, goods, custom clearance or cargo handling operations authorizations.
- Operational data related to port services and processes such as, tugs, mooring or pilotage services, bunkering, waste collection services, and freight scheduling.
- Financial and business data, such as invoicing, payment processing, statistics.

[20] In the context of port communities, stakeholders may agree to collaboratively identify key services without providing specific asset or system details.

- Navigation and traffic management data, such as GPS vessels position in port area, AIS data, GNSS data, navigation tools (electronic lighthouse, traffic monitoring system, locks and bridges system automation).

Port activities can be identified according to the following services:

- Navigation services (in particular e-navigation) support data exchange regarding e-navigation using AIS systems, GNSS and radar, or even radio telecommunications. Navigation systems are increasingly being used for vessel arrival planning and port operation optimization.
- Ship berthing services rely on data exchange between vessels (merchants, passengers, fisheries) at sea, traffic within the port via PCS and VTS systems, and the ship-shore interfaces.
- Cargo information exchange services exchange data between the port and the facility storing and warehousing goods.
- Distribution and transfer services provide interconnection with logistics and industrial stakeholders, ensuring connectivity of data exchanges with multimodal stakeholders (inland waterways, rail, road), controls on goods or passengers. These exchange chains are key to pre and post routing delivery services efficiency. These cover a vast number of interfaces.
- Data exchanges with competent authorities, Maritime Single Window, health services, border control, photo-sanitary services at national and international level, including administrative documents required by IMO and other relevant authorities, must be handled electronically in adherence with established regulations. Such data exchange will intensify in the coming years.
- Ship loading and unloading services involve data exchange linked to cargo services. Often highly automated, these exchanges are enabled by terminal operating systems (TOS) or PCS.
- Support services can also include stakeholders responsible for port and infrastructure maintenance services.
- Security and safety services involve data relating to perimeter protection and surveillance capabilities, which often involve video, access control and remote sensing technologies, but also the tools that allow remote monitoring, as well as ensuring the security of the port and operations.

As a following step, **port and port facility leaders should identify all critical third-party systems in order to fully understand their operational ecosystem** in order to determine their cybersecurity resilience objectives. These can be organized along the following lines:

- Systems used by maritime stakeholders (seafarers, shipping agent, captain and ships crew, etc.).
- Systems used by other transportation stakeholders to share cargo or passenger information and enable transshipment (inland waterway transport, road companies, railway companies, etc.).
- Systems used by authorities at local, national or regional levels.
- Systems used for satellite and maritime surveillance.

In closing, **port and port facility cyber ecosystems are dynamic and its stakeholders are highly interdependent. Therefore, periodic review of the ecosystem and its critical activities, and making appropriate adjustments, are recommended** to offer better resilience to cyber-attacks and transversally across all port business processes.

6. ASSESSING FOR RISK AND VULNERABILITIES

6.1 Assess for vulnerabilities

The purpose of a cybersecurity vulnerability assessment is to identify and evaluate the cybersecurity vulnerabilities within the complex operating environment of a port or port facility. The vulnerability assessment requires input from all critical stakeholders and includes the identification of prioritized mitigation options which the organization might invest in.

Cybersecurity vulnerability assessments are not uniform, but most include a similar set of activities, such as: identifying assets; ranking asset value and importance; defining asset vulnerabilities; and implementing risk-based mitigation tactics. Ports and port facility environments frequently involve some degrees of integration, so IT/OT/IIoT systems should be identified and reviewed. Furthermore, as vulnerabilities in one functional area could, if compromised, jeopardize another area, all data, network connections, and IT-enabled OT systems and processes should be identified. For example, non-segmented networks, lack of updated antivirus software, poorly configured systems, and poor password discipline represent vulnerabilities common to port and port facilities.

6.2 Assess for impact

***Impact* refers to the potential harm that a cyber threat might cause to a port or port facility.** Impact is based on the key criteria affecting the organization's business functions or operations, facility security, staff safety, and environmental risk. Loss scenario analysis (Section 2.1.2) supports this activity. For example, in 2017, the *NotPetya* attack disrupted A.P. Moller-Maersk operations, resulting in reported losses of around USD 300 million (Section 3.1).

6.3 Assess for risk

The primary aim of a cybersecurity risk assessment is for the port or port facility to gain insights into the cyber risks to its operations. *Risk can be* generally defined as a measure of the extent to which a port or port facility is threatened by a potential circumstance or event, and typically derives from the adverse impacts that would arise if a circumstance or event occurs; and the likelihood of that occurrence.

For example, the NIST CSF[21] provides a framework for how a port or port facility might achieve this:

Identify and document asset vulnerabilities, as well as internal and external threats.
Acquire threat and vulnerability information from external sources.
Identify and analyze business impact; determine likelihood of risk factors by reviewing threats, vulnerabilities, and the likelihood of their impacts.
Define and prioritize risk response activities.

Cybersecurity risks are those risks arising from the loss of confidentiality, integrity, or availability of information, such as the loss of data relating to cargo manifests, dangerous goods declarations, or data processed by IT systems (Section 3.3), and that could generate adverse impacts to a port or port

[21] U.S. National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1), also commonly referred to as the "NIST CSF".

facility's operations (e.g., cargo operations, scheduling) or assets, individuals, key third parties, or even critical national infrastructure. [22]

Risk assessments identify and quantify the risks applicable to the port or port facility's operating environment. The key steps in a risk assessment are risk identification, risk analysis and risk evaluation.

6.4 Risk identification

6.4.1 Asset identification

To identify risk, a port or port facility should identify its key assets and threats and create risk scenarios for ways that potential threats could affect its assets.

Asset visibility is critical to ensuring that unauthorised devices are not connected to a port or port facility's networked environment, and enables stakeholders to distinguish between authorized and unauthorized assets, systems, platforms, and equipment. A port or port facility should establish and maintain a list of physical and logical assets and systems that are authorized to connect to the networked environment, including all IT/OT/IioT equipment, systems, and applications. Furthermore, some of assets might be located in various locations in the port which are not easily to monitor. Furthermore physical protection and surveillance measures should also be deployed to prevent unauthorized access.

Critical equipment are equipment or systems whose direct failure will lead to a potentially hazardous situation or an accident, thereby potentially causing injury, loss of life, or damage to property or the marine environment. **All critical equipment dependencies (e.g. third-party services rendered to support the equipment) related to operational safety, health, and environmental protection, along with impact to operations and business, should be identified.** Examples of critical IT/OT/IIoT-enabled systems might include dangerous goods declaration system, cargo reception and handling systems, supply chain management systems, Customs clearance systems, and/or marina operations.

Referencing asset inventories, the organization should also develop data flow and network architecture diagrams. Such diagrams can assist stakeholders in identifying potential access points attackers might exploit to gain access to primary and secondary assets, and should also indicate connection points to other networks and/or the Internet.

6.4.2 Understanding data as an asset

Port and port facility leaders should recognize that the data their organizations generate, process, transmit, and store are assets worth protecting. Port and port facility executives should remember that whenever data is processed or transmitted it is vulnerable. Sensitive data includes customer records, shipment instructions, manifests, bills of lading, banking information, contact and address information, and purchasing histories. It also includes key logistics information, such as cargo characteristics, vessel loading data, passenger manifests, customs inspection notifications, and national tax collection and disbursement information, etc.

[22] NIST SP 800-53 (Revision 4); See also: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, and *Guide to Cybersecurity Risk Assessments for Critical Information Infrastructure*, CSA Singapore (December2019)https://www.csa.gov.sg//media/Csa/Documents/Legislation_Supplementary_References/Guide-to-Conducting-Cybersecurity-Risk-Assessment-for-CII---Feb-2021.pdf

Although not every employee may have access to the organization's data, data theft can affect individuals specifically, as well as the organization overall. Employee data[23] loss can result in privacy violations, financial fraud, and/or emotional injury to an individual. Theft or manipulation of commercial data can result in financial losses stemming from fraud.

To identify and prioritizing key data assets, executives and key stakeholders should collaborate to answer the following questions:

- What data is most critical to my organization's operations? What is non-critical?
- What data is most valuable and to whom it is valuable?
- How is my organization's data managed? Who has access to what data?
- How is my organization's data protected? How is it backed up?
- Can my organization recover from an attack if all data was lost and unrecoverable? And how fast?

6.4.3 Assess for threats

Risk and threat assessments are designed to identify which assets, systems, operations, and processes require protection. They determine their value, along with the consequences of disruption.; They also identify threats and vulnerabilities affecting them as well as mitigating actions. A *threat event* is when a threat agent acts against an asset that potentially could result in harm to that asset. To ascertain possible threat events that could exploit asset vulnerabilities, third-party sources (e.g. vendors of cyber threat information) can assist with identifying threats to ports and port facilities. Such threat events can be applied to each asset that presents an entry point by attack vector into the system. Applicable threat events affecting assets are documented. Cyber threat actor attack stages can also be incorporated into such analysis[24].

6.4.4 Create risk scenarios

Consistent with loss scenario analysis (Section 2.1.2), the purpose of developing accurate risk scenarios is to detail how a cyber threat might affect a port or port facility's critical asset(s) and provide a reasonable risk analysis based on operational context, system complexity, and potential threats. Risk scenarios can also facilitate stakeholder communication and systematic analysis of key risk factors.

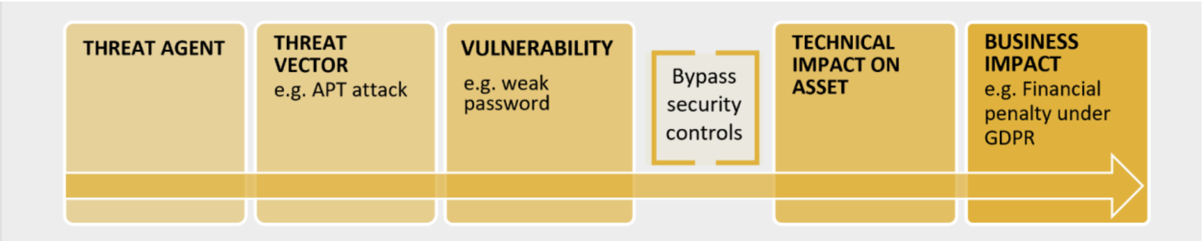


Figure 8 - Design of risk scenario

[23] Also referred to as *Personally Identifiable Information*, or "PII".

[24] Examples include Lockheed Martin's Cyber Kill Chain® and MITRE ATT&CK models.

6.4.5 Risk analysis

***Risk analysis* evaluates the likelihood of a risk scenario occurring and its potential consequences (i.e., impact).** Using the loss scenario analysis methodology detailed in Section 2.1.2, ports and port facilities should consider the following parameters when ascertaining risk likelihood:

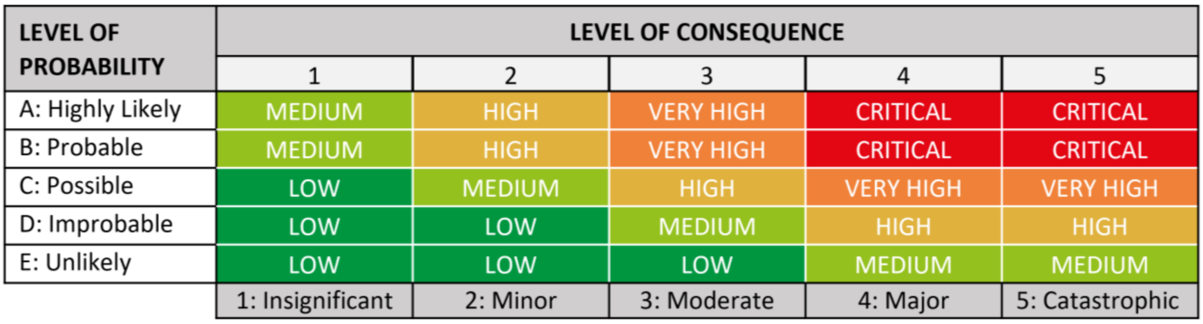
- ***Exploitability* –** This characterizes the degree of difficulty of exploiting an asset's vulnerability. Factors such as tool sophistication, technical skills to execute the attack, access control rights, current security controls in place, etc., affect this.
- ***Discoverability* –** This characterizes the degree of difficulty of discovering an asset's vulnerability, which could be estimated based on asset exposure (e.g., via Internet connectivity) and if vulnerability information is readily available.
- ***Reproducibility* –** This refers to the degree of difficulty of re-creating the vulnerability to compromise an asset. Depending on an organization's defense measures (e.g., monitoring and detection), a cyber threat actor may need to design exploits of varying complexity targeting an asset and existing operating conditions.

Applying this approach, a risk assessor could assign a score scheme to any of the above factors (for example, between 1 to 5), then calculate a score average. The ensuing score characterizes risk scenario likelihood.

Realization of any of the risk scenarios could disrupt a port or port facility's business operations, damage its reputation, or trigger financial loss. To further determine risk **impact**, ports and port facilities should consider developing an assessment table with organization-specific descriptors (e.g., business objectives or performance metrics) for the impact rating, then assign an impact score. Impact ratings can then be applied to each risk scenario to gauge risk to confidentiality, integrity, and availability.

6.5 Risk evaluation

Once a risk scenario is developed, port and port facilities should ascertain risk scenario significance by prioritizing and documenting the risk. Risk prioritizations are derived from the likelihood and impact analysis results, and cyber breach consequences can be mapped to a **risk matrix**



LEVEL OF PROBABILITY	LEVEL OF CONSEQUENCE				
	1	2	3	4	5
A: Highly Likely	MEDIUM	HIGH	VERY HIGH	CRITICAL	CRITICAL
B: Probable	MEDIUM	HIGH	VERY HIGH	CRITICAL	CRITICAL
C: Possible	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
D: Improbable	LOW	LOW	MEDIUM	HIGH	HIGH
E: Unlikely	LOW	LOW	LOW	MEDIUM	MEDIUM
	1: Insignificant	2: Minor	3: Moderate	4: Major	5: Catastrophic

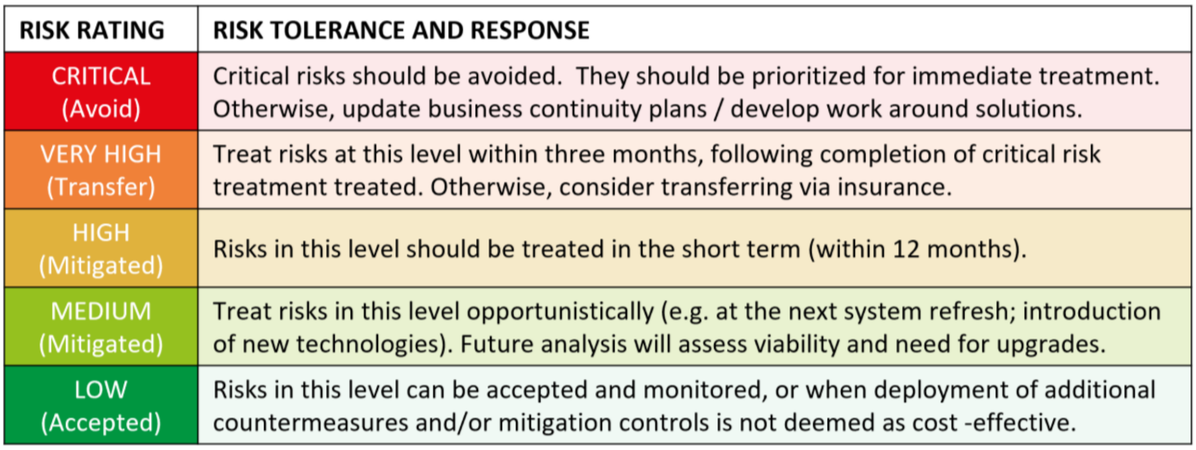
Figure 9 - Risk matrix for determining risk level for individual risk scenario

All risk evaluation outcomes should be documented in a **Risk Register** that pairs risk scenarios to risk levels. The Risk Register aids stakeholder communication and should be regularly maintained and reviewed to ensure leadership is aware of relevant cyber risks. Risk Register elements include:

- ***Risk scenario –*** A scenario describing how a cyber threat actor could successfully exploit a potential vulnerability to access an asset that might result in a debilitating impact.
- ***Date of identification –*** The identification date of the risk scenario.
- ***Existing controls and processes –*** Controls and/or processes needed to mitigate a risk scenario.
- ***Initial risk –*** The risk level (i.e. function of likelihood and impact) of the individual risk scenario after assessment of existing controls and processes.
- ***Residual risk –*** Risk exposure that remains following the implementation of mitigating controls.
- ***Treatment plan –*** The actions (e.g. implementation of new controls and processes) and timeline required to reduce the gross risk to a level deemed tolerable to a port or port facility leadership.

6.6 Risk tolerance

Risk tolerance refers to the level of risk-taking acceptable to achieve specific business objectives, and risk tolerance determinations enable executives to identify acceptable risk limits. When defining risk tolerance performance objectives should be defined, mitigation options identified, and risk acceptance thresholds established. Specific risks should be compared against defined risk tolerance thresholds. Risk scenarios with risk ratings exceeding defined tolerance thresholds should be prioritized for treatment until such risks fall to within acceptable tolerance limits. Timelines for risk treatment should be defined. Figure 10 highlights how port and port facility leaders can approach risk tolerance determinations.



RISK RATING	RISK TOLERANCE AND RESPONSE
CRITICAL (Avoid)	Critical risks should be avoided. They should be prioritized for immediate treatment. Otherwise, update business continuity plans / develop work around solutions.
VERY HIGH (Transfer)	Treat risks at this level within three months, following completion of critical risk treatment treated. Otherwise, consider transferring via insurance.
HIGH (Mitigated)	Risks in this level should be treated in the short term (within 12 months).
MEDIUM (Mitigated)	Treat risks in this level opportunistically (e.g. at the next system refresh; introduction of new technologies). Future analysis will assess viability and need for upgrades.
LOW (Accepted)	Risks in this level can be accepted and monitored, or when deployment of additional countermeasures and/or mitigation controls is not deemed as cost -effective.

Figure 10 - Sample risk tolerance

7. PROTECTION, DETECTION AND MITIGATION MEASURES

Ports and port facilities across the digital divide should adopt a holistic approach to managing their cyber risk as outlined in Section 3. **Since perfect security is impossible to achieve, establishing the ability to protect critical assets and information, identify threats, detect breaches, and initiate appropriate countermeasures in a coordinated response action is critical.** Unfortunately, intrusion detection capabilities have long been an area suffering from underinvestment. For example, the average organization takes 280 days to detect a cybersecurity breach and begin the mitigation process.[25]

To develop effective cybersecurity measures, the port or port facility should:

- Identify all critical assets, relevant dependencies, and network and data flow diagrams (Section 6.4). **Asset inventories and network and data flow diagrams provide stakeholders with key insights related to all the applications and IT, OT, and IIoT enabled systems, equipment and infrastructure, as well as digital assets (data) that require protection.**
- Identify, assess, and prioritize all cybersecurity vulnerabilities that should be addressed for mitigation (Section 6).
- **Identify, characterize and regularly review all cybersecurity threats** to the organization, evaluating how each could impact the organization's operations (Section 4).
- **Identify an appropriate security framework** to customize this to the organization's specific operating environment[26]. Security measures should be structured to drive a continuous improvement process (Section 11) that should be maintained in order to manage organizational cyber risk within acceptable risk tolerances.
- **Understand how various cyber threat analytic frameworks** can be leveraged to understand how attacks and indicators of compromise (IOCs) can be leveraged to help protect, detect, and respond to cyber-attacks.

7.1 Protection measures

Identification of critical assets, data, diagrams, dependencies and threats will inform the scope, range, strategies, and depth of appropriate protective measures.

Most port and port facility stakeholders on either side of the digital divide will frequently assume that accounts, applications and integrated IT, OT, and IIoT systems can be *trusted*. While such perceptions continue to persist, increasing interconnectedness and the accelerated adoption of cloud services conspire to blur the boundaries between external and internal access rights and privileges. **Unfortunately, the weaknesses that inevitably emerge from trusted relationships - are often exploited by cyber threat actors after gaining initial entry to the organization's trusted network operating environment**. This allows what would be a relatively small problem to quickly spread.

[25] See: https://www.ibm.com/security/data-breach

[26] Available resources offering guidance on protective measures can be obtained from ENISA, NIST, and ISO.

The concept of a "trusted network" within a port or port facility's perimeter should be abandoned in favor of adopting the "zero trust" concept. This is due to the complexities of modern maritime operations that require a broad range of internal and external connections – consisting of users, partners, vendors, customers, suppliers, and so on. In its simplest form, the zero trust concept means that no user, device or application should be trusted without verification, irrespective of whether the user, devise or application resides inside or outside the organization's networked environment.

In addition, port and port facility executives can protect their organization against cyber threat actors by considering the employment of security measures within the context of the following categories:

- ***Organization* – An internal security team should be organized (or third-party services retained) to anchor the port or port facility's cybersecurity measures.** Clear accountabilities and responsibilities should be defined and assigned. In addition to identifying key staff for overseeing cybersecurity (Section 2), clearly identifying all critical digital asset owners, as well as the owners of cyber risks, should be performed.
- ***Processes* –** Using the basic cybersecurity measures described in these guidelines, port and port facility stakeholders should **integrate cybersecurity control measures into organization-specific processes that also support defined performance objectives.** Examples include embedding security requirements with compliance-based risk management activities, enterprise risk management policies, and vendor contracts. Reviews of supplier agreements should be performed with a specific focus on cybersecurity clauses (e.g. breach notification requirements).
- ***People* –** While people represent the weakest link in a port or port facility's cybersecurity program, they also represent the first line of defense. Thus, **protective measures should be established for all staff granted access rights to digital assets, systems and/or infrastructures.** These include pre-employment background checks, initial cybersecurity awareness training (Section 9), defining cybersecurity commitments during the onboarding process, and regular cybersecurity awareness training activities (e.g., phishing). De-provisioning practices should be employed during off-boarding process. When staff changes occur, physical and logical access permissions should be revised and/or withdrawn (and coordinated among IT and security stakeholders) in a timely manner to avoid credential accumulation and preempt the potential for unintended access.
- ***Technology* –** Technological measures represent the largest part of the protective measures and include access control, network monitoring, communication, and protections for systems, equipment, data, applications and networked infrastructures. **Technology measures are intended to block unauthorized access and data traffic (access control), prevent attacks and malware, and protect systems and data from being compromised or lost.**

AREA	EXAMPLES
Access Control	▪ Identity and access management ▪ Privileged account management ▪ Role-based-access and least privilege ▪ Password conventions ▪ Multi-factor-authentication ▪ Regular reviews of accounts an access rights
Endpoint and Network Security	▪ Network segmentation (e.g. separation of operational networks and administrative networks from office IT) ▪ Firewalls (traditional and Web Application Firewall – WAF) ▪ Isolation of critical or vulnerable systems ▪ Remote access, VPN

	▪ Network Access Control (NAC) ▪ Malware protection ▪ System hardening
Data Security	▪ Encryption to protect data in port/port facility systems, at rest, in transit and in use ▪ Data classification. ▪ Removable media controls ▪ Equipment disposal including data destruction ▪ Use integrity checking mechanisms to verify software and firmware ▪ Data leakage prevention/protection – DLP
Operational Security	▪ Change and update Management ▪ Patch management ▪ Separation of duties ▪ Vulnerability management ▪ Fraud prevention ▪ System hardening ▪ Cyber intelligence

Figure 11 - Example of protection measures

Physical protection measures

Protection against physical threats, such as unauthorized access, sabotage or spying on information is achieved by employing suitable physical security measures. Physical security systems and their supporting practices are often relegated to traditional management practices and procedures aimed at complying with international standards, such as the IMO's ISPS Code. Organizationally, **cybersecurity and physical security stakeholders should regularly collaborate and communicate.** For example, suspicious activity reports should be shared, notifying both stakeholder groups of possible events that could impact one or both areas of responsibility.

Physical security capabilities enable cybersecurity, for example, by controlling access to OT systems and network-enabled equipment and infrastructure(s) that frequently reside in restricted areas. Such systems and components also often depend on IT enabled networks, which may also include integration points connecting IT, OT and IIoT and automation platforms that can often be easily compromised, resulting in catastrophic effects on port security (Section 3.7).

7.2 Detection measures

Detection measures are critical for determining when protective measures have failed, and there are several ways port and port facility stakeholders can determine if an event has occurred or if a cyber-attack is in progress. The most obvious is when an asset or system ceases functioning, such as in the case of a ransomware attack. In other cases, an asset or system may exhibit unusual or irregular behaviors. More concerning, however, are attacks that render no immediate or obvious results leaving the incident often undetected unless additional detective measures are in place. For IT-enabled OT/IIoT equipment, platforms or infrastructure, the results could threaten staff safety or the environment. Similarly, undetected threat actors in administrative systems could affect financial activities.

Port and port facility executives should ensure that adequate levels of protection are implemented in order to detect anomalous or nefarious activities that if left unaddressed could leave their organizations vulnerable to cyber-attack. The specific capabilities that need to be implemented depends on the specific requirements of the organization. Depending on resource availability and risk tolerances, port and port facility executives should consider technical solutions and activities such as:

- Intrusion detection systems / intrusion protection systems (IDS/IPS).
- Security Information and Event Monitoring (SIEM) systems.
- Vulnerability scanning.
- Threat hunting.
- Continuous monitoring, managed security services and/or managed detection and response.

Organizational measures

Clearly defined stakeholder responsibilities and processes (Section 2) are needed to support effective cyber event detection. **Employees are critical for the detection process and should be appropriately trained to recognize cybersecurity incidents and report them to designated staff.** Depending on the size and maturity of the port or port facility, consideration should be given to organizing an internal Cybersecurity Incident Response Team (Section 10), the development of a Security Operations Center (SOC) or even outsourcing these capabilities. Also, establishing formal relationships with national and/or international CERT/CSIRT organizations, as well as the nurturing of key third-party services providers can prove useful regardless of the maturity level, e.g., for the exchange of cyber threat information.

Technical measures

To support technical detection capabilities, ports and port facilities should allocate dedicated resources to both identify and evaluate suspected cybersecurity events. This can be accomplished by employing a SIEM platform, which centrally collects, aggregates and collates log data, correlates security events, and alerts on anomalies. Examples of relevant events that SIEMs alert on are listed below:

- Failed login attempts.
- Permission changes, such as privileged user groups.
- Unusual user behavior, e.g. incorrect login attempts, login hours.
- Unusual access attempts, e.g. to confidential areas or to honeypot systems.
- New account creation.
- Detected attack patterns (intrusion detection), Indicators of Compromise (“IoCs”) or malicious code (malware detection) in the data stream or on systems.
- Abnormal network activity (new/unknown endpoints, unusual communication or data volume).
- Changes to security-related settings, such as disabled virus scanners.
- It is important that all phases of a cyber-attack can be detected in order to quickly identify an attack. The MITRE ATT&CK® Framework[27] can be established to facilitate cyber-attack classification and is structured phases (Figure 12).

[27] See: https://attack.mitre.org/

PHASE	EXPLANATION
Reconnaissance	Finding out information about the target to prepare an attack, e.g., through active scanning, phishing, or open source intelligence (OSINT).
Resource Development	Preparing the attack by creating necessary resources, such as infrastructure, accounts, or capabilities.
Initial Access	Techniques used to take initial access to the target's internal structures, such as exploiting vulnerabilities, drive-by compromise, or phishing.
Execution	Execution of malicious code that allows attackers to perform an attack.
Persistence	Creating persistent access to the target's resources, e.g., by installing backdoors or modifying authentication credentials.
Privilege Escalation	Extending privileges within the target's networks and systems, e.g., by exploiting vulnerabilities or misconfigurations.
Defense Evasion	Taking steps to prevent detection and defenses, e.g., by changing security settings or disabling protection software.
Credential Access	Accessing authentication data, such as passwords, e.g., by trying (brute force), reading passwords from password stores, or using key-loggers.
Discovery	Exploring the target's environment, e.g. by observing network traffic, reading user directories or file repositories.
Lateral Movement	Extending access across the target environment (e.g., via remote services, software distribution, using stolen credentials to compromise assets, or exploiting vulnerabilities).
Collection	Gathering data that may be of interest to the attacker, e.g., file repositories, databases, email and browser data, or taking screenshots and recording keystrokes.
Command and Control	Remote control of the victim's compromised systems, usually by impersonating unobtrusive traffic to avoid detection.
Exfiltration	Exfiltration of collected data, e.g., in encrypted or compressed form, to avoid detection.
Impact	Manipulation of systems, data disruption or destruction (e.g., by removing access permissions, encrypting, or deleting files).

Figure 12 - Cyber-attack classification

7.3 Mitigation measures

An appropriate response to a cybersecurity incident is only possible if trained staff are identified and assigned, and they are provided with the necessary authorities, processes, procedures and technologies to perform mitigation activities. While Section 10 specifically covers cybersecurity incident response, pre-incident planning activities represent critical elements of protection and defense.

Business continuity / disaster recovery plans

Ensuring business continuity or returning to a suitable state of operation within an acceptable period of time is the goal of a business continuity and disaster recovery plan, regardless of the cause. **Business continuity / disaster recovery (BC/DR) plans specify the advance precautionary measures that should be taken, as well as the specific actions to be employed in the wake of a cyber incident (Section 10.6).**

Effective BC/DR planning requires port and port facility executives and key decision-makers to understand the critical issues that will arise in the event the organization suffers a cyber incident and to be aware of and be properly trained in appropriate recovery procedures.

BC/DR planning begins with an assessment of organizational cybersecurity capability strengths (Section 8) and the cyber risks the organization is confronted with if its IT, OT or IIoT systems are no longer functioning. Specifically, responsible stakeholders should know the critical OT or IIoT functions that may be impacted in the event of specific IT systems being rendered inoperable. A risk assessment with identified mitigation measures can help clarify how the organization might be affected. In addition, loss scenarios (Section 2.1.2) that address cyber-physical risks can offer specific insights into critical recovery times.

Data backup / data recovery

Data backup is a critical element of both cyber risk management and disaster recovery planning and represents the ability to access functional data backup and to restore such data within required timelines. If the organization's data is compromised, stolen or destroyed, or even erased accidentally by an employee, a backup copy will facilitate recovery and can allow a return to normal operations.

Ports and port facilities should implement backup policies, which describe all backup activities, and define backup frequency (e.g. daily). Identify in the policy the roles, responsibilities and authorities of individuals responsible for backup activities. Identify where and how the backups are stored. Consider implementing the following best practices:

- ***Back up all information and test backups*** – Create, manage, and regularly test backup efforts, ensuring copies of data, software and system images are consistent with cybersecurity policies.
- ***Protect backup storage facilities*** – Identify all backup equipment or software needed to restore key functions and ensure all storage areas (e.g., lockers/closets) have appropriate security, such as locks, and environmental controls, such as dehumidifiers or water-resistant closures, to protect electronic equipment. Backups should be retained off-site (alternate facility if possible) and if necessary stored offline.
- ***Encrypt data in transit*** – Use software to protect data in transit through encryption.
- ***Encrypt backup data*** – Encrypt all backups. Create multiple backups so that, in the event of a breach, restoration can be performed with a version predating the infection.
- ***Consider the cloud*** – Cloud storage costs continue to drop and are a viable option for ports and port facilities seeking cost savings while realizing enhanced network scalability and availability.
- ***Establish redundancies*** – Ensure redundancies are established for key IT, OT and IIoT systems, Identify safety, security, and operational needs for systems with high-availability requirements.
- ***Train and exercise*** – Train staff to engage manual processes for re-establishing critical operations. Exercise recovery plans for cyber incidents compromising IT, OT and/or IIoT systems.

8. INFORMATION SHARING, COMMUNICATIONS AND COORDINATION

8.1 Information sharing, communication and coordination

Cybersecurity information sharing, communication and coordination represent a broad, yet essential component of every cybersecurity program as outlined in NIST's *Guide to Cyber Threat Information Sharing*[28]. This chapter does not repeat the NIST documentation, or other technical information sharing references, but instead presents C-Suite considerations for cybersecurity information sharing, including why, what, and how cybersecurity information sharing can reduce the cybersecurity risks for ports and port facilities.

8.2 Why share cybersecurity information?

The concept of information sharing is often viewed through two lenses: "sharing is giving" and "sharing is exchanging". The "giving" approach is often negatively perceived as being one-way, of little to no benefit, and a pathway to exposing one's faults. Alternatively, the "exchanging" approach fosters an environment of two-way communication, mutual responsibility, feeling of community, building trust, and creating value for each other. The latter approach is recommended for ports and port facilities.

Cyber Information Sharing Benefits

- **Strategic Alignment** through integrated business and cybersecurity strategies.
- **Greater Compliance** with existing and emerging regulations.
- **Consistent Messaging** with all stakeholders resulting in a complete and common understanding.
- **Improved Resilience** with greater collective knowledge, experience and resources of the sharing community.

Figure 13 - Cyber information sharing benefits

Above all else, **cybersecurity information sharing enables informed decision-making for ports, port facilities, and their stakeholders**. Cybersecurity information sharing represents more than Cyber Threat Intelligence (CTI) for technical incident prevention and response; cybersecurity information sharing also includes sharing of non-technical cyber business risk information (CBRI) for internal coordination of cyber efforts. Effective sharing of both CTI and CBRI **provide a holistic understanding that can improve strategic alignment, resourcing, compliance, messaging and resilience**.

[28] NIST Special Publication (SP) 800-150: Guide to Cyber Threat Information Sharing; Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

8.3 Information sharing basics

Knowledge-based building blocks can be applied to initiate cybersecurity information sharing among key stakeholders and empower them with a foundational understanding of the necessary best practices from which an effective cybersecurity program can be created.

Levels of information sharing
Many levels of cybersecurity information sharing communities are available to ports. Considerations of different communities are presented below.

- ***Port or port facility (internal)*** – Sharing of CTI and CBRI internally, including technical information for incident prevention and response, and non-technical information to assess business risks.
- ***Port community (external)*** – Sharing CTI between port facilities and other supply chain partners in a port complex. This may include cyber threats against the port community, joint investigations, post incidents reports and analyses, exercises, and best practices.
- ***Port to port (or community to community)*** – Fostering bi-lateral cooperation by sharing CTI directly between known ports or port communities. This may include agreed upon cyber threat information, post incidents reports and analyses, exercises and best practices.
- ***Port sector*** – A sector-specific CTI sharing and analysis entity to share relevant cyber threat information that is common to ports in general. This serves as an option for large or small ports that may have common security goals to support port-to-port information sharing relations.
- ***Maritime sector*** – Similar to a port sector sharing entity, a maritime sector sharing entity shares CTI relevant to the maritime industry. Such an entity enjoys a broader risk perspective affecting the maritime sector and will also have CTI directly relevant to ports or port facilities, as well as vessel owners and operators and other maritime stakeholders.
- ***National*** – The maritime sector should be supported by a national level cybersecurity response center, usually the national Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), or equivalent. National CERTs are usually exposed to classified intelligence on cyber threats, and may provide ports and port facilities with key information regarding incidents, threats, alerts, analyses, directives, and provisions. Some national CERTs will operate a portal or information platform to exchange information with its constituencies.
- ***International*** – Performed on multiple levels, including port-to-port, community-to-community, sectorial unit to parallel unit, ministry-to-ministry, and/or government-to-government. Information shared depends on established policies, and can be affected by political trends. In some cases, the information shared, and its intensity, is subject to bilateral agreements signed between the countries or other stakeholder groups.
- ***General public*** – Some countries mandate public breach notifications. Ports and port facilities in these environments should consider predefined public notification procedures.

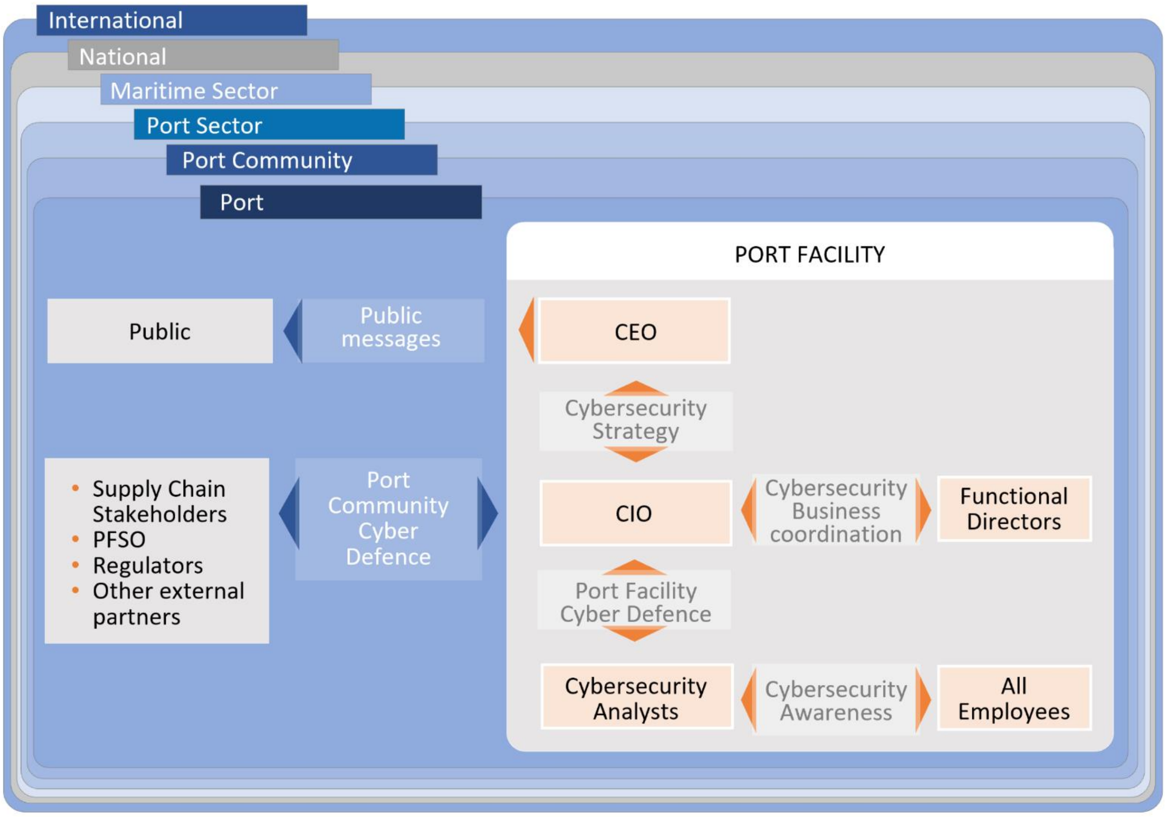


Figure 14 - Cyber information sharing model for ports and port facilities

8.4 Establishing a strong cybersecurity information sharing program

This section presents key considerations for port or port facility executives to establish an effective cybersecurity information-sharing program. Notably, the cybersecurity information sharing practices are highly dependent upon country-specific laws, cybersecurity operational and institutional deployment, inter-dependencies between entities and the culture of information sharing in the community.

Declare cybersecurity as an organizational priority

A **CEO or Managing Director's declaration of cybersecurity as a top priority will be effective in advocating for a cyber aware culture and aligning the organization's functional areas**, including key areas such as operations, IT, legal, risk management, finance, media relations, customer relations, government affairs, human resources, and procurement. **With the absence of such support, cybersecurity may continue to be viewed as a responsibility solely of the IT Department** and limit communications.

Designate a cybersecurity lead

The Designated Cybersecurity Lead will be responsible for implementing the cybersecurity information-sharing program[29]. The lead is the central role, serving as the coordinator for all key cyber activities. This role **must be able to translate organizational business strategy to cybersecurity technical strategy, coordinate cybersecurity efforts across different functional areas, engage with external stakeholders, and meet compliance requirements**. This role is frequently codified under the CIO, CISO, or another title, and for smaller ports or port facilities may even be contracted or outsourced. Whoever the Designated Cybersecurity Lead is, they should regularly meet with the port

[29] As outlined in NIST SP 800-150.

or port facility's Executive Leadership regarding the organization's cybersecurity strategy. This role should also initiate the communication company-wide in order to ascertain the understanding and execution of the measures derived from the strategy.

Establish information sharing relationships

Cybersecurity information sharing involves communications outside of the organization, including required and voluntary communications with stakeholders. Although the Designated Cybersecurity Lead will implement the program, the CEO or other designated **executive leadership is typically needed to secure the commitment from their peers in other organizations** for them to share their cybersecurity information.

Participate in sharing relationships

Executive participation will demonstrate the importance of cybersecurity information sharing and maximize its value. This may include periodic monitoring of the cybersecurity information-sharing efficacy, continuing to dedicate resources to the efforts, participating in community governance, and communicating internally and externally.

Continuously improve

As the cybersecurity information sharing community matures, it should seek to continuously self-evaluate. **Periodic reviews of changing risks, and refinement of sharing objectives and protocols is also recommended**. In addition, other information sharing communities, including from other industries, can be a source of learning for best practices[30] that can improve cybersecurity sharing in ports and port facilities.

[30] IAPH Port Community Cybersecurity paper, 2021, US Coast Guard, CG-5P Policy Letter, 12 December 2016, The National Institute of Standards and Technology (NIST) of the United States has developed Special Publication 800-150, UK National Cyber Security Centre, Cyber Security Information Sharing Partnership (NCSC CiSP), Cybersecurity Information Sharing Act of 2015

9. TRAINING

9.1 The importance of establishing organizational cyber awareness

9.1.1 The Human as a risk

Employee behaviors – curiosities, carelessness, prejudices, and desires – collectively represent weak links in a port or port facility's cybersecurity program. Ports and port facilities on either side of the digital divide face one universal challenge in cybersecurity: *managing the human*. Human error alone generates a vast array of cyber risk, and it is estimated that 95 percent of cybersecurity breaches are the result of human error, rather than IT-related faults[31].

Many of the most successful strategies cyber threat actors leverage the *psychology and behavior of people* in their interactions with digital technology. The range of professions, skills, languages, cultures of the people who interact with a port or port facility's assets makes the task of addressing human error a recurring challenge. Cyber threat actors are constantly seeking to penetrate IT/OT/IIoT assets and infrastructure, which control essential processes, or other systems involved in data creation, processing, storage, and transmission. They seek out human errors or tailor their attacks to exploit behaviors, prejudices, social connections, and/or cultural affiliations. Such errors offer footholds into networks, allowing cyber threat actors to penetrate more deeply into and across networks.

Although investments into various technical resources (e.g., access control systems, firewalls, etc.) enhance cyber defenses, such efforts can be rendered useless when an individual with the appropriate credentials (user name/password) exercises poor cyber hygiene by clicking on an email attachment or a URL link to a malware-infected website. **The challenge facing port leadership is how to provide adequate resources for delivering the necessary training** to develop awareness, monitor progress, and manage the resources and investments needed to achieve operational cyber resilience.

Types of Human Errors

- The ***compromised employee*** brings infected devices into (and connects to) an organization's IT/OT networks.
- The ***careless employee*** rushes to complete a task, often with no ill intent. Their errors are the result of violating security policies.
- The ***malicious employee*** creates deliberate harm by compromising an IT/OT system or stealing data. Their reasons may be financial, dissatisfaction or simply malicious.

Figure 15 - Types of human errors

9.1.2 Recognizing the Human as the first line of defense

Ultimately, executive sponsorship is required to ensure any training program's success. Port and port facility leaders should communicate clear expectations about training to non-IT staff across all of the organization's functional operating environments.

[31] https://www.cybintsolutions.com/cyber-security-facts-stats/

Although cyber risk is pervasive, training is a low-cost, high value-add investment. For cybersecurity training to be effective, it cannot be relegated to an annual 'check-the-box' activity or solely to IT staff. Although IT staff are directly responsible for assuring data integrity and ensuring network security, and **the obligation for sponsoring a cyber-aware culture rests on port and port facility executives, the responsibility for sustaining cyber resilience through ongoing engagement and awareness is ultimately a shared one. The Human represents the organization's first line of defense.** This involves all management and key decision-makers from IT, security, administration, risk management, human resources, procurement, contracts, training, health and safety, marketing, and communications.

Ports and port facilities with cyber-aware staff advantageously position their organizations within the local port community and the global maritime industry. **Specifically, a more cyber-aware workforce translates into a more cyber-resilient, competitive organization. When people are trained to both recognize cyber threats and understand how to respond to incidents, then the organization can more rapidly recover from cyber disruptions.**

9.2 Training is an integral part of a cyber risk management program

9.2.1. Workforce development and management

As ports and port facilities increasingly invest in and deploy IT/OT/IIoT-enabled technologies across their operating environments, they face the challenge of cultivating both a cyber-aware *and* cyber-competent workforce. Port and port facilities should require both general cyber awareness training for all staff to maintain attentiveness and more advanced training for IT/OT personnel to sustain skills and develop new competencies. This program could be developed respecting a personnel cycle perspective from onboarding until retirement or departure of individuals.

Developing workforce capacity as part of a long-term program requires coordinated actions that include identifying port requirements, tailoring training to specific staff, setting goals, identifying and tasking responsible parties to deliver training products, and assigning appropriate duties and responsibilities (which include management and oversight). Budgets should be established to sustain investments in training materials; technologies and related implementation activities should be organized for key functional areas. Training content should be presented in a manner that reinforces established plans, policies, procedures, and deployed technologies. All training should be monitored and knowledge gaps (including trends) consistently and regularly identified. Staff competencies should be mapped across all functional areas. Recruiting and hiring practices should address identified workforce gaps. Training strategies should be designed to mitigate shortfalls in any knowledge and skills area. Where possible, partnerships with local academic institutions should be explored and leveraged to develop workforce capacity. Communicating useful and practical tips and awareness campaign can support these training measures more effectively. Employees can apply these in their daily routine influencing their behavioral change and sensitivity to cyber-related issues.

Individuals Subject to Cyber Awareness Training

- All executives and senior managers.
- Finance, accounting and administration.
- Security, operations and equipment operators.
- Sales, marketing, and communications.
- Human resources and personnel management.
- Health, safety and training.
- Procurement, contracting and legal.
- Third parties – vendors, contractors and partners.

Figure 16 - Individuals subject to cyber awareness training

9.2.2 General awareness training

Regardless of a port or port facility's size, location, or complexity, **cybersecurity awareness training should be required for all staff accessing networked systems**. Where possible, cyber awareness training should be tailored to the organization. This involves:

- **Training for all administrative staff** accessing IT-enabled systems, such as desktop computers, which should address how to recognize malicious emails, adhere to defined policies as a condition for accessing network-enabled devices, employ strong password controls, and maintain secure credentials.
- **Training for operations staff** should include cyber threats to OT/IIoT-enabled systems, such as, cargo-handling equipment, bulk liquid transfer and storage systems, and conveyor systems.
- **Training for Port Facility Security Officers** should facilitate greater understanding of cyber threats and how to collaborate effectively with IT staff. Training should address how to recognize cyber-physical interconnections. For example, instruction should cover how to recognize an IT security hazard, such as unsecured ICT assets, and how to report on and/or investigate observed suspicious activities.

9.2.3 Technical cybersecurity training

Ports and port facility leaders with technical staff responsible for information security duties and responsibilities (e.g. CISOs, CIOs or IT Managers) should encourage ongoing advanced cybersecurity training. Training should enable cybersecurity operations, be structured to support defined performance objectives, and be adequately resourced. As a best practice, ports and port facilities should define cybersecurity skills, education, and/or training requirements prior to hiring IT staff. In addition, some technical staff, such as software developers, may require defined minimum cybersecurity knowledge levels, such as a working knowledge of secure software development lifecycle best practices.

Ports and port facilities seeking specialized cybersecurity training (including certifications) for technical staff can consider a wide range of professional development organizations offering globally recognized certifications and recurring training programs[32].

9.2.4. Training implementation

9.2.4.1 Tailored training activities

The first step for raising cyber awareness at a port or port facility is to implement a series of "all staff" events, such as lectures and webinars, sponsored by executive management, that emphasize cyber risk awareness. Ports and port facilities can then reinforce learning objectives through additional cybersecurity awareness-training options, such as computer-based (CD/DVD) and/or web-based cybersecurity awareness training courses designed for the maritime industry. Since vendors and third parties are increasingly performing back-end administrative monitoring and content

[32] SANS Institute (www.sans.org),Information Systems Audit and Control Association (ISACA) (www.isaca.org), International Information System Security Certification Consortium (ISC2) (www.isc2.org), Computing Technology Industry Association (www.comptia.org)

management tasks, training leaders should consider instituting compulsory cyber awareness training as a prerequisite for external stakeholders, who may be required to access critical IT/OT/IIoT systems.

Ports and port facilities should consider enriching cybersecurity awareness through onsite or virtual cybersecurity training programs, which can be tailored by to meet specific needs. The training materials may differentiate to suit comprehensive communication for different target groups of workforces. Ports or port facilities participating in port community systems or local information exchanges might also consider pooling resources to develop and maintain localized training materials.

9.2.4.2 Drills

Ports and port facilities subject to regulations, such as the ISPS Code, are already conducting quarterly drills. **Drill scenarios should be reviewed and expanded to accommodate cybersecurity situations that test the readiness of port or port facility personnel**. Drills should be designed as a collaborative effort between cybersecurity, security, and operations staff.

Incorporation of cyber risk factors into quarterly drills reinforces awareness of how a cyber threat can directly or indirectly impact operations. Cyber risks can be injected into many drill scenarios to test cross-functional incident alerting, escalation, and communications procedures. Drill scenarios should also include aspects of information and real-time threats sharing (Section 10), or scenarios involving third-party dependencies and port supply chains. Drills test cyber awareness across all drill participants regarding incident response knowledge (Section 10), effectiveness of assigned duties and responsibilities, response behaviors, and overall effectiveness. Results should be analyzed for impact and considered for revision of the cyber security strategy or plans, as required.

9.2.4.3 Exercises

Tabletop exercises (TTX), performed annually, are aimed at testing the effectiveness of the training. They should reflect the operating environment of the participants in order to determine how the organization might respond to hypothetical challenges. They should test general awareness, validate plans and processes, and assess the systems and procedures for incident response and recovery actions. Unforeseen challenges, consequences, and capability gaps can be revealed to highlight vulnerabilities. Results should be analyzed for impact to the organization directly, as well as any potentially affected third parties.

Training, security, operations, and IT staff should collaborate to review existing security and response plans to design risk scenarios that incorporate physical and cyber threats into a range of systems and processes. When performed, TTXs should measure the time and processes associated with detecting and alerting to a cyber incident and identify whether plans, staff, equipment, and alerting and communication procedures perform as expected. Integrated cyber-physical threat scenarios should stress the organization's administrative and operational environments. As appropriate, third parties, such as port community system partners (including port SOC members), regional or national CERTs/CSIRTs, specialized incident response vendors, and even designated authorities, can be included.

9.2.5 Training as a means for driving continuous improvement

Audits, inspections and reviews

Ports and port facilities should **regularly evaluate the performance and effectiveness of their cyber training program** by:

- Including cyber awareness in the annual security inspection and pre-audit process.
- Conducting randomized audits of key operational areas to test the awareness and behaviors of personnel and evaluate policies and procedures for effectiveness.
- Providing updated training and certification for IT security staff.

- Establishing oversight and reviewing controls to ensure regular monitoring of all training programs, content, and activities.

In implementing these strategies, staff knowledge gaps will be identified and subsequent corrective actions developed. These include training content and strategies, new tools and/or technologies, controls, policies and procedures, budget changes, and even new hires.

Develop lessons-learned

Documenting identified gaps, response activities, and mitigation recommendations in after-action reports will help leaders pinpoint opportunities for improvement. For example, breakdowns in the chain of command, confusion about responsibilities and authorities, and the impacts of cyber-attacks on operations should be clearly identified, characterized, and described. In addition, improvements for training content, resource requirements, and required skills should be clearly identified, defined, and prioritized.

10. INCIDENT RESPONSE AND RECOVERY

10.1 Incident response planning and preparation

In the language of cyber incident response, the maxim "*an ounce of protection is worth a pound of cure*" holds true[33], and today's **port and port facility leaders should assume their organization will one day suffer a cybersecurity breach.** Unfortunately, the continued growth in ransomware and email phishing schemes, along with the budding adoption of AI by criminal networks will challenge ports and port facilities on either side of the digital divide. Under such pressures, it is less a question of *if* rather than *when* a port or port facility will be breached.

To prepare for such contingencies, port and port facility executives should take the necessary steps to proactively prepare their organizations to respond to and recover from a cybersecurity incident. Doing so will serve to protect their organization's interests, mature its ability respond to and recover from an incident, and advance not only their operational resilience, but also strengthen broader cyber resilience of the port community within which they reside and the global maritime industry overall.

While the circumstances of cyber incidents will vary, there exist two types of incidents. The first is *enterprise* in nature, which impacts numerous areas across an organization. Since enterprise-level incidents can threaten the entire organization, they often require the mobilization of various staff from different functional areas (including the CEO and board of directors), as well as external technical experts who can be readily engaged to perform expert analysis and take corrective actions.

Types of cyber incidents

- ***Physical breach*** – Physical theft, the unintentional loss of an asset (its function is disrupted or lost), or the physical compromise of an asset that enables the facilitation of data theft, compromises data confidentiality and integrity, or enables access to an asset that has been removed from the organization that has not been properly degaussed.
- ***Data breach*** – The intentional or unintentional exposure, release, or loss to an untrusted environment of data classified as confidential, private, or sensitive.
- ***Network and/or system security breach*** – When a computer, network router, firewall or any network component is either compromised by a malware infection or is accessed by authorized or unauthorized users for malicious intent.

Figure 17 - Types of cyber incidents

The second type may be limited to a discreet site, asset, system, or operational process. Although initially physically localized or constrained, an incident of this type which goes undetected can result in a significant impact with immediate and/or cascading consequences. Depending on the severity, incident response actions might require the same level of resources mobilized for response and recovery. **Therefore, incident response planning and preparation efforts should be harmonized with the port or port facility's operational safety management activities.**

[33] Benjamin Franklin is often attributed to this quote, who regularly advised Philadelphians of fire risk.

10.2 Key components of cybersecurity incident response and implementation steps

Cyber incident response planning begins at the executive level because properly managing a breach response effort is not simply a technical matter. Proper incident response involves a range of disciplines, spanning all areas of port or port facility's operations, and should include stakeholders responsible for various functional areas and overlapping areas of responsibility.

Individuals assigned the responsibility for incident response can reference freely available resources and best practices to help guide their planning, organization, implementation, and sustainment efforts for an appropriate incident response program. For example, NIST and the European Commission offer free resources for stakeholders[34].

When planning any incident response for a port or port facility, port and port facility executives should collaborate with their leadership teams to consider the following steps:

Step 1: Create an incident response policy and plan

- Top management should c**ommit to establishing specific performance requirements and assign responsibilities**. Policies should outline scope, define actions, and identify members of the cyber security incident response team.
- **Implement a Cybersecurity Incident Response Plan (CIRP) and assign key stakeholders to develop, maintain, and execute it.** CIRPs should include scenarios relevant to the port or port facility's actual operating environment. In this case the classification of the port facilities would help design the scenarios. For example, a CIRP that only addresses office-based scenarios will not be helpful to port facilities with complex IT/OT/IIoT environments. CIRPs should include cyber incident escalation criteria, such as thresholds and triggers for contacting and engaging with internal and external resources.

Step 2: Develop clear procedures for incident handling, including responses to common attacks.

- In addition to the CIRP, **define and document which procedures are followed in the event of a cyber incident**. This includes event triage, analysis, and incident declaration. It should also include procedures guiding incident declaration, classification and prioritization.
- To accelerate decision-making process during incident response, **prepare strategic key-decisions in advance and maintain them in hardcopy format**. Depending on the organization's operational objectives, such decisions may define how the organization overall manages a cyber incident, which should include a communication strategy, key legal decisions and a list of essential stakeholders, including the executive team, who need to be involved (with contact information).
- **Define and document how the organization will contain a declared incident.** Define procedures for threat eradication, mitigation and recovery. Procedures should be clearly defined and flexible. Ports and port facilities executives should encourage the drafting of procedures for handling specific types of incidents, such as the following:

  - Successful phishing attack
  - Malware, including ransomware, Trojans, worms, droppers, etc.
  - Denial of service attack
  - Web application attack (cross site scripting, cross site request forgery, SQL injection)
  - DNS spoofing

[34] NIST SP 800-61 (R2), *Computer Security Incident Handling Guide* is a commonly used guideline; and, The EC Transport Cybersecurity Toolkit; See: https://ec.europa.eu/transport/themes/security/cybersecurity_en

Step 3: Establish reporting requirements for incidents

- Within the incident response plan, **identify the individuals responsible for reporting to third parties**, such as national and/or international governance bodies (e.g. regulators), law enforcement, port state control, insurers, customers, partners, and other stakeholders.
- When responding to a cyber incident, **managing internal stakeholder communication is key**. It is important for executives to recognize that not everyone within the organization may understand the implications of a cyber incident in the context of their work or specific department. Incident management communication plans should be developed clearly identifying who should be notified and involved (Chapter 10). Members of the crisis team and the executive team should be identified, including protocols for notifying and involving relevant asset, system, equipment, infrastructure owners and those dependent on their functions should be established.
- **Managing external stakeholder communication is critical.** The first reaction might be to close off any outbound communications or information updates. However, executives should recognize that third parties within the port community may quickly learn of a breach. If a port or port facility can no longer operate, then proactive communication and engagement is strongly encouraged.
- **Communications with media should be consistent, coordinated and disciplined,** and all messaging should be delivered through a designated representative. Notification templates should be prepared in advance to enable rapid modification and external notifications.

Step 4: Establish and train a Cybersecurity Incident Response Team (CsIRT)

- Critical to effective incident response planning and preparation is the establishing of a Cybersecurity Incident Response Team (CSIRT). **The CSIRT should be staffed by a dedicated group of individuals specifically trained to respond to cyber incidents** and understand how to perform all phases of a response and recovery effort.
- **When organizing the CSIRT ensure that assigned individuals are empowered to make decisions in order to take action to quickly respond to events.** A member from the executive leadership team (e.g. CISO or CIO) should be assigned to the CSIRT. It should include staff from IT, security, legal, communications / public relations and the functional operations of the port or port facility. Each department should be represented to ensure engagement during a response activity. In some cases, a CSIRT might be organized around an existing crisis response team that is structured to deal with a range of major incidents.
- **Nominate a member from the CSIRT who is the most experienced at leading the organization through the complexities and stress of crisis recovery activities. Formally designate them as the CSIRT Chair.** This individual should be perceived as a unifier, focusing on collaboration, and facilitating clear communications among other organizational members and executive staff.
- **Identify alternates to the CSIRT Chair and all key representatives to the CSIRT.** Since cyber incident recovery actions can be complex it is important for the port or port facility to maintain fresh stakeholder engagement throughout the effort, and alternates can be engaged to support extended recovery activities.

Step 5: Identify key resources

- **Critical to incident response planning is the need to identify the expertise needed to bring systems, equipment and/or infrastructure back online.** Handling IT/OT/IIoT systems requires special technical skills, and when these are urgently needed the challenges can prove daunting depending on staff or third-party expertise availability. Ports and port operators may wish to consider identifying and engaging a third-party organization that specializes in cybersecurity incident response involving IT/OT/IIoT environments. Engaging with national cybersecurity organizations, such as CERTs or national CSIRTs is another recommended option worth considering (Section 8.3).

Step 6: Test incident response plans and CSIRT capabilities

- **Test the CIRP in regular drills to ensure CSIRT capabilities remain fresh and team members are familiar with one another,** which should include awareness of individual strengths and weaknesses. Since the organization will most likely be working with other entities within the port community, invite third-party stakeholders to participate in drills. These individuals might be from other terminals or service organizations, as well as emergency or law enforcement organizations.
- **Test the CIRP at least annually in a comprehensive exercise.** Exercises should not focus on worst-case scenarios, but should be designed to specifically test how the CSIRT , and the organization in general, performs during a crisis. Exercises can result in key experiences and findings that are quite different from typical day-to-day activities. Ensure exercises are designed to express an interruption of IT systems and IT-enabled services that result in operational stress. Deliberately incorporate challenges that affect IT/OT/IIoT systems into exercises in order to force the CSIRT team to collaborate with staff from different operational areas. It is also valuable to assign a person or a group of observers to get the overview of the processes executed in the exercise for the lessons-learned together with the experiences of individuals involved in the test scenario.
- **Establish protocols for the CSIRT to gain rapid access to key systems and data sets in the event of an incident.** As a best practice, the CSIRT should have ready access to information such as security logs, which will likely be needed to support analysis, triage, classification, prioritization, and mitigation decisions. Logs should be regularly stored and maintained in a separate environment (e.g. network segment or cloud environment) independent from the port or port facility's primary network environment. Such separation will position the CSIRT to quickly determine how widespread a cyber threat may have penetrated and identify what systems may have been impacted and those that might remain operational.

10.3 Detection and analysis

As IT-based event detection was covered in Section 7, the focus here will be on OT systems. Cyber-attacks are not only constrained to IT systems but can also be launched against vulnerable OT systems. The consequences of **a compromised OT system can jeopardize the health and safety of staff, damage the environment and/or destroy equipment and infrastructure.** Worse, the cascading impact of a successful OT cyber-attack can affect the broader maritime supply chain. For example, failure of the onboard computer systems of remote sensors or safety-instrumented systems may lead to a system failure, resulting in operational stoppages and supply chain backups.

OT-enabled systems operated from one or more automated or remote locations can be vulnerable to cyber-attack. Analysis of detected events should focus on the most critical OT systems to port or port facility operations, cargo handling, critical infrastructures, equipment (i.e., cranes), as well as to the safety instrument systems and security monitoring. In some cases, a port authority might serve as a coordinating body in response and recovery actions where multiple facilities, including remote facilities, may have been impacted.

Analyzing a cyber incident resulting in the possible breakdown of the maritime supply chain should be performed and key findings shared with the affected parties. For some ports and port facility stakeholders sharing such information might appear counterintuitive, since the initial reaction might be to keep the cyber incident confidential. However, since ports and port facilities all contribute to the global maritime supply chain, executives are encouraged to recognize that a cybersecurity best practice is to share key insights discerned from successful cyber-attacks. Section 8 offers in-depth insights and guidance regarding information sharing best practices.

10.4 Containment and recovery

Containment and recovery involve activities required to constrain the effects of an incident and the steps needed to return the organization back to normal operations.

Business continuity plans (BCPs) are critical to restoring operations following a major incident. As IT/OT/IIoT assets and systems are increasingly integrating every aspect of a port or port facility's operational processes, BCPs in port and port facilities are commonly dominated by technical content which addresses their IT/OT/IIoT systems.

BCPs share four general components:

- ***Emergency response*** – Focuses on people, communication, personnel accountability, and evacuation, and transitioning to the crisis management team.
- ***Crisis management*** – Focuses on decision processes related to incident containment, command, control, and collaboration.
- ***Business resumption*** – Focuses on restoring business processes and their continuity.
- ***IT Disaster Recovery Plan*** – Focuses on recovery of information systems and availability of technology assets to provide business services.

Figure 18 - BCPs share four general components

While a BCP is a broad-based plan guiding operational recovery efforts, a port or port facility's incident response plan should provide specific direction on how the organization responds to an incident. The organization's CIRT should identify the specific actions needed for restoring business and technical functionality to key assets and systems that support its IT/OT/IIoT operating environment.

With a well-developed and tested incident response plan, a port or port facility can leverage a cybersecurity risk management framework by implementing applicable Containment, Eradication and Recovery functions. Each of these elements, depending on the size and complexity of a port or port facility's operations, can prove comprehensive and technically complex. A primary objective of proactive incident response is to quickly escalate the organization's overall security posture with a series of relatively rapid, high-value changes designed to prevent follow-on incidents. More specifically:

- ***Containment*** strategies are essential to implement before an incident overwhelms internal resources, disruption expands and/or damage to assets occurs.
- ***Eradication*** of components of an incident from all affected hosts so they can be remediated.
- ***Recovery*** involves restoring systems to normal operations and remediating the vulnerability to prevent similar incidents.

10.5 Containment and eradication

Coordinated incident containment activities are critical to port or port facility operations. **Once an incident has been detected, it should be contained. Containment actions should initially focus on the potential impact to life-safety, security, and operations.** During cyber incident response the physical security of the port or port facility should remain a priority – especially controlling access to restricted areas, such as server rooms. This is where communication between IT staff and the Port Security Facility Officer (PFSO) is needed. Depending on the extent of the incident and its potential impact to security systems, the PFSO may be required to change the security level of the facility consistent with applicable security plans.

For OT systems, **incident response should focus on isolating the affected assets and/or systems.** In some cases, specific BCP elements, or procedures, may be enacted to find workarounds with alternative systems. While doing this, the safety of the facility processes should always be kept in mind.

Once the extent of the cyber incident is determined, incident response efforts should follow internal and external risk mitigation paths. Internally, as the organization's CIRT contains the attack and implements mitigation measures, **an impact analysis should be made to determine 'real life' implications of how internal and external stakeholders might be affected.** For stakeholders responsible for or dependent on IT/OT/IIoT systems, this means confirming which information remains accessible, and which data has retained its integrity. Mitigation efforts might involve the reimaging or reloading of key IT systems by reverting to backups. While such an approach might result in a rapid recovery, this might not always be an option.

External containment also involves maintaining good relations with key partners, customers, port partners, and critical third parties in the maritime supply chain. By informing them of the incident response measures your organization is taking, they can act accordingly.

10.6 Post incident recovery

Post incident **recovery depends for a large part on the incident planning and preparations that have been made in advance of the cyber incident.** Depending on the type of incident, if system backups are performed and crisis management measures have been established, then post-incident recovery efforts may be more quickly achieved. In some cases, a cyber incident might occur where backups are not the only answer. Most often, it is essential for stakeholders to understand which organizational components require sequencing – that is, the ordering and speed to which systems are brought back online. The degree of integrated systems in port environments elevates the criticality of this.

10.7 Develop lessons-learned with relevant stakeholders

Once an incident has been mitigated it is important to learn from the incident, to identify its specific causes, contributing factors and impact. It is imperative to investigate the causes of the incident, determine the operational impact on the affected IT/OT/IIoT asset or system, gain an understanding of the consequences (financial, regulatory, legal, reputational, etc.), and develop a set of lessons learned. Performing an investigation will lead to further understanding into the full scope as to how the vulnerability was exploited, its impact on operations, and the implications for data confidentiality, integrity, and availability. It is recommendable to develop a set of lessons-learned and incorporate findings into future drills and exercises as well as training materials.

Where appropriate, share lessons among the port community, as well as with industry partners, such as the MTS-ISAC. Port community stakeholders can then benefit from this by implementing security measures of their own in advance of possible cyber-attacks. The result is a strengthened, more cyber-resilient port community.

11. CONTINUOUS IMPROVEMENT AND CYBERSECURITY MATURITY

To conclude the guidelines, this chapter summarizes the key take aways for executives and senior management of port or port facilities responsible for managing cyber risk aiming to take concrete actions:

- Why cybersecurity is not just for the "IT department".
- How cybersecurity capability drives cyber resilience.
- Leadership strategies for driving cyber resilience.

11.1 Why cybersecurity is not just for the "IT department"

Cybersecurity is an essential concern for every port or port facility. Maritime executives face the tasks of ensuring that their organizations understand the risks and setting the appropriate priorities. Unfortunately, with limited cybersecurity experience, many executives have misconceptions about how to approach cyber risk and as a result many perceive of cybersecurity as a mystery managed by IT staff.

As previously emphasized, managing cyber risk encompasses technologies, processes, structures, and practices that are appropriately tailored to best protect port and port facility assets, systems, infrastructure, and data. However, executives tend to overemphasize the role of technology as *the* solution to the cyber risk challenge. To be sure, IT staff plays an essential role in supporting critical cybersecurity activities because they administer and monitor the networks and IT infrastructure through which cyber threats may emerge. But focusing on technology alone presents a false promise, as it cannot entirely eliminate a port or port facility's cyber risk. In this sense, **relegating cyber risk management responsibility entirely to IT staff, or, as is the case with many small to medium-sized port facilities, outsourcing it entirely, is no longer appropriate.**

To underscore this point, **cyber threat actors commonly target non-IT staff**, which represents the majority of an organization's personnel, in order to breach a secured network environment. For example, cyber threat actors can exploit open-source information to formulate and execute targeted social engineering-based e-mail attacks, known as spear-phishing. When successful, such attacks circumvent IT-managed cyber defenses, rendering security technologies and protocols worthless.

The importance of implementing an organization-wide, "all-hands" approach to cybersecurity in the maritime domain will only increase as ports and port facilities become progressively dependent on automation and integrated IT/OT/IIoT technologies. The maritime transportation industry has always faced operational risk, and it has over time successfully mitigated those risks through careful risk management strategies, compliance regimes, and organization-wide participation. As with safety and security, the same risk management philosophy should be applied in addressing cyber risk and this can be achieved by working toward organizational cybersecurity maturity.

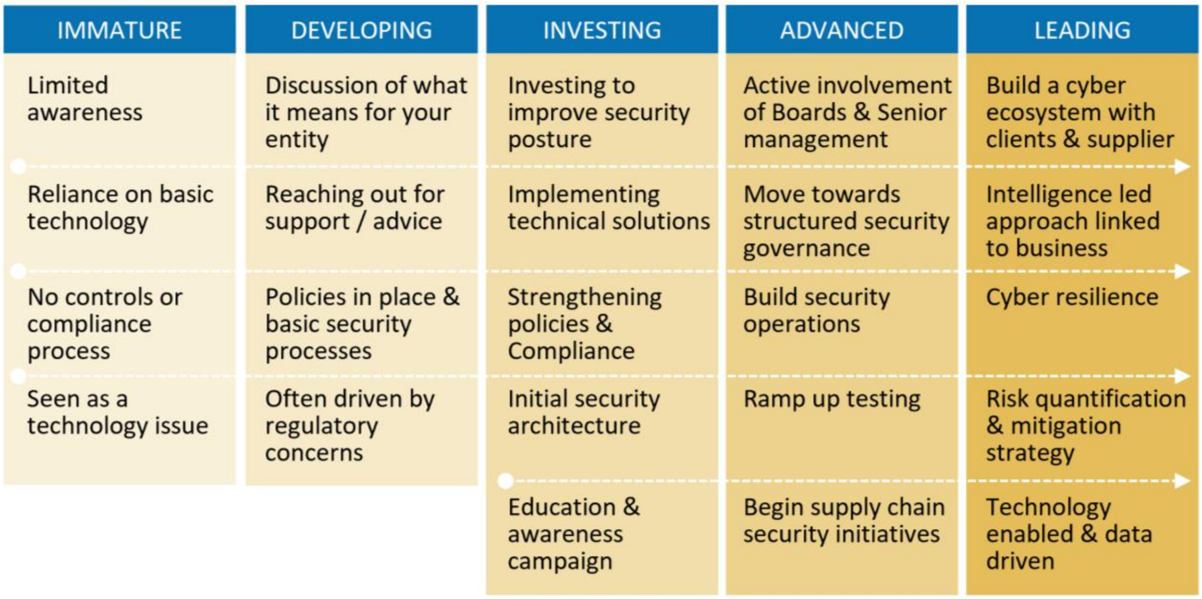
11.2 How cybersecurity capability drives cyber resilience

As cyber threats evolve, **ports and port facilities should focus on building cybersecurity capabilities to achieve and sustain a cyber-resilient posture**. Specifically, they should be able to anticipate, identify, detect, respond, and recover from cyber-attacks. For ports and port facilities on both sides of the digital divide, this means more than investing in technical solutions – it requires its leaders to take ownership of cyber risk and to build an effective model for cyber risk management. It requires identifying and applying proactive risk management techniques; cross-functional collaboration among staff; cultivating and maintaining a cyber-aware risk culture; and implementing best practices that foster continuous improvement.

There are practical steps a port or port facility can take to improve their organization's cybersecurity capabilities. The first step is to get the top management engaged – Port and port facility leaders must assume oversight responsibility for their organization's cyber risk management efforts and do so in a holistic manner covering all areas of their organization. Those organizations with boards should include cybersecurity as a regular topic in regular briefings. Oversight activities should include constant monitoring of activities in the context of the cybersecurity strategy.

To be effective, executives should have adequate understanding of the organization's capability and define the future direction for risk controls. To achieve this, **ports and port facilities may wish to consider first performing a cybersecurity capability maturity assessment of their *entire* organization**.

Cybersecurity capability maturity analysis provides a flexible structure for assessing every functional area of a port facility and offers a methodology for baselining current capabilities vis-à-vis cyber risks in order to support continuous improvement efforts. Properly executed, such analysis enables executives to determine where cybersecurity strengths or weaknesses may exist within their organizations. Making well-informed decisions about how and where to invest funds and allocate precious resources is of paramount importance. Some capabilities may be more suitable for investing in than others. Employing cybersecurity capability maturity analysis calibrates capability relevance, creates a basis for recurrent benchmarking, and guides investment planning. Once complete, this analysis will help port and port facility executives characterize their organization's overall current-state capabilities and measure cybersecurity maturity within a model similar to the one outlined in Figure 19 [35].



IMMATURE	DEVELOPING	INVESTING	ADVANCED	LEADING
Limited awareness	Discussion of what it means for your entity	Investing to improve security posture	Active involvement of Boards & Senior management	Build a cyber ecosystem with clients & supplier
Reliance on basic technology	Reaching out for support / advice	Implementing technical solutions	Move towards structured security governance	Intelligence led approach linked to business
No controls or compliance process	Policies in place & basic security processes	Strengthening policies & Compliance	Build security operations	Cyber resilience
Seen as a technology issue	Often driven by regulatory concerns	Initial security architecture	Ramp up testing	Risk quantification & mitigation strategy
		Education & awareness campaign	Begin supply chain security initiatives	Technology enabled & data driven

Figure 19 - Building cyber resilience

[35] Building Cyber Resilience in Asset Management; KPMG (May 2018)

Where within this model a port or port facility falls will depend on a variety of factors, including the complexity of its operating environment, the degree to which IT/OT/IIoT and automation technologies have been implemented and networked, and the extent of cybersecurity capabilities employed to protect the operating environment. Since cybersecurity capability maturity determinations are unique to individual ports, a small port with engaged leadership and limited deployed technology would be able to self-identify with a higher state of cybersecurity capability maturity than a large, highly automated and integrated port that may not have invested appropriately in cybersecurity measures or suffers from disengaged leadership.

Ports and port facilities may build their cybersecurity defenses around leading industry frameworks[36], which can assist organizations to:

- Build a trusted environment with their business partners.
- Heighten security awareness among the staff.
- Develop an organized risk-based approach to understand the business value of information and information systems and their integrations with operational systems.
- Demonstrate maturity of processes.
- Provide a structure for continuous improvement.

11.3 Leadership strategies for driving cyber resilience

To achieve greater cyber resilience, port and port facilities should consider developing the following cybersecurity capabilities, which are the culmination of the topics covered in these guidelines:

- ***Engaging executives in cybersecurity matters****:* Executives should assume responsibility for and oversight of cyber organizational-wide risk management. Awareness of cyber risks are required to guide decision making, which can be achieved through training and/or regular briefings from technical staff or third-party experts who can be engaged, as required. Authorities should be established to determine who has oversight over what and communication/reporting protocols should be clearly defined to identify who reports to whom and when.
- ***Developing an organization-specific cybersecurity capability maturity model:*** Executive should consider working with key stakeholders to define the organizational context within which a maturity model such as the one in Figure 19 can be applied. For example, by identifying and evaluating each of the organization's functional areas within the cybersecurity capability maturity structure. Functional areas will vary by organization, but can include IT, administration, operations, security, training, health and safety, compliance/risk management, legal, etc. Senior management from each area should participate in initial and ongoing cybersecurity capability analysis, resource allocation, and planning efforts as well as in the coordination for recovery activities, if required.
- ***Managing the cybersecurity capability maturity-based risk management model:*** For a port or port facility to achieve greater cyber resilience, it is important to identify and recognize the threats they might face. This requires making an inventory and mapping all assets (e.g., information, data, IT systems, etc.); performing threat impact analysis; determining the people, processes, tools, and money at risk; identifying and implementing mitigation measures; defining risk tolerances for risk acceptance, avoidance, treatment, and transfer options; and regularly reporting both cross-functionally (across functional areas) and to executives and the board.

[36] Examples include those promulgated by NIST and ISO, among others.

- ***Cultivating a culture of cybersecurity awareness:*** Managing cyber risk is more about people than technology, which is why it is crucial to educate, train, and empower staff at all levels. A cyber-secure culture is only successful when top executives sponsor training. It starts with basic cyber hygiene. All personnel should: 1) be informed of risks to the organization; 2) understand what is expected of them; and 3) know what to do in the event of a breach.
- ***Ensuring effective third-party management:*** A port or port facility's supply chain represents a significant source of cyber risk. Stakeholders should collaborate and coordinate efforts to develop cybersecurity requirements for procurement processes, contracting (e.g., breach notification clauses), testing and vulnerability analysis of newly contracted services. Service level agreements should define incident response and service restoration standards. A port or port facility should also establish a security-monitoring program for suppliers based on risk analysis and prioritization.
- ***Implementing appropriate cybersecurity solutions to respond to security incidents:*** No matter how much a port or port facility invests in its cyber defenses, cyber-attacks will occur. It is critical for executives to implement the capabilities necessary for their organization to adequately detect, prevent and deal with cyber threat actors from gaining unauthorized access to key systems. Some organizations may be able to deploy internal Security Operations Centers (SOCs), while others may seek to organizations outsource them. In either case, SOC capabilities empower stakeholders with the necessary tools for detecting events when they occur and coordinating rapid response and recovery actions to limit event impact. Integrated with the right policies, procedures, controls, and reporting mechanisms, cyber mature organizations will benefit by reducing the potential for downtime and improving their ability to recover and re-start operations.

Following these key takeaways, the foundation of cyber resilience program of the port and port facility can be initiated and established. It is the ambition of the IAPH that these guidelines support ports, their facilities and the relevant organizations at a port in implementing true cyber resilience.

12. ANNEXES – PORT FACILITY CYBERSECURITY ASSESSMENT AND PLAN TEMPLATES

12.1 Introduction

The purpose of the Annexes is to provide the designated cybersecurity lead with practical assistance in developing their Port or Port Facility Security Plan (P/PFSP). The Annexes include guidance and the table of contents of a sample P/PFSP that can be used as a template. The organization should adapt this template to their specific requirements as appropriate.

12.2 Port and Port Facility Cybersecurity Assessment Template

- Background
- Assessment Methodology Overview
    - Facility Overview
    - Facility Details / Cybersecurity Contact Information
    - Asset Identification
        - Summary
        - Data
        - Information Technology (IT) Systems
        - Operational Technology (OT) Systems
        - Industrial Internet of Things (IIoT) Systems
        - Other Critical Infrastructure and Equipment
        - Critical External Support Entities / Functions
        - [e.g. Utilities]
        - [Third-party Service Providers, e.g. ISPs, etc.]

- Threat / Vulnerability Identification and Risk Analysis
    - Summary
    - Cybersecurity Threats to [Organization]
    - Risk Register

- Governance
    - Security Administration and Organization
    - Records Management
    - Audits and Inspections

- Cybersecurity Considerations for Existing Security Measures
    - Enterprise Architecture
    - OT Operating Environment [as appropriate]
        - Technical Protection Measures for
            - OT Systems – Fixed Infrastructure
            - OT Systems – Mobile
        - Procedural (Plans, Policies, Procedures, Controls)
            - OT Systems – Fixed Infrastructure
            - OT Systems – Mobile

    - IT Operating Environment
        - Technical Protection Measures
        - Procedural (Plans, Policies, Procedures, Controls)
    - Physical Security Measures
        - Perimeter Security
        - Access Controls
        - Restricted Areas
        - Monitoring Security Measures
        - Security systems and equipment maintenance
    - Communications
        - Ship – Shore Interface
        - Wireless
        - Radio
        - Security Levels
    - Cargo Handling Operations
    - Training
    - Incident Response and Recovery
    - Impact Analysis Summary

- Summary of Findings and Prioritized Recommendations
    - Findings
    - Prioritized Recommendations

- Strategies for Improving Cybersecurity

12.3 Port and Port Facility Cybersecurity Plan Template

- Background
- Facility Overview
- Facility Details
- Cybersecurity Contact Information

Name of Designated Chief / Cyber Information Security Officer ("CISO" or "CYSO")	*INSERT NAME*
CISO Office Telephone No.	*INSERT*
CISO Mobile Telephone No.	*INSERT*
CISO Email Address	*INSERT*
Deputy CISO Name	*INSERT NAME*
Deputy CISO Mobile Telephone No.	*INSERT*
Deputy CISO Email	*INSERT*
Name of Port Facility Security Officer (PFSO):	*INSERT*
PFSO Office Telephone No.	*[INSERT SAME FROM PORT SECURITY PLAN – "PFSP"]*
PFSO Mobile Telephone No.	*[INSERT SAME FROM PFSP]*
PFSO Email	*[INSERT SAME FROM PFSP]*
Deputy PFSO Name	*[INSERT SAME FROM PFSP]*
Deputy PFSO Mobile Telephone No.	*[INSERT SAME FROM PFSP]*
Deputy PFSO Email	*[INSERT SAME FROM PFSP]*
PFSO Security Office Location / Address	*[INSERT SAME FROM PFSP]*
CISO Office Location / Address	*[INSERT SAME FROM PFSP]*

- Cybersecurity Overview
  Guidance:
  - *Provide a general overview of the organization's digital operating environment, which should include general descriptions of all networked administrative and operational environments. For example, are separate networks supporting administrative information technology (IT) systems and operational technology (OT) systems? Are wireless networks employed? Identify significant assets (e.g., networked cranes) or OT-enabled infrastructure (e.g., vessel traffic control systems, berths, gates, terminal cranes, storage facilities, its access points, gateways and pipelines). Are multiple networks employed?*
  - *Describe at a high level all administration, security, cargo reception and handling, warehousing and logistics, and communications operations that depend on IT-enabled assets. List all networked facility buildings and structures (e.g., administration, vessel traffic management control centers, data centers, warehouses, etc.), linear infrastructure (e.g., rail systems, conveyors, etc.), plant and machinery (e.g., cranes, barriers, locks, etc.), and other systems, such as electronic security, scanning systems, and other communications and operational infrastructures.*

- Security Levels

Guidance: Identify cybersecurity activities performed for each Security Level. At each level cyber threats should be communicated to port partners.

- Maritime Cybersecurity Considerations and Definitions
    - Overview
    - Confidentiality
    - Integrity
    - Availability
    - Functionality
    - Cyber Resilience
    - Health, Safety and Environmental Protection
    - Functionality

- Risk Assessment

  Guidance: Input descriptions to accurately reflect the organization's current operating environment as per findings described in the PFSA and any supplemental cybersecurity assessment previously performed.
  - Threats
  - Vulnerabilities
  - Consequences
- Referenced Standards
- Security Measures
- Cybersecurity Steering Committee (or other Internal Working Group)
- Management of Security

  Guidance: Identify key cybersecurity personnel, such as the Chief Information Security Officer (CISO), including how and when physical security and cybersecurity personnel coordinate activities and conduct notifications for suspicious activities, breaches of security, and Security Level changes.
  - Cybersecurity Administration and Organization
  - Security Operations Center
  - Port Security Committee (Cyber Sub-Committee)
  - Security Level Changes
  - Cybersecurity Duties, Responsibilities and Authorities of [Facility] Personnel
  - Cybersecurity Training
  - Cybersecurity Drills and Exercises
  - Security System Equipment Maintenance
  - Port Facility Security Plan Review, Amendment and Audit
  - Cybersecurity Incident Assessment and Reporting
  - Contingency Plans
  - Information Security
- Dangerous Goods and Hazardous Substances
- Record Keeping and Documentation
- Communications
  - Ship and Port Facility Communications
    - Ship Security Alert
    - Declaration of Security
  - Suspicious Activity and Incident Reporting
- Cybersecurity Incident Response and Recovery
- Cybersecurity Measures
  - Cybersecurity for Restricted Areas and Controlled Facilities
  - Cybersecurity for Cargo Handling, Stores Delivery and Storage
  - Cybersecurity for Electronic Security Systems
    - Access Control

    - Perimeter Monitoring
    - Security Operations Center
- Other Cybersecurity Requirements

GLOSSARY OF TERMS

Term	Definition
Access Control	The discipline, technology, process and/or control for limiting access to an organization's applications, systems, platforms, critical assets, and facilities to authorized entities (e.g., authorized personnel, workflows, and/or data exchanges).
Advanced Persistent Threat (APT)	A cyber attacker or adversary that possesses sophisticated technical capabilities, expertise and resources which allow it to employ a range of tactics, techniques and procedures (e.g., cyber, physical, deception, etc.) to carry out an attack against a targeted victim
Anomaly	Exhibited behavior that is eccentric or inconsistent or deviates from what is considered normal or typical.
Anti-Virus Software	Specialized software that is designed to detect, and, where possible, mitigate malware before it attacks a system. To be effective, anti-virus software must be maintained with the latest updates so that it can effectively identify, isolate, and repair infected files.
Authentication	The process employed to verify the identity and authenticity of a named user, device, system, or application as a condition for gaining access to a protected resource.
Authorization	The process for approving or permitting an individual, application, and/or system to do something.
Availability	The condition for facilitating timely and consistent access to an asset, data set, or information-based system or service.
Backdoor	An undocumented gap in a software application or computer system that allows unauthenticated users access, circumventing security processes.
Backup	A practice designed to save electronic files against inadvertent loss, destruction, damage or unavailability. Methods include high-capacity tape, disc, or cloud-based managed service provided by a third party. Backup efforts should be performed off-site, physically far enough away from the organization's primary site (e.g., administrative headquarters) to reduce the risk of potential environmental risk factors (e.g., earthquake, flood, fire) from impacting both the primary site and the backup site.
Blacklisting Software	Software blacklisting enables the filtering of websites that have been identified and specified as unsafe. Companies sometimes use it to prevent staff from visiting harmful websites, such as those that have been identified as common watering holes. While blacklisting is effective at preventing access to known websites, it is less effective against websites with unknown risks.

Bot	A computer connected to the Internet that has been surreptitiously compromised with malware that direct the computer to perform specific activities directed by a remote administrator with command and control privileges
Brute Force Attack	A methodical process whereby a cyber attacker employs an exhaustive trial and error approach to gaining access to sensitive information. Typically, software is applied to automatically generate massive quantities of simultaneous "guesses" in the hopes that one will eventually succeed.
Business Impact Analysis (BIA)	A quantitative analysis that distinguishes critical and non-critical organizational controls, functions, processes, and activities and prioritizes their impact as a result of a compromise or loss of an application, system or platform. Asset criticality and/or sensitivities are then qualitatively and/or quantitatively assessed and the acceptability of the identified risk, including recovery costs, is then determined.
Common Operating (Operational) Picture (COP)	Often reflected in a single display (or set of displays), a COP is the consolidation and integration of multiple and relevant activities and technologies that have been configured to collect, analyze, alert on, visualize, and use cybersecurity information, including status and event summary information. It is designed to provide situational awareness, facilitate collaboration and support informed decision-making on cybersecurity matters.
Computer Security Incident	A violation of established computer security policies, including acceptable use policies or other standardized security practices as defined within the organization's security plans. (See also *Incident*)
Confidentiality	The protected state achieved by a set of clearly defined rules and authorized restrictions that determine data access and /or disclosure. It includes constraints designed to protect data related to personal privacy and other proprietary information. For an information-based or managed asset, confidentiality is sustained by only allowing authorized and authenticated individuals, processes and/or devices access to it.
Configuration Management	A set of defined processes and controlled activities designed to establish and maintain the integrity of an asset, application, system or platform throughout its lifecycle. Configuration management usually involves documented specifications and procedures for managing information technology and operational technology-based systems, assets or platforms. It also provides a common means for tracking and managing the initialization, change, and long-term monitoring of their configurations.
Contingency Plan	A plan, typically expressed as a management procedure, for supporting response activities in the event an asset, application, system, and/or platform capability lost, interrupted or compromised. It is often the first plan stakeholders use to characterize what happened, understand why it occurred, and identify initial mitigation activities. It may also directly reference Company and Facility Security Plans as well as Continuity of Operations and/or Disaster Recovery plans in the event of a major disruption.

Continuous Monitoring	A risk management approach to achieving and sustaining an ongoing awareness of an organization's cybersecurity state. Continuous monitoring collects, analyzes, alerts, visualizes, and supports informational technology, operational technology and security practitioners by identifying anomalous events, vulnerabilities and threats across the organization's operating environment. Its purpose is to support incident response activities and risk management decision-making.
Controls	A set of defined operational policies and/or technical procedures, which may be either manual or automated, that support information technology, operational technology and business processes in the protection of data confidentiality, integrity, and availability.
Cookie	A cookie is a small file downloaded from a website that stores an information packet on the viewer's browser. They are used to store collected data such as login and personal identification information, site behaviors, preferences, and pages viewed. Although convenience-oriented, cookies represent security vulnerabilities. Browsers can be configured to alert on cookies, and users can accept or erase cookies.
Cyber Attack	An event that is launched against a target with the intent to deny, disrupt, destroy, or exploit a computer-enabled operating environment. Many cyber-attacks are intended to compromise for exploitation purposes or destroy the integrity of targeted data, steal data, or manipulate data for nefarious purposes.
Cyber Ecosystem	The interconnected information infrastructure of an organization's enterprise that facilitates electronic data exchange, communication and interactions among authorized users, applications, systems, platforms, and processes.
Cybersecurity	The capability to protect or defend against unauthorized access to or use of cyberspace from cyber-attacks. It consists of the collective measures implemented to defend a computer or computer-enabled system against cyber-enabled threats, such as hackers, Hacktivists, foreign intelligence services, and organized criminal syndicates, among others.
Cybersecurity Architecture	A foundational element supporting an organization's enterprise architecture, cybersecurity architecture consists of the structure and related behaviors of security-focused technologies, processes, systems, operational practices, and personnel responsibilities that align to the organization's defined objectives. See also: *enterprise architecture* and *network architecture*.
Cybersecurity Event	A visible incident that occurs in a networked-enabled environment or computer-enabled system related to defined cybersecurity requirements. A cybersecurity event affects data confidentiality, integrity, or availability. See also *event*.
Cybersecurity Impact	The consequences resulting from a *cybersecurity event*, which also includes the effect on the cybersecurity capabilities and processes currently in place.
Cybersecurity Plan	A document that identifies and defines the cybersecurity requirements and associated controls necessary for meeting those requirements.

Cybersecurity Policy	A set of principles, measures, and conditions that have been defined to support cybersecurity capabilities and planning across an organization.
Cybersecurity Program	An integrated set of coordinated activities that include governance, strategic planning, executive sponsorship, reporting, and training that is managed to meet defined cybersecurity objectives for an organization. While cybersecurity programs can be implemented at a divisional or practice-level, a higher (enterprise) level can often benefit an organization by coordinating investment planning and resource allocation, aligning business processes and procedures, and other resources and capabilities, as may be required.
Cybersecurity Program Strategy	A set of defined actions tailored to the organization's specific cybersecurity capabilities and related performance objectives.
Cybersecurity Risk	The risk to an organization's information technology and/or operational technology-based assets and resources, along with its supporting functions, processes, and reputation as a result of unauthorized access, compromise, exploitation, disruption, denial, or destruction.
Data Breach (Also "Data Spill")	The unauthorized access to, exfiltration of, or disclosure of confidential and/or privileged information to a third party or entity that does not have authorization to access, view, or utilize the information.
Denial of Service Attack (DoS)	A type of cyber-enabled attack that results in the temporary or indefinite disruption of authorized access to an application, system, platform or other resource. It typically involves the overloading of a targeted system with an overwhelming number of needless requests, preventing legitimate requests from being addressed. A *Distributed Denial of Service* (DDoS) attack involves the attacker employing thousands of unique IP addresses to simultaneously carry out an attack.
Dependency Risk	The risk to an organization due to a supplier, vendor, service provider, or other external party on which the delivery of a critical service or key function depends. It is evaluated and measured by the possibility and severity of damage that may be experienced by an application, information technology system, operational technology asset or platform in the event of a compromise.
De-Provisioning	It is a risk management process that defines the revocation or removal of an individual's user identity and associated privileges enabling authenticated access to a facility, application, system, or platform.
Digital Certificate	A form of electronic credentials (e.g., virtual ID or passport) that supports trusted communications and/or business transactions over the Internet. It contains an individual's name, a defined identification (e.g., serial number), expiration date, a copy of the certificate holder's public key (used for encryption and digital signatures), and the digital signature of the certificate-issuing authority for verifying the certificate.

Domain Hijacking	A form of cyber-attack that occurs when an attacker takes over a domain registration by blocking the victim's Domain Name Server (DNS) and then illegally replaces it with its own without the authorization of the original registrant.
Encryption	A cryptographic method used to encode a set of information for the purpose of protecting it from unauthorized access or modification prior to sending it to a specified recipient. The recipient then decodes the message using an encryption key.
Enterprise	The highest organizational level of a defined entity.
Enterprise Architecture	The organizational blueprint, design, and description of an organization's entire information technology and operational technology operating environment. It identifies how applications, systems, and platforms are configured, integrated, and connected across internal and external boundaries. It also identifies how they are sustained, how they support the organization's performance objectives, and how they support enterprise-level security capabilities.
Event	An observable occurrence in an asset, application, system, network, or platform. Risk criteria established by the organization inform how some events are characterized and escalated for response and mitigation actions.
Event and Incident Response, Continuity of Operations	The organization and sustainment of an integrated set of plans, procedures, and capabilities that are designed to support the detection, analysis, and response to cybersecurity events. In addition, they are designed to provide guidance to support continued operations through a declared cybersecurity event in a manner that is both aligned and commensurate with the risk to the organization's capabilities and overall objectives.
Exfiltration	The unauthorized removal, transfer or relocation of privileged information from an information system.
Firewall	A hardware device or software link in a network that is designed to inspect data packets (e.g., data traffic) between devices, systems or networks. They can be configured to restrict network traffic according to defined rules.
Identity	A set of attributable characteristics or other defined values (e.g., a randomly generated user identification number) that have been assigned and can be verified in a manner that can distinguish one individual or entity from another.
Incident	An event that arises out of deliberate or accidental circumstances, violating established security policies and/or protocols that can result in harmful consequences to critical assets, applications, systems, platforms, and/or other critical infrastructure elements. A declared incident should warrant activation of incident response resources in order to respond to and contain its impact to the organization, and limit its effects on peripheral systems, platforms, operating environments, or other dependent assets. See also *computer security incident* and *event*.

Information Assets	Information or data that the organization has identified and/or classified as essential to the functioning of the mission. This also includes operational data (e.g., process data, command and control information), security plans, network diagrams, confidential designs, intellectual property, customer and financial information, and contracts.
Information Sharing and Communications	Information sharing involves the conscientious exchange of knowledge, expertise, data, and threat information. It assumes pre-existing relationships among internal as well as trusted external third parties (e.g., advisors, partners, law enforcement agencies, port state control authorities, etc.) with whom to share cybersecurity information, including any relevant information about current or emergent cyber threats, threat actors, or maritime industry-specific vulnerabilities, as well as lessons-learned and similar findings.
Information Technology (IT)	Any application, asset, equipment, system, platform, or interconnected system or subsystem that involves the creation, consumption, exchange, dissemination, processing, management, protection, and/or storage of discrete electronic information. In the context of this publication, the definition includes any and all interconnected and/or dependent systems supporting shore-based and shipboard operating environments, and the operational technologies that they support and/or operate.
Insider Threat	Represents a malicious or unintentional threat to the organization from employees, contractors, or service providers who enjoy trusted privileged access to controlled assets, applications, systems, and/or platforms.
Integrity	In the context of cybersecurity, *integrity* is the preservation of information authenticity and correctness. It involves the protection of information from improper or unauthenticated alteration or destruction. Information can be in the form of electronic files, commands, instructions and queries.
Internet Protocol (IP) Address	A computer's IP address is a unique series of four 8-bit numbers, separated by periods. It is the identification assigned to all computers and network devices connected to a TCP/IP network. In short, it represents the device's inter-network address. All websites also have an IP address. IP addresses are managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries.
Keystroke Logging	Keystroke logging (also referred to as 'keylogging') is the surreptitious recording of computer keyboard keystrokes that are captured as the victim types. Recorded keystrokes are then automatically transmitted to the attacker. This form of attack can be accomplished through either software or hardware. Attackers typically employ keylogging to capture victim user names, passwords and other personal data, such as credit card information.
Least Privilege	A control established by an organization that allows only a minimum level of access for authorized users who require it in order to perform their assigned duties and responsibilities. The purpose of least privilege is to mitigate risks related to the possible misuse and corruption of authorized privileges related to specific functions, processes and/or services.

Logging	Recordkeeping is either a manual or automated process designed to monitor and track user activity and behaviors. As part of an information technology or operational technology system or networked environment, logging is an automated process. Manual processes include the application of physical processes (e.g., manual sign in or use of smart cards) employed to control access to restricted environments, such as vessels, shore-side facilities and office environments. Regular auditing of logs (either manually or through the use of automated tools) supports a critical cyber risk management process that provides situational awareness to security practitioners.
Malware	A generic term for software that compromises the operating system of an IT or networked asset with different types of generic or customized malicious code.
Man-in-the-Middle Attack	A type of attack that involves a threat actor who poses as an online vendor or financial institution and encourages a victim to sign in using their credentials over a Secure Sockets Layer (SSL) connection. The attacker then uses the victim's credentials to access the valid server in order to steal targeted information (e.g., intellectual property, financial data, etc.)
Monitoring	*Monitoring* involves the collection, aggregation, recording, analysis, and distribution of specific information sets related to application, system and user behaviors. It supports an ongoing process regarding the identification and analysis of risks to an organization's critical assets, applications, systems, platforms, processes, and personnel.
Multifactor Authentication	The required application of two or more factors a user must employ to authenticate to an application, system or platform. Applicable factors can include: A) *something you know* (e.g., a unique password); B) *something you have* (e.g., an identification device); C) *something you are* (e.g., a biometric, such as a fingerprint); or D) *you are where you say you are* (e.g., a GPS token or device).
Network	Two or more computer systems or networked devices connected to share information, software, and hardware.
Network architecture	A framework that portrays the overall structure of Information Technology and Operational Technology assets, systems and platforms (including integrated systems). It describes the behavioral rules supporting the communications and interconnectedness among IT and/or OT assets. See also *enterprise architecture* and *cybersecurity architecture*.
Operational Risk	The potential impact on key assets, applications, processes and/or platforms, including their related services, that could result from insufficient capabilities or failed internal processes, systems or technologies, or the deliberate or inadvertent actions of people, or external events.
Operations Technology (OT)	Programmable controls, systems, or devices that are engineered to direct, monitor or interact with systems facilitating physical processes, such as industrial control systems, building management, cargo management, security, engine controls, etc.

Password	A confidential set of alphanumeric characters that is combined to use as a means of authentication for confirming a user's identity in order to access an application, system, platform, or integrated set of systems.
Patch	A small, customized security update issued by a software provider in order to correct known bugs in existing software applications. Most software programs and/or operating systems can be easily configured to automatically check for patches or other updates.
Provisioning	The creation, maintenance, and activation of a user profile, including roles and access privileges. An organization should continuously monitor and track access rights to ensure the security of the IT, OT, and communications resources.
Ransomware	Computer malware that installs on a system, encrypts the system's data, prevents access to this data, and holds the data hostage or threatens to publish the data until a ransom is paid.
Risk	A probability or threat of a negative circumstance of event exploiting a vulnerability and that can be addressed through pre-emptive action.
Residual Risk	Risk exposure after risk mitigating controls are considered or applied.
Risk Analysis	The definition and understanding of potential consequences to the organization if certain risks were to come to fruition and a determination of appropriate steps to manage those risks.
Risk Assessment	An identification and evaluation of potential risks that result from a certain activity and a determination of an acceptable level of risk for the organization in question.
Risk Management	The estimate and assessment of potential risks and the establishment of actions or procedures to accept, avoid, control, mitigate, or transfer the consequences of those risks.
Risk Management Program	A defined plan to estimate and assess potential risks and establish actions or procedures to mitigate the consequences of those risks.
Risk Management Strategy	A structured approach toward estimating and assessing potential risks and establishing actions or procedures to mitigate the consequences of those risks. This also includes a defined procedure for periodically reviewing the approach to incorporate new information.
Risk Mitigation	Actions taken to reduce the occurrence and/or negative consequences of a risk.
Risk Mitigation Plan	A defined, documented set of actions to take to reduce the occurrence and/or negative consequences of a risk.

Risk Register	A structured repository of identified risks, with information that supports risk management, such as risk nature, risk consequences, and risk mitigation strategy.
Risk Response	The process of developing strategies to reduce the occurrence and/or negative consequences of a risk. These strategies might include acceptance, avoidance, sharing, or transfer.
Router	A network device connected to two or more data lines in different networks that sends data to the next appropriate network. This function is akin to directing the traffic of the internet.
Script	A simple file that contains programmed commands that can be performed by a computer without user direction.
Secure Software Development	The process of including security best practices as an integral part of software development, including code review, security architectures, and other recognized processes and tools. Programmers and software architects with specific training in secure software development are often deeply involved in this process.
Secure Socket Layer (SSL)	The standard encryption system for providing a secure link for data exchanged between a website and a user. A website whose URL begins with https is using this system.
Service Level Agreement (SLA)	A contract between a service provider and a customer, including the services the provider will supply and the performance standards the customer expects these services to meet. The performance standards should include cybersecurity requirements.
Situational Awareness	The awareness of the current state of a system or environment and an understanding of how a change in a variable might alter that current state. This awareness stems from having sufficient and accurate data and the ability to appropriately analyze this data to inform decision-making.
Social Engineering	The psychological manipulation of people in order to trick an unsuspecting person into bypassing normal security controls or providing access to business networks.
Social Networking Websites	An online platform on which users create online profiles and post written words, pictures, videos, and other personal information to share with one another. These platforms facilitate the social connection between and among users with similar interests.
Spam	The use of unsolicited and unwanted bulk messages in an attempt to convince the recipient to purchase something or reveal personal information, such as a phone number, address, or bank account information. Email is the most typical medium for spam, but spam also occurs in other areas, such as text messages, instant messages, and social networking websites.

Sponsorship	Senior management support of cybersecurity objectives across an entire organization is often demonstrated through formal declarations or policies. Full sponsorship also involves senior management review, monitoring, and ongoing improvement of the organization’s cybersecurity program.
Spoofing	An attack by which a malicious actor attempts to impersonate a trusted actor to hide his/her true identity.
Spyware	Software that is installed covertly on a computer to allow an attacker to steal data and, possibly, personally identifiable information. This malicious software is often combined with software a user voluntarily downloads and will remain on the user’s computer even if the voluntarily downloaded program is deleted.
Supply Chain & Supply Chain Risk	A sequential set of processes, performed by various otherwise unrelated actors, that result in the creation, transportation, and distribution of a product. The supply chain is typically understood to span across the design, development, production, integration, distribution, and disposal of a product. Supply chain risk is the probability or threat to the supply chain of a negative circumstance of an event caused by vulnerability and that can be addressed through pre-emptive action.
Threat	An action or event that can, through the exploitation of IT, OT, or communications infrastructure vulnerability, cause a risk to become a loss or damage, with negative consequences for the operations and resources of an organization. This could, for example, occur through unauthorized access, denial of service, or spoofing.
Threat and Vulnerability Management	A structured approach toward estimating and assessing threats and vulnerabilities and establishing actions, plans, or procedures to mitigate the consequences of those threats and vulnerabilities. This approach should incorporate the organization’s risk assessments and risk mitigation plans.
Threat Assessment	An evaluation of potential threats, including their severity, and their possible effects on an organization’s IT, OT, and communications infrastructure.
Threat Profile	The identification of the characteristics of the complete set of threats to a given function. This combines the organization’s set of threat assessments to its IT, OT, and communications infrastructure.
Trojan Horse	Malicious software that tricks victims into believing it is innocuous. Typically spread by some sort of social engineering, many Trojan horses provide unauthorized access to a victim’s computer, enabling access to personal information, such as banking information and passwords.
Upstream Dependencies	An external actor who must act or complete a task before a function may be performed or completed. Upstream dependencies include certain operating partners, including suppliers.
URL	A method of denoting where a specific web resource is located on a computer network. Also known as a web address.

Virus	A type of malware that inserts itself into and infects another computer program then reproduces itself and infects other programs. Because a virus cannot run by itself, it requires the execution of a host program in order to become active. A virus can spread through email attachments, text messages, internet scams, and even mobile app downloads.
Vulnerability	A weakness in an IT, OT, or communications system that an attacker might exploit to gain unauthorized access to that system and the information that system stores.
Worm	A type of malware that, unlike a virus, can run independently, replicate itself on to other hosts on a network, and cause damage to a computer and network, such as, at a minimum, consuming significant network bandwidth.