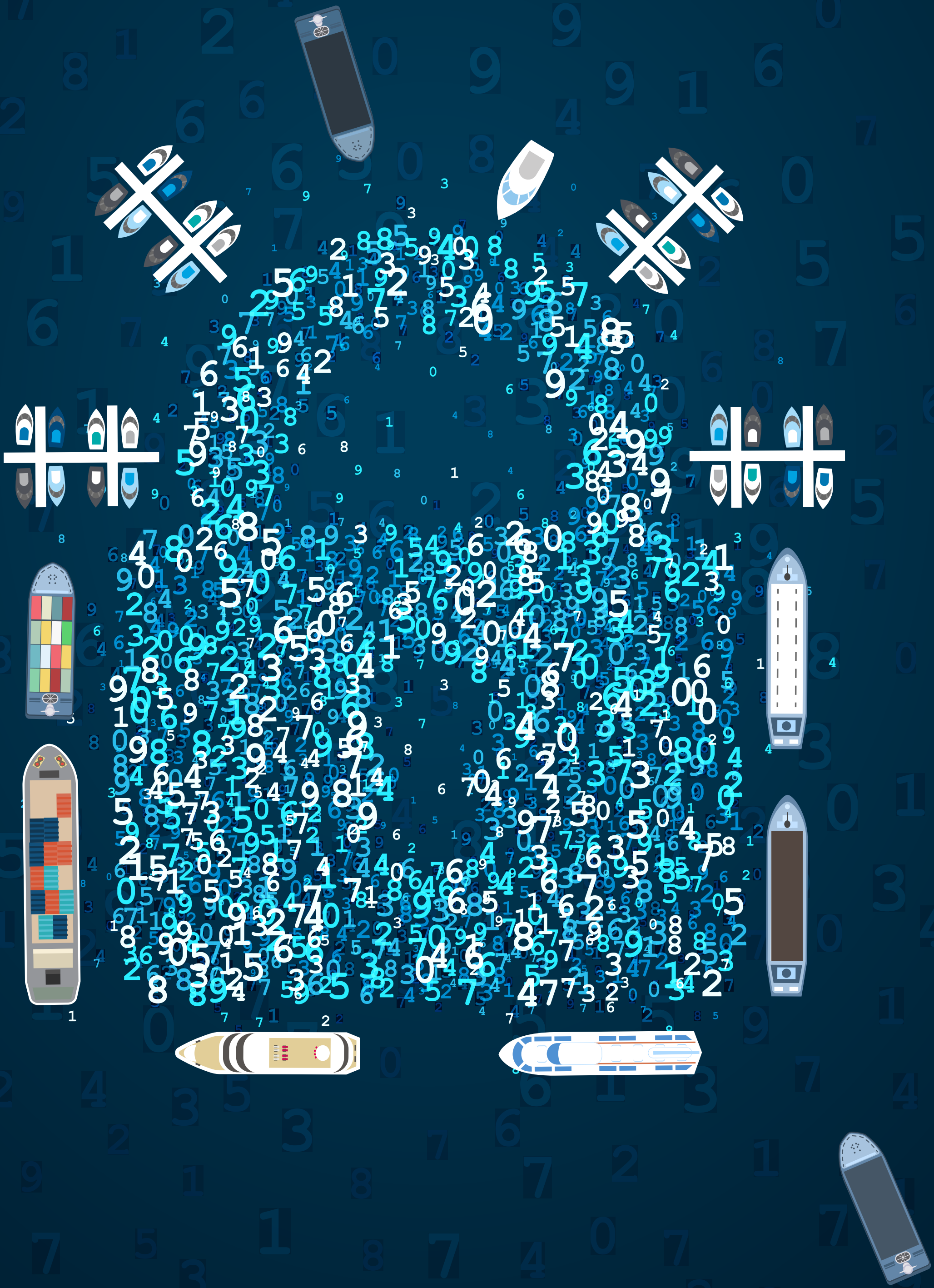
CESNI

EFIP European Federation of Inland Ports

Good practice guide
Cybersecurity in inland navigation

Especially for ports

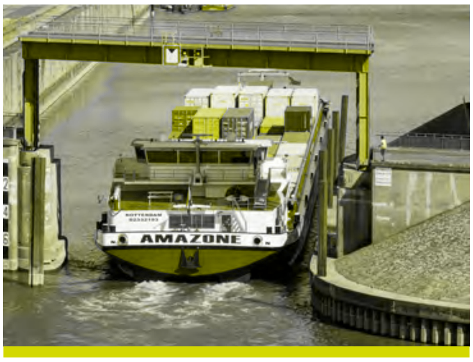


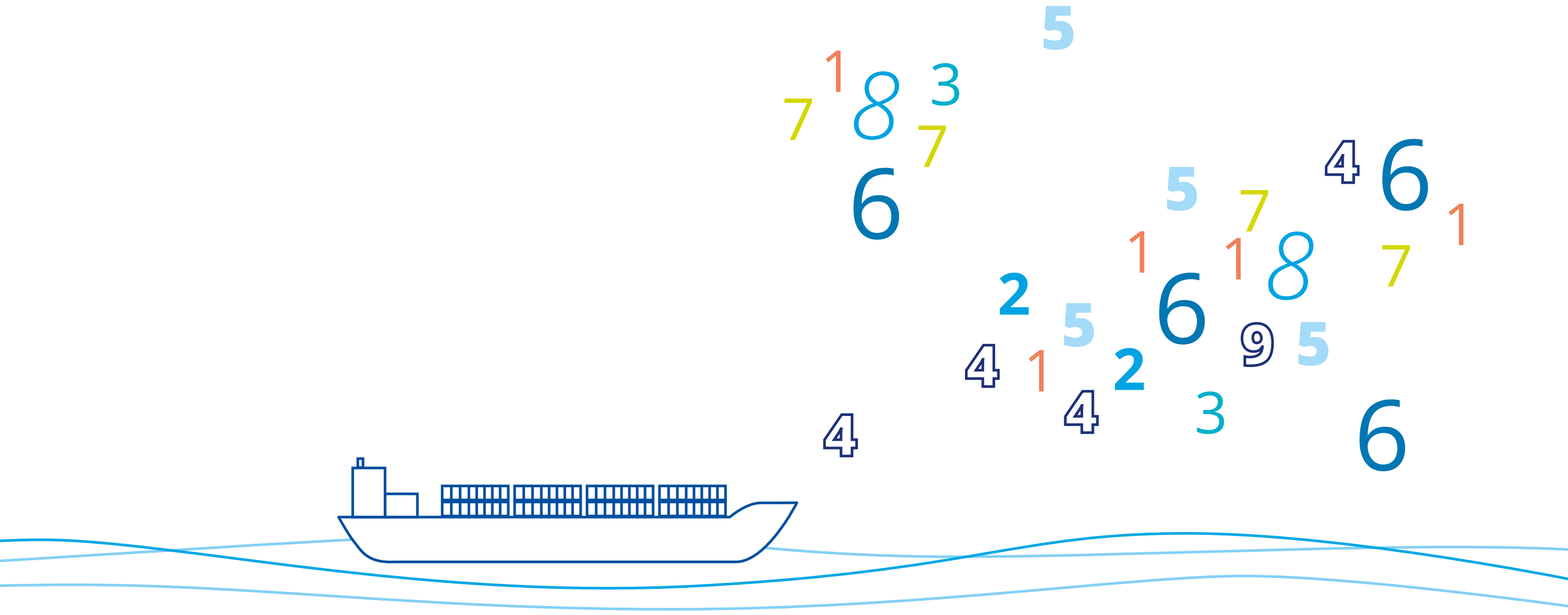
This document does not create any legal obligations for the CESNI, its Member States or its Secretariat, and it does not create any rights for users. Neither the CESNI and its secretariat, nor any person acting on behalf of the CESNI can be held responsible for the use which may be made of the information contained in this document.

Table of contents

Part 1

Part 2





Introduction

Context

Creation of this guide by the European Committee for drawing up Standards in the field of Inland Navigation (CESNI).

The primary remit of the European Committee for drawing up Standards in the field of Inland Navigation is:

- to adopt technical standards in various fields, in particular as regards crafts, information technology and crew, to which the respective regulations at the European and international level, such as those of the European Union and the Central Commission for the Navigation of the Rhine, may refer with a view to their application;
- to deliberate on priority topics regarding safety of navigation, protection of the environment, and other areas of inland navigation.

The Mannheim Declaration[1] adopted by the transport ministers of the member States of the Central Commission for the Navigation of the Rhine (CCNR) and the European Commission's NAIADES[2] action plan both identify digitalisation as a strategic subject for the future of inland navigation. This digitalisation is accompanied by new challenges and risks such as cybersecurity.

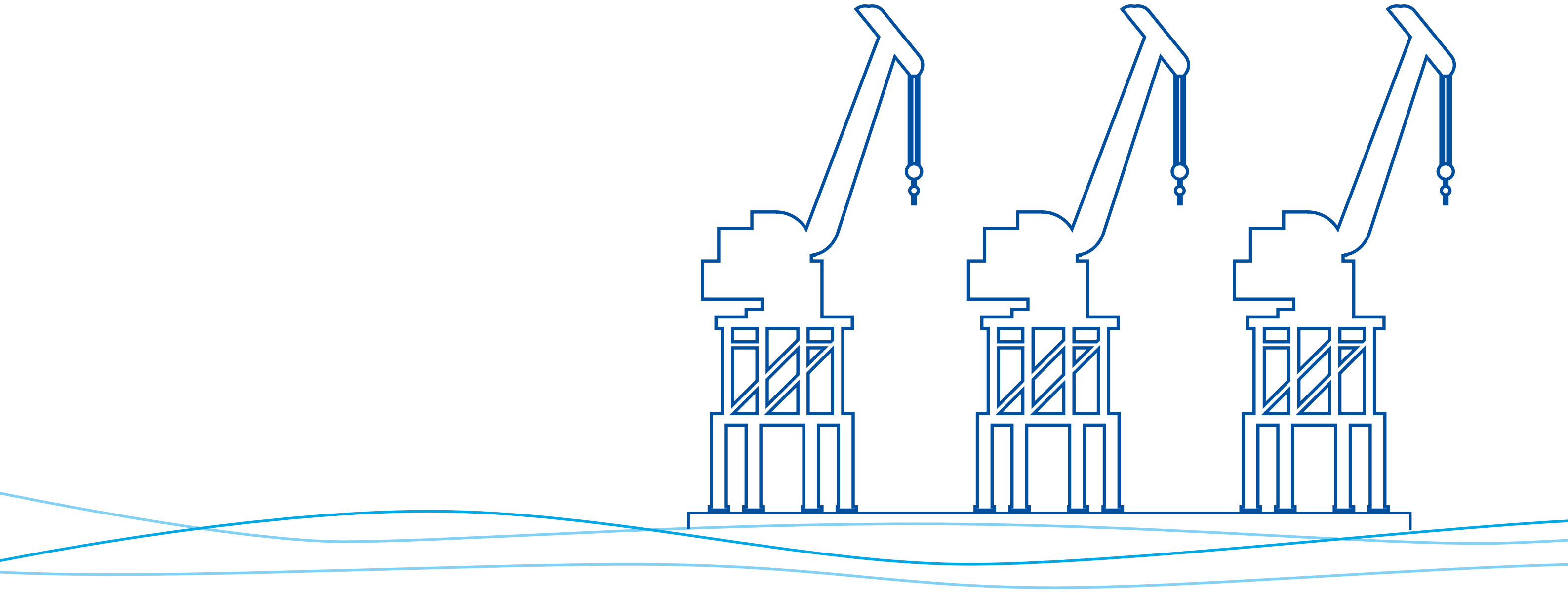
In partnership with the European Federation of Inland Ports (EFIP), the CESNI has therefore decided to draft a good practice guide for cybersecurity for inland ports.

Relevance to inland navigation ports

As the world continues to become more interconnected and more reliant on digital services, cybersecurity attacks are continually increasing. Several ports have been victims of cyber-attacks in the past few years, demonstrating that this sector is not an exception to the rule.

By way of example, in June 2017, the APM terminal in Rotterdam's "Maasvlakte" harbour basin was struck by a ransomware virus. The Port of Rotterdam was severely paralysed by the virus, being unable to operate for a period of days. Cranes were out of action and container processing fell idle. The impacts of this cyber-attack were felt throughout the port and shipping ecosystem, confirming the already widely known fact that cyber-threats are no longer confined to purely IT dependent sectors.

Indeed, as ports such as Rotterdam's become increasingly connected, digitalised, and dependent on advanced IT systems, they also become more vulnerable to such cyber-attacks[3].



[1] https://www.ccr-zkr.org/files/documents/dmannheim/Mannheimer_Erklaerung_en.pdf

[2] https://transport.ec.europa.eu/transport-modes/inland-waterways/promotion-inland-waterway-transport/naiades-iii-action-plan_en

[3] https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/

To address threats such as these, it is desirable to understand and mitigate cybersecurity risks in the inland navigation port environment. Some inland navigation ports are still dependent on non-connected, physical assets for day-to-day operations. They may not feel they are concerned by cybersecurity issues, but these ports are undeniably becoming more interconnected over time. This will require more investment to safeguard assets that are vulnerable to cyber-attack such as complex logistics software, connected camera and gating systems, remote ship navigation programmes, container management applications, and other ”smart” technologies intended to increase the efficiency of port operations. As such, reinforcing cybersecurity is not merely a question of strengthening the security of inland navigation port computer and IT systems. It also implies boosting cybersecurity awareness of port stakeholders operating all kinds of connected devices used to deliver various port-related services.

In this wider context, this guide aims to be an accessible framework for cybersecurity good practices for inland navigation ports[4].

Scope of this guide and tips on how to read it

Generally speaking, when faced with a cyber-risk, there are five possible responses:

1. accept the risk, namely do nothing and take the consequences;
2. avoid the risk, namely eliminate it completely by radical measures, for example taking a lock out of service, closing the port to navigation or prohibiting certain crafts that may pose a given risk;
3. transfer the risk, for example by taking out an insurance policy or by recourse to a third party who will bear the consequences on the port’s behalf;
4. share the risk, namely conclude an agreement with third parties to share the cost or the consequences if the risk materialises;
5. mitigate the risk, namely implement various measures that will reduce the probability of the risk materialising or else limit its impact.

In the main, this guide adopts a **risk mitigation** approach. It contains a number of components of a transfer or sharing nature, but only marginally so. It should be noted that doing nothing as far as cybersecurity is concerned is tantamount in effect to accepting all the risks, identified or otherwise.

This guide is intended to provide an overview of cybersecurity risks, threats, and mitigation measures, primarily within the scope of inland navigation ports. It is intended to enable to the target audience (see below) to understand the motivations and actors behind cyber-attacks, the assets of ports to be considered when evaluating cybersecurity threats and risks. This guide also gives an overview of good practices for the implementation of cybersecurity risk mitigation measures.

However, in order to provide a better picture of the port ecosystem, assets relevant for inland navigation craft have been included in this guide.

[4] https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/

The guide is divided into three parts:

1. cybersecurity threat landscape of inland navigation ports: providing the description of the port threat landscape, including threat actors, port assets, threat taxonomy, and attack scenarios.
2. mitigating cybersecurity risks for inland navigation ports: detailing the portfolio of mitigation actions that should be taken to reduce cybersecurity risks for ports.
3. tips for the implementation of risk mitigation measures: outlining actionable security hygiene measures to be taken as a first step by IT and non-IT stakeholders.

This guide is intended to be used as a reference point for port stakeholders and is not meant to substitute published cybersecurity risk evaluation methodologies. On the other hand, it must enable each stakeholder to identify the most appropriate measures for evaluating and dealing with cyber risks.

Target audience

First and foremost, this guide targets port actors, namely:

- port authorities or subcontractors;
- terminal operators or subcontractors;
- logistic companies working with port authorities or terminal operators.

However, a wider audience may also be interested in reading this guide, which concerns them indirectly:

- national inland waterway authorities;
- shipping companies;
- public institutions with inland waterway regulatory power;
- craft operators;
- boatmasters;
- the crew of the crafts;
- manufacturers of inland navigation sector products.

Within this public, this guide differentiates between three types of stakeholders who need to be closely involved with the implementation of the good practices contained in this guide:

IT teams **Operations managers** **Management**

References to international standards

This guide is not a substitute for international cybersecurity standards, nor even the existing literature on this subject. Its objective is to popularise cybersecurity issues in an inland port context.

To make things more tangible, a package of measures is proposed in the form of recommendations and good practices to be found in the market and consistent with the normative principles in ISO/IEC 27001.

The implementation of this guide does not in itself constitute compliance with standards that may result in certification. Nevertheless, this guide marks the beginning of a journey and a greater awareness of cybersecurity issues that will subsequently greatly facilitate a more formal cybersecurity certification procedure (for example ISO/IEC 27001).

The introduction of an information security management system (ISMS) is for example an important step in implementing standard ISO/IEC 27001. This standard includes requirements governing the definition, documentation, implementation, monitoring, maintenance and continuous improvement of an ISMS. This guide does not address these points in such detail, but it does provide for measures that will pave the way for and facilitate the implementation of an ISMS, should the organisation decide to do so.

Reference to national regulations

Just as this guide is not a substitute for international cybersecurity standards, nor is it a substitute for existing regulations, especially at national level, which are to take precedence, if applicable, over this guide.

Existing local regulations or recommendations enacted by national agencies or international bodies may (or shall) be used to increase IT security in ports.

How to use this guide

If you are reading this guide to obtain a **general understanding of the inland navigation port cybersecurity threat environment**, it is recommended you begin by reading Part 1 of this guide.

Part 2 relates to all the cybersecurity risk mitigation measures inland navigation ports are being recommended to take. This constitutes the core of this guide, with about 120 measures tailored to the inland navigation port situation, divided into three categories:

1. measures relating to organisational policies and procedures (OPP);
2. measures relating to information technology and operational technologies (ITOT) policy, and finally;
3. technical cybersecurity measures (TSM).

These measures are explained and graded according to **the level of cybersecurity target maturity** in each port.

If you are reading this guide to focus on **specific security measures to implement or to obtain an idea of your organisation's maturity**, it is recommended you begin with Part 3, which has been created to facilitate the implementation of the mitigation measures presented in Part 2. Part 3 of this guide can be read independently and used as a quick checklist to evaluate whether your organisation has implemented the appropriate measures to achieve its cybersecurity objectives. These tips are intended to be accessible and informative to all kinds of readers.

Part 3 proposes an ”applicability table” or a grid for reading the mitigation measures presented in Part 2, based on the cybersecurity objectives the port has set itself and on the type of stakeholder (IT teams, operations managers and management) in question.

If you are reading this guide to obtain a primer on cybersecurity for inland navigation ports, you may read the guide from start to finish in order to have a holistic view on the topic.

Izmail, Ukraine - Danube

Some terminology used in this guide

To make it easier to read this guide, certain terminology has been simplified.

Ports

By default and unless explicitly mentioned otherwise, the term “port” refers to an inland navigation port. The term may also refer to a hybrid port, namely a port that is both a maritime and an inland navigation port, unless the context requires a distinction to be made between a strictly inland navigation port and a hybrid port.

Asset

In the context of this guide, an “asset” is always used to refer to a “digital asset”. A digital asset is defined as a digital dataset, the ownership or right of use of which is part of an inland navigation port’s estate. (Digital) assets are therefore intangible. These may be for example data or software (the term “data item” is to be understood here in the broad sense). It should be noted that, occasionally, a digital asset may be closely associated with a tangible “conventional” asset, ensuring that it functions correctly. For example, a lock is a tangible asset, but it requires software and numerous specific data items to operate. Each tangible component of the lock: the walls, gates, but also the sensors, computers, computer cables, cameras etc. are not “assets” as construed by this guide. However, all software products (and their configuration) used by any of these tangible components are digital assets and will therefore be an “asset” as construed by this guide.

IT/OT systems

Certain sections of this guide refer to IT/OT systems. In this context, the term IT (Information Technologies) refers to that part of the system responsible for processing the information (the data item), this part being highly programmable and modifiable. The term OT (Operational Technologies) refers to that part of the system responsible for controlling machinery or physical processes. The OT component is generally highly independent and programmed to achieve a specific task (for example regulating temperature or ventilation). Put simply, the IT component processes data whereas the OT component manipulates physical objects. These two types of system can of course be used interactively, and this is especially so when one talks about “IT/OT systems”.

Cyber security: This term is used very extensively in this guide, beginning with its title. In this guide, the term “cybersecurity” is to be understood in a very broad sense. It refers to the implementation of a suite of techniques, practices, resources and tools for protecting information systems and their data. This protection is also to be construed in a broad sense, from prevention to repair, via the detection of and response to events. This protection is brought to bear against cyber-threats that can also assume several guises. They may be attacks against information systems, but also acts of negligence, accidents, natural catastrophes or human error. “Cybersecurity” encompasses threats to information systems, but also threats pertaining to physical and organisational aspects. Other terms exist with different meanings depending on country and culture, such as “data security” or “information systems security” or “IT security”.

Part 1

Cybersecurity threat landscape of ports

General cybersecurity trends and consequences for ports

The European Union Agency for Cybersecurity (ENISA) released a Threat Landscape report in 2020 applicable to maritime ports. It indicates the following findings of note when discussed in the context of the port sector:

TREND IDENTIFIED	IMPLICATIONS FOR PORTS
Financial reward is still the main motivation behind most cyber-attacks.	As hubs for economic transactions and trade dealing with potentially valuable cargo, inland ports may become a target for individuals seeking to perform criminal operations motivated by financial gain.
Finely targeted and persistent attacks on high-value data, such as intellectual property and State secrets, are being meticulously planned and executed, often by State-supported actors.	As critical trade centres receiving necessary goods, inland ports may be targets to obtain specific information on the States they are supplying.
Ransomware remains widespread with costly consequences to many organisations throughout the world.	A ransomware attack is a real threat to port environments that often depend on the availability of systems for operations.
The number of potential vulnerabilities in a virtual or physical environment continues to expand as a new phase of digital transformation arises (as technology will keep diversifying).	Inland ports are among the industrial environments undergoing heavy digital transformation projects, especially in the context of IT/OT convergent technologies. As these changes occur, cybersecurity risks should be properly evaluated and mitigated.

These findings apply to the context of inland ports and indicate that cybersecurity issues must be considered as a true risk to the critical transport and economic operations provided by ports. It is therefore desirable to take measures to mitigate this risk.

IT security of ports, their principal assets, and of inland navigation craft

Before beginning to examine security threats and ways to protect an organisation from these threats, the organisation in question must first understand what they are specifically trying to protect. To do this, conducting an asset cartography is a useful exercise with the objective of mapping all assets that could be targeted in the context of a cyber-attack.

To facilitate this task, this guide proposes a framework for the evaluation of port and craft assets. While these assets may not be present or relevant to all readers, the list below is meant to serve as a benchmark for the evaluation of assets in your perimeter. It is also important to note that the criticality of assets may vary from one organisation to the next. Indeed, the most critical asset of a port specialised in shipping could be systems supporting the operations of a container terminal, while another port may accord special importance to a central lock management system. For ports transporting passengers, such activities may be considered mission critical. Therefore, as an organisation, the first step to better understand and mitigate security risks would be to perform a complete asset scan. The objective is then to identify assets critical to its perimeter and define the list of "crown jewels" (assets to protect at the highest level).

In the case of ports, it is worth noting that there is, in some cases, an increasing presence of Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems where industrial systems and machinery are connected to networks to be operated remotely or from land. Even when these mechanical assets are not themselves a direct target, they are however accessible via the network and operate with legacy systems (no longer updated by vendors). ICS can therefore be used as entry points for targeting other assets. It is, therefore, worth including ICS in the critical asset lists.

The following description details the ports' main assets and certain assets relating to craft, especially those that may, at a given moment, be connected to the port systems.

Paris, France - Seine

Main port assets

Craft reception and docking

Related to the entry and docking of the craft in the port. Includes river infrastructure systems such as Lock Bridge Management (LBM), connected lock sensors and mechanisms, traffic planning systems.

Passenger and tourist craft systems

Web applications for the reservation and ticketing of passenger craft are an important business asset for tourist ports, and are particularly vulnerable as they are public-facing assets. Without access to these systems, tourist operations could be interrupted or paused, causing significant business impacts to port affiliates or partners.

Mooring of the craft

Tools and processes allowing the servicing of craft entering the port to refuel, renew food supplies, replenish water supply, provide craft repair, and other crew services, etc.

Container storage and staying

Craft loading and unloading management (CFM), container unloading and storage tools such as container moving, storing and handling software, bulk handling and sorting tools, refrigerated container storage and monitoring tools, etc.

Security and safety

Any tools contributing to the physical security of the port sites such as connected gates, CCTV camera services, connected doors and passageways, badging systems, connected alarm systems, guardian posts.

IT systems involved in traffic planning, such as a Vessel Traffic Service (VTS)

VTS control centres in ports in the front line of port operations, which may use Internet or VHF connections, making them potential targets for cyberattacks.

Automatic Identification System (AIS)

Automatic system for exchanging messages between crafts by VHF radio, which enables crafts and traffic monitoring systems to establish the identity, status, position and route of crafts within the navigation area.

Energy service

IT management tools and applications for supervising and controlling energy lines, equipment, plants, and power grids that are required to supply energy to the port and its infrastructure.

Authorities and customs

Tools allowing the declaration and evaluation of goods, customs payment, coordinating customs approval, distributing declarations, directing requests to authority bodies, and dealing with their responses.

Support service

Port IT hardware, software, applications, port employees' communication systems, real estate and facility management applications, dangerous goods management and refrigeration management applications. Support service assets also include "dedicated passenger and tourist craft systems" (see specific definition) .

Distribution service

Connected tools allowing the distribution of containers or bulk material to marshalling yards, transport hubs – systems complementing distribution such as container scanning systems – and distribution communication platforms. This also includes connected tools that can be found in and around railroad stations, and train cars for the transportation of containers.

Craft assets

Note

Except for assets communicating between the craft and the port or other land locations, the craft assets themselves are considered out of scope for the purposes of this guide.

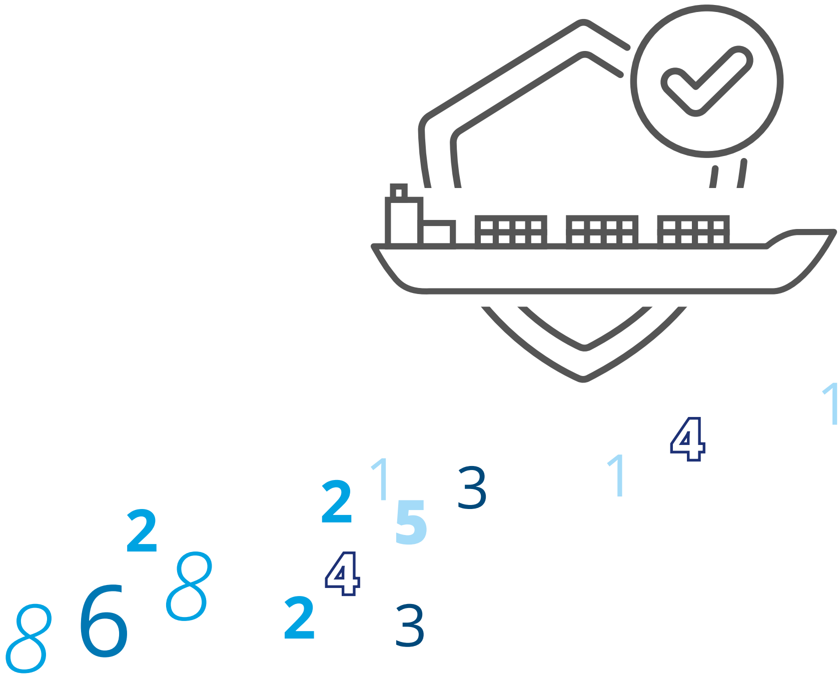
River Information Services (RIS)
Tracking and Tracing of Inland Navigation craft (Inland AIS), Inland Electronic Chart Display Information System (ECDIS), Notices to Skippers for Inland Navigation (NtS), Electronic Ship Reporting in Inland Navigation (ERI).

Communication and crew technology
Radio, satellite and other remote connected devices facilitating connection between the craft and land; crew cell phones, computers and tablets used on and off the craft.

Machinery
IT and electronic craft operation devices including propulsion and machinery equipment, power supply control systems, wheelhouse systems, fuel, battery and cargo systems.

Cargo
Tools used to communicate both on the status of cargo on board and on land regarding the delivery, contents and type of cargo.

Operational assets
Assets for operating port activity-related devices, onboard and offboard, including personal computers, laptops, smart tablets, and their business applications.



Port threat taxonomy

Once we have determined the list of critical assets of a port, or systems upon which a cyber-attack can cause damage, we can consider the types of threats to which these assets are exposed.

"Cybersecurity threats" signify any circumstance or event with the potential of adversely impacting organisational operations, organisational assets, individuals, other organisations, or the public interest.

That could occur, for example, as a result of unauthorised access, destruction, disclosure, modification of information, and/or denial of service. A threat can be identified by correlating the vulnerability of a port with the motivations of malicious actors.

As such, to evaluate threats, we must begin by detailing the cybersecurity attributes an asset must have. The basic attributes in cybersecurity are confidentiality, availability, and integrity (known commonly as the CIA triad).

In the context of ports and craft, the notion of possession[5] has been added.

The table below serves to illustrate the four main attributes applied to the port ecosystem.

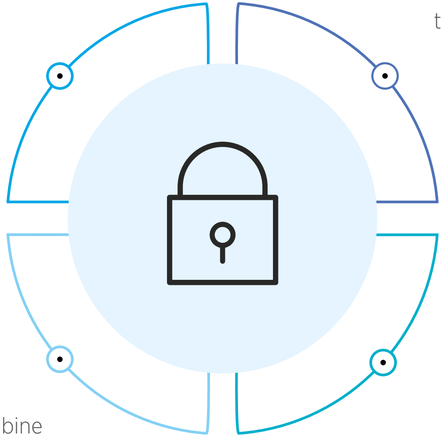
Cybersecurity attributes

Confidentiality

The data and information passing through the assets of the port are kept private as needed. Unauthorised users do not have the ability to access, download or transmit information.

Availability

The necessary information, applications, tools, or devices for the operation of port activities and craft activities are available. Their operation must be guaranteed at (predefined) times when they are required. Availability is also a measure of resilience, namely the time required to get a system or service back up and running after an incident (in nominal or degraded mode).



Possession

Operational control over port and craft assets is restricted to authorised personnel.
Keeping control over craft, machinery and other connected devices is a key attribute for ports and crafts. Obtaining unauthorised control of a system such as a craft or a key operational tool is a scenario every bit as worrisome as those described below.
Possession is different from integrity as it entails physical (rather than virtual) possession and control. Indeed, in comparison with other environments with only digital assets, ports combine IT with Operational Technology (OT) assets to provide a combination of physical and digital services. These physical services, if abused, can have significant impacts over financial and reputational ones and potentially result in human injury or death.

Integrity

The information, applications, tools, or devices for the operation of port activities and craft activities provide accurate, authentic information that has not been altered between sender and receiver. Integrity also includes the assurance of non-repudiation, namely the (unfalsifiable) proof that an item of information has indeed been produced or validated by a particular entity.

[5] The notion of possession has been added to take account of the good practice guide published by the Institution of Engineering and Technology, entitled "Cyber Security for Ports and Port Systems (2020)".

Potential threat actors

Cybersecurity threat actors can cause harm to digital systems or networks in intentional or non-intentional ways. This guide concentrates on potential threat actors broken down into seven categories:

Actor type	Action	Sample application in the context of inland navigation poorly trained or unsensitized employee
Malicious employee or one who is insufficiently trained, or unaware	Unaware (intentionally or otherwise) of cybersecurity good hygiene measures, this threat actor may nor may not have any malicious motivations. But be that as it may, his actions may endanger his organisation, whether deliberately or simply through negligence.	Clicking on an unsafe link sent in an email by an attacker, leading to the download of malicious files on port IT systems.
Criminal	Driven by financial gain, this actor engages in actions such as theft, smuggling of goods and people, evasion of taxes, criminal damage.	Intercepting communications to steal containers or smuggle them without paying duties, stealing cargo from a craft, sending ransomware to freeze port IT assets, and requesting payment.
Competitors	Driven by the desire to obtain business or market information, these actors aim to intercept information to gain an economic competitive advantage.	Obtaining classified information on port management processes to use for own business development.
Activist or "Hacktivist"	Motivated by civil disobedience, this actor uses the Internet to spread its idealism or create pressure on behalf of a specific cause.	Steering a craft to block a port entrance in protest. Tampering with river infrastructure works (bridge, lock etc.) to disorganise the system
Nation State	Working for a nation State or other sovereign government structure, these actors are driven by a desire to disrupt or stop activities as a form of warfare (declared or otherwise).	Executing a denial-of-service attack on port assets to block access to a river or body of water, such as a lock system.
Terrorist	Use of the Internet to instil fear or cause some type of physical or economic chaos.	Taking control of a craft to damage a port, inflict casualties. Intercepting information regarding the arrival of dangerous material to the port and using this material to spread a form of chaos.
Espionage	Exploitation of connected devices to obtain secret or sensitive data, for resale or informant purposes. Espionage can be conducted by other States or by competitors.	Other nation States obtaining information on sensitive cargo material transiting via a port (for example vaccines, medical equipment). Spying on port operations to obtain competitor information.

Certain examples in the table above, such as the terrorist threat, are external threats beyond the scope of this guide inasmuch as ports cannot take effective measures, at their level, to mitigate these risks. However, these threats need to be taken into account when coordinating cybersecurity between ports and other inland navigation actors.

It is important to note that the actors above can vary in terms of their motivations but also in terms of their resources and determination. Actors with ties to States performing warfare and espionage campaigns may have deep resources to draw from. Indeed, State-sponsored hacking is on the rise, as noted in a recent study by ENISA, which provides an overview of IT espionage trends[6]. In this 2020 study, it is noted that around 38% of malicious actors are connected to nation States and 11.2% of cyber-incidents were motivated by cyber-espionage.

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

This study highlights the risks facing raw materials transport hubs. Even if inland navigation ports are not expressly mentioned, they fit this description and are often vital to a country's activities. In this context, the study highlights that State-sponsored attacks are increasing, particularly in the utilities, natural gas, oil, and manufacturing sectors. This type of State-sponsored threat should not be underestimated as they are well-funded, have highly qualified personnel, whose campaigns are relentless, and whose objectives are highly damaging.

Threat taxonomy

Taking into account the attributes and the threat actors above, various threat scenarios can be defined. Based on these scenarios, the port threat taxonomy can be produced, or the list of threats to which an inland port may prove vulnerable, depending on its own characteristics.

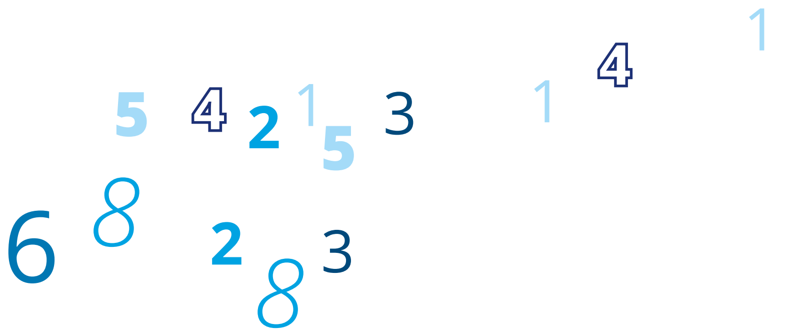
A threat taxonomy provides a scan of types of cybersecurity events that could lead to potential impacts. The following threat types have been identified through a survey of existing literature on threats to ships and maritime ports. It has been modified to apply to the port ecosystem.

Description applicable to ports	Example
Failures, malfunctions Systems or devices necessary for port operations are compromised and cannot operate to necessary extent.	▶ The bridge or lock operation system is compromised by a denial-of-service attack, freezing operations and leading to the interruption of bridge or lock operations.
Physical attacks A cyber-attack is combined with an operational technology (OT) system, leading to the physical takeover of a machine for fraud, sabotage, vandalism, theft, terrorism, hacktivism, or unauthorised access.	▶ A craft machinery system is taken over by activating an advanced threat attack. The craft is then driven into a port for terrorist purposes.
Eavesdropping, interception, hijacking Malicious actions on the network lead to the interception of sensitive data or network traffic or the hijacking of a user session.	▶ Data stored in the application for container management with information about containers with dangerous goods is intercepted by terrorists for the interception of these goods.
Information spoofing or jamming Disguise of a communication or data source (sender of an SMS, GPS position) to make it seem as if it originates from a known, trusted information source when it is in fact information that has been modified or created by the attacker.	▶ GPS information is spoofed to give wrong location leading to a threat to navigation.
Disaster Environmental or natural disaster is caused to the port ecosystem from the exploitation of vulnerabilities in connected port assets.	▶ A hacker tampers with container management application data, leading to mishandling of dangerous containers. This, in turn, can lead to a port fire, causing serious physical damage to the port assets.
Outages Supplies of resources to ports necessary to conduct operations are interrupted. Resources can include network, personnel, fuel, water and electricity.	▶ A widespread attack on a connected power grid leads to a major power outage and the freeze of port operations, delaying the transport of goods.
Unintentional damage Damage to port data, systems or physical infrastructure is caused due to accidental manipulations of an insider.	▶ An employee downloads a file with ransomware, freezing the entirety of the port's IT systems. A ransom demand is displayed on the locked screen.

Potential impacts

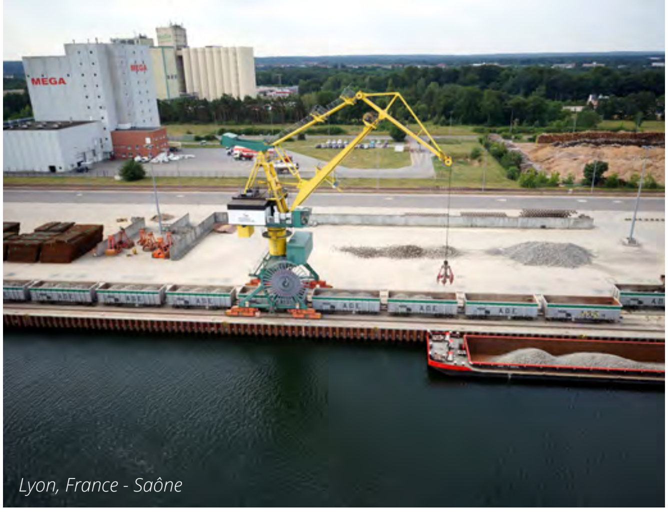
Threats are considered worrisome because if exploited, they have the capacity to inflict real damage on an organisation. The cybersecurity attributes described above, if violated, may have very different impacts on the port or port business affiliates. The following is a list of the type of impacts possible through the exploitation of vulnerabilities by cybersecurity threats.

Type of impact	Detail
Reputational impact	A cyber-breach or incident can cause lasting reputational damage to the organisation, its name and brand. Reputational damages are hard to calculate, as they are often intangible, but have multiple secondary effects such as costs to recuperate past customer trust, increased regulatory scrutiny, and foregone business.
Financial loss	Costs incurred to the organisation following a cyber-incident can be multiple, including disaster recovery and crisis management costs, lawyers' fees, insurance premium increases, merchandise loss and costs from the delay of port services.
Regulatory sanctions	A cyber-incident can result in regulatory sanctions such as fines and increased accountability measures for the organisation in question.
Destruction of property	An attack on port IT systems can cause destruction of digital property such as data and information if not properly backed up. It may also result in the destruction of physical property such as IT hardware, SCADA systems and – because of an attack – port craft, operations assets, containers and container contents.
Human loss or injury	In the event of a terrorist inspired cyber event, people may be injured or even killed. Flooding may be caused by a lock malfunctioning. Dangerous substances may cause an explosion.
Criminal activities: fraud, illegal trafficking	Criminals may use cyber-attack techniques such as network interception to obtain information and perform illegal activities such as trafficking of unauthorised substances in containers, or smuggling humans.
Theft of property	Criminals may use cyber-attack techniques with the objective of stealing items in the port: containers, their contents, goods, or assets (machinery, vehicles, spare parts…).
Environmental disaster	A cyber-event could cause the mismanagement of dangerous materials or fuel, which could result in an environmental disaster affecting inland waterways.



Sample port attack scenarios

This guide will explore three sample attack scenarios selected from the threat scenarios mentioned above, involving different motivations and threat actors. The objective of this survey is to provide tangible examples of the kinds of ways assets described above can be threatened. Each attack scenario has been selected from a real attack example from recent years, applicable to the port ecosystem.



Lyon, France - Saône

Wijk bij Duurstede, Netherlands - Amsterdam-Rhine Canal

Scenario 1

Infiltration of control systems to operate machinery

In 2013, two hackers infiltrated the control systems of a small dam in New York State[7]. The dam, used to guard against the effects of a storm, was controlled by a SCADA system connected directly to the Internet via a cellular modem. The system used this Internet link to provide status and operational data (water levels, etc.). That allowed remote operators to control the sluice gate systems, which in turn enable the management of water levels and flow rates. The hackers failed to operate the gates, which fortunately happened to be disconnected from the system for maintenance. This attack scenario aiming to disrupt or commandeer critical port operations such as lock machinery, illustrates a typical scenario relevant for ports. Such an attack could have significant repercussions in terms of safe navigation and have a significant business impact.

This attack scenario could be duplicated and applied to target port facilities, such as port power grids, water treatment plants, the operation of locks, etc.

[7] https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

The main steps of a malware infection on industrial systems, such as the one potentially executed described above and in other Industrial Control Systems (ICS) attack scenarios, are detailed below:

Step 1 - Infiltration

A malicious actor succeeds in infecting connected plant systems. An external device such as a USB stick, a clickable link, downloadable file, or simply through an external Internet page may enable him to achieve his aims. In the case of the USB stick, it is inserted in a computer with the executable code capable of spreading through computer networks.

Step 2 - Spying

The malware embeds itself in the plant's systems, spying on network communications to identify paths for duplication and expansion.

Step 3 - Sabotage of security processes

The malware identifies software with vulnerabilities or backdoors to be exploited to prevent the trigger of potential intrusion or threat detection mechanisms. It remains untraceable by using attacks that gradually affect operating systems and in the case of a port power grid, programmable industrial logic controllers (PLCs) present in operational technology systems. The compromising of the PLCs potentially allows for the performance of industrial functions, such as sensors monitoring for water pressure, or even valves opening and closing.

Step 4 - Exert control

The malware hijacks the functions the PLC is supposed to perform, for example by manipulating the input data or its internal programming. In the case of a lock between two basins within a port, the PLC could actuate the command to open the gates based on incorrect data on the water level on either side, thus causing them to open dangerously. If the malicious code were to reverse the opening and closing function on one of the two gates, the outcome could be the simultaneous opening of the two lock gates.

Step 5 - Action

The hacker abuses the system to perform a certain action with the objective of achieving a certain goal. For example, in the case described above, instead of closing the lock's upstream gate, the downstream gate is opened when a large convoy is inside the lock, projecting it violently downstream, causing injuries or deaths among the crew and physical damage to the craft comprising the convoy, both upstream and downstream of the lock owing to the violent outflow of the water.

Step 6 - Replication

The malware replicates itself to target other systems or devices. In the example of the lock between two basins, the malware tries to detect and target other PLC systems in the vicinity.

Scenario 2

Compromising data to facilitate illicit drugs smuggling

In 2013, Belgian and Dutch authorities arrested a dozen suspects attempting to smuggle more than 1,000 kilos of cocaine and 1,000 kilos of heroin through containers by accessing the harbour company's computer systems[8]. Working with hackers, the criminals took control of container terminal computers to tag and track the containers containing their illicit drugs. Their approach, highly applicable in a port context, was as follows:

Nomur, Belgium - Meuse

Step 1 - Intrusion

The criminal sends emails to container terminal employees with malicious attachments containing downloadable software, allowing the criminal to install spyware on the employees' computers

Step 2 - Control

Criminals obtain control over infected computers and can thus access container management systems and/or databases.

Step 3 - Monitor

The containers containing illicit drugs to be smuggled are identified in the system and tagged to track movement. Criminals acquire knowledge of the whereabouts of their shipments and of any upcoming controls (scans, x-rays, inspections, etc.)

Step 4 - Retrieval

The criminals use their access to the container management systems to pick a container location and drop-off time. They access the container before the port staff do so and are thus able to retrieve their illicit drug shipments.

The key takeaway from this approach is that control over container system applications began with the unknowing error of an employee. All studies agree that social engineering, and the "human factor" in general, is the principal cybersecurity risk factor, and that this factor is generally underestimated. Figures differ, but the human factor is said to be the key factor in at least half of all cases.

This case study demonstrates how, by downloading a malicious file, employees put their organisation and employer at risk, enabling the success of a criminal operation. Only regular staff training and awareness raising can help gradually reduce this human factor within an organisation.

[8] https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf

Scenario 3

Jamming of AIS equipment

Inland AIS equipment is used to transmit the location of a craft to other nearby craft using VHF. Static antennas located along the waterways capture these transmissions and pass them to traffic centres ashore, which use them to build a picture of the traffic and the location of each craft. As these VHF transmissions are unencrypted and require no authentication, they are quite vulnerable to cyber-threats.

In 2017, at least 20 ships in the Black Sea reported that their AIS equipment showed their position at a location 30 kilometres inland[9]. Given that the AIS transceiver plays an important role in safe navigation, this cyber-incident (based on a technique known as “spoofing”) directly impacts the safety of the craft and of its crew. Motivations could be multiple, ranging from terrorism to hacktivism or criminal activity. Attack steps for spoofing would be as follows:

Budapest, Hungary - Danube

Step 1 - Reconnaissance

Craft whose AIS equipment is turned on are connected to a company by antenna or remote connection for the transmission of geo-localisation. This localisation and positioning detail can be accessed by intercepting this connection or transmission information.

Step 2 - Interception

A malicious actor could capture AIS signals on land, by tracking the location of the craft using information available on the Internet. The malicious actor could then transmit radio signals with craft positioning to confuse receivers or simply jam/block the signal.

Step 3 - Action

The actor could jam radio signals with multiple action plans such as sending the wrong location to the AIS equipment and causing the false representation of the craft’s position, or preventing the ship from sending accurate positioning. This is a risk to navigation.

This threat scenario is particularly relevant for ports as port employees rely on the position transmitted by the AIS equipment to facilitate and manage port area navigation. Port authorities also use AIS equipment to transmit specific messages. Compromising the reliability of these systems could have serious impacts beyond financial and reputational implications, cutting across to safety and risk of human casualties.

[9] https://www.ship-technology.com/features/ship-navigation-risks/

Case study
Social engineering campaigns

As we have seen from the examples above, at any given time very different attack scenarios can exploit the human factor. Cyber-criminals know this and almost systematically exploit this vulnerability to achieve their goals.

Cyber-criminals and malicious actors looking to achieve a cyber-intrusion often rely on social engineering techniques to obtain information and execute the initial phases of their attacks. Broadly speaking, social engineering is the process of attempting to trick someone into revealing information through engineered interactions. In these interactions, malicious actors often use psychological tricks to create deception. Sometimes, social engineering can be real and not only virtual. For example, an individual may attempt to gain access to a physical site using processes involving deceit (dishonesty...). The objective of a social engineering campaign may be to dupe a victim into clicking a malicious link, providing confidential information such as PINs, passwords or privileged data.

One of the main types of social engineering attacks is **phishing**, a process consisting in sending a message (email, telephone, SMS...) containing a trap to a (very) large number of people in the hope that at least one of them will be hoodwinked. When the trap works, the attacker expects to benefit financially or else to obtain certain items of personal or confidential information he will subsequently be able to use for measures purposes. We also talk about spear phishing when the target population is smaller (occasionally a single individual), but typically with a more elaborate, personalised and thus convincing trap.

In this case study, we will dig deeper into five common phishing campaigns based on social engineering: link manipulation, smishing, vishing, website forgery and pop-ups.

Link manipulation is a process where a malicious actor directs a user to click a link to a fake website. It may entail an email, a text message, a publication on social media or another type of sharing platform. This website in question will resemble a known or trusted source but in fact will have been manipulated to serve the needs of a malicious actor.

Smishing is a form of phishing where someone tries to trick a victim into giving their private information via a text message. The most common form of smishing is a text with a link that automatically downloads malware. An installed piece of malware can steal personal data such as banking credentials, tracking locations, or telephone numbers from contact lists to spread the virus in the hope of multiplying exponentially. Another smishing tactic is to pose as a legitimate and well-known institution to solicit personal information from victims.

Vishing is a voice scam, or a type of phishing relying on a phone call or human interaction to trick victims into sharing information such personal or private information, passwords or other personal data. Callers may pose as someone from an official organisation such as a bank or government authority or else from the company's (or head office's) IT or HR department, or even from a line manager, to gain the victim's trust and obtain the desired information.

Website forgery works by making a malicious website impersonate an authentic one, to make the visitors give up their sensitive information such as account details, passwords, credit card numbers.

Pop-up messages are an intrusive way of phishing for information by directly sending a pop-up to a victim's device prompting for the input of information. Often, as the pop-up appears on their device, the victim may be easily tricked into providing information that is then received by malicious actors.

Social engineering techniques as described above often exhibit the following characteristics:

1. misleading information: URLs often look slightly different and emails/SMS communications can have spelling mistakes, as they are usually drafted by non-professionals, or by foreigners using automatic translation services;
2. use of urgent language: actors rely on fear and panic to trick victims into providing information they normally would not divulge;
3. promises of attractive rewards: incentives such as the promise of cash prizes or other gifts are used to entice interactions with victims;
4. requests for confidential information: asking personal information, which is rarely done by official organisations, is the basis of many phishing requests;
5. suspicious attachments: in the case of link manipulation or pop-ups, criminals may ask victims to download malicious files onto their devices.

If you receive a phishing email or a message that appears to be suspicious, the best actions to take are as follows:

1. do not click on any links or download any files in the email;
2. mark the message as spam or as undesirable;
3. if applicable, send a copy of the email or a screenshot of the address to your organisation's IT security representative to inform him/her of the situation and potentially prevent any further actions.

In the context of cyber-threats to the port environment, it is important to understand that most cyber-threats depend on the human factor at some point in the process. This is why social engineering techniques, and especially the phishing campaigns described above are very widely used and must be taken very seriously. And sometimes all it takes is just one employee to compromise the entire organisation.

The positive conclusion from this case study is that making the port's employees, management, suppliers and other stakeholders more aware is "all it takes" to very effectively counter many cyber-threats. It is a simple, inexpensive and very effective matter regularly to inform all these people of the existence of social engineering stratagems and to encourage them to help maintain security by remaining vigilant and engaged.

Part 2

Mitigating cybersecurity risks for ports

Vienna, Austria - Danube

Overview of legislation and policies relevant to the port context

At present, there are no common, mandatory approaches for the mitigation of cybersecurity risks specifically directed towards ports. This can be attributed to the multitude of regulators involved in the inland navigation port sector. In addition, the bulk of the existing regulation is applicable to maritime ports but does not specifically treat the case of inland navigation ports. It is in this context that this guide seeks to provide a framework for cybersecurity risk mitigation measures, filling in gaps in the current fragmented literature and regulatory environment.

This being said, it is worth mentioning – for the sake of European Union member States – that the EU provides a legal framework also known as the NIS Directive to boost the overall level of cybersecurity in the EU (Directive 2016/1148 of the European Parliament and of the Council). This Directive entered into force in August 2016 and makes specific provisions for individual actors identified as being "operators of essential services" . . Inland water transport operators are mentioned in the Directive, even if it is each State's responsibility to identify its essential service operators. It is recommended that readers of this guide who belong to an EU member State, and who are looking for additional compliance information, should familiarise themselves with the sections of the NIS Directive applicable to operators of essential services, especially if the inland navigation ports under examination may be deemed an essential service by their State.

In addition, there is a range of national authorities that publish approaches to mitigating cybersecurity risks for inland navigation actors. It is recommended that readers, in addition to this guide, familiarise themselves with the technical regulations and compliance measures applicable in their State.

Organisation of mitigation measures in this guide

For the purposes of this guide, mitigation measures to curb the potential cybersecurity risks described above have been organised into three sections:

1. **Organisation Policies and Procedures (OPP, Organisation Policies and Procedures)**
   This section groups together recommendations directed at organisational structure, roles and responsibilities, governance measures as well as organisation policies that can be implemented to boost the cyber-maturity of a port.
2. **Information Technology/Operational Technology Policies for Ports**
   This section discusses the policies that can be implemented to secure the assets identified in Part 1.
3. **Technical Security Measures for Ports (TSM, Technical Security Measures)**
   This section is meant to provide a general overview of basic security measures that can be implemented by port IT personnel to secure the IT infrastructure.

Each of these sections is intended to provide a general overview of mitigation measures to be considered by a port but they are not meant to replace the cybersecurity requirements that are requested in the context of an audit, or a regulation issued by certification agencies, individual States, or other regulatory bodies.
The mitigation measures proposed have been organised in ascending order of cyber maturity level. The measures to be found at the beginning of each table below should be implemented first in any approach encompassing cybersecurity. Then, as these measures are implemented and cybersecurity maturity increases, the following measures can be implemented in their turn. A colour scheme has been used to identify the maturity level of each of these measures:

●	Maturity level: **low**
●●	Maturity level: **medium**
●●●	Maturity level: **high**

For more information on these classifications, please refer to the maturity evaluation framework in Part 3.

Meppel, Netherlands - Meppelerdiep

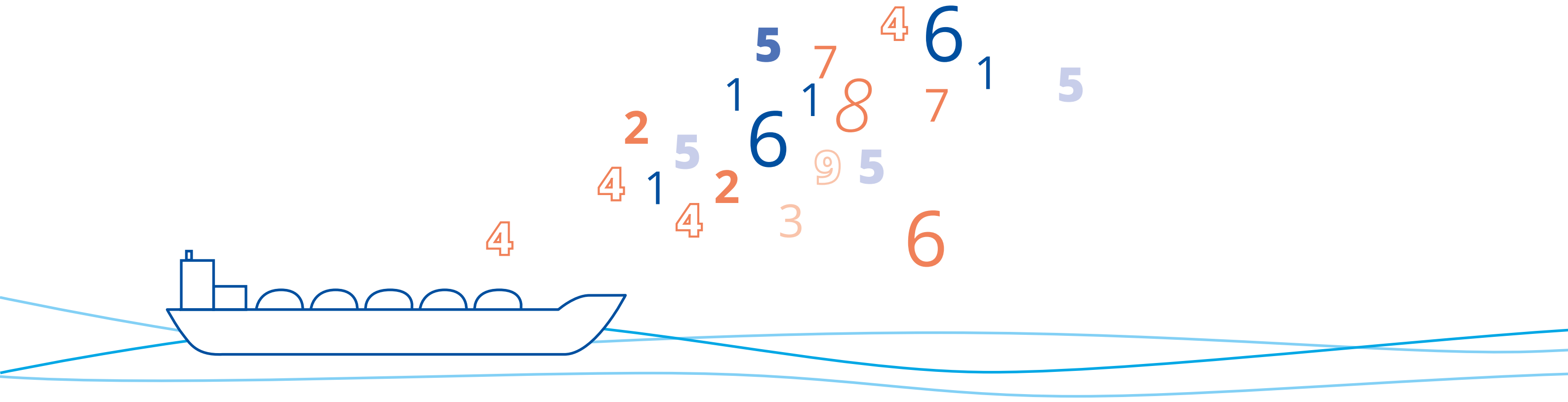
Organisational policies and procedures

This section provides an overview of organisational policies and procedures that can be implemented for a mature cybersecurity organisation. These actions can be implemented by the port's Chief Information Security Officer, or in the case of a smaller port or organisation, some other manager. These measures are generally applicable but can vary in size, depth, and scope depending on the different resources at the port's disposal.

Roles and responsibilities

Assigning clear roles and responsibilities is the first step in creating accountability to boost the cybersecurity maturity of an organisation. Ports should implement the following measures to cover this domain.

	Number	Measure
●	[OPP] 1.1	The management needs to incorporate cybersecurity aspects in its priorities and provide the wherewithal and adequate resources to implement appropriate measures, for example those proposed in this guide. The management must begin by identifying a focal point for all cybersecurity measures, and this person's contact information and role should be communicated widely to all employees and to subcontractors. The management must bear in mind that although it may delegate the implementation of cybersecurity, it cannot delegate its responsibility.
●●	[OPP] 1.2	An overarching cybersecurity charter with clear expectations from all employees should be drafted and signed by employees and port stakeholders.
●●●	[OPP] 1.3	A general cybersecurity strategy or information systems security policy should be defined and approved by the management.
●●●	[OPP] 1.4	The cybersecurity strategy should clearly define the roles of each port stakeholder (port authority, terminal operators, service providers, suppliers, etc.)
●●●	[OPP] 1.5	All security aspects of the partnerships with third parties should be defined and documented, especially for critical systems provided by third parties.
●●●	[OPP] 1.6	The cybersecurity strategy should be regularly reviewed and updated following risk assessments, organisational updates, or security incidents.



Organisational processes

Once the roles and responsibilities have been clarified, the second step is to document these processes and requirements to ensure service continuity, to comply with certain security regulations, and to ensure proper transfer of information in the event of services being reorganised in the port.

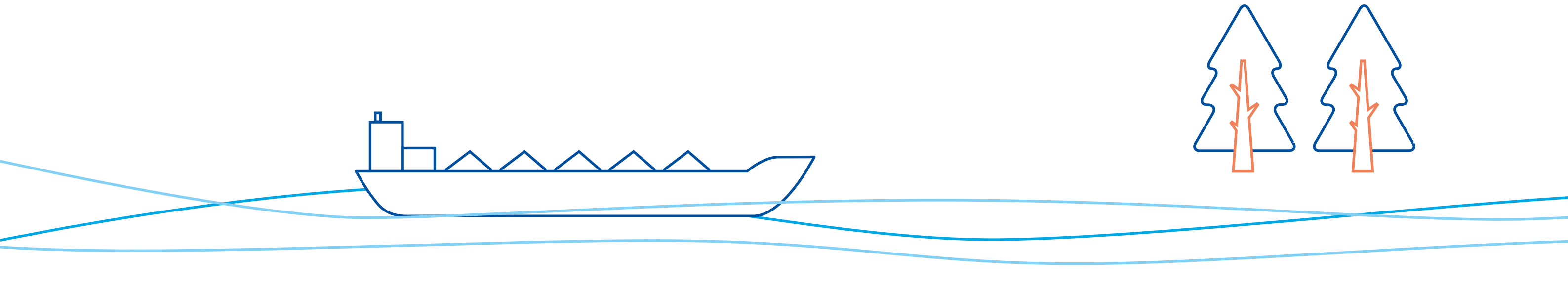
	Number	Measure
●	[OPP] 2.1	A complete assessment of the port should be performed to identify the central assets, ranked by criticality.
●	[OPP] 2.2	Basic cybersecurity requirements for relevant suppliers are to be documented, communicated to suppliers. Standard contractual cybersecurity clauses could for example be drafted then used in all contracts with suppliers. Compliance with these requirements should be monitored by competent port employees or by a trusted third-party whose exclusive role it is.
●	[OPP] 2.3	People in key leadership roles or significant IT roles (system administrators, IT/OT operators) should be subject to a background check before employment. Proof of this check should be retained on file if needed for regulator purposes.
●●	[OPP] 2.4	The dependencies and information flows of the assets identified above should also be documented.
●●	[OPP] 2.5	A corresponding risk assessment should be performed to identify the cybersecurity risks tied to each asset. The management should ensure that cybersecurity risk assessments are performed for each new project or initiative, especially those using new technologies.
●●●	[OPP] 2.6	Regular internal or external cybersecurity audits and compliance assessments on port assets should be conducted. The frequency and nature (internal/external) of these audits and compliance assessments is to be determined by the management. The port might consider automating certain technical audits, where possible. For ports that have developed specific software, it is possible for example to schedule a regular analysis of the source code with specialist tools to look for any known vulnerabilities or security flaws.
●●●	[OPP] 2.7	Cybersecurity processes defined and applied should be documented, validated, and regularly reviewed. The following topics are potential subjects for written policies (including, but not limited to): • cybersecurity measures in place to secure web portals and services; • cybersecurity measures for networking or communication links (including wireless communication technologies); • cybersecurity measures for software configuration; • requirements and rules regarding the connection of devices to the IT environment (including the connection of personal devices); • measures for software updates and change management tasks (once ITIL has been implemented); • rules regarding the use of personal mobile radios; • rules regarding adequate use of IT infrastructure by employees, in compliance with the general cybersecurity charter; • configuration and management of user and systems account privileges, including those of third party personnel with access to inland port systems (such as power, heating, electricity, etc.); • crisis management and cybersecurity incidents process.

Physical security

In the cybersecurity context, we talk about "physical security" when it is helpful or necessary physically to protect IT equipment. "Physical security" is often used in distinction to "logical security", which consists in protecting IT equipment in terms of access through software or the network. However, physical security is a dimension of cybersecurity in its own right because it may play a role in numerous attack scenarios. Mere access to an on/off button may be all it takes to put a server out of action just as access to a USB port enables malware to be introduced by bypassing network protection mechanisms. Physical security also includes fire security, or overvoltage protection, or power cuts.

Physical security requirements should be considered in the creation of a cybersecurity plan. Critical IT infrastructure can be vulnerable if left accessible to external individuals with potential malicious objectives. As such, cybersecurity plans should address risks stemming from physical security breaches.

	Number	Measure
●	[OPP] 3.1	The port management should define clear physical security rules and implement physical access control measures to prevent access to sensitive port systems and their exposure to the risk of theft and degradation. The list of these sensitive systems should be compiled and approved in advance by management.
●	[OPP] 3.2	In addition to protecting sensitive inland port systems, the port should protect utilities (including heating, ventilation, and cooling systems) from non-authorised individuals through physical access control barriers or locked doors.
●	[OPP] 3.3	All authorised accesses to the port should be logged and audited at least once a year.
●●	[OPP] 3.4	A procedure and corresponding availability of port personnel and external agencies for reaction and response in the event of a physical intrusion should be documented and communicated.
●●	[OPP] 3.5	The extent to which certain port areas are accessible to third parties or the public should be documented and evaluated to ensure acceptable risk is being taken.
●●	[OPP] 3.6	A physical access control policy should provide step-by-step procedures to critical security operations such as the collection of badges from departing employees, the update of alarm codes, the management of CCTV footage, etc.



Incident response and crisis management

Clear policies and procedures should be defined and implemented in the event of a **cybersecurity incident** or crisis. For the purposes of this guide, a distinction is made between cybersecurity incidents (situations that can be solved by IT/security personnel without escalation and consultation) and **cybersecurity crises** (situations of larger magnitude impeding on the functioning of the inland port and requiring the input of multiple managerial stakeholders).

	Number	Measure
●	[OPP] 4.1	The port should have an incident management plan, signed off by management, that is based upon an understanding of cybersecurity causes of disruption applicable to its environment, essential systems identified in the critical asset inventory, and the resources and capabilities available to it.
●●	[OPP] 4.2	The port should have a crisis management plan, signed off by management, containing detailed information on the decision-makers and the communication process to be followed in incidents, and should an incident escalate into a crisis.
●●	[OPP] 4.3	The crisis management plan should account for reporting and liaising with national authorities, if applicable.
●●	[OPP] 4.4	The crisis management plan should include a procedure for communicating with affected parties and victims of cyber-incidents, when necessary.
●●	[OPP] 4.5	The personnel in charge of managing incidents in the port should monitor industry news to keep abreast of potential cybersecurity incidents affecting their peers; and a threat intelligence process to gather relevant information on security threats facing inland ports should be defined.
●●	[OPP] 4.6	The incident management plan should provide a precise definition of what constitutes a cybersecurity incident, roles and responsibilities when dealing with an incident, and the process detailing when an incident escalates to a crisis.
●●●	[OPP] 4.7	A business continuity plan to ensure ongoing port operations in the event of a crisis or incident should be defined. This plan should have clear objectives. It includes important parameters for the port's business continuity, such as a recovery time objective (RTO), recovery point objective (RPO), maximum tolerableThese criteria are indicative outage (MTO), and minimum business continuity objective (MBCO).
●●●	[OPP] 4.8	The crisis management plan should include a post-incident analysis phase to determine the cause of the incident.
●●●	[OPP] 4.9	Processes defined to deal with incidents or crises should be regularly evaluated and tested, potentially through crisis simulations or tabletop exercises. These should be extended to as many stakeholders as possible to ensure preparedness along the supply chain.
●●●	[OPP] 4.10	Following significant (unusual or which had an operational impact) cybersecurity incidents, the management should ensure incidents are reported and shared so that the industry can learn from these.
●●●	[OPP] 4.11	The port should consider the set-up of a Cybersecurity Operations Centre (SOC) to support security and manage cyber-incidents.

Cybersecurity plans: Various cybersecurity-related documents are touched on in the above measures, which may be considered independently, but which ultimately constitute a coherent entity:

- Incident management plan
- Crisis management plan
- Business continuity plan

"Security policy" is another document (touched on in "Roles and responsibilities" measures at a high level of maturity, developed above), part of which is given over to explaining how these various plans are to be implemented, revised, and tested.

Training and awareness

Training and awareness activities pitched at all stakeholders are crucial in the dissemination of cybersecurity good practices. Indeed, as explained in the first part of this guide exploitation of the human factor by the cyber-criminal is essential, in practice, to most real-life attack scenarios. The following measures can help in diminishing the human factor risk by sensitising employees to the key role they play in ensuring cybersecurity.

	Number	Measure
●	[OPP] 5.1	Employees should be sensitised to the careful use of emails. The following points should be emphasised: • check the identity of the sender; • do not open attachments and do not click on Internet links arriving from suspect or unknown senders.
●	[OPP] 5.2	The port should define a password management policy. This policy must include an educational dimension to make personnel more aware of the need to use strong passwords. It must also specify the applicable rules for renewing passwords. This policy must differentiate between individual user passwords and passwords associated with system or administrator accounts that can be shared for operational reasons or which are used by programs.
●	[OPP] 5.3	Employees should be sensitised to the proper use of social networks, forums, forms, etc., especially when dealing with information about the port.
●	[OPP] 5.4	Employees should be sensitised to installation of programs and software. Requirements for the approval of port administrators when downloading software should be expressly communicated.
●	[OPP] 5.5	Employees should be sensitised to the use of Wi-Fi, 4G/5G and secure networks: when travelling on business, employees should exercise caution as regards public Wi-Fi networks.
●	[OPP] 5.6	An employee policy on separating personal and professional uses and on working on individuals' own devices (BYOD) should be established and communicated.
●	[OPP] 5.7	The port should define a periodic cybersecurity awareness programme for all employees addressing general basic cybersecurity hygiene.
●●●	[OPP] 5.8	The port should define a cybersecurity training programme to develop cybersecurity skills of IT staff and staff dealing with IT/OT assets.
●●●	[OPP] 5.9	All staff using connected machinery should be trained on basic IT/OT cybersecurity hygiene practices.

What is a "strong password"?

A strong password is one that is difficult for a human or computer to guess. But beware: humans program computers to try thousands of passwords a second. So what do you do? Most systems propose "complexity" rules for passwords (minimum number of characters, letters, numerals, special characters, etc.). It is a good beginning but not enough because it is possible to create a weak password that complies with these rules. For example, "P@ssw0rd". Good practice includes the fact that a password needs to be sufficiently long (at least 8 if not 10 characters) and not be based on a dictionary word, even remotely. Nor should it be related to the keyboard layout" ("qwerty", "azerty", "123456", etc.) nor directly to its user (birthday, children's first name, etc.). Current good practice tends to use "multi-factor" authentication, namely supplementing the password with another means of authentication (for example a One Time Passcode sent by SMS, email or a smart phone application). The password management policy referred to in rule [OPP] 5.2 will be required to specify the relevant rules and recommendations to be complied with.

Case study
Employee awareness programmes

This guide emphasises the role all employees, suppliers, and other stakeholders play in ensuring the cybersecurity of ports. As discussed in the attack scenarios mentioned in Part 1 of this guide, a significant portion of cybersecurity incidents stem from human error. As such, the implementation of an employee awareness programme is a central mitigation measure and a ”quick win” that can be adopted by port organisations to boost their cybersecurity posture. To facilitate this task, this case study provides an overview of the steps involved in launching a cybersecurity awareness programme, details the types of modules that can be included in these programmes, and provides some key success drivers to its execution.

Overview of steps

Step 1

Define a baseline benchmark for the current level of cybersecurity awareness in the port. The assessment of the current maturity level in the port will allow leadership to understand where the awareness programme should begin, identify particular points of focus to be addressed by the programme, and will provide a clear maturity level from which to track progress following awareness sessions. This could be done through a questionnaire or other informal survey method sent to port employees.

Step 2

Draft a cybersecurity awareness strategy for the port. This strategy should include tangible goals, a realistic timeline, a distribution of the roles and responsibilities, and a budget to match. To ensure the effective rollout of a programme, buy-in from management should be obtained with the presentation of this strategy.

Step 3

Select the format of awareness modules to be implemented. An awareness campaign can range from a mandatory course to webinars, training exercises, phishing exercises, etc. The specific awareness module should be selected to meet the criteria defined in the strategy, particularly with regard to the budget and timeline available to the port. Awareness programmes can also be designed in collaboration with external experts if the skills to produce such an initiative are not available to the organisation. They can also be relevant to the private use of IT at home for employees.

Step 4

Roll out the awareness programme.

Step 5

Document results to satisfy regulatory requirements and for the port’s development needs, feedback following the awareness programme should be collected from the individuals involved. A summary of the awareness objectives addressed and met through this programme should be documented and saved. In addition, organisations should ensure continuous improvement by noting the good results and potential improvements of the awareness programme.

Step 6

Plan for a next iteration. Awareness programmes, to be efficient, should be updated and re-delivered as the port evolves. A target date for this second phase should be aimed for, agreed with the management.

Types of modules that can be included in awareness programmes

Awareness programmes and initiatives can take many forms and can be adapted according to the needs of the port. Below, the main types of awareness programme modules have been detailed.

Awareness module type	Short description	Key advantage(s)	Key disadvantage(s)
In-person or virtual courses	Awareness courses are delivered in the format of a real-time session with an instructor and course format.	• A dedicated instructor to ensure understanding and answer questions. • Presence and attention to material can be monitored.	• Time and resource intensive, requiring dedication during working hours. • Costly solution.
E-learnings	Courses are automatically delivered via an online platform, usually in video format.	• Awareness courses online today are widely available, some even for free. • Stakeholders can complete e-learnings.	• Difficult to monitor participant presence and attention.
Serious games	Stakeholders ”play” an online or mobile game designed to boost cybersecurity awareness and have a debrief on key takeaways and lessons learned.	• Fun and different ways of conveying information may capture attention and remain a memorable experience to stakeholders. • Delivery of this training requires less time and implication of those receiving the awareness training.	• Requires detailed planning to select a serious game, configure it to meet organisation needs and to deliver the awareness programme. • Attention and ”game” completion is difficult to ensure.
Phishing exercises	Simulation exercise where a phishing email is sent to port employees; those falling for the phishing exercise will be traced and are usually re-directed to a training module.	• Tangible experience that stays in the mind of those who fail the exam. • Documentation and statistics on the types of stakeholders who fall for the phishing email.	• Only covers one aspect of cybersecurity: phishing. • Does not ensure a boost in awareness to those who pass the test, and no guarantee that a ”pass” means they simply missed the email.
Malware campaign simulation	Customisation of malware awareness campaigns to evaluate the level of awareness of employees regarding external devices and connections. These campaigns have the same characteristics as the phishing campaigns but distribute malware. Malware scripts are not persistent. The scripts will only capture the victim and system’s real-time data.	• Tangible experience that stays in the mind of those who participate. • ”Fire drill” effect, providing a crisis simulation exercise to improve organisation performance in the event of a real crisis.	• Time and labour intensive to plan and execute this simulation. May require the help of an external firm. • Potential trust issues created with employees who fall victim to this test.
Informative material	Monthly content with narrated examples of real attacks in organisations, the security problems encountered, the impact of these attacks, solutions applied, and lessons learned. Can also include trending security topics for the industry.	• Relatively simple conception and distribution: a simple email will suffice. • Recurring information blasts allowing stakeholders to stay up to date.	• Difficult to monitor success of these information blasts: some stakeholders may simply ignore/bypass communication.
Events	Specific event (breakfast, lunch and learn, etc.) organised to provide a discussion or demo on a cybersecurity awareness topic.	• Groups organisation stakeholders in one session and allows for the exchange of information and discussion. • Relatively simple conception and execution.	• Short-lived interaction. • More difficult to track the lessons learned and the boost in awareness from one event.

Key success drivers of an awareness programme

1. **Alignment of awareness programme with operational issues and challenges**
   Making an awareness programme tailored to the operational issues faced by the port will ensure it has greater impact and is therefore more successful. An awareness programme should specifically focus on the critical systems of ports and on potential impacts of cybersecurity events.

2. **Involve as many stakeholders as possible**
   Consisting of the maximum number of stakeholders, including third parties and suppliers, will ensure knowledge and awareness are disseminated down the supply chain. This notion is particularly important for ports as a significant number of third parties are involved in port activities.

3. **Measure of impact and progress**
   The best way to evaluate the effectiveness of an awareness campaign is to provide some sort of knowledge check or evaluation at the end of the module. This can be a short survey or quiz distributed to participants.

Koblenz, Germany - Rhine

Case study
Building a cybersecurity risk assessment

To implement most of the mitigation measures described above, such as implementing a cybersecurity strategy requires identification of the assets to be protected. To identify these assets, ports will be required at some point to conduct a cybersecurity risk assessment. This exercise will generate the building blocks for a robust cybersecurity strategy. Indeed, current good practice emphasises needs-driven approaches, an understanding of critical processes, and the identification of critical assets, rather than previous compliance-driven approaches. The case study below will provide the generic steps to conduct a thorough cybersecurity risk assessment for a port and will highlight some key success drivers in executing the assessment.

Overview of steps

Step 1

Identify port assets and potential cybersecurity event impacts on these assets.

- Identify the port's main operations and the assets that are required to perform these operations. Be sure to include a range of assets, such as control systems, craft technical management systems, control rooms, CCTV/alarm tools, navigation systems communicating with craft, cabling routes, port systems used for the planning and receipt of cargo, and data collected and stored by ports.
- Define a criticality criterion for assets: which operations are the most critical? On what assets does the implementation of these operations depend? Are any of these assets common between operational processes, and thus central to port operations?
- For the port assets, document the systems that support them. Note if these systems are connected to the Internet or if they depend on a particular energy source.
- For a selection of the assets, define potential business impacts in the event of the integrity or availability of these assets being compromised.
- **Key end product:** A list of all port assets. For each, a major business impact if this asset/device were compromised. This final product should of course be protected and remain strictly confidential, given its sensitivity.

Step 2

Detail port business processes

- Map out the business processes and the assets these processes rely on to operate.
- Document the information flows and data exchanges that are necessary to carry out these processes. This will provide a view on the types of interactions essential to conducting operations that could result in serious business impacts if interrupted.
- **Key end product:** A diagram of data and information flows for the top three activities carried out by the port. This final product should also be protected and remain strictly confidential.

Step 3

Identify security threats

- Identify the possible threats to the assets identified in step 1. Threats can be gathered through existing research on cybersecurity threats pertinent to the port environment (as those described above) or can be created through a more comprehensive threat research activity. This operation does not have to be highly sophisticated: a standard threat list can be defined, and these threats can be associated with port assets to generate a complete list of pertinent threats to the port.
- **Key end product:** A threat intelligence report on major threats facing the port.

Step 4

Evaluate the feasibility and likelihood of the exploitation of these threats

- Assign a feasibility estimation of each threat. This estimation can be generated by evaluating metrics such as prior knowledge of the systems required to generate this threat, need for physical access or the level of privilege needed to execute specific operations, level of user interaction needed to obtain privileges, the technical complexity of the operation required and the port's ability to overcome this threat by means of resilient operation modes (possibly in degraded mode).
- Assign an attacker profile to each threat to provide a reality check on the realisation of the threat. Attacker profiles can be generated by evaluating the level of skill required by the attacker to exploit the threat, the motivation/reward of exploiting the threat, the amount of resources required, and the awareness/information required.
- Cross attacker profile with feasibility information to generate a likelihood score for the exploitation of each threat.
- **Key end product:** A list of major threats with an associated feasibility and likelihood score.

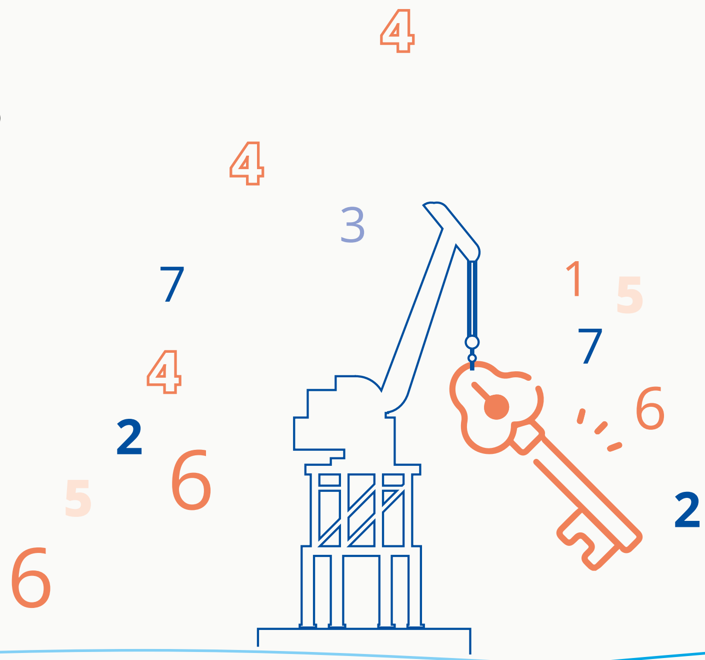
Step 5

Correlate likelihood and impact on asset for the threats

- Using a table, correlate the business impact attacking an asset can have on the port with the likelihood such a threat will be exploited. This allows the isolation of critical risks (those with high impacts and high likelihood).
- The risk assessment operation is now complete, and the management should be equipped with a clear picture of the main cybersecurity risks facing the port today. These risks can be used to prioritise security measures or generate a full-scale organisational cybersecurity strategy.
- **Key end product:** two-dimensional table (feasibility/likelihood) with the threats positioned in the table, with the ability in a subsequent step to plan the necessary measures.

Key success drivers of a risk assessment

- **Business relevance of threats**
  Threats examined in the assessment should be in line with the business context of the port. More precisely, to generate a relevant threat assessment, ports should focus on the threats facing their sector today, perhaps by relying on specialised sector threat intelligence reports, on sharing information with peers, or by participating in cybersecurity working groups of their industry.
- **Independent and objective insight on potential impacts**
  When performing a self-assessment, a challenge is to put aside one's convictions about one's capacities and organisations to make objective judgements on the potential impacts a cyber-attack could have. It is essential to recall that impact analyses aim to deduce in a reasoned and factual way the potential impact a cyber-incident could have on an asset, and not to conduct an opinion poll on its presumed impact. Indeed, taking measures to mitigate a presumed impact could result in very onerous and expensive, yet futile, work being carried out, this work being based on unfounded or ill-judged assumptions.



Information technology (IT)/ Operational technology (OT) policies for ports

This section, applicable to ports and to their suppliers, aims to provide general best practices for the security of IT/OT systems. As a reminder, the term IT/OT is defined in the "Introduction" section of this guide. In simple terms, IT refers to systems to do with data processing whereas OT refers to systems the purpose of which is to interact with physical objects. These two types of system can of course be used interactively, and this is especially so when one talks about "IT/OT systems".

This section is therefore directed at the port stakeholders working with operational systems and the equipment to be found in ports. IT/OT systems can vary from one port to another but are generally considered as systems performing operational or physical tasks, operated through a computer, or connected gateway. In the context of ports, these can include but are not limited to:

- port traffic control systems (traffic monitoring, berth management, weather monitoring tools);
- navigation devices communicating with port networks (AIS, GNSS);
- terminal operations management systems: operational machinery, transshipment and warehouse systems, terminal operating systems;
- security and safety systems: access control, intrusion detectors, surveillance systems and other alert systems.

IT/OT systems are particularly relevant in the cybersecurity of a port as they are becoming increasingly connected, especially through the ever-wider adoption of Internet of Things (IoT) devices. IT/OT systems are particularly vulnerable as they have often been designed without the cybersecurity configurations considered in contemporary IT software. Moreover, they often operate on legacy systems with little to no update capabilities and it is the case that they are left out of cybersecurity projects and maintenance plans.

IT/OT general responsibilities

In addition to defining general roles and responsibilities described in the chapter above, the management sensitive should assign responsibilities, particularly pertaining to IT/OT systems. Indeed, the group working with these systems may be entirely different from those working in the management of port operations and IT systems. As such, it is important to remember that those operating machinery and systems critical to port operations have an important role to play in cybersecurity. These operational systems should be included in port cybersecurity risk analyses.

	Number	Measure
●●	[ITOT] 1.1	An asset inventory of all IT/OT assets used in port operations should be conducted. This asset inventory should then be ranked by criticality of the system.
●●	[ITOT] 1.2	Cybersecurity responsibilities should be clearly defined and documented for each of the stakeholders working with the assets inventoried above, regardless of the aspect concerned (e.g. development, integration, operation, maintenance).
●●●	[ITOT] 1.3	Cybersecurity risk analyses should be conducted before implementing a new IoT device or system.
●●●	[ITOT] 1.4	The most critical IT/OT assets should be subject to a cybersecurity risk analysis.

Identity and access management (IAM)

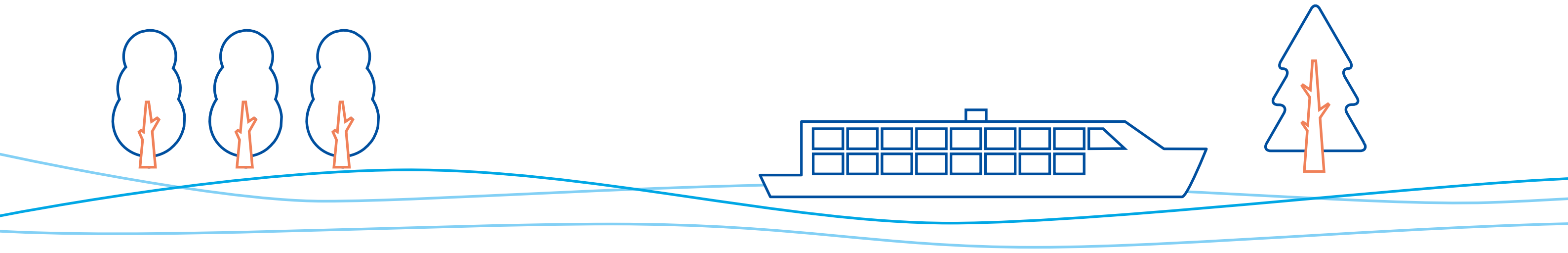
Ports should have clearly defined policies on the access and use of industrial systems, connected machinery, and other operational systems used to conduct port operations. The following measures can be taken to manage identities and access.

	Number	Measure
●	[ITOT] 2.1	Machines and systems should, if possible, be accessed only using a username and password. Passwords should be robust.
●	[ITOT] 2.2	Default passwords on operational systems should be changed and a procedure should be implemented to change these passwords regularly, in accordance with a policy defined by the organisation.
●	[ITOT] 2.3	When authentication cannot be applied (in particular, due to operational constraints), additional measures should be considered, including the use of physical access control, limiting the functionalities available on the system, implementing authentication with a badge, etc.
●●	[ITOT] 2.4	Ports should document which stakeholders have access to which critical systems. This list should be updated frequently.
●●	[ITOT] 2.5	A time-out delay should be implemented rather than a lockout in case of authentication failure.
●●	[ITOT] 2.6	Particularly sensitive systems should be subject to multi-factor authentication (for example using a PIN code and smart card).

Physical security

As operational systems, industrial systems and other machinery are usually directly physically accessible (unlike other assets such as data, IT components, software, IT applications, etc.), physical security measures tailored and applicable to these systems should be defined and implemented. In particular, the physical security measures described below are some best practices to physically protect assets from cybersecurity risks.

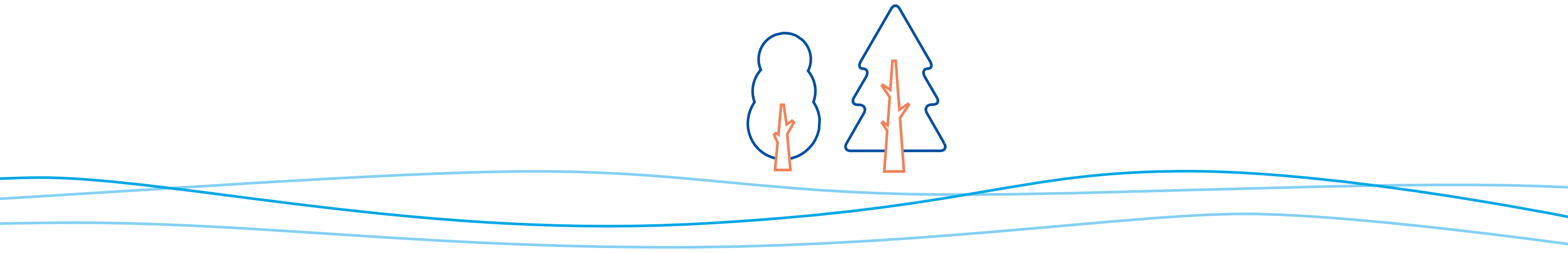
	Number	Measure
●	[ITOT] 3.1	Access points for Industrial Control Systems and other operational devices should not be accessible to unauthorised persons. This restriction applies especially to ports with heavy pedestrian or tourist traffic.
●	[ITOT] 3.2	Workstation central units, industrial network devices and Programmable Logic Controllers (PLCs) should be placed in locked cabinets or in locked rooms.
●	[ITOT] 3.3	IT and OT systems hosted in the port should be protected following established best practices for safety (fire detection, air-conditioning, etc.) and security (access control, CCTV, etc.).



Maintenance and operation of IT/OT systems

As mentioned above, IT/OT systems are often left vulnerable to cyber-attacks as they often run on legacy systems and are excluded from traditional cybersecurity efforts such as system updates and patching. IT/OT systems are also subject to routine maintenance. A best practice as regards cybersecurity is to incorporate some basic security principles to the maintenance processes of IT/OT systems. Security should also be considered in the decommissioning and disposal of IT/OT systems.

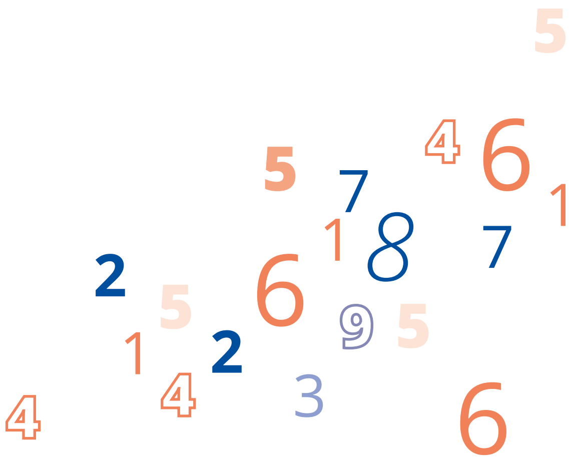
	Number	Measure
●●	[ITOT] 4.1	A procedure should be defined for the update and maintenance of operational systems. This procedure should include the frequency of updates and the roles and responsibilities of individuals tasked with performing these updates. System updates should be detailed in supplier maintenance contracts.
●●	[ITOT] 4.2	Tools or procedures should be in place to check the differences between the current version and the version to be installed in the context of system update operations.
●●	[ITOT] 4.3	All maintenance operations should be validated. A validation procedure should be defined and communicated to personnel working with operational systems.
●●	[ITOT] 4.4	A procedure for the decommissioning of operational systems should be implemented. This procedure should document the date of decommissioning, parties involved in the decommissioning and details on the proper disposal of the equipment.
●●●	[ITOT] 4.5	Interventions and update operations should include documentation of the following: • the person performing the work and the ordering party; • the date and time of the intervention; • the perimeter on which the work is performed; • the activities carried out; • the list of devices removed or replaced (including, where applicable, the ID numbers); • the modifications made and their impact.
●●●	[ITOT] 4.6	A regular audit plan (frequency to be determined by the port) to evaluate whether the update procedure is being correctly complied with. Following audits, a follow-up should be performed on audit recommendations.



Technical security measures for IT/OT systems

These technical security measures should be considered by port staff tasked with the configuration of networks, the set-up and configuration of operational systems, and the general technical maintenance of these systems. As a rule, care should be taken to isolate critical systems from the generally available networks and from the rest of the iIT infrastructure, if possible.

	Number	Measure
●	[ITOT] 5.1	Access to the Internet from critical industrial systems (such as lock bridge management systems, power stations, drinking water stations) should be limited to the minimum.
●	[ITOT] 5.2	Development tools should not be installed on active and running machines. Only production systems should be active on IT/OT installations.
●	[ITOT] 5.3	With regard to operational systems, unsecured protocols (e.g. HTTP, Telnet, FTP) should be disabled in favour of secured protocols (e.g. HTTPS, SSH, SFTP).
●●	[ITOT] 5.4	Separate networks zones should be used for the connection of operational systems, for any IoT devices, for professional use Wi-Fi, and for public Wi-Fi.
●●	[ITOT] 5.5	Industrial Control Systems (ICSs) should be divided into consistent functional or technical zones. These zones should be separated from each other.
●●	[ITOT] 5.6	A filtering policy between zones and at administrative gateways should be implemented following a defined strict protocol (i.e. protocol regarding data streams, activity logging, IP address logging, etc.)
●●	[ITOT] 5.7	Where possible, a VPN should be deployed to gateways, blocking outside traffic to operational system zones.
●●	[ITOT] 5.8	Workstations that are authorised to log on to parts of the network with high privilege levels (administration) should, as far as possible, be separated from the main network. These workstations should be controlled and should not be used for other purposes. They should be frequently updated and reinforced using hardening policies.
●●●	[ITOT] 5.9	When the remote control of operational systems is required, remote connections should be certified, connection passwords should be managed in the context of the password policy defined by the organisation, logging should be enabled, secure communication protocols should be in place, and remote connection sessions should be automatically ended after a period of inactivity.
●●●	[ITOT] 5.10	Mechanisms should be in place to secure machine-to-machine exchanges (including EDI messages and API mostly used with external stakeholders, such as shipping companies) and provide mutual authentication, integrity, and confidentiality with the port systems, especially when exchanges are carried out on the Internet. Examples of these mechanisms are encryption, PKI or digital certificates, integrity checks, digital signature, and timestamping.



Monitoring IT/OT systems

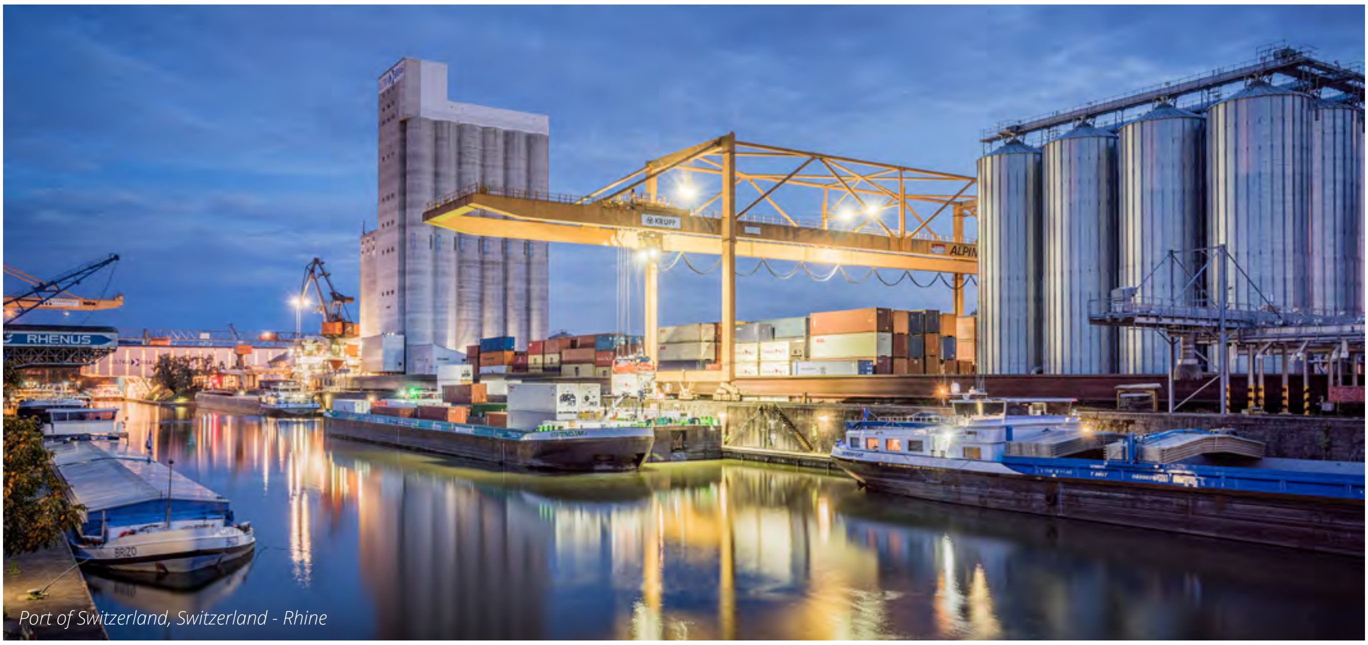
Monitoring activities on operational systems may be out of reach for ports with few operational assets or with limited resource capabilities. The management should consider these measures if their operational systems are critical to port operations and if a strategic cybersecurity priority is to detect and anticipate cybersecurity threats to their systems.

	Number	Measure
●●	[ITOT] 6.1	Parameter changes to critical operations systems should be tracked and logged.
●●	[ITOT] 6.2	Functions to trace activities and events on operational systems should be activated on critical systems.
●●●	[ITOT] 6.3	A process for managing cybersecurity events of operational systems should be implemented by system owners. This process should define event storage (if logs are stored, how they are stored, how they are backed up and secured), should provide basic indications on what defines anomalous system activity, and should provide conditions for declaring if and when an event becomes a cybersecurity incident.
●●●	[ITOT] 6.4	Commercial supervision tools should be considered by the port for the cybersecurity monitoring of operational systems.

Incident response and crisis management for IT/OT systems

As a complement to the incident response and crisis management measures mentioned in the organisational policies and procedure section, these measures are directed particularly at stakeholders working with IT/OT systems.

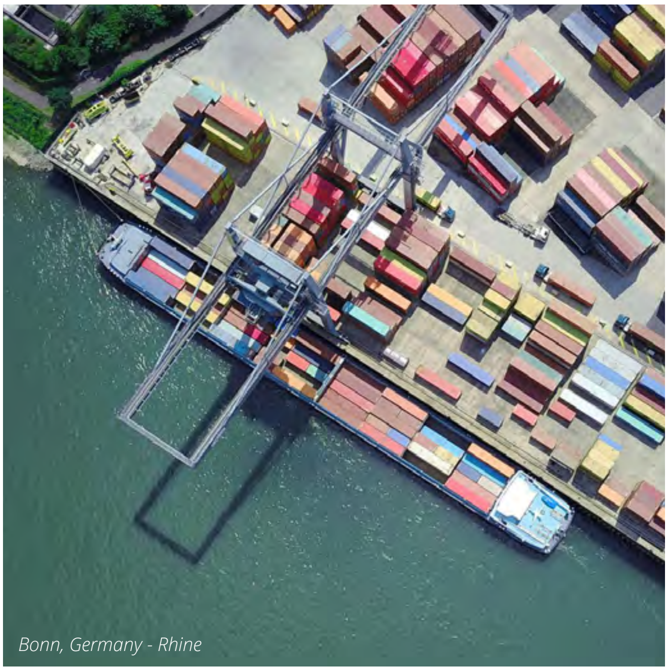
	Number	Measure
●●	[ITOT] 7.1	An incident management plan specifically applicable to IT/OT systems should be defined. This plan should include details on backup of data needed to operate IT/OT systems, intervention procedures, activation of emergency mode of IT/OT systems and should plan for the traceability of actions performed during the management of an incident.
●●	[ITOT] 7.2	Degraded operation modes should be available for operational systems, allowing them to stop or operate in a manual mode in the event of an incident.



Port of Switzerland, Switzerland - Rhine

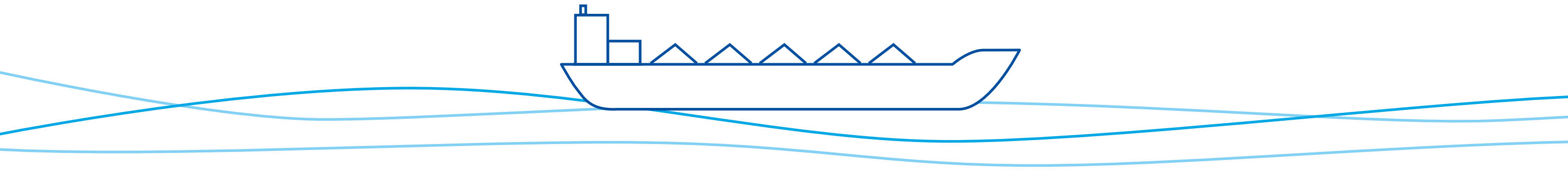
Securing navigation systems

This section has been included to provide some mitigation measures that apply to the IT/OT navigation systems that link ports to navigating crafts. Only the systems that are relevant to ports have been included for the purposes of this guide. Systems that only concern the crew or craft are not dealt with in this guide. These mitigation measures could address risks presented in the specific port attack scenarios described above.



Bonn, Germany - Rhine

	Number	Measure
●●	[ITOT] 8.1	An emergency manual describing how to override any automatic programming of remote communication devices should be made available to users. Port staff should also be informed of the crucial role they can play in detecting erratic or abnormal behaviour of the systems.
●●	[ITOT] 8.2	Port operators should take special precautions in monitoring the security of networks that have access to Electronic Chart Display Information Systems (ECDIS) and ensure they are protected from outside Internet access. Software updates and patches related to ECDIS systems should be systematically installed.
●●●	[ITOT] 8.3	Ports sending and receiving GNSS, and GPS signals should consider adopting mitigation measures against signal spoofing risks. These measures could include implementing tools and techniques to aid in the detection of anomalies in received signals, such as Receiver Autonomous Integrity Monitoring (RAIM) techniques that check for inconsistencies in satellite signals.
●●●	[ITOT] 8.4	Ports that receive AIS data from craft should consider adopting mitigation measures to monitor for potential abnormal behaviour. Data monitoring activities can be used to detect unexpected changes in routes taken by craft or static information that could signal potential malicious activity.



Case study
Protection of container terminals

Container terminals, to be found in certain ports, require numerous IT/OT items of equipment to conduct operations, making it an interesting case study for the implementation of IT/OT cybersecurity risk mitigation measures. These terminals having been identified as critical by many ports, this guide offers a case study presenting the major services and assets of a container terminal and their potential associated cybersecurity risks.

Services and assets of container terminals

Container terminals serve clients of the port by transitioning containers from inland navigation craft to road or rail transporters, or vice versa. Container terminals are usually reliant on a **Terminal Operating System** to interact with clients, transporters, and to conduct activities internally. This operating system provides the following services through connection with other devices:

Client requirement management

Clients have access to an online applications platform to provide information on the containers they are seeking to transport, and any requirements specific to this container (type of goods, weight, size, handling requirements, etc.). This platform relies on the information stored in the terminal operating system.

Container servicing

The operating system centralises information on container damage, the state of containers received and sent, and in the event of damage, sends estimates for container repairs or cleaning to clients.

Container handling

Based on the information stored in the terminal operating system (size, position, handling requirements and type of containers but also the facilities available for container storage). This system can send information to **handling machines/cranes** that then move, lift, and stack containers for storage or movement.

Operational Personnel Management

Terminal operating systems send information on tasks, servicing requirements or other information to port employees via **tablets or hand-held devices**.

Client invoicing and finance management

Through the system, **invoices are sent** directly to clients based on services provided and payment confirmation is received and tracked.

Third-party/supplier management

Third parties involved in the transport of containers such as truckers have access to an **application** to authenticate their collection or deposit of containers and to provide them with information on pick-up and drop-off times and locations.

Cybersecurity risks for container terminal operating systems

Based on these assets and services identified above, two main cybersecurity risks have been identified by crossing the probability of occurrence with the potential business impact for container terminal operating systems. These risks are as follows:

- **A ransomware attack** on the systems used by container terminals, notably on the terminal operating system, freezing container terminal business operations. This attack would prevent the terminal operating system from operating correctly and would therefore have an impact on some or all the services mentioned above. It should be noted that, if the container-handling cranes do not have the option to function without the inputs of the terminal operating system, operational activities would then be disrupted, or even paralysed.
- A malicious intruder **intercepting critical data** on container pick-up and drop-off dates, their location or details as to their contents, could engage in illegal activities (theft, smuggling and retrieval of illicit goods...) it could be more difficult for an intruder to actually steal a physical container, due to the size and logistics required to move the object, an intruder could spy on port systems to obtain information on the location and movement of a certain container, a scenario that has been described above. That could be seriously prejudicial to the port's reputation, affect its security but also make it liable for the consequences of these data being intercepted.

Technical cybersecurity measures for ports

The technical cybersecurity measures detailed below are directed towards the IT or information security departments of a port or an organisation working with ports. The measures recommended below have been adapted to meet the context of a port but are general IT security measures that can be found in all organisations with robust information security policies. Indeed, it should be noted that not all measures may be relevant or feasible for ports with limited resources and staff, such as a port with no specific IT department. These measures should be consulted nonetheless as they can provide a good baseline on the basic security expectations to be considered as an organisation matures from an IT point of view.

Identity and access management (IAM)

This section aims to provide security measures regarding the management of users on IT systems and devices of the port. For the purposes of this guide, IAM measures applicable to general IT systems and those applicable to operational technologies, have been separated. For more information on IAM measures for IT/OT systems in particular, measures have been detailed in section [ITOT] 4. However, for practical purposes, the two topics can be dealt with together.

	Number	Measure
●	[TSM] 1.1	The IT security representative should ensure that authentication options are activated on all PCs, tablets, software, applications, and that default passwords are changed. Passwords should, where possible, have complexity policies and rules.
●	[TSM] 1.2	All the users of the IT system should be identified and should use Individual nominative accounts.
●	[TSM] 1.3	Access to port IT systems or databases to third parties or suppliers should only be granted for a specific time period and for a specific purpose.
●	[TSM] 1.4	“User” accounts and “Admin” accounts should be distinguished. Attribution of “Admin” accounts should be given only to those who need them. “User” account privileges should be kept to the strict minimum. Rights should be granted according to the segregation of duties principle, namely that each user should only have access to the data required to perform his duties, and only his duties.
●	[TSM] 1.5	“Admin” accounts should be used only for administrative operations such as managing “User” accounts, installing, or updating software, and performing maintenance. “Admin” accounts should avoid being used for other actions such as browsing the web and responding to emails.
●	[TSM] 1.6	Anonymous or generic accounts should be deleted from IT systems.
●●	[TSM] 1.7	A procedure should be established for the granting and removal of ”User” account privileges.
●●	[TSM] 1.8	A procedure should be established for managing the lifecycle of ”User” accounts including account creation, modification, updates, data backup, and removal. This procedure should also include the arrangements governing the provision of an additional device to, or withdrawing a device from, the user.
●●	[TSM] 1.9	A regular review of account access rights should be performed. Following these reviews, rights should be revoked where they are granted and not needed. Old user accounts should be deleted when possible or deactivated/archived when not possible.
●●●	[TSM] 1.10	Depending on the number of stakeholders involved in port operations, port stakeholders should consider setting up a tool to manage the accounts and access permissions granted to the port IT assets. Relevant stakeholders include port authorities, terminal operators, local authorities, third parties, etc.
●●●	[TSM] 1.11	Multi-factor authentication (MFA) for the most critical applications and databases, especially databases with personal data, sensitive operational data such as detailed information on craft, and dangerous goods and cargo information should be implemented (see measure [ITOT] 2.6).
●●●	[TSM] 1.12	A Privileged Account Management (PAM) process should be defined with corresponding security requirements on those accounts and rules to manage their lifecycle. This process should be particularly enforced regarding the third-party privileged accounts.

System security

This section details operations that should be performed on IT systems and assets to enhance their overall security. These tasks will most likely have to be performed by an IT or IT security expert as they require specific configuration of IT assets.

	Number	Measure
●	[TSM] 2.1	IT teams should ensure that anti-malware, anti-spam and anti-virus software is installed and up to date on all port systems, including desktops and servers. Priority for these updates should be given to the most sensitive and vulnerable IT equipment.
●●	[TSM] 2.2	A complete inventory of IT assets including hardware, devices, software, systems, servers, networks, and network components should be kept and updated regularly.
●●	[TSM] 2.3	Using the IT asset inventory, a corresponding update policy should be defined with update frequency, means of update, responsibilities, and potential validation processes. This policy should specify that only trusted sources should be used for obtaining updates, such as official websites of publishers.
●●	[TSM] 2.4	IT teams should ensure remote connections are secured properly, using techniques such as VPNs with high levels of encryption. “User” passwords for accessing remote resources need to be made stronger or accompanied by supplementary devices (multi-factor authentication, certificate installed on the PC, single use password, etc.) so as not to present an exploitable vulnerability. The question of whether remote access should be restricted to specific users or systems should be evaluated.
●●	[TSM] 2.5	A policy should be established on the use of removable media (which should preferably be prohibited), including USB sticks, CD-ROM, diskette, etc.
●●●	[TSM] 2.6	A change management process (as construed by the ITIL) to introduce new devices into port systems should be defined.
●●●	[TSM] 2.7	A list of authorised hardware and software should be compiled and regularly updated (including the specific versions authorised for each software product).
●●●	[TSM] 2.8	IT teams should define an endpoint protection strategy (PC, tablet, telephone, and all items of equipment connected to the network and directly accessible to users) with the aim of monitoring them and stepping up security by implementing security tools and mechanisms such as antivirus products, encryption, mobile device management and hardening (making them more secure by deleting all applications and software installed by default but not necessary for the intended use).
●●●	[TSM] 2.9	IT teams should define installation and configuration policies and rules and establish security policies to only install needed services and functionalities and authorise essential equipment for the security and the functioning of port systems.
●●●	[TSM] 2.10	IT teams should perform regular audits of software updates and servers.

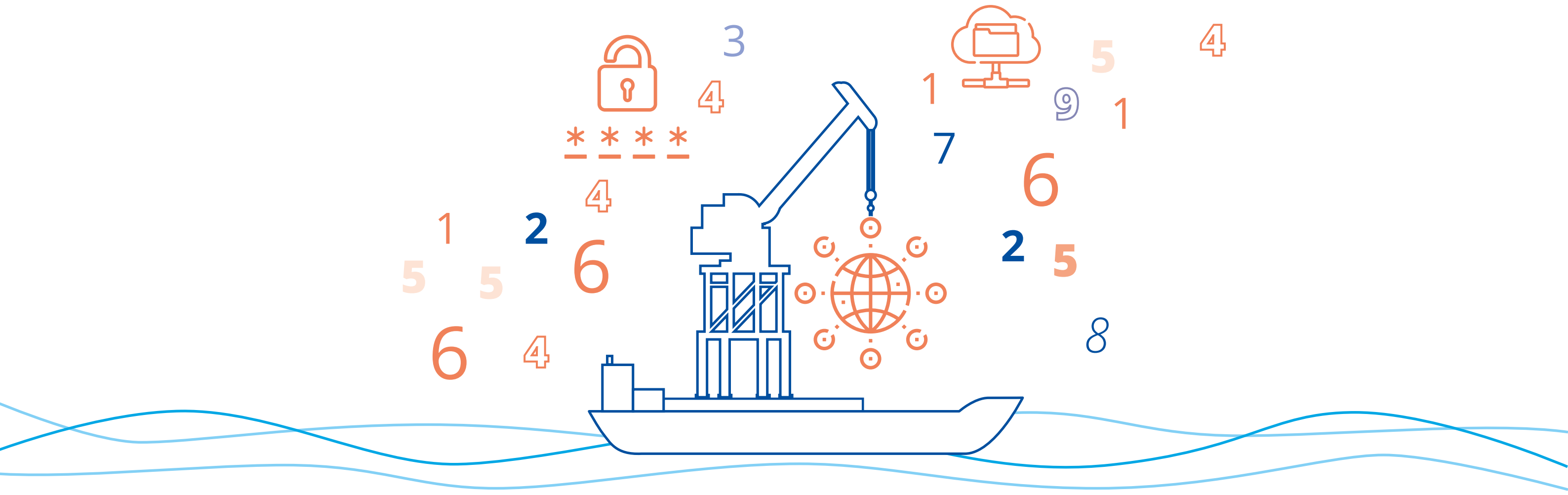
Network security

This section details the measures that can be put in place to secure the networks used by ports. As in the section above, the implementation of these measures will most likely require the implication of IT (security) personnel. In the case of ports not equipped with IT security personnel, the engagement of an external IT security provider could be considered.

	Number	Measure
●	[TSM] 3.1	IT teams should ensure the Wi-Fi password is complex and is changed on a regular basis.
●	[TSM] 3.2	The Wi-Fi networks used by port IT teams must be configured to offer the "WPA2 enterprise" or "WPA3 Enterprise" encryption protocol. If this is not possible, the WPA2-PSK-AES or WPA3 (Personal or Transition) protocol should be used.
●●	[TSM] 3.3	Appropriate network filtering rules (for example, concerning IP addresses or authorised traffic) should be implemented.
●●	[TSM] 3.4	A professional Wi-Fi network (typically for professional use by duly authenticated employees) should be differentiated from a public Wi-Fi network (typically for guests/visitors or for personal use by employees) and segregated. A network segregation policy should be implemented to prevent the propagation of attacks within the port systems and to mitigate risks of access from the Internet.
●●	[TSM] 3.5	A network segregation policy should be implemented to prevent the propagation of attacks within the port systems and to mitigate risks of access from the internet.
●●	[TSM] 3.6	Network access points should be clearly identified and documented by IT teams. This list should be updated regularly. Unused network access points should be disabled.
●●●	[TSM] 3.7	Regular reviews of network rules should be conducted, and adjustments should be made as needed. Regular scans of networks should be performed to detect unauthorised network activity.
●●●	[TSM] 3.8	A policy for declaring and dealing with anomalous network activity should be established in coordination with the incident management processes described in measure [OPP] 4.3.
●●●	[TSM] 3.9	A strategy for monitoring network activity should be defined. This strategy may include a variety of network monitoring tools and technologies. However, this strategy should also provide for these tools being operated, configured, and regularly checked by trained and competent staff.

Data protection

This section pertains to the management of data collected, processed, and used by port stakeholders. It is noted that ports located in the European Union are subject to the General Data Protection Regulation (GDPR) published in 2016. GDPR legislation, if it is applicable, should be consulted as a matter of priority regarding the proper treatment of data and information.



	Number	Measure
●	[TSM] 4.1	Relevant port personnel should understand regulatory requirements (such as GDPR) which are applicable to them, and which pertain to data collection and retention. A data management policy should be implemented that complies with these regulatory provisions, possibly with clarifications or additional provisions.
●●	[TSM] 4.2	A data retention policy should be defined with clear indications on data classification rules and data disposal rules. Personally identifiable data and other particularly sensitive data should be encrypted or secured where stored, but also when they are circulating on the internal network.
●●	[TSM] 4.3	A policy regarding data backups should be defined and implemented. These data backups should be regularly tested to ensure they are functional, prioritising the backups of critical systems and data.
●●	[TSM] 4.4	A Data Recovery Plan (DRP) should be established, detailing the protocol to be followed in the event of a cybersecurity incident or another event capable of resulting in data loss.
●●●	[TSM] 4.5	A data asset analysis should be detailed with information regarding: • the kind of data that the inland port needs access to in order to perform minimum required operations; • the sources of data and data flows treated by the port; • the storage details of data collected and treated; • the current accesses to databases by internal stakeholders and third parties; • the lifecycle of data and retention needs.
●●●	[TSM] 4.6	Spare disks and online data storage should be available in the event of a cybersecurity incident.
●●●	[TSM] 4.7	Storage servers on the network device storage should be inspected regularly to detect potential disk/data storage malfunctions as early as possible.

Vulnerability management and systems monitoring

Vulnerability management measures are intended to obtain information to better address existing vulnerabilities. Monitoring activities can help detect malicious cyber behaviour within port systems..

	Number	Measure
●	[TSM] 5.1	Ports should define a process for cybersecurity monitoring to be aware of newly disclosed vulnerabilities (by employees, vendors, third parties, industry peers) and take quick corresponding mitigation actions. This process should be coordinated with those of IT/OT systems and their owners (see [ITOT] 6.1).
●	[TSM] 5.2	IT teams should define a vulnerability management process to identify asset vulnerabilities (using vulnerability scans, for example) and a process for addressing them.
●●	[TSM] 5.3	A logging system should be set up to record activity and events, in particular events such as user authentication, management of accounts and access rights, modifications to security rules, and any modifications or alterations to the functioning of systems.
●●	[TSM] 5.4	Each vulnerability identified should have corresponding mitigation measures defined and implemented. If none are possible or if no mitigation measures are defined, a documented explanation should be kept on file.
●●●	[TSM] 5.5	IT teams should put in place tools or processes to monitor the availability of port systems and devices in real time. Critical systems (admin work stations, communication devices, navigation devices) should be prioritised in these activities.
●●●	[TSM] 5.6	Ports should set up log correlating and analysis systems to detect events and contribute to cybersecurity incident detection.

Part 3

Tips for the implementation of risk mitigation measures

The purpose of this part is to facilitate the implementation of the mitigation measures presented above. Given the wide range and the different complexity levels of the measures proposed, ports should prioritise the implementation of measures based on their resources, target maturity level and their cybersecurity needs.

The table below proposes priority measures to be implement based on two criteria: the level of cybersecurity maturity of the port and the stakeholders concerned.

This level of maturity can be measured at any given moment, for example using the evaluation framework proposed below. Once this level is known, it can be retained, reinforced, or else increased. Each of these options entails an effort, and therefore costs. Management needs to decide the target level of maturity having regard to numerous criteria such as the size of the port, its exposure, its technological dependence, the number of suppliers and subcontractors, its technical and financial resources, but also its experience and its own cybersecurity challenges.

Here are some examples of criteria that can help set the cybersecurity target. These criteria are for information purposes only or as a source of inspiration for management, whose responsibility it is in any event to set them.

Target maturity level

Low

Possible criteria

- The port is not a major shipping or trading hub for the region.
- The existing IT teams are very small and the stakeholders responsible for IT are external service providers.
- Port activities require scarcely any digital infrastructure to operate.

Medium

Possible criteria

- The port has some important infrastructure but is not the central port trading hub in the region.
- IT service providers are present and intervene frequently, or there is some form of IT team in the organisation.
- Some port activities are reliant on digital infrastructure.

High / strong

Possible criteria

- The port is identified as a major trading hub for the region. It is home to an important shipping/container hub or is a major transit zone.
- There is an internal IT team and corresponding decision-makers.
- Port activities are heavily reliant on digital infrastructure, there are even some ”SmartPort” technologies.

The various stakeholders in question are the actors required to implement each measure. Some measures proposed above can only be accomplished by IT or security specialists, while others require the implication of port managers or leadership.

By its very nature, the level of maturity cannot develop too quickly. A port assessing its level of maturity to be “low” can aim for a “medium” level after several years of sustained effort, but it cannot aim directly for the “high” level within the same timeframe, even if it were to commit large financial resources to achieve it. Indeed, cybersecurity maturity is also a question of experience, culture and practice, all of which take time.

The level of maturity should also be consistent, and as uniform as possible. For example, a port should not accept a “low” level of maturity for the “organisational policies and procedures” yet aspire to achieve a “medium” or “high” level for “network security”. Likewise, it is pointless, or even counter-productive, and certainly expensive, to aspire to implement a measure that belongs to a “high” level of maturity if the vast majority of “low” and “medium” measures (or even all of them) have not yet been implemented. Indeed, if implementing cybersecurity measures is often compared to building fortifications, it will be readily understood that there is no point fortifying one side if another is left completely exposed. Cybersecurity incidents and attacks very frequently occur where cybersecurity is at its weakest. A good strategy therefore consists in strengthening cybersecurity at this weakest point. It is however possible, without neglecting everything else, to go a bit furtherin specific areas where they have been identified is particularly critical.

Maturity evaluation framework

At this point, this guide proposes an evaluation framework for ascertaining a port's current level of maturity.

This is a self-assessment method consisting in giving a score of between 1 and 5 for each measure defined in Part 2. Ideally, the self-assessment should be carried out by a small multi-disciplinary team with a minimum of one representative for each stakeholder, namely:

- a member of the management, ideally responsible for cybersecurity;
- a member of the IT team with a good overview of the infrastructure and applications;
- an operational manager with good knowledge of how the business systems work (several managers if a single such manager is not sufficient to cover all the business systems).

Each team member should evaluate each measure independently of the other members. Ideally, each member will evaluate each measure based on his knowledge and awareness, but at a minimum he will evaluate all the measures in his column of the applicability table but should be prepared to request colleagues to assist on certain points.

In a second step, the members meet and review their notes. When discrepancies are noted, members will discuss and explain the reasons for their score. After this discussion, having regard to the other members' comments, the member representing the stakeholder with which the measure is associated will decide on the final score.

The scoring scale of 1 to 5 can be expressed as follows:

Points	Description
1	This measure is uncoordinated or unstaffed, there is no formal programme in place or no particular controls of the type exist.
2	There is informal communication or an informal process around this measure, although documentation and official procedure is lacking.
3	Some roles and responsibilities related to this measure have been formalised. Corresponding processes exist but are not checked for implementation systematically.
4	Roles and responsibilities are clearly defined, and there are formal process verification steps in place to ensure this measure is implemented.
5	There is a culture of continuous improvement around this measure, processes behind it being quantitatively monitored for understanding and improvement.

Once this self-assessment process has been concluded, the average of the scores given to the measures featuring in each of the three lines of the applicability table below is calculated. The outcome therefore boils down to three averages between 1 and 5 for each of the levels of maturity ("low", "medium" and "high").

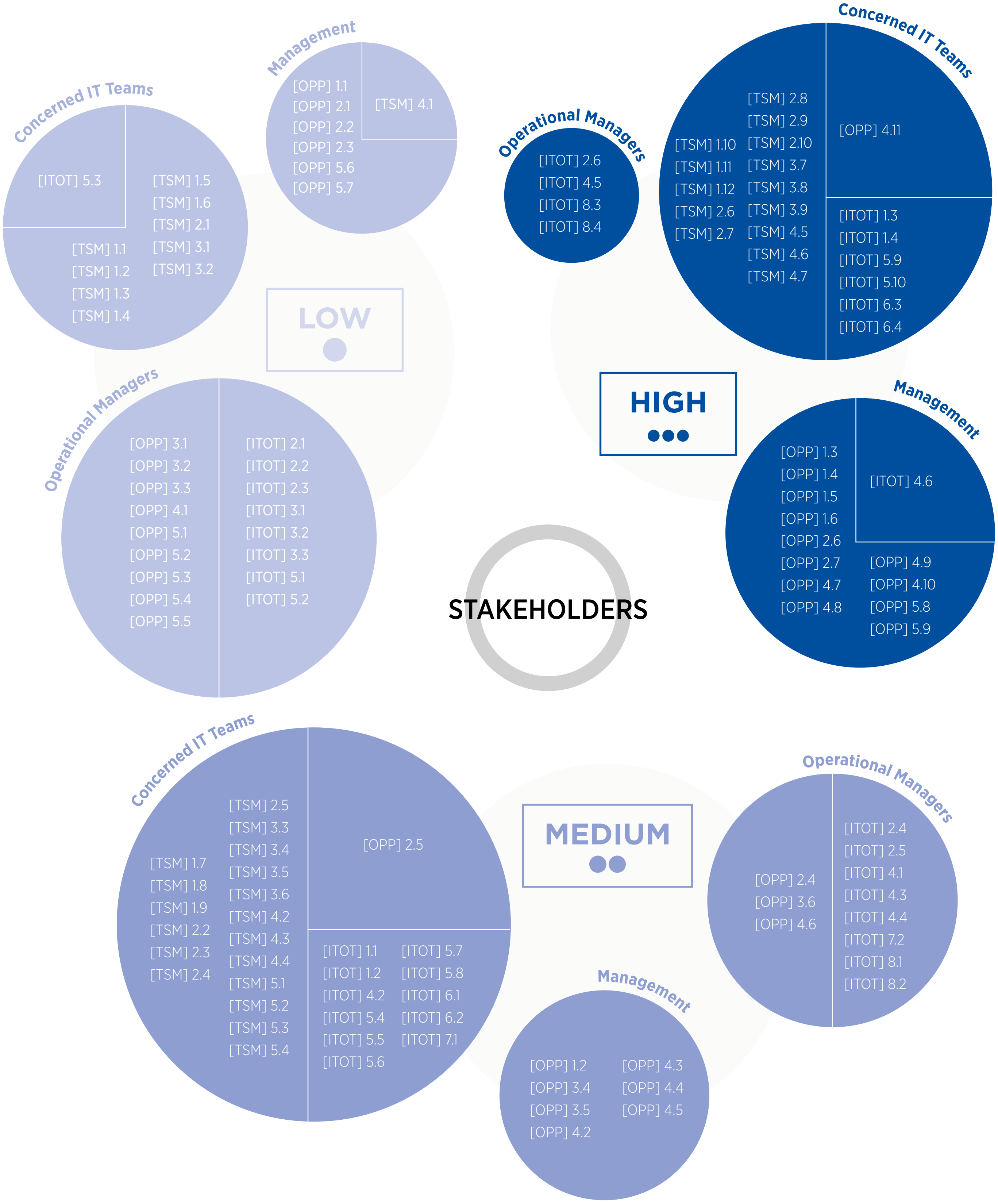
The level of maturity is deemed to have been achieved if:

1. the average of the measurements of the target level is a minimum of 2.5;
2. the average of the measurements of the level immediately below the target level is 3.5;
3. the average of the measurements of the level below that is a minimum of 4.

For example, to achieve the level "medium", the average of the scores of the medium measurements must be 2.5 or better, and the average of the measurements of the level "low" must be 3.5 or more. To achieve the high level requires an average of the measurements of the high level of 2.5 or more, an average of the measurements of the medium level of 3.5 or more, and an average of the low levels of 4 or more.

Applicability table for measures

The table below proposes measures to be implemented by the stakeholders depending on the maturity level being targeted by the management.



STAKEHOLDERS

LOW

Concerned IT Teams

[ITOT] 5.3

[TSM] 1.1
[TSM] 1.2
[TSM] 1.3
[TSM] 1.4

[TSM] 1.5
[TSM] 1.6
[TSM] 2.1
[TSM] 3.1
[TSM] 3.2

Management

[OPP] 1.1
[OPP] 2.1
[OPP] 2.2
[OPP] 2.3
[OPP] 5.6
[OPP] 5.7

[TSM] 4.1

Operational Managers

[OPP] 3.1
[OPP] 3.2
[OPP] 3.3
[OPP] 4.1
[OPP] 5.1
[OPP] 5.2
[OPP] 5.3
[OPP] 5.4
[OPP] 5.5

[ITOT] 2.1
[ITOT] 2.2
[ITOT] 2.3
[ITOT] 3.1
[ITOT] 3.2
[ITOT] 3.3
[ITOT] 5.1
[ITOT] 5.2

HIGH

Operational Managers

[ITOT] 2.6
[ITOT] 4.5
[ITOT] 8.3
[ITOT] 8.4

Concerned IT Teams

[TSM] 1.10
[TSM] 1.11
[TSM] 1.12
[TSM] 2.6
[TSM] 2.7

[TSM] 2.8
[TSM] 2.9
[TSM] 2.10
[TSM] 3.7
[TSM] 3.8
[TSM] 3.9
[TSM] 4.5
[TSM] 4.6
[TSM] 4.7

[OPP] 4.11

[ITOT] 1.3
[ITOT] 1.4
[ITOT] 5.9
[ITOT] 5.10
[ITOT] 6.3
[ITOT] 6.4

Management

[OPP] 1.3
[OPP] 1.4
[OPP] 1.5
[OPP] 1.6
[OPP] 2.6
[OPP] 2.7
[OPP] 4.7
[OPP] 4.8

[ITOT] 4.6

[OPP] 4.9
[OPP] 4.10
[OPP] 5.8
[OPP] 5.9

MEDIUM

Concerned IT Teams

[TSM] 1.7
[TSM] 1.8
[TSM] 1.9
[TSM] 2.2
[TSM] 2.3
[TSM] 2.4

[TSM] 2.5
[TSM] 3.3
[TSM] 3.4
[TSM] 3.5
[TSM] 3.6
[TSM] 4.2
[TSM] 4.3
[TSM] 4.4
[TSM] 5.1
[TSM] 5.2
[TSM] 5.3
[TSM] 5.4

[OPP] 2.5

[ITOT] 1.1
[ITOT] 1.2
[ITOT] 4.2
[ITOT] 5.4
[ITOT] 5.5
[ITOT] 5.6

[ITOT] 5.7
[ITOT] 5.8
[ITOT] 6.1
[ITOT] 6.2
[ITOT] 7.1

Operational Managers

[OPP] 2.4
[OPP] 3.6
[OPP] 4.6

[ITOT] 2.4
[ITOT] 2.5
[ITOT] 4.1
[ITOT] 4.3
[ITOT] 4.4
[ITOT] 7.2
[ITOT] 8.1
[ITOT] 8.2

Management

[OPP] 1.2
[OPP] 3.4
[OPP] 3.5
[OPP] 4.2

[OPP] 4.3
[OPP] 4.4
[OPP] 4.5

Glossary

Düsseldorf, Germany - Rhine

Back door

In software, a back door is a feature unknown to the legitimate user, which provides secret access to the software.

BYOD

Means "Bring Your Own Device". In a corporate context, BYOD is an employee practice, sometimes encouraged and sometimes curbed, of using certain personal devices for their work. Typically, this may be their smart phone and occasionally also their laptop. For the employees, the objective is the convenience of using devices with which they are familiar and which they value. For the company this practice may save them money. In terms of cybersecurity, personal devices may be a challenge because it is often impossible to make them properly secure, and the numerous brands and models translate into more numerous risks.

CFM

Craft loading and unloading management.

Crown jewels

The "crown jewels" are the most critical assets to the accomplishment of an organisation's mission. An analysis is required to identify them from among the totality of assets[10].

Hacktivism

Computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism[11].

Hardening

Process of making a system secure by eliminating components not needed in order for the system to operate (for example a PC or server). Hardening consists in reducing the system's "attack surface", namely removing everything that is not necessary, and which was installed by default, and which might (potentially) contain vulnerabilities (applications, software libraries, optional modules, etc.). It is generally accepted that the quantity of vulnerabilities in a system is roughly proportional to the number of lines of code it contains. The fact therefore of eliminating unnecessary components also has the effect of reducing the number of vulnerabilities that can be exploited by an attacker.

Impact

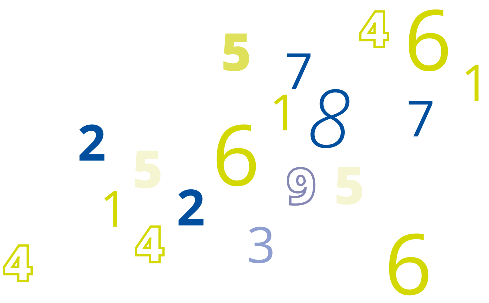
This term refers to the consequences of a cybersecurity incident when it occurs (and independently of the probability of its occurrence). The key question one needs to ask oneself therefore is: if such a cybersecurity incident occurs then – in the worst case – what happens next? From the outset, the impact may or may not be large. For example, the destruction of a server (the cybersecurity incident) may have a very different impact depending on whether it is a development server or a critical operational server. However, the impact can be reduced by developing circumvention strategies and by making the system more resilient, for example by means of emergency procedures. In the case of a critical server, a second such server can be provided, ready to take over if the first fails. In the event of data being lost, there can be a backup, etc. The impact is always evaluated without taking account of the threat (see definition).

Incident (Cybersecurity)

A generic term used to describe an event with negative cybersecurity consequences. This incident may be caused by a hardware failure (a hard disk failure), a crash (a server rebooting), sabotage (deliberate insertion of a computer virus), human error (unfortunately clicking on a booby-trapped email) or even negligence (an employee writes his PIN code on the back of his smart card). When the consequences of this incident are dealt with in time, the incident is over. When this is not the case, the incident may become a crisis with a knock-on effect and consequences that become worse over time more or less quickly.

LBM

Lock and Bridge Management. Bridges and locks are managed by machines, such as moveable bridges and equipment for changing water levels, such as sluices and locks, which are particularly critical systems as they present the risk of widespread flooding in the event of a cyber-attack.



[10] https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis

[11] https://www.merriam-webster.com/dictionary/hacktivism

Phishing

A scam by which an Internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly[12].

Programmable Logic Controller (PLC)

Programmable digital electronic device for controlling industrial processes by means of sequential processing. It sends orders to (pre) actuators based on input data (sensors), instructions and/or a computer program. PLCs are used extensively in almost all industrial processes. For complex processes, a SCADA is typically present to ensure coordination between several PLCs and their wider networking[13].

Risk

This term is formally used in cybersecurity to evaluate a set of threats facing a system with a greater or lesser degree of probability, and with consequences of varying severity. We talk about high risk when the probability and the impact of threat are high, and about low risk when they are limited. Risk analysis consists in independently evaluating the probabilities and impact of the various threats and drawing overall conclusions from them. By way of illustration, the “flood risk” is evaluated both in terms of the probability of flooding (flood-prone areas) and of the characteristics of the area in question, for example if it is heavily populated or not. The flood risk is therefore considered to be virtually identical in a flood-prone area with a very low population, and in a non-flood-prone area but that is very highly populated (“non-flood-prone area” refers to a low – but not zero – risk of flooding). The risk can therefore be reduced by limiting the impact or by reducing the probability. In the case of flood risk, watercourses can be canalised, dams and containment basins built (to reduce probability) or levees created to protect houses, or preference given to buildings on stilts, and population increase avoided in a flood-prone area (to limit the impact)[14].

SCADA

Supervisory Control And Data Acquisition. A SCADA system is a large-scale remote-management system for processing many remote measures in real-time, and remotely controlling technical facilities. It is an industrial instrumentation technology. In terms of cybersecurity, SCADA equipment is a major challenge because it is connected to a network which, if one takes control of it, enables control of the underlying technical facilities.

Security Operations Center (SOC)

A Security Operation Center is a department within an organisation that coordinates IT security operations. This department is capable of taking action as regards the organisation’s employees, processes, and technology to continuously monitor and improve an organisation’s security posture while preventing, detecting, analysing, and responding to cybersecurity incidents[15].

Social engineering

Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons[16].

Spoofing

In the cybersecurity context, spoofing is a range of techniques for deceiving a target as to the real origin of an item of information it is receiving. Depending on the techniques used, we also talk about masking, substitution etc.

Threat

A threat is an actor, circumstance, or event with a potentially negative impact on an organisation (its operations, its assets, its image, or people associated with it) or, through it, on other organisations associated with it. To generate this impact, the threat must exploit one or more vulnerabilities in accordance with a specific scenario. The more plausible the scenario, the greater the vulnerabilities, and the more numerous the threats, the greater the probability is of a cybersecurity incident occurring. Then we talk about a high threat. For example, the threat level of a server exposed on the Internet is greater than that of a server that is exposed only on an internal network, because there are potentially more people who may attempt to hack it. Very often, to reduce the threat, action is taken against vulnerabilities, either by eliminating them (or by reducing the number) or by making it more complex to exploit them (by adding various protections, for example). Occasionally it is possible to act directly on the number of actors, circumstances, or events with a potentially negative impact. The threat is always evaluated without having regard to the impact (see definition).

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[12] https://www.merriam-webster.com/dictionary/phishing

[13] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[14] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[15] https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html

[16] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

WEP/WPA/WPA2/WPA3

These acronyms refer to security protocols governing access to a wireless network (Wi-Fi). WEP (Wired Equivalent Privacy) appeared in 1999. WEP is very insecure, which is why the WPA protocol (Wi-Fi Protected Access) was invented to replace it in 2003. From the outset, WPA was designed as a temporary protocol. Indeed, it was replaced by APA2 in 2004, which is based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11i standard. WPA3 was published in 2017 but is merely a development of WPA2, which is not (yet) obsolete and remains very widely used in 2023. WPA2 exists in two versions. On the one hand a "personal" version of WPA2 (also known as WPA2-PSK for "Pre-shared Key") based on a shared key and intended for domestic or family use, or in a very small building. On the other hand, "Enterprise" WPA2, based on RADIUS authentication (several users with different accounts) and intended for corporate use. It should be noted that WPA2-PSK provides for the use of two encryption algorithms: AES and TKIP. The AES algorithm is more secure.

Photo credits

Pictures, courtesy of European Federation of Inland Ports (EFIP)
p 28 : © Steve Haider
p 45 : © Patrik Walde, patrikwalde.com
p 46 : © AZS Group Bonn
p 58 : © Port of Düsseldorf

Shutterstock
Adobe stock

Artistic direction & Layout: dot. Deloitte Agency France

European committee for drawing up standards in the field of inland navigation (CESNI)
Secretariat of the Central Commission for the Navigation of the Rhine (CCNR)
2 Place de la République – CS10023
F-67082 Strasbourg cedex
France
comite_cesni@cesni.eu
https://www.cesni.eu

In partnership with the European Federation of Inland Ports (EFIP)
The European Port House
Treurenberg 6
B-1000 Brussels
Belgium