# PORT COMMUNITY CYBER SECURITY

*Courtesy Port of Los Angeles*

IAPH International Association of Ports and Harbors

ICHCA INTERNATIONAL

TT CLUB established expertise

WPSP WORLD PORTS SUSTAINABILITY PROGRAM

> *“ Digital connectivity plays a crucial role in enabling innovation and prosperity around the world but increasingly cyber threats present a major obstacle to society’s continued path to progress. From data breaches and identity theft to the disruption of operations and critical infrastructure, the World Economic Forum Global Risks Report 2019 ranks cyber attacks among the top five global risks. At the same time, cyber criminals take advantage of a borderless playing field to build their criminal enterprises and launch targeted attacks, with limited risk and high return. ”*

World Economic Forum: https://www.weforum.org/centre-for-cybersecurity/

## About IAPH

Founded in 1955, 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. Its member ports handle more than 60 percent of global maritime trade and around 80 percent of world container traffic. IAPH has consultative NGO status with several United Nations agencies. In 2018, IAPH established the World Ports Sustainability Program (WPSP). WPSP covers five main areas of collaboration: energy transition, resilient infrastructure, safety and security, community outreach and governance.

## About ICHCA International

Founded in 1952, the International Cargo Handling Coordination Association (ICHCA) is dedicated to improving the safety, security, sustainability, productivity and efficiency of cargo handling by all modes and through all phases of national and international supply chains. ICHCA International’s privileged NGO status enables it to represent its members and industry at large in front of national and international agencies and regulatory bodies including IMO. ICHCA’s International Technical Panel also provides technical advice and publications on a wide range of practical cargo handling issues.

## About TT Club

TT Club is the established market-leading independent provider of mutual insurance and related risk management services to the international transport and logistics industry. TT Club’s primary objective is to help make the industry safer and more secure. Founded in 1968, the Club has more than 1100 Members, spanning container owners and operators, ports and terminals, and logistics companies, working across maritime, road, rail, and air. TT Club is renowned for its high-quality service, in-depth industry knowledge and enduring Member loyalty. It retains more than 93% of its Members with a third of its entire membership having chosen to insure with the Club for 20 years or more.

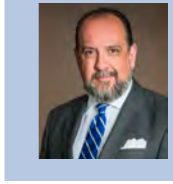
# Table of Contents

## Acknowledgements:

We would like to thank the following contributors to this report as expert advisors, authors and editors:

Richard Brough (ICHCA) and Peregrine Storrs-Fox (TT Club), Max Bobys, HudsonAnalytix; Lance Kaneshiro, Port of Los Angeles; Chronis Kapalidis, HudsonAnalytix; Pascal Ollivier, Maritime Street; Frans Van Zoelen, Port of Rotterdam; Ward Veltman, Port of Rotterdam; Rachael White, Next Level Information.

# Foreword



**Dr. Patrick Verhoeven**
Managing Director,
International Association of Ports and Harbors (IAPH)
Coordinator, World Ports Sustainability Program (WPSP)

The initiative to produce a report on Port Community Cyber Security goes back to a meeting the authors of this paper had at the TT Club offices in London, during the 2019 edition of London International Shipping Week. At that time – September 2019 – only few people had heard of the term 'coronavirus', let alone that anyone could imagine how profound the impact of the COVID-19 variety would be on our industry.

The COVID-19 crisis did emphasise the critical role of seaports in keeping supply chains moving and economies across the world functioning. A great variety of business and government actors interact in port communities to ensure multimodal flows of vital medical and food supplies, critical agricultural products, energy streams and other goods and services reach their intended destinations in time. Their interactions comprise physical interactions, such as cargo handling operations, vessel-related services, and multimodal transfers, as well as exchanges of data that facilitate clearance of cargo between jurisdictions.

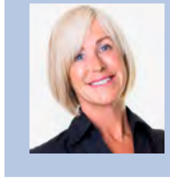
The COVID-19 crisis has painfully demonstrated the heterogeneous landscape that currently exists across ports worldwide when it comes to digitalization. While some port communities seized the opportunities of the fourth industrial revolution and developed into full-fledged 'smart' ports, many others have barely grasped the essentials of digitalization and continue to struggle with larger reliance on personal interaction and paper-based transactions as the norms for shipboard, ship-to-shore interface and shore-to-hinterland based exchanges.

With the world's attention now focused on exiting from lockdowns and preparing for a 'new normal', there is an urgent need for inter-governmental organisations, governments and industry stakeholders concerned with maritime trade and logistics to come together and accelerate the pace of digitalisation so that port communities across the world can at least offer a basic package of electronic commerce and data exchange.

Increased digitalization of port communities means we need to pay increased attention to cyber security risks. This Port Community Cyber Security paper therefore comes at a time which is even more relevant than when we initially conceived it in September 2019.

The paper is the result of great teamwork. I am most grateful to Pascal Ollivier (Maritime Street), Max Bobys (HudsonCyber), Chronis Kapalidis (HudsonAnalytix), Lance Kaneshiro (Port of Los Angeles), Ward Veltman (Port of Rotterdam Authority) and Frans van Zoelen (Port of Rotterdam Authority/IAPH) for their contributions. My warmest thanks also go to Rachael White (NextLevel Info) and my colleague Victor Shieh for the editorial and design work. Finally, I would like to thank our partners Richard Brough of ICHCA International and Peregrine Storrs-Fox of TT Club for their facilitation and support.

# Introduction and Executive Summary



**Rachel White**
CEO
Next Level Information (NLI)

Digitalization and automation of maritime trade, logistics, transport and cargo handling have been underway in various guises for many decades now. The trend has clearly accelerated in the past few years and looks set to ramp up substantially in light of the COVID-19 pandemic that has now shone a very public spotlight on the vital need to keep trade flowing while keeping people safe.

As gateways for regional, national and international trade, seaports have always been just as much exchange hubs for information as they are for physical goods. Ensuring efficient interaction between all the public and private parties that make up port communities is critical to trade competitiveness and supply chain performance. But as port community stakeholders collaborate more intensively to create richer digital ecosystems, better visibility and deeper connectivity, the cyber security stakes continue to rise.

Collaboration within and between port communities around the world, and in particular cooperation with the broader maritime supply chain, is now vital to foster better cyber security awareness, knowledge transfer and best practices.

This IAPH White Paper is the product of a collaborative effort between port and cyber security experts, collectively offering many decades of experience.

Equipped with a glossary of common terms and phrases, each chapter in the paper explores a different dimension of the cyber conundrum, with practical recommendations, advice and examples.

The first chapter explores why cyber security is such a vital issue for port communities, looking at trade, regulatory, geo-political and defense dimensions The second discusses the vital importance of ‘speaking the same language’ around cyber security, calling for development of common terms and phrases to facilitate a global dialogue on cyber risk management in port communities. Chapter 3 looks at what is commonly missing in port community cyber security and offers practical suggestions on steps to increase cyber resilience. The fourth outlines essential building blocks for a cyber resilient port community. It also explores the US National Institute of Standards and Technology (NIST) 5-step framework as a tool that can be readily adopted by port authorities and communities. And finally Chapter 5 looks at current cyber security provisions in the IMO rules and discusses the potential evolution of the Port Facility Security Officer role for the future.

# Chapter 1

## Why is Cyber Security such a Vital Subject for Port Communities?

***Increased use of digital technologies within port communities and along cyber supply chains brings potentially positive as well as negative opportunities. Both need to be well managed.***

As recently underscored by European Union Directive 2016/1148 (NIS Directive), port communities are characterized by national governments, regional and international regulators as critical infrastructure for sustaining international trade, driving economic security and facilitating collaborative defense in the face of new geo-political, economic and technological risks. From a policy making and governance perspective, cyber security is becoming a hot topic for port communities around the world seeking to avoid operational chaos, business disruption and financial loss. Cyber issues have become one of the top five risks cited by global business leaders, along with geo-political dynamics, regulatory compliance and sustainability. According to the World Economic Forum, economic loss owing to cyber crime is predicted to reach USD3 trillion in 2020, representing 3.4% of global GDP.[1]

The time has come to not only initiate but, crucially, to **expand** the cyber security dialogue within and between port communities in order to develop collaborative approaches and enhance cooperation between public and private sector stakeholders.[2] Initially, the primary objective must be to establish a dedicated cyber security governance framework and toolkit that can be deployed on a global basis.

*The time has come to not only initiate but, crucially, to expand the cyber security dialogue within and between port communities in order to develop collaborative approaches and enhance cooperation between public and private sector stakeholders.*

*Courtesy PortXchange*

### The Port Authority as Orchestrator

Port authorities are inherently endowed with a natural orchestration role. This can and should be leveraged to facilitate dialogue throughout the whole port ecosystem and promote a holistic approach that includes not only trade stakeholders, but also city and regional governmental agencies and ministries, including those responsible for national security and defense. Cyber security resilience is also an increasing part of the 2030 UN Sustainable Development Goals (SDGs), which are the bedrock of IAPH's World Port Sustainability Program (WPSP). Launched in May 2017, WPSP aims to enhance and coordinate future sustainability efforts of ports worldwide and foster international cooperation with partners in the supply chain.

In the emerging digital and automated era for ports, commonly termed the 'Smart Port' generation, a growing number of port authorities are coordinating the implementation of new digital technology solutions to deliver connectivity, visibility and control, improving service across supply chains, including port community systems (PCS) to manage digital trade logistics.

PCS entities are recognized as trusted third parties facilitating key 'one-to-many' mission-critical business relationships and infrastructure-based services that could be deliberately targeted with the intent to disrupt operations and interrupt entire local, regional, national and global supply chains. The European Cyber Security agency (ENISA) has also recently introduced four cyberattack scenarios at the port community level:[3]

- **Scenario A:** Acquiring critical data to steal high value cargo or allow illegal trafficking through a targeted attack
- **Scenario B:** Propagation of ransomware leading to a total shutdown of port operations
- **Scenario C:** Compromise of port community systems for manipulation or theft of data
- **Scenario D:** Compromise of operational technology systems creating a major accident in port areas

The Fourth Industrial Revolution (4IR) – a phrase coined by the World Economic Forum is ushering a growing number of disruptive technologies into the supply chain that could significantly impact smart port community entities at various levels. This includes such capabilities as artificial intelligence (AI) and machine learning (ML), advanced analytics (including descriptive, predictive and proscriptive), blockchain, Industrial Internet of Things (IIoT) devices and sensors, robotics, automation, autonomous systems, digital twins and 5G networks.

In the context of autonomous systems, the development of unmanned aerial vehicles ("UAVs", but also more commonly known as drones) introduce both threats and benefits to port community critical infrastructures. The rapid development of maritime autonomous surface ships (MASS), along with the emergence in ports of fleet digital remote operation centers and digital fleet security and supervision centers will establish cyber security as a primary risk that will need to be managed robustly. Beyond the digital transformation of port communities, the 4IR has brought its own challenges that now need to be addressed with a more holistic approach to global trade security.

Recently, some port communities have taken key first steps to drive cyber security capability development in their environments by engaging with investors and experts. For example, cyber security efforts are rapidly strengthening at key port trade hubs as a direct result of a new wave of investment accelerators, technical centers of excellence, and academic programs focused on innovative technologies, including start-ups in ports and maritime trade logistics. Some of the companies around the world leading these efforts include PortXL in Rotterdam, the Dock Innovation Hub, and Pier71 in Singapore.

In 2019 alone, venture capital firms invested an historic USD7.86 billion in 646 cyber security start-ups, and with the emerging information security global market currently estimated at USD120.6 billion further fueled by the growth of the cloud, mobile devices, IoT/ IIoT and operational technology (OT) devices in business-critical functions, opportunities for technological disruption will continue to expand and grow at an exponential pace. And so too will the cyber threat landscape continue to evolve.

As port communities continue to employ integrated, connected technologies, the need to proactively manage this fast-changing cyber threat landscapes will only increase.

[1] *World Economic Forum Global risks Report 2020*

[2] *Cyber security in the maritime and logistics supply chain, IPCSA, 2015*

[3] *Port Security - Good practices for cyber security in the maritime sector from the United States, ENISA, 2019*

*Courtesy MIT Panama*

# Chapter 2

## The Importance of using a common global language to address cyber security issues for port communities

***Effective cyber risk management depends on a common understanding of terms, financial grounding and recognition of shared responsibility across both the organization and the port community overall.***

As the cyber threat landscape continues to evolve, port community stakeholders are increasingly seeking to invest in technological solutions. But while high-profile cyber attacks like that suffered by Maersk focus leadership attention on technical responses, a more mundane problem continues to challenge the global maritime industry overall and port communities in particular: that of *language and communication.*

With numerous and increasingly sophisticated cyber security solutions available on the market, port community stakeholders often deploy resources – people, processes, tools, funding, strategies – and ad hoc tactics that employ different principles but with distinctive terminologies. Certain terms, common to some, can have entirely different meanings within the context of a community or organization's specific operating environment. For example, a cyber 'incident' for one company may represent a wide range of possible events, while within another company the term may indicate a narrower, more significant meaning.

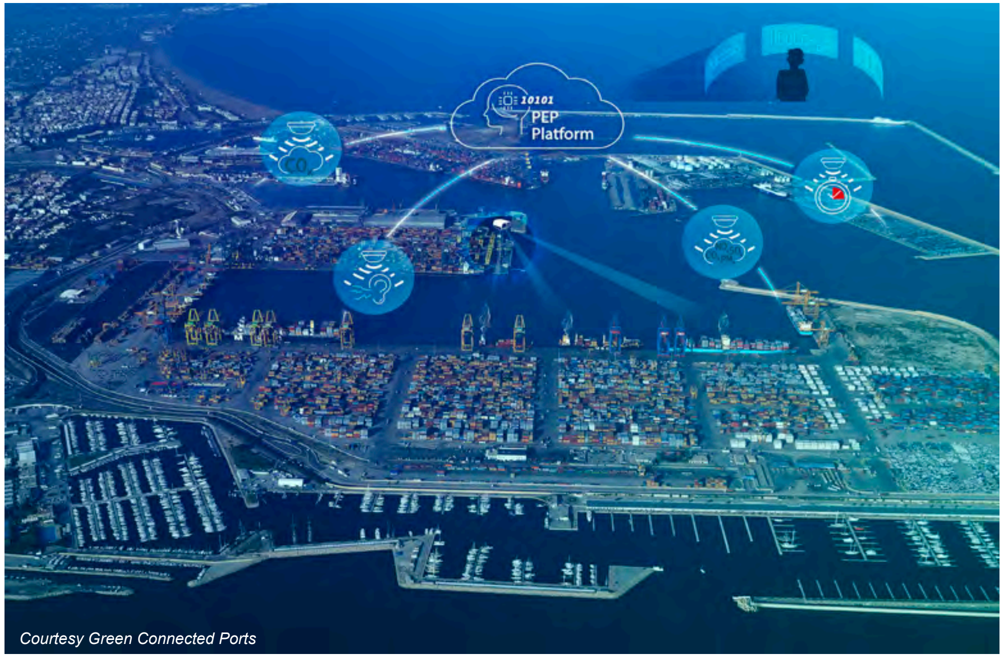
At the organizational level, lack of clear definitions can result in inconsistent behaviors, such as erratic notification and reporting activities that, when manifested, can jeopardize the business and indirectly or inadvertently place port community partners at risk. This can result in frustration among port community stakeholders who advocate for the implementation of standardized methods, principles, controls and processes to manage cyber risks to port ecosystems.

To make matters worse, connotations will fill the vacuum created by the absence of common definitions. For example, when the term 'cyber security' arises in the management meetings of many organizations, non-technical leadership frequently point to the "IT Person" as the de-facto individual responsible for managing the risk. Such a reaction, and the almost blind dissemination of this perception inside many organizations and groups thereof, essentially represents a rejection of collective responsibility. C-level management might rather embrace the understanding that digitalization and cyber security "are not IT issues, but business issues."

In order to function in today's cyber-enabled world, organizations rely on groups of individuals, each with their own occupational frame of reference, along with their diverse personal knowledge, skills and expertise, to perform their jobs. However, we take what is by nature a hard problem – that of understanding and managing organizational cyber risk – and make it more difficult and problematic when people neither perceive of, nor speak about, cyber risk management in the same way.

When stakeholders fail to find common ground in speaking about and understanding cyber risk management in terms of shared understanding, they unintentionally place their organizations at greater chronic risk to cyber-attack. In the worst-case scenario, an organization's key stakeholders might talk past one another during highly stressful situations, such as during an initial incident response to a debilitating cyber breach.

The first step in establishing a common language must and should involve defining a **shared set of terms**. Numerous sources of common cyber security terms exist today, however port communities and organizations must identify and define a clear set of baseline terms for their specific ecosystem in order to facilitate clear and unambiguous communication across organizations. Adopting commonly accepted, shared terms will benefit stakeholders by improving the accuracy and timeliness of cyber communications at the organization and community levels and reduce the likelihood of misunderstanding and miscommunication. To assist port community stakeholders, a *Glossary of Terms* is enclosed.



*Courtesy Green Connected Ports*

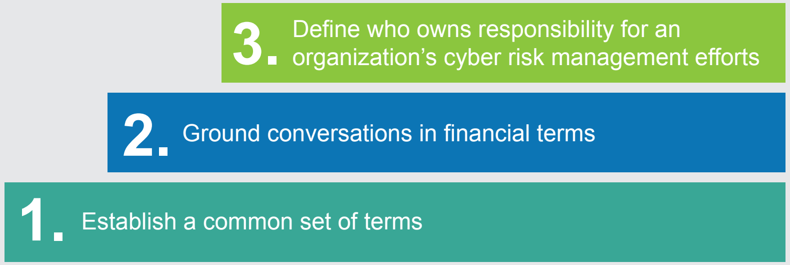
However, establishing a shared vocabulary is just the first step in creating a common language. The challenge remains to bridge the language barrier between technical and non-technical leadership, with the latter group representing most port community stakeholders.

When confronted with the challenge of managing cyber risk, many port community leaders – most of whom are not experts in information technology or cyber security – are left asking questions such as *What do we invest in first? How much do we budget? What are our priorities? How can we measure the effectiveness of our investments? Will our investments be sustainable?* These are legitimate business questions, and, of course, the common linguistic denominator of business is that of *money.*

Therefore, in addition to establishing a common vocabulary for managing cyber risk within port communities, the **conversations must be grounded in financial terms**. Doing so translates cyber risk management into the structural conceptions and financial management metrics of business. Establishing the *cyber-risk-to-money* intersection across all areas of an organization will offer a means of measurement to inform investment decisions regarding resource identification, allocation and prioritization. Critically, this empowers decision makers with relevant commercial context and the key inputs necessary to make such judgments in a consistent manner.

Ultimately, gaining a better understanding as to who participates in the cyber risk management decisions of port community stakeholders leads us to the third and final step in establishing a common language: that of **characterizing who owns the responsibility for understanding and managing an organization's cyber risk management efforts.**

## 3 Steps to Establish a Common Cyber Risk Management Language for Port Communities



3. Define who owns responsibility for an organization's cyber risk management efforts

2. Ground conversations in financial terms

1. Establish a common set of terms

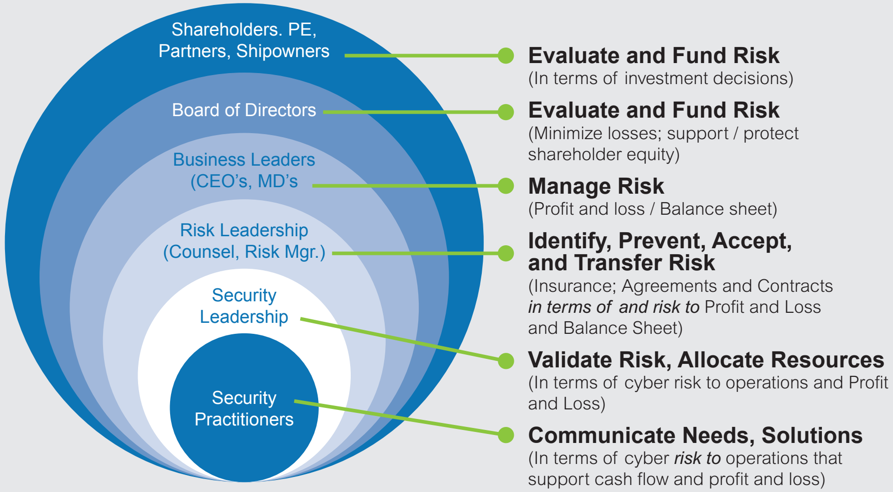
Those who initially evaluate cyber risk in terms of risk to foundational investments are the owners, shareholders and institutional investors (e.g., private equity) of the port community.

Those who evaluate cyber risk to invested capital in terms of supporting and protecting investor and/or taxpayer equity are the boards of port commissioners and the boards of directors for public and privately owned entities respectively.

Those who identify, prevent, accept, and transfer cyber risk related to balance sheet, cash flow, and profit and loss performance are organizational leaders such as CEOs and Managing Directors.

Those who evaluate and manage cyber risk to organizational integrity are found in risk leadership positions, such as finance, in-house counsel, risk management, and business unit leaders.

## Risk Ownership Relationship Hierarchy



Shareholders. PE, Partners, Shipowners
Board of Directors
Business Leaders (CEO's, MD's
Risk Leadership (Counsel, Risk Mgr.)
Security Leadership
Security Practitioners

**Evaluate and Fund Risk**
(In terms of investment decisions)

**Evaluate and Fund Risk**
(Minimize losses; support / protect shareholder equity)

**Manage Risk**
(Profit and loss / Balance sheet)

**Identify, Prevent, Accept, and Transfer Risk**
(Insurance; Agreements and Contracts *in terms of and risk to* Profit and Loss and Balance Sheet)

**Validate Risk, Allocate Resources**
(In terms of cyber risk to operations and Profit and Loss)

**Communicate Needs, Solutions**
(In terms of cyber *risk to* operations that support cash flow and profit and loss)

Those who evaluate and validate cyber risk to allocated resources are the security leaders of information and physical security operations.

And, finally, those who identify cyber risk to day-to-day activities, evaluate operational needs, identify gaps and solutions, and who communicate these to senior leadership are those serving in front-line operations, such as information technology and security practitioners (among them, the "IT Person").

So, is it only the "IT Person" who is the sole curator and communicator of all cyber language and meaning; who is responsible for managing risk to the 'balance sheet' of the organization or ensuring the economic viability of the port community; who is the privileged guardian of budgets; and, ultimately, who is the only one endowed with cyber risk management decision-making authority?

Developing a set of common terms and definitions is critical to driving cyber security capability and resilience across a port community ecosystem. Doing so will improve the accuracy and timeliness of cyber communications, which will increase the effectiveness of cyber defense and overall organizational resilience. To achieve this, port community stakeholders must agree on a common cyber lexicon to ensure communication clarity, distill the cyber risk management discussion into the common business *lingua franca* of money, and drive a common understanding toward a recognition that **the responsibility for managing cyber risk is a shared one.**

# Chapter 3

## What is Often Lacking in Cyber Defense and how does that Relate to Recent Cyber Security Incidents?

***Taking into account the doctrines of defense ministries and their role regarding critical assets, port communities need to adopt a more collaborative, cohesive and coordinated approach to cyber defense to harness the collective strength and knowledge of all stakeholders***

Cyber defense in the port community often lacks a community approach. Today, individual companies are focused on protecting their own systems, with limited or no coordination with other members of the port community. As a result, the port community does not benefit from the collective strength of community defense and it is at greater risk of disruption from a coordinated cyber attack.

While the reasons for the lack of a community approach vary with each port, typical contributing factors include:

- **Lack of a Port Community Policy**
  Establishing and implementing a cyber defense policy for the port community is a challenge because no one member has governance over the entire community. Differences in cyber capabilities, standards and reporting requirements throughout the community add to the issue. A universal policy across the industry is not the answer, because each port community is unique and the policy should be effective and appropriate cyber security for each specific community

- **Lack of Visibility**
  While companies may understand the cyber risks to them individually, they may not have visibility to the risks within and for the community as a whole. This includes the growing interconnectivity and dependencies with other community members and the potential new risks as a result. Community cyber defense requires more than securing the isolated enterprise alone

- **Unwillingness to Share Cyber Information**
  Community members are often unwilling to share cyber information. Stakeholders in the port community are often direct competitors with each other, therefore members may not want to share information that could, in their perception, help their competitors, or may not want their information to be used against them

- **Lack of Resources**
  Community cyber defense requires resources, including qualified staff and funding. Allocating limited resources to community cyber defense may be viewed as a lower priority than other more visible and traditional needs

The concept of community cyber defense is not new. For example, government doctrines and legislation have encouraged cyber security information sharing in the maritime and critical infrastructure communities.[1] However, due to limited participation, if any, the benefits of port community cyber defense are also often limited. Community based benefits include:

- **Greater Collective Knowledge**
  Community cyber defense results in a greater collective knowledge base of the threats against the community. Similar to a traditional neighborhood watch scheme, individual companies can now know about threats that they didn't see, but others in the community did and shared

- **Improved Resilience**
  Port community members depend on each other as goods are moved from one entity to the next within a supply chain. A disruption to one member will have ripple effects, as the recent Shen Attack Cyber Risk Scenario by the University of Cambridge and Lloyd's[2] aptly indicates. Community cyber defense provides the community with greater resilience, including reducing the risks of supply chain disruptions

- **Early Warning System**
  Community cyber defense provides its members with an early warning of threats against their community. Members could be alerted of threats before the information is made available through other channels

- **Collaboration Forum**
  In addition to the technical aspects, port community cyber defense provides the forum for collaboration among members. Developing a body of knowledge, procedures and policies for the whole community is paramount

While the major incidents in the maritime industry over the past several years are well known, those were individual incidents. A disturbing recent trend, although not yet in the maritime industry, is an increase in coordinated attacks on similar entities. In July 2019, three school districts in Louisiana were victims of a coordinated attack, resulting in Louisiana declaring a state of emergency. In August 2019, 22 towns and cities in Texas were victims of a coordinated attack.

The concern is the coordinated attacks against similar entities, performing similar functions, likely having similar computer systems and consequently similar vulnerabilities. In a port community, similar entities exist throughout the ecosystem. A coordinated attack against multiple entities in the ecosystem could cut off the flow of goods at a port and disrupt the entire community - and indeed national economies and international trade - by breaking the supply chain. The most effective counter measure to a coordinated cyber attack is a coordinated cyber defense by the port community.

[1] *Examples from the United States include: FAA Reauthorization Act of 2018 (Section 1805 - Cyber security Information Sharing and Coordination in Our Ports), Strengthening Cyber security Information Sharing and Coordination in Our Ports Act of 2017, 2017 Presidential Executive Order (Trump) on Strengthening the Cyber security of Federal Networks and Critical Infrastructure (Section 2), 2013 Presidential Executive Order (Obama) on Improving Critical Infrastructure Cyber security.*

[2] *For more information click here*

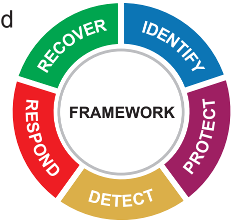
# Chapter 4

## Essential Building Blocks for a Resilient Port Community Policy on Cyber Security

***Exploring the US National Institute of Standards and Technology 5-step framework for reducing cyber risks to critical infrastructure and how (port) authorities can effectively deploy it***

The National Institute of Standards and Technology (NIST) of the United States has developed a framework for reducing cyber risks to critical infrastructure.[1] It has become widely accepted as a tool that can help manage and reduce risks related to cyber threats. It focuses on five separate functions that need to be addressed to increase cyber resilience: identify, protect, detect, respond and recover.

In this section of the paper we discuss the five functions and explain what they may mean for your organization and port community.



*NIST Framework*

### Identify

The first function of the framework – 'identify' - provides a necessary basis for any organization to start or further professionalize their cyber security measures. This function serves to understand the business context and critical functions in order to determine the areas where cyber security measures should be taken and prioritized.

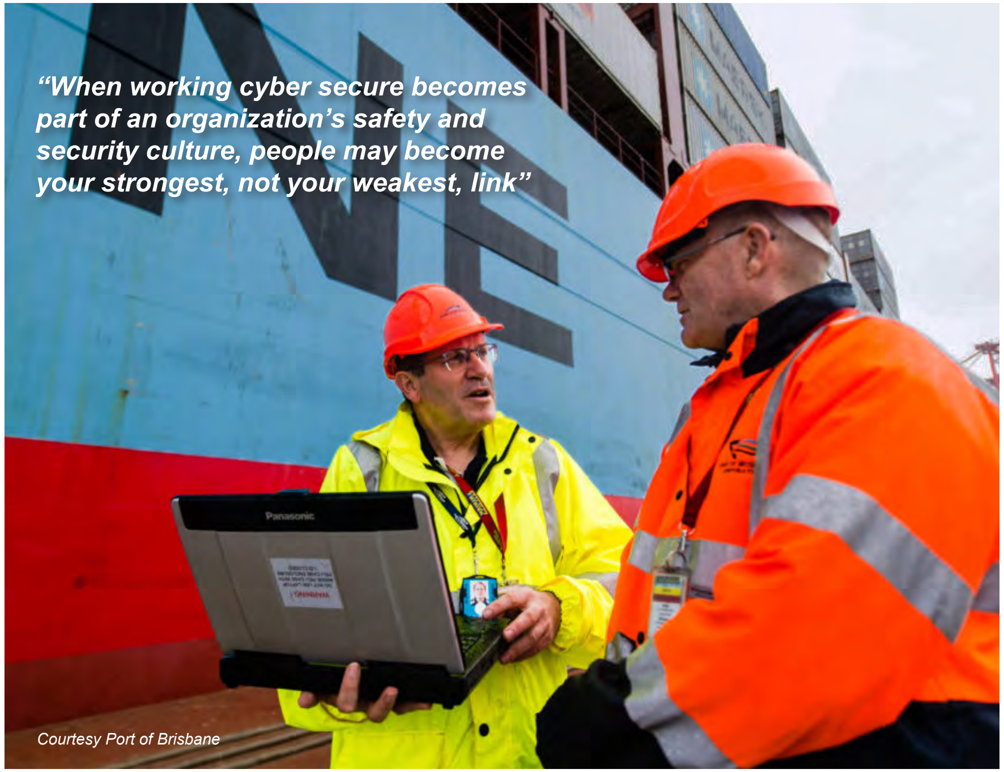
***Identify Case Study Example:***

*The nautical and maritime stakeholders in the Port of Rotterdam performed an analysis of the vital process 'safe and efficient handling of shipping' and determined which systems and partners are vital to the continuation of the process. This resulted in an overview of applications and IT infrastructure that the nautical and maritime partners rely on. It also identified the interdependencies between these systems. With this analysis in hand the organizations were able to prioritize a set of measures that aim to ensure the availability and integrity of this vital process.*

### Protect

The protect function of the framework includes taking measures such as putting identity and access management in place, ensuring that access to data and systems is only granted to those who need it for executing their tasks.This aspect is also relevant to comply with national and international privacy legislation such as GDPR. The protect function also focuses on managing protective services such as firewalls, end-point protection and managing vulnerabilities and patching procedures. Furthermore, ongoing investment in staff training (IT, OT and support) should be made to keep pace with the fast-changing challenges of cyber security.

Another aspect of the protect function is creating awareness. When professionals discuss cyber resilience, they often refer to people as the weakest link. And indeed, this may be true in breaches that involve phishing, social engineering or another form of human contact. However, when "working cyber secure" becomes part of an organization's safety and security culture, people may in fact be your strongest link. When employees are taught to detect and report suspicious behavior, e-mails and changes in IT, they become a robust line of defense. It is therefore vital to invest in ongoing efforts to raise cyber security awareness.



***"When working cyber secure becomes part of an organization's safety and security culture, people may become your strongest, not your weakest, link"***

*Courtesy Port of Brisbane*

Awareness is also vital at board level. In the end, the objective of cyber resilience is to reduce risks. The work of your cyber security professionals contributes to decreasing the risk that the confidentiality, integrity or availability of your data, processes and business are compromised. Without awareness at the top, organizations' commitment to cyber security may result in a mismatch between their cyber security maturity and the boards' risk appetite.

### Detect

The third function of the framework - 'detect' - is one of increasing importance. Even though you have protective measures in place, your organization may suffer from a breach or hack. It is important to be able to detect a breach. Benchmark research conducted in 2018 by IBM Security showed that on average a breach is detected after 197 days [2]. The same research revealed that the mean time to contain the breach was 69 days. Knowing the normal behavior of your IT and OT (your baseline) is crucial in detecting potential malicious activities.

***Detect Case Study Example:***

*The Port of Los Angeles Cyber Security Operations Center employs advanced technologies with layered detection capabilities. At the perimeter of the network, some 40 million unauthorized intrusion attempts are blocked every month. Within the network, multiple intrusion detection layers are used to continuously search for, detect and contain suspicious activities.*

### Respond and Recover

The statistics on mean time to contain a breach show that it is of critical importance to work on incident response and recovery; these are the final two functions of the NIST framework. Incident response planning and training are crucial to decrease the mean time to contain a breach as well as prevent excessive damage, not least reputational.

Your IT incident response team should be ready to act according to a predefined response and recovery strategy. This strategy should include communications departments to ensure appropriate internal and external crisis communications and protect your reputation. A computer emergency response team (CERT) is an example of a response capability. Vendors may offer this as a service or organizations may decide to set-up a response team by extensively training and educating in-house staff.

***Respond and Recover Case Study Example:***

*The Port of Rotterdam Authority has developed its own cyber crisis response strategy which includes a Port Crisis Team. The aim of this team is to make strategic decisions on the continuation of safe and efficient handling of shipping. The Port Crisis Team is supported by three action centers. One focuses on maritime issues, another on solving the IT issue at hand and the final center aims to align communication (both inward and outward) between the parties involved.*

### Next Steps

The building blocks described in this section should guide your IT security department in growing towards a more cyber security mature organization. They should be enabled and empowered to perform their work by ensuring top-level commitment to the cause.

[1] *NIST Framework* [2] *IBM Research*

# Chapter 5

### Where does the International Maritime Organization (IMO) come in?

***A review of IMO security-related regulations impacting ports and terminals and to what extent these currently encompass cyber security***

This chapter reviews security-related instruments from UN global shipping regulator the International Maritime Organization (IMO) that directly affect ports and terminals and explores to what extent current rules encompass cyber security. It is vital for ports, terminals and port communities to have a clear understanding of how IMO regulates cyber security in order to embed compliance within broader port and port community cyber risk management.

The starting point is that within the maritime domain, including port facilities, security has been focused traditionally on physical operations. But as discussed extensively in this white paper, ports and terminals today are increasingly reliant for their physical operations on information and communication technology (ICT). With the physical and virtual worlds ever-more entwined, it is equally crucial to maintain appropriate safeguards in relation to ICT systems, networks and personnel.

Ports and terminals must therefore identify the scope of regulatory responsibilities that they have under IMO regarding cyber security in order to mitigate the specific risks that might arise.

The two main IMO regulatory instruments in the context of port security are the International Ship and Port Facility Security (ISPS) Code as part of the Safety of Life (SOLAS) Convention and the International Safety Management (ISM) Code which has been extended by Guidelines on Maritime Cyber Risk Management.

### IMO International Ship and Port Facility Security (ISPS) Code

The ISPS Code as part of the SOLAS Convention is a comprehensive mandatory security regime for international shipping and port operations. It aims to provide a standardized, consistent framework for evaluating risks, enabling governments to ensure that proportionate security measures are implemented.

The ISPS Code entered into force on 1 July 2004 and focuses on threats posed to maritime security and more specifically, to ships and shipping, in the wake of the tragic events of 11 September 2001 in the USA.

The ISPS Code is divided into two parts. Part A is mandatory and covers detailed security-related requirements for ports and terminals. Part B is non-mandatory and contains a series of recommendatory guidelines about how to meet these requirements.

The focal point for ports and terminals is the ship/port interface: the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons and goods to and from the ship and the provision of port services.

In order to comply with ISPS regulations, competent authorities must undertake port facility security assessments (PFSAs) and plans, port facilities must appoint port facility security officers (PFSOs) and invest in certain security equipment. Port facilities will also need to monitor and control access, monitor the activities of people and cargo and ensure that security communications are readily available.

Compliance with the requirements involves the production of a port facility security plan (PFSP) that details the measures at various security levels.

As an instrument aimed at threat reduction towards a ship, the ISPS Code also has the effect of reducing unauthorized third-party access to port infrastructure.

### ISPS Code and Cyber Security

As we have outlined, the ISPS Code's primary objective is to reduce physical threats towards a ship. However, there are obvious indicators that cyber security is indeed relevant to this regulatory instrument.

The PFSA identifies radio and telecommunication systems, including computer systems and networks, as relevant elements (ISPS Code, Part B, 15.3 sub 5). This implies that if cyber security might endanger maritime security, and more specifically a vessel, this aspect should be considered.

### ISPS Code and Cyber Security on a Broader Level

A next step to explore comes from the awareness that cyber threats might originate from ships and port facilities themselves, with negative implications for operations. An example is the malfunction or non-functioning of cargo-related IT systems either on the ship or shore side. As we have seen from incidents in the last few years, this can lead to a breakdown in port operations with broader implications for supply chains, and for national and international economies.

So, are managing these broader cyber risks an objective of the ISPS Code? There are clear indications that the Code authors have thought in this direction, as ISPS stipulates that the PFSA shall include the identification of possible threats to assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures (ISPS Code, Part A, 15.5 sub 2).

This stipulation has to be read in combination with the consideration that while the focal point of the ISPS Code is the physical protection of a ship during its stay at port, there could be circumstances under which a ship might itself pose a threat to the port facility, e.g., it could be used as a base from which to launch an attack (ISPS Code, Part B, 1.4). This leads to the conclusion that the PFSA and PFSP should reflect this issue.

All of this leads to the conclusion that the role of the PFSO must evolve to encompass cyber security at the ship/port interface, rather than being focused purely on physical threats. Indeed, this applies not just to cyber security at the ship/port interface, but more generally to cyber issues relevant for the wider well-being of maritime assets, infrastructure and supply chain operations.

The challenge when considering the future role of the PFSO is how to determine their wider outreach to the broader cyber hygiene of a port facility. Taking the unpredictability and ever-changing nature of cyber threats into account, a limited or partial approach probably will not suffice.

### International Safety Management (ISM) Code - Guidelines on Maritime Cyber Risk Management

Helpful in this context is IMO's International Safety Management (ISM) Code, which was extended in 2017 with specific [Guidelines on maritime cyber risk management (MSC-FAL.1/Circ. 3.]()

The guidelines recognize that cyber technologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. The guidelines further acknowledge that the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. In summing up the different areas for attention, cargo handling and management systems are specifically mentioned.

IMO's decision to extend the ISM Code with Guidelines on maritime cyber risk management (MSC-FAL.1/Circ. 3) acknowledges the functionality of a broader cyber hygiene to the security of shipping. As this basic approach closely mirrors the Cyber Security Framework of the US National Institute of Standards and Technology as outlined in Chapter 4, and is also transferrable to port facilities, a next step at the IMO level is welcomed to define how this is to be operated in the context of the ISPS Code.

*Courtesy Port Authority of NSW*

# Glossary of Cyber 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). |
| Adware | Specialized advertising software designed to present pop-up messages, windows, or banners on an application that is running. Adware typically captures, tracks, and passes on a user’s personal information to third parties without the user’s knowledge or agreement. Over time, adware degrades computer performance. |
| 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. |
| 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. (Part 1 of the AAA framework) |
| Authorization | The process for approving or permitting an individual, application, and/or system to do something. (Part 2 of the AAA framework) |
| Accounting | The process to measure the resources a user consumes during access, such as the amount of system time or the amount of data that a user has sent and/or received during a session. (Part 3 of the AAA framework) |
| 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 access to unauthenticated users, 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. |
| 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. |
| CERT<br>(also CSIRT) | Computer Emergency Response Team (CERT). Also: Computer Security Incident Response Team (CSIRT). |
| 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. |

| | |
|---|---|
| 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 is 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. |
| 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 the presence of cookies, and users can accept or erase them. |
| Cyber Attack | An event that is launched via the Internet 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. |
| Cyber Security | The capability to protect or defend against unauthorized access to or use of cyber space from cyber attacks. Cyber security 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. |
| Cyber Security Plan | A document that identifies and defines the cyber security requirements and associated controls necessary for meeting those requirements. |
| Cyber Security Policy | A set of principles, measures, and conditions that have been defined to support cyber security capabilities and planning across an organization. |

| | |
|---|---|
| Cyber Security Program | An integrated set of coordinated activities that include governance, strategic planning, executive sponsorship, reporting and training that is managed to meet defined cyber security objectives for an organization. While cyber security 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. |
| Cyber Security 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 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. |
| 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. |
| 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 cyber security events. In addition, they are designed to provide guidance to support continued operations through a declared cyber security event in a manner that is both aligned and commensurate with the risk to the organization's capabilities and overall objectives. |
| 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. Firewalls can be configured to restrict network traffic according to defined rules. |
| Cyber Governance | A framework for defining and providing strategic direction and guidance for an organization to ensure that it manages cyber risks while meeting its performance obligations. This involves the appropriate development of policies, as well as allocation of human capital, technical and financial resources. An effective cyber governance framework assumes active sponsorship of leadership, regulatory-related compliance activities, and alignment of strategic objectives. |

| | |
|---|---|
| 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 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 cyber security 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 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 cyber security, 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. |
| ISAC | Information Sharing and Analysis Center, an institution that supports the gathering, analysis and sharing of cyber threat 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. |
| 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. |
| Maturity | In the context of cyber risk management maturity is a measure of the extent to which a process, practice or capability has been adopted within an organization's cyber security program and employed across its enterprise. |
| 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 (MFA) | The required application of two or more factors that 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., biometric, such as a fingerprint); or D) you are where you say you are (e.g., a GPS token or device). |
| Operational Resilience | The organization's overall capability to recognize, adapt and respond to risks that affect its critical assets, applications, systems, and/or platforms. A key characteristic of operational risk management, operational resilience is further reinforced and enabled by physical security practices, business continuity and continuity of operations. |
| Operational 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. |

| | |
|---|---|
| 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. |
| Phishing | A digital form of social engineering to deceive individuals into providing sensitive information. |
| Ransomware | Computer malware that installs on a system, encrypts the system's data, prevents access to these data, and holds the data hostage or threatens to publish the data until a ransom is paid. |
| Social Engineering | The psychological manipulation of people in order to obtain unauthorized access to data or systems. This typically involves tricking an unsuspecting person into bypassing normal security controls and divulging confidential information or providing access to business networks. |
| 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. |
| Spear Phishing | Phishing (see definition above), but personalized and directed at an individual, usually a senior person in the organization. |
| Spoofing | An attack by which a malicious actor impersonates as a trusted actor by using a trusted IP address to hide the malicious IP address. An attacker might do this to attack a network host, spread malware, steal information, or other actions that require bypassing access controls. |
| 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 that 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 or event caused by vulnerability that can 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 for 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. |
| 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. |
| Vishing | An attack in which a scammer solicits private information via social engineering over the telephone. Victims are encouraged to share user names, confidential passwords, private financial account information or credit card numbers. |

## Contributors

### Max Bobys

Max Bobys is Practice Leader forHudsonCyber, which specializes in best-in-class cyber risk management, enterprise assessment, threat intelligence, and training solutions for the global maritime industry. In previous executive roles at Civitas Strategy Group, BAE Systems, Stanley, and Ciber, he has advised US Government civilian and military agencies, NATO, and various allied governments across Europe, Latin America, and the Middle East. He is an advisor to IAPH and the Organization of American States on port-sector maritime cyber risk management, and serves on the Delaware Bay Area Maritime Security Committee's Sub-Committee on Cybersecurity.

### Lance Kaneshiro

Lance Kaneshiro is Chief Information Officer at the Port of Los Angeles. As CIO, Lance leads the Information Technology Division of the busiest container port in the United States. Lance is a certified information systems security professional (CISSP), has presented on cyber security at international conferences, and is the Co-Chair of the Cyber Resilience working group of ChainPORT, which includes leading ports from around the world.

### Chronis Kapalidis

Chronis Kapalidis is the Regional Integrated Security Practice Lead for HudsonAnalytix in Europe. Chronis is also an Academy Associate at the International Security Department, Chatham House. Before joining HudsonAnalytix, Chronis was a Navy Officer at the Hellenic Navy for 15 years. He is currently pursuing his PhD at the University of Warwick where he also teaches cyber security.

### Pascal Ollivier

Pascal Ollivier is President of Maritime Street, a digital trade logistics strategic advisory and expert services firm dedicated to governments and technology solution providers to shape the future of Trade.

Pascal is a world-renowned PCS expert and has been the founding Chairman of IPCSA and Chairman of the IPCSA research committee. Pascal is also a member of the IAPH - WPSP Covid19 Task Force.

### Frans van Zoelen

Frans van Zoelen (Erasmus University Rotterdam) is Head Legal Emeritus of the Port of Rotterdam Authority and assigned to Special Projects, as well as Legal Counselor to the International Association of Ports and Harbors (IAPH), and heading up its Legal Committee. He also chairs the Dutch Legal Network for Shipping and Transport, and is a member of the Board of the Dutch Transport Law Association.

### Ward Veltman

Ward Veltman is Cyber Security & Risk Officer for Port of Rotterdam Authority. Ward's role focuses on cyber security risk management, awareness, GDPR and security project management. He's working actively to enhance cyber resilience within the port area through the FERM programme. Ward has a Masters Degree in Criminal Justice as well as a Masters Degree in Crisis and Security Management from the University of Leiden in the Netherlands.

### Rachael White

Starting as a journalist and then editor, Rachael White has subsequently worked for the past three decades as researcher, international conference organiser, market consultant, community builder, content creator and influencer in the global maritime trade and logistics industry. Her current focus is on the new wave of digitalization, automation and sustainable technologies in maritime trade, ports and logistics.

### DISCLAIMER

This guidance document has been prepared for general information purposes. Although all efforts have been made to ensure the accuracy, currency and reliability of the information contained in this document, neither the International Association of Ports and Harbors (IAPH), nor the ports and individuals that have contributed to the publication shall be liable for any loss, claim, charge, damage, liability or damages howsoever arising in connection with the information provided in this document. The use of the information is at the sole risk of the reader.