European Commission

Transport cybersecurity toolkit

Introduction

The European Commission Directorate-General for Mobility and Transport (DG MOVE) has contracted the development of this toolkit to enhance the awareness and preparedness of transport stakeholders to cyber threats. It provides insights for understanding cyber threats and mitigating their impact on transport services, systems, and operations. This toolkit provides alternative awareness paths targeting different transport profiles:

- All transport staff (providing general information and guidance).

- Transport decision-makers in cybersecurity across the different transport modes.

Hyperlinks connect the different parts forming the toolkit in order support the navigability of the awareness paths tailored to the specific transport profiles.

The practices listed in this toolkit are of an advisory nature only. Any recommendation that is formulated is neither binding nor mandatory. Moreover, this toolkit does not represent the formal views of the European Commission and is not meant to provide means of compliance with existing or future EU legislations.

Cybersecurity Awareness Profiles

Profile I: All transport staff. The first path targets all staff of transport organisations, from staff in transport service operations to administrative staff. It provides guidance towards an increased understanding and awareness of the most common cyber threats targeting transport services and systems. Additionally, it provides insights on how to deal with potential cyber threats, including identifying, reporting, and mitigating them by cybersecurity good practices.

Profile II: Decision-makers in transport cybersecurity. The second path targets staff who have decision-making responsibilities for cybersecurity in transport organisations. This path highlights good practices tailored to the different transport modes for enhancing cybersecurity posture of transport organisations. In particular, it provides good practices in order to identify, protect, detect, and respond to emerging cyber threats targeting transport organisations.

European Commission

Transport cybersecurity toolkit

Transport Threat Landscape

Emerging cybersecurity threats affecting different modes of transport.

Cybersecurity Awareness Profiles

Alternative cybersecurity awareness paths targeting different transport profiles.

European Commission

Transport Threat Landscape

The cyber threat landscape is dynamic and continuously evolving. Nevertheless, it is possible to identify cyber threats, which all transport modes face in operations of services and systems.

European Commission

Threat Actors

Individuals or organisations that may potentially impact safety and security of transport services and systems.

Emerging Cyber-Threats

Selected cyber-threats that may potentially represent attack vectors impacting safety and security of transport services and systems.

Threat Actors

Individuals or organisations may intentionally or unintentionally expose and exploit vulnerabilities, which have the potential of causing incidents and affecting transport services including their safety, security, business, finance and reputation. Threat actors involve, among others, state-sponsored groups, cyber criminals, cyber terrorists, hacktivists, hackers (including script kiddies), and insiders (including privileged insiders).

The most significant malicious actors intentionally targeting transport organisations are **cyber criminals**, **insiders**, nation states and **state-sponsored groups**.
Adversaries such as cyber criminals conduct massive attack campaigns and are often in the game for monetary rewards.

Insiders, know the singularities of the organisations they work for and are often well aware of subtle security vulnerabilities. Insider threat actors may involve disgruntled employees, suppliers and individual contractors.
As global geopolitical tensions intensify, nation states and **state-sponsored groups** target strategic long-term objectives. They often try to conceal themselves in the depth of organisations' systems and collect sensitive information. Once they establish their foothold into systems, state-sponsored attackers look to gain a position that has the potential to create the worst damage possible. For example, they may target other organisations' systems by exploiting the organisations' network connections.

Other threat actors involve insiders, who may unintentionally or accidentally perform actions resulting in cybersecurity events and, in worst cases, cyber incidents affecting the safety and security of transport services.

European Commission

Emerging Cyber-Threats

There are a substantial number of cyber threats targeting transport: **distributed denial of service**, **denial of service**, data theft, **malware** diffusion, **phishing**, software manipulation, unauthorised access, destructive attacks, falsification or bypassing of security operator decision process, masquerading of identity, abuse of access privileges, **social engineering**, defacement, eavesdropping, misuse of assets, and hardware manipulation.
Based on comprehensive literature research of publicly available documentations and interviews with experts, the most pressing emerging cyber threats affecting transport are: Malware, (Distributed) Denial of Service, Unauthorised Access and Theft, and Software Manipulation.

European Commission

Threat #1: Malware

Malicious software that may potentially affect individuals or organisations across transport modes.

Threat #2: (Distributed) Denial of Service

Cybersecurity attacks preventing individuals or organisation access relevant transport services and resources.

Threat #3: Unauthorised Access and Theft

Unauthorised access, appropriation, and exploitation of critical assets.

Threat #4: Software Manipulation

Cybersecurity attacks targeting software in order to modify its behaviour and conducting specific attacks.

Threat #1: Malware

Malware consists of malicious software, which may include different types of software applications such as viruses, trojans, worms, ransomwares, cryptocurrency-miners, or any software that may have potentially adverse impacts on organisations or individuals across transport modes.

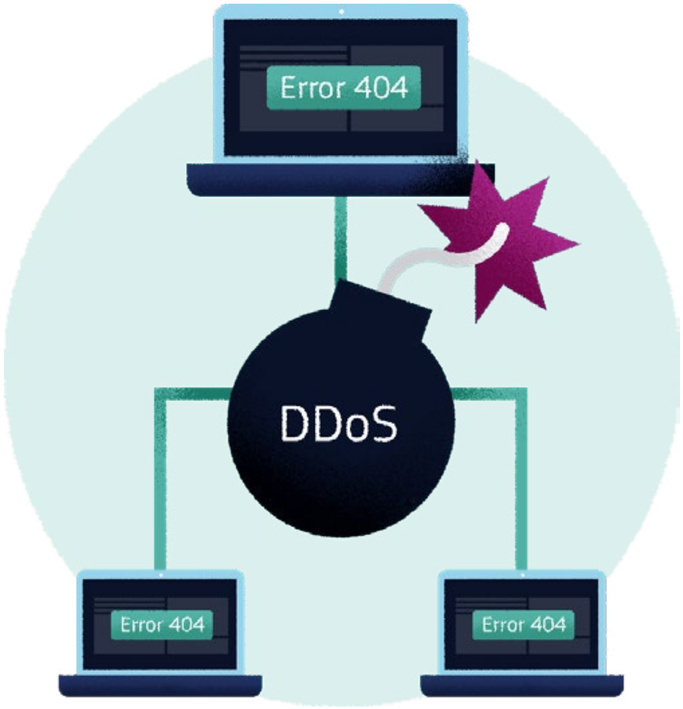
Mitigating the diffusion of malware designed for intentionally damaging computers, servers, clients, networks, or all of them is amongst the main priorities of cybersecurity across all modes of transport. A typical attack vector may involve phishing emails targeting employees. Other attack vectors may involve different and sophisticated social engineering strategies such as plugging in a USB key into a free port (e.g. charging of mobile phone). By clicking hyperlinks in suspicious emails or opening file attachments, the user may unknowingly be installing software or knowingly jeopardising transport services and resources.

For example, the WannaCry ransomware cyber-attack affected more than 150 countries and infected over 230,000 systems. It involved a ransomware that usually spreads via phishing emails containing malicious attachments or hyperlinks. This type of attack exploits social engineering maliciously in order to mislead system users into installing (or activating) specific malware.

Threat #2: (Distributed) Denial of Service

Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks affect availability and accessibility of data, services, systems, and other resources. These types of attacks can range in duration and may target more than one service or system at a time. DDoS attacks employ multiple systems (or channels of attack) in order to overload target services or systems with requests. Successful attacks affect service and system capabilities to deal with unexpected volume requests. This results in denying access to services and resources.

Note that affected services and systems belonging to transport organisations may be exploited in order to conduct DDoS and DoS attacks to target specific systems in operations or other organisations as well.
For example, corporate information systems (such as personal computers and devices) may be targeted in order to access operation technologies, which may be connected to the internet or accessing networks in order to transfer operational data. Connections between different systems and networks (such as corporate networks, operation technologies and remote maintenance accesses) may represent exploitable vulnerabilities for conducting DDoS or DoS attacks to critical transport services and systems. For example, DDoS and DoS attacks can exploit common network and communication protocols such as the Web Services Dynamic Discovery (WS-Discovery), which IoT devices may use to automatically discover each node on Local Area Networks (LANs). If IoT devices present vulnerabilities, attackers may exploit them in order to discover other connected devices and conduct DDoS or DoS attacks.



Threat #3: Unauthorised Access and Theft

Threat actors may want to gain logical or physical access without permission to a network, system, application, data, or another resource in order to conduct malicious activities, including theft of sensitive data or resources (including physical resources).
Unauthorised access and theft threats target confidential and proprietary assets (including personal identities, credentials of privileged accounts, systems, and other types of confidential and proprietary information). These threats may exploit systems vulnerabilities as well as unaware individuals disclosing sensitive data such as credentials (e.g. login, password, etc.) or personal data (e.g. email, personal identification number, etc.).

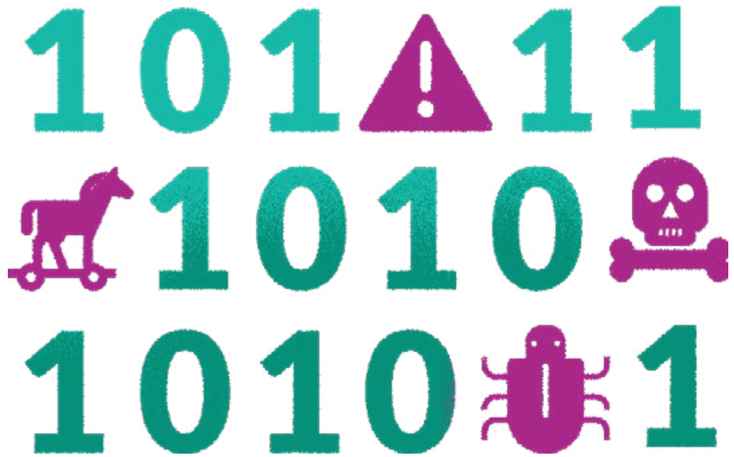
In relation to unauthorised access, identity theft is the illicit use of personal data or unique identifiers in order to impersonate persons or services and systems to gain access to private or proprietary resources (e.g. including financial and physical resources). Such cybersecurity threats may target also physical assets across transport modes.

European Commission

Threat #4: Software Manipulation

Misconfigurations and manipulations of software and related systems or components may have a direct impact on the security posture of transport services and systems. Cybersecurity attacks exploiting software manipulations modify software settings or affect the integrity of data in order to change the behaviours of systems and services. Attackers may intentionally manipulate software (or part of it) in order to gain advantages (e.g. obtaining unauthorised access, preventing legitimate individuals or systems access to necessary resources, collecting sensitive information, changing functional behaviours, etc.) over sensitive assets.

For example, attackers may target communication channels of manufacturers in order to upload malicious software updates on services and systems (including operation technologies) in operations. A threat agent uses compromised authorisation credentials to access a secured remote maintenance network interface in order to install manipulated software and further compromise other accessible services and systems. The threat agent installs manipulated software that further compromises target services and systems, or attacks other connected services or systems



European Commission

Cybersecurity Awareness Profiles

European Commission

1

Profile I: All transport staff

The first path targets all staff of transport organisations, from operational to administrative staff. This path provides guidance towards an increased understanding and awareness of the most common cybersecurity threats targeting transport services. It also provides insights on how to deal with potential cybersecurity threats, including identifying, reporting, and mitigating them through cybersecurity practices. This path is common to all transport modes.

2

Profile II: Decision-makers in transport cybersecurity

The second path targets staff who have decision-making responsibility for security or cybersecurity in transport organisations. This path provides good practices tailored to the different modes of transport. It provides good practices in order to identify, protect, detect, and respond to emerging cybersecurity threats targeting transport organisations.

European Commission

Profile I: All transport staff

This part targets all staff of transport organisations, from operational to administrative staff. It provides guidance towards an increased understanding and awareness of the most common cybersecurity threats targeting transport services. It also provides insights on how to deal with potential cybersecurity threats, including identifying, reporting, and mitigating them through cybersecurity practices.
This part provides recommended practices and useful tips, which are relevant **across all modes of transport.**

Good practices against Malware

You can help to protect your organisation by following good practices for **identifying and preventing the diffusion of malware**, such as:

- ***Follow security policies*** *such as scanning storage media and files for viruses, avoiding opening and emailing specific types of files (e.g. executable files such as .exe, .bat, .com, etc.), installing only authorised software, ensuring software (including antivirus) is up to date and functioning properly, and other policies.*

- ***Backup your data*** *regularly into secure (and authorised) data storage devices or services, which should support encryption mechanisms in order to protect data at rest and being available for data restore procedures.*

- *Protect with suitable* ***security measures*** *(e.g. password, encryption, etc.) all systems including mobile and endpoint devices, and remember to lock (physically and digitally) securely all systems if unattended.*

- *Avoid opening attachments and clicking on hyperlinks contained in unexpected emails and suspicious web browser popup windows with a strange body text or from unknown senders and internet domains.*

- *Avoid inserting into your computer* ***untrusted or unknown removable devices*** *such as USB sticks, hard disks, and other storage devices.*

- *Avoid disabling malware security measures (e.g. antivirus software, content filtering software, firewall, etc.).*

- ***Update installed software*** *regularly to the latest available versions (which information security officers or system administrators may release with regular updates).*

- *Avoid using privileged (e.g. administrator-level) accounts and credentials for regular activities and operations.*

- *Report to information security officers or system administrators any suspicious email or unexpected system behaviour.*

- *Focus attention on information security among daily routine work in order to recognise IT security concerns and respond accordingly.*

Good practices against (Distributed) Denial of Service

You can help in protecting your organisation by identifying **Distributed Denial of Service (DDoS)** and **Denial of Service (DoS)** attacks. You should contact immediately your security and IT teams if you detect or experience any of the following indicators of potentially ongoing DDoS and DoS attacks for your services or systems:

- *Increasing requests consuming network capacity (perceived as slow services and responses) resulting in service or system failures due to overload.*
- *Increasing demand of memory resources usage without an obvious reason.*
- ***Unexpected behaviours of services and systems**, frequent crashes and strange error messages due to malicious consumptions of computational resources or network connections.*
- ***Degraded performances** of devices, long executions for trivial tasks and noticeable activities (e.g. noisy fan while devices performing slowly).*
- ***Unexpected internet connections or loss of connections** to services and systems.*
- *Subtle behavioural changes of operation controls or technologies resulting in physical damages.*
- *Denials of accesses to privileged or administrative accounts in order to block incident response procedures from recovering.*

Good practices against Unauthorised Access and Theft

In order to prevent attacks involving unauthorised access and theft, it is necessary to follow principles such as *'need to know'* and *'security and privacy by default'*, which emphasise that sensitive and confidential assets (including personal and sensitive data, transport systems, etc.) should be accessible only to whom has the right to access them in order to perform their duties. You can help in protecting your organisation by following good practices for identifying and preventing unauthorised access and theft, such as:

- *Follow security organisational policies.*
- *Avoid sharing and publishing online credentials and personal data, including pictures that may contain such information.*
- *Avoid using or transmitting credentials and personal data (and other sensitive data) to untrusted and unsecure networks, devices or web services (e.g. websites that use unsecure protocols or addresses http:// and not secure ones https://).*
- ***Never reveal to anyone your credentials** (e.g. login and password) even via email or phone.*
- *Protect sensitive data typed on keyboards or shown on screens (including on mobile devices) from unauthorised individuals, install privacy screens, and avoid working from public places with private devices, and avoid leaving any device unlocked and unattended.*
- ***Use complex passwords** (e.g. sufficiently long password combining alphanumerical and special characters) complying with relevant organisational security policies in order to prevent unauthorised access.*
- ***Change default passwords** of connected systems and devices (e.g. printers, routers, cameras, smart lock, etc.).*
- *Avoid using the same credentials (e.g. login and password) for multiple services and systems, and avoid using the same credentials for services and systems that require privileged accounts.*
- *Send passwords and keys for transferred protected files (e.g. ZIP archives) only via an out of band channel (e.g. SMS via GSM and phone call) and never via email.*
- ***Activate Two-Factor Authentication (2FA)** or Multi-Factor Authentication (MFA), if possible.*

European Commission

Good practices against Software Manipulation

You can help in protecting your organisation by following good practices for identifying and preventing software manipulation, such as:

- *Avoid installing unreliable software on systems and devices (including personal computers, servers, peripherals, network devices, smartphones, etc.).*
- *Always install software and updates from official sources and websites (e.g. producers, corporate repositories, etc.).*
- *Avoid downloading software and applications (and any file) from illegal sources.*
- *Uninstall unnecessary or not recently used software, and disable unnecessary connections (e.g. network protocols and services) including access to remote services (e.g. cloud storage services).*
- *Scan any software or storage devices with a reliable and updated antivirus.*
- *Download safe industrial software (e.g. updates, patches, new products, etc.) from trusted suppliers using white station principle.*
- *Update all installed software in compliance with organisational policies and practices.*

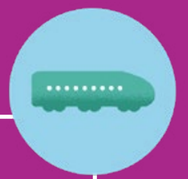
European Commission

Profile II: Decision-makers in transport cybersecurity

This part targets staff who have decision-making responsibilities for security or cybersecurity in transport organisations. This path highlights good practices tailored to the different modes of transport. In particular, it provides good practices in order to identify, protect, detect and respond to emerging cyber threats.

European Commission

Cybersecurity good practices tailored to Air Transport

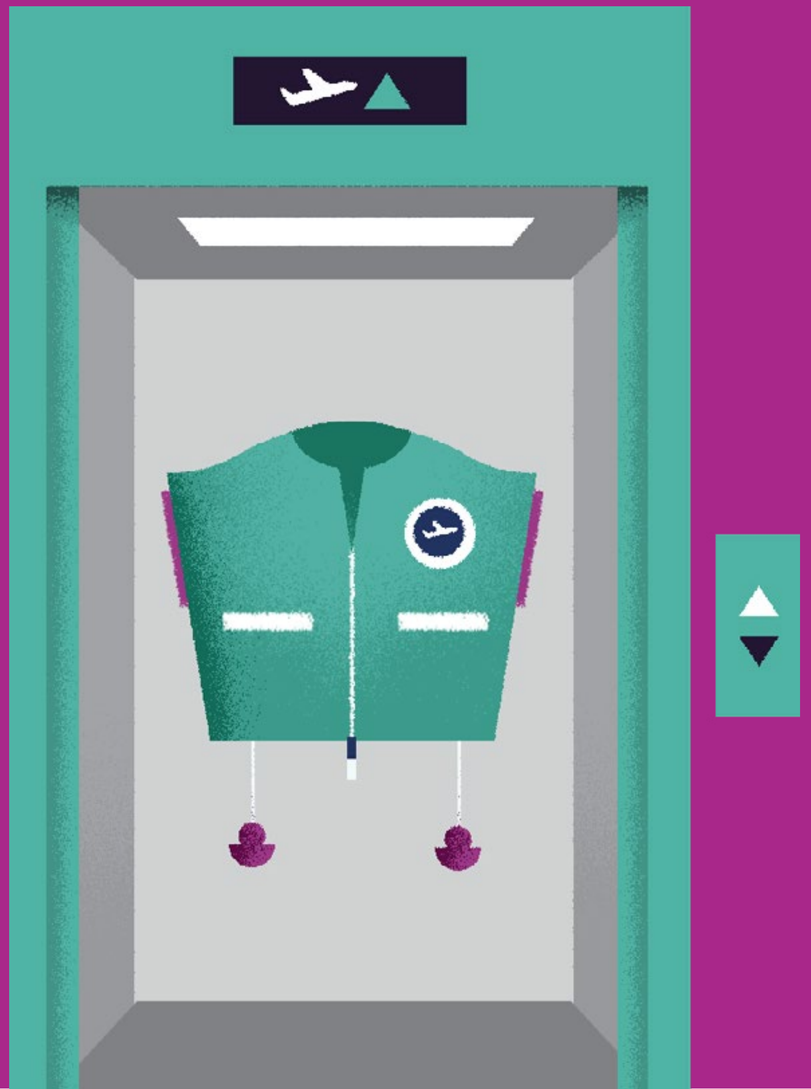


Cybersecurity good practices tailored to Land Transport

Cybersecurity good practices tailored to Maritime Transport

European Commission

Good Practices and Security Measures tailored to Air Transport



Governance to Identify Cybersecurity Threats

Governance: Aviation organisations need clear understandings on emerging threats in order to define management policies and processes to govern their approaches in order to enhance cybersecurity of services and systems in operations, including Information Technology (IT) and Operational Technology (OT).

Good practices for organisations of any size involve:

- Ensuring that senior management levels report cybersecurity concerns to executives and boards, who can make informed decisions on resource allocations.

- Appointing a senior role, accountable for cybersecurity as well as physical security, with overall management responsibilities for the security of Information Technology (IT) and Operational Technology (OT), but without involvement in operations in order to avoid conflicts of interest.

- Defining clearly, roles, responsibilities, competences, and clearances related to cybersecurity and communicating and agreeing on them with relevant personnel, in particular, for members of Computer Emergency Response Teams (CERTs).

- Ensuring cybersecurity governance throughout the entire security supply service chain, including both physical and digital interfaces, from technology manufacturers and installers to security providers.

- Agreeing on activities and controls, including shared responsibilities, to manage cybersecurity risks, and ensuring that these responsibilities are sustained throughout the lifetime (e.g. by service agreements) of security solutions and services.

- Defining governance mechanisms (e.g. policies) in order to comply with obligations drawn from relevant regulations and directives such as, for example, Regulation 2018/1139 on common rules in the field of civil aviation and Commission Implementing Regulation 2017/373 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight as well as the NIS Directive (EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems).

Examples of services and systems in air transport:
Examples of IT are those accessible to employees (e.g. personal computers, mobile phones, office peripherals, etc.) as well as passengers (e.g. public Wi-Fi routers and connections, etc.). Examples of OT are Supervisory Controls and Data Acquisition (SCADA) systems, heating, ventilation, and air conditioning (HVAC) systems, security checkpoints for cabin baggage, baggage handling systems (BHS), access control, monitoring, surveillance, alarm response, screening technology, airfield lighting control systems, radar systems and sensors, Global Positioning Systems (GPS) systems, Air Traffic Management (ATM) systems, Communication, Navigation and Surveillance systems (CNS), Aeronautical Information Systems, Meteorological Systems, Security Operation Centre Systems, airline on-board systems, and others.

Identify Cybersecurity Threats

Risk Management: Aviation organisations need to take appropriate steps to identify, assess, and understand cybersecurity risks to the network and information systems supporting the operations of essential functions.

This requires an overall organisational approach of risk management, which involves:

- *Ensuring a clear overview over the various hardware and software systems deployed for delivering different services. In the context of aviation, such systems involve Information Technology (IT) as well as Operational Technologies (OT).*

- *Performing **cybersecurity risk assessments**, which take into account emerging threats, known vulnerabilities, and operational data in relation to the systems in scope. Organisations such as the European Air Traffic Management Computer Emergency Response Team (EATM-CERT) and the Aviation Information Sharing and Analysis Centre (A-ISAC) may provide insights on threats targeting air transport.*

- *Ensuring that the risk assessments also cover the risks related to personnel daily activities (e.g. social media usage, personal device usage, data processing, information sharing, etc.).*

- *Identifying and implementing risk treatment measures and plans to mitigate cybersecurity risks.*

- *Implementing a comprehensive **Information Security Management System** (ISMS) and a **Privacy Information Management System** (PIMS) aligned with other management systems. Such management systems (i.e. ISMS and PIMS) involve implementing security (as well as data protection and privacy) controls in order to mitigate and prevent emerging threats affecting security of aviation services and systems (including their data).*

- *Taking into account any constraints concerned with **asset management and resource planning** (that is, constraints that may affect the delivery, maintenance and support of critical systems for operations of essential functions in air transport).*

Examples of risk management frameworks: Different frameworks (e.g. standards in the ISO/IEC 27000 family, NIST cybersecurity framework, MITRE ATT&CK Framework, BSI IT-Grundschutz, etc.) may inform and underpin a tailored risk management approach for air transport. International organisations such as IATA and ICAO provide guidance for cybersecurity risk assessments. ENISA, EASA, EUROCONTROL, and Airports Council International (ACI) among others highlight good practices for securing airports, air traffic management providers, and other aviation organisations. SESAR Joint Undertaking coordinates and concentrates all EU research and development (R&D) activities in Air Traffic Management covering also aspects of safety as well as security.

Protect against Cybersecurity Threats

Organisations in air transport should implement adequate and proportionate security measures in order to protect their networks and information systems – including Information Technology (IT) and Operational Technology (OT) from cyber-attacks Security measures include:

- ***Security Policies and Processes:*** *defining, implementing, communicating, and enforcing appropriate policies and processes, which define an overall approach to securing systems and data that support operations of essential functions in aviation. Such security policies (e.g. password and storage policies) and procedures should also cover patches and vulnerability managements of hardware and software systems (including IT and OT), Incident Management, System and Network protection.*

- ***Identity and Access Management:*** *understanding, documenting, and managing access to networks and information systems (including IT and OT) supporting the operations of essential functions in air transport. Users (or automated functions) that can access data or systems are appropriately verified, authenticated, and authorised. This should take into account also the different roles and responsibilities for regular and privileged accounts.*

- ***Data and System Security:*** *protecting data (stored and transmitted electronically), critical networks and information systems (including IT and OT) from cyber-attacks. Taking into account a risk driven approach, organisations should implement security measures to effectively limit opportunities for attackers to compromise data, networks, and systems. These security measures should also include the adoption of encryption and secure communication protocols in order to protect data at rest and in transit from cybersecurity threats resulting in man-in-the-middle attacks. Furthermore, it is necessary to combine such measures with physical security measures in order to protect access to systems (e.g. systems should be located in confined rooms with restricted access).*

- ***Resilience of Networks and Systems:*** *building resilience of networks and systems (including IT and OT) by designing and implementing them (and their operational procedures) in order to resist and mitigate the impact of cyber-attacks. Examples of design and implementation solutions enhancing resilience are: formally verified critical functions, redundancy of systems and networks, segregation of networks (in particular, segregation of IT and OT), multi-layer security measures, and many others. Note that from an information security viewpoint, security domains implementing network and system segregations may provide a suitable security solutions. However, operational needs (e.g. maintenance activities, data transfers, etc.) of systems may require bypassing or connecting different security domains (e.g. segregated systems and networks), including connecting IT and OT.*

Detect Cybersecurity Threats

Organisations should ensure that security measures remain effective, and detect any cybersecurity events affecting or with the potential to affect security controls as well as essential services and systems. In order to detect cybersecurity threats, relevant security measures are:

- ***Security Monitoring:*** *monitoring the security status of networks and information systems – including Information Technology (IT) and Operational Technology (OT) – supporting operations of essential functions in air transport services. In order to support security monitoring, data taken into account are, for example:*

  - *security logs*
  - *virus detection logs*
  - *intrusion detection logs*
  - *identification, authentication, and authorisation logs*
  - *system and service logs*
  - *network traffic logs*
  - *data processing logs*

- ***Security Event Discovery:*** *detecting malicious activities (that is, security events) affecting or with the potential to affect the security of networks and information systems (including IT and OT) supporting operations of essential functions in air transport services.*

These measures may require adopting specific technologies (e.g. Security Information and Event Management, Intrusion Detection System, Intrusion Prevention System, etc.) and setting up a SOC (Security Operations Centre) or equivalent. That is, developing means to detect, analyse, respond, and recover from cyber-attacks locally.

National Computer Security Incident Response Teams (CSIRTs), sectorial CERTs (e.g. the European Air Traffic Management Computer Emergency Response Team EATM-CERT) of EUROCONTROL), commercial CERTs of Airlines, and the Aviation Information Sharing and Analysis Centre (A-ISAC) may provide Cyber Threat Intelligence (CTI) informing security monitoring and discovery.

Response and recovery planning

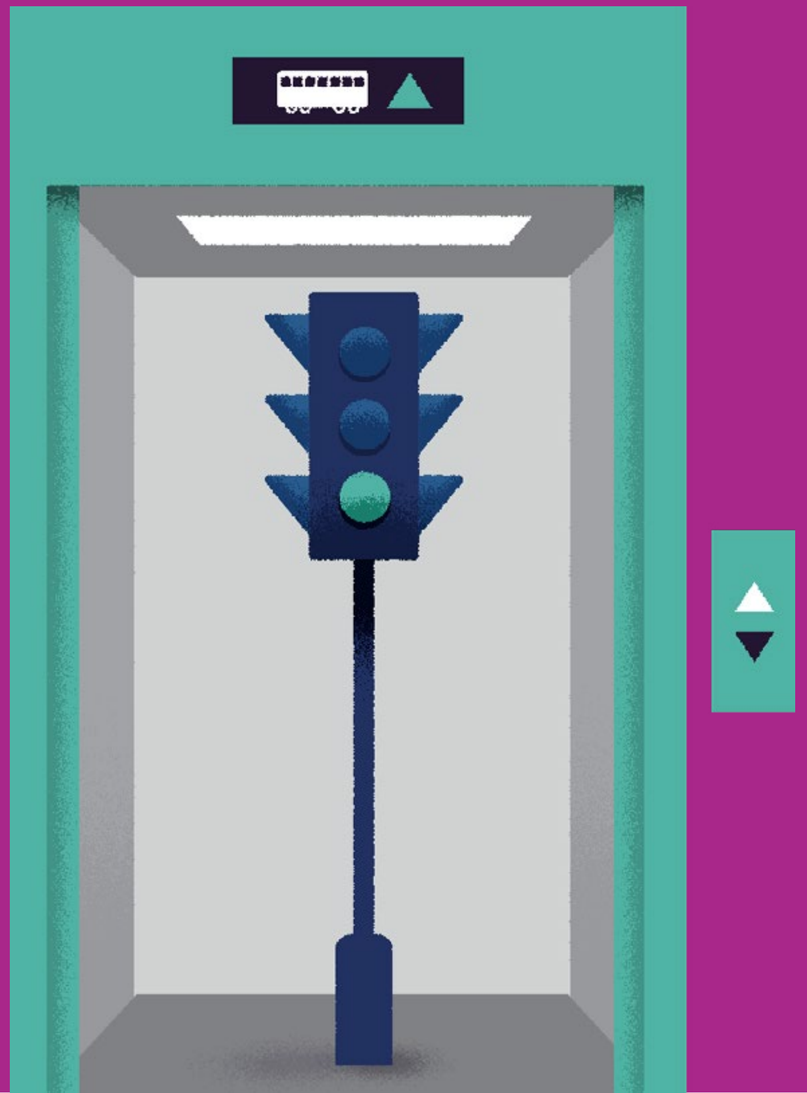
Organisations should define, implement, and test incident management procedures, which intend to ensure business continuity of services and systems in the event of cybersecurity incidents. Mitigation measures intend to contain or limit the impact of cybersecurity incidents.

Response and recovery planning should take into account security measures, mitigating the impact of specific cybersecurity attacks, such as:

- *Coordination and collaboration with National CSIRTs, (public and commercial) CERTs and ISACs during cybersecurity incidents, coordination of incidents, and crises at Pan-European level.*
- *Information sharing with other organisations, including providers in the supply chain of aviation services.*
- *Conducting periodic **cyber-attack exercises** (table top coordination as well as technical) for assessing security measures and procedures as well as organisation resilience to deal with cyber incidents.*
- *Access to archived or backup storage locations in case of compromised integrity and availability of data storages.*
- ***Security playbooks** with detailed procedures for managing cybersecurity incidents and bringing back services and systems to normal operational conditions.*
- *Network traffic redirections to redundant services during denial of service attacks.*
- *Manual procedures for operating with services and systems in degraded operational modes.*
- *Define procedures in order to deal with data breaches, including procedures for dealing with data breaches affecting personal data in compliance with the General Data Protection Regulation (GDPR) and any other relevant sectorial regulation or directive.*
- *Acquire **cyber insurance** in order to outset partially the risk associated with severe cyber incidents.*
- *Contract an incident response retainer with one or more specialised firm(s) for extra capacity and expertise.*
- *Define procedures for **information sharing of cybersecurity incidents** with relevant stakeholders, including procedures for incident notification in compliance with the NIS Directive (EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union).*

European Commission

Good Practices and Security Measures tailored to Land Transport



Governance to Identify Cybersecurity Threats

Governance: Organisations in land transport (rail and road) need clear understandings on emerging threats in order to define management policies and processes to govern their approaches in order to enhance cybersecurity of services and systems in operations, including Information Technology (IT) and Operational Technology (OT).

Good practices for organisations of any size involve:

- *Ensuring that senior management levels report cybersecurity concerns to executives and boards, who can make informed decisions on resource allocations.*

- *Appointing a senior role, accountable for cybersecurity as well as physical security, with overall management responsibilities for the security of Information Technology (IT) and Operational Technology (OT), but without involvement in operations in order to avoid conflicts of interest.*

- *Defining clearly, roles, responsibilities, competences, and clearances related to cybersecurity and communicating and agreeing to them with relevant personnel. This is necessary, in particularly, for members of Computer Emergency Response Teams (CERTs).*

- *Ensuring cybersecurity governance throughout the entire security supply service chain, including both physical and digital interfaces, from technology manufacturers and installers to security providers.*

- *Agreeing on activities and controls, including shared responsibilities, to manage cybersecurity risks, and ensuring that these responsibilities are sustained throughout the lifetime (e.g. by service agreements) of security solutions and services.*

- *Defining governance mechanisms (e.g. policies) in order to comply with obligations drawn from relevant regulations and directives. This encompasses a broad set of policies covering the specific transport modes as well as different types of stakeholders (e.g. including manufacturers of vehicles and rail systems) as well as the NIS Directive (EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems).*

Examples of services and systems in land transport:
Examples of IT are those accessible to employees (e.g. personal computers, mobile phones, office peripherals, etc.) as well as passengers (e.g. public Wi-Fi routers and connections, etc.). Examples of OT are Supervisory Controls and Data Acquisition (SCADA) systems, heating, ventilation, and air conditioning (HVAC) systems, Global Positioning Systems (GPS) systems, access control, monitoring, surveillance, alarm response, and screening technology. Specific systems for rail transport are, for example: operational (control and command systems) including signalling systems, the European Rail Traffic Management System (ERTMS), on-train systems, maintenance systems, and others.

Identification of Cybersecurity Threats

Risk Management: Land transport organisations need to take appropriate steps to identify, assess, and understand cybersecurity risks to the network and information systems supporting the operations of essential functions. This requires an overall organisational approach of risk management, which involves:

- *Ensuring a clear overview over the various hardware and software systems deployed for delivering different services. In the context of land transport, such systems involve Information Technology (IT) as well as Operational Technologies (OT).*

- *Performing cybersecurity risk assessments, which should take into account emerging threats, known vulnerabilities, and operational data in relation to the systems in scope. Examples of systems in the land transport modes are: payment systems, network and communication systems (e.g. internet, radio communication, WiFi, etc.), on-board equipment, operational control centres, identity management systems, safety systems, and others. For rail infrastructures, examples of systems are: rolling stock, operation and traffic management subsystems, control command, and signalling on-board and trackside subsystems, and others.*

- *Ensuring that risk assessments also cover the risks related to personnel daily activities (e.g. social media usage, personal device usage, data processing, information sharing, etc.).*

- *Identifying and implementing risk treatment measures and plans to mitigate cybersecurity risks. Such as implementing a comprehensive **Information Security Management System** (ISMS) and a **Privacy Information Management System** (PIMS), aligned with other management systems. Such management systems (i.e. ISMS and PIMS) involve implementing security (as well as data protection and privacy) controls in order to mitigate and prevent emerging threats affecting security of land transport services and systems (including their data).*

- *Taking into account any constraints concerned with **asset management and resource planning** (that is, constraints that may affect the delivery, maintenance, and support of critical systems for operations of essential functions in land transport).*

Examples of risk management frameworks:
Different frameworks (e.g. standards in the ISO/IEC 27000 family, NIST cybersecurity framework, MITRE ATT&CK Framework, BSI IT-Grundschutz, etc.) may inform and underpin a tailored risk management approach for road and rail transport. Organisations such as ENISA defines good practices for cybersecurity of smart-cars and intelligent public transport, which inform industry manufacturers and associations (e.g. European Automobile Manufacturers' Association – ACEA). In the rail transport, the European Union Agency for Railways (ERA) defines Technical Specifications for Interoperability (TSIs), which must be met by each subsystem or part of subsystem in order to meet the essential requirements and ensure the interoperability of the railway system of the European Union. Shift2Rail Joint Undertaking is also driving innovation (including cybersecurity) initiatives and projects for the rail transport.

Protect against Cybersecurity Threats

Organisations in land transport should implement adequate and proportionate security measures in order to protect their networks and information systems – including Information Technology (IT) and Operational Technology (OT) from cyber-attacks Security measures include:

- ***Security Policies and Processes:*** *defining, implementing, communicating, and enforcing appropriate policies and processes, which define an overall approach to securing systems and data that support operations of essential functions in land transport modes. Such security policies (e.g. password and storage policies) and procedures should also cover patches and vulnerability managements of hardware and software systems (including IT and OT), Incident Management, System and Network protection.*

- ***Identity and Access Management:*** *understanding, documenting and managing access to networks and information systems (including IT and OT) supporting the operations of essential functions in land transport modes. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised. This should take into account also the different roles and responsibilities for regular and privileged accounts.*

- ***Data and System Security:*** *protecting data (stored and transmitted electronically), critical networks and information systems (including IT and OT) from cyber-attacks. Taking into account a risk driven approach, organisations should implement security measures to effectively limit opportunities for attackers to compromise data, networks, and systems. These security measures should also include the adoption of encryption and secure communication protocols in order to protect data at rest and in transit from cybersecurity threats resulting in man-in-the-middle attacks. Furthermore, it is necessary to combine such measures with physical security measures in order to protect access to systems (e.g. systems should be located in confined rooms with restricted access). This is very important for those systems that may have an impact on safety of life.*

- ***Resilience of Networks and Systems:*** *building resilience of networks and systems (including IT and OT) by designing and implementing them (and their operational procedures) in order to resist and mitigate the impact of cyber-attacks. Examples of design and implementation solutions enhancing resilience are: formally verified critical functions, redundancy of systems and networks, segregation of networks (in particular, segregation of IT and OT), multi-layer security measures and many others. Note that from an information security viewpoint, security domains implementing network and system segregations may provide a suitable security solutions. However, operational needs (e.g. maintenance activities, data transfers, etc.) of systems may require bypassing or connecting different security domains (e.g. segregated systems and networks), including connecting IT and OT.*

Detect Cybersecurity Threats

Organisations should ensure that security measures remain effective, and detect any cybersecurity events affecting or with the potential to affect security controls as well as essential services and systems. In order to detect cybersecurity threats, relevant security measures are:

- ***Security Monitoring:*** *monitoring the security status of networks and information systems – including Information Technology (IT) and Operational Technology (OT) – supporting operations of essential functions in land transport modes. This is necessary in order to detect potential security threats and to track the ongoing effectiveness of protective security measures. In order to support security monitoring, data taken into account are, for example:*

  - *security logs*
  - *virus detection logs,*
  - *intrusion detection logs*
  - *identification, authentication and authorisation logs*
  - *system and service logs*
  - *network traffic logs*
  - *data processing logs*

- ***Security Event Discovery:*** *detecting malicious activities (that is, security events) affecting or with the potential to affect the security of networks and information systems (including IT and OT) supporting operations of essential functions.*

These measures may require adopting specific technologies (e.g. Security Information and Event Management, Intrusion Detection System, Intrusion Prevention System, etc.) and setting up a SOC (Security Operations Centre) or equivalent. That is, developing means to detect, analyse, respond, and recover from cyber-attacks locally.
National Computer Security Incident Response Teams (CSIRTs), sectorial and commercial CERTs or road and rail operators, and the European Rail Information Sharing and Analysis Centre (ER-ISAC) may provide Cyber Threat Intelligence (CTI) informing security monitoring and discovery.

Response and recovery planning

Organisations should define, implement, and test incident management procedures, which intend to ensure business continuity of services and systems in the event of cybersecurity incidents.

Response and recovery planning should take into account security measures, mitigating the impact of specific cybersecurity attacks, such as:

- *Coordination and collaboration with National CSIRTs, (public and commercial) CERTs and ISACs during cybersecurity incidents, coordination of incidents and crises at Pan-European level.*

- *Information sharing with other organisations, including providers in the supply chain of land transport services.*

- *Conducting periodic **cyber-attack exercises** (table top coordination as well as technical) for assessing security measures and procedures as well as organisations resilience to deal with cyber incidents.*

- *Access to archived or backup storage locations in case of compromised integrity and availability of data storages.*

- ***Security playbooks** with detailed procedures for managing cybersecurity incidents, and bringing back services and systems to normal operational conditions.*

- *Network traffic redirections to redundant services during denial of service attacks.*

- *Manual procedures for operating with services and systems in degraded operational modes.*

- *Define procedures in order to deal with data breaches, including procedures for dealing with data breaches affecting personal data in compliance with the General Data Protection Regulation (GDPR) and any other relevant sectorial regulation or directive.*

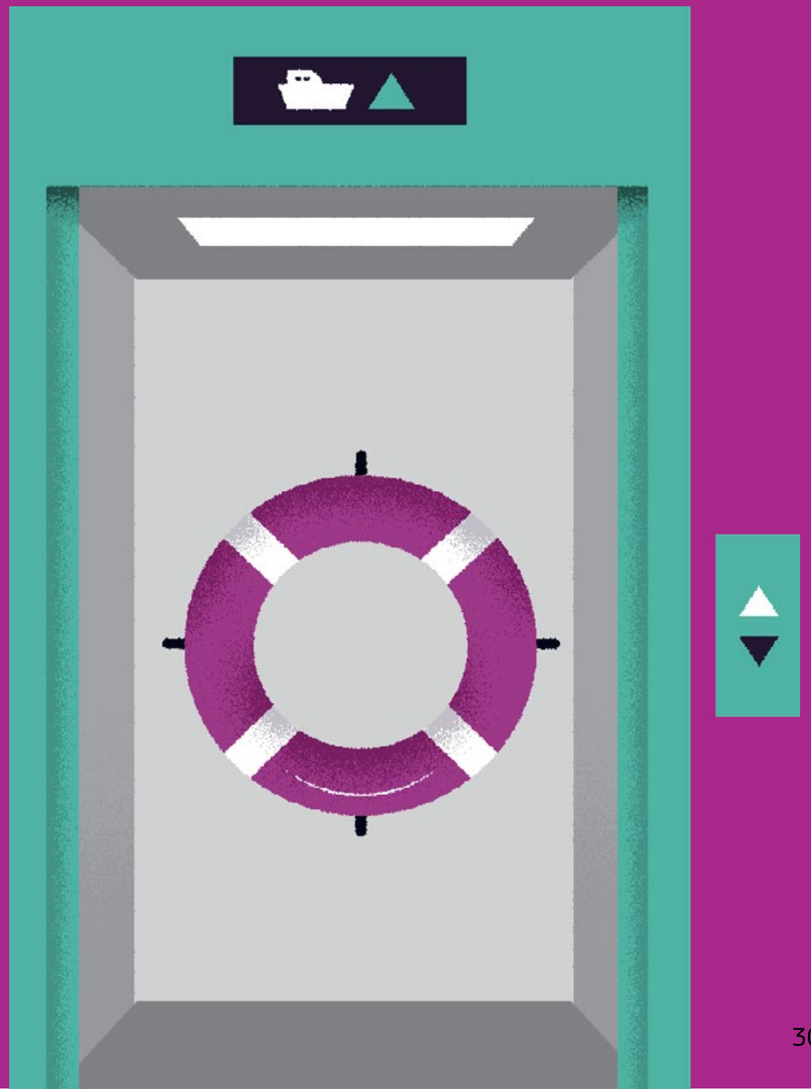
- *Acquire **cyber insurance** in order to outset partially the risk associated with severe cyber incidents.*

- *Contract an incident response retainer with one or more specialised firm(s) for extra capacity and expertise.*

- *Define procedures for information sharing of cybersecurity incidents with relevant stakeholders, including procedures for incident notification in compliance with the NIS Directive (EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union).*

European Commission

Good Practices and Security Measures tailored to Maritime Transport



Identification of Cybersecurity Threats

Governance: Organisations in maritime transport need clear understandings on emerging threats in order to define management policies and processes to govern their approaches in order to enhance cybersecurity of services and systems in operations, including Information Technology (IT) and Operational Technology (OT).

Good practices for organisations of any size involve:

- *Ensuring that senior management levels report cybersecurity concerns to executives and boards, who can make informed decisions on resource allocations.*

- *Appointing a senior role with overall management responsibilities for the security of Information Technology (IT) and Operational Technology (OT). This role should be accountable for cybersecurity as well as physical security.*

- *Defining clearly, roles, responsibilities, competences, and clearances related to cybersecurity, defining levels of authority and lines of communication between, and amongst, shore and shipboard personnel, and agreeing on them with relevant personnel. This is necessary, in particularly, for members of Computer Emergency Response Teams (CERTs). Personnel with roles relating to EU maritime security and safety legislations, such as Port Facility Security Officers, Port Security Officers or Company Security Officers or the Designated Person Ashore (DPA) and the Master on board, should at least be familiar with the cybersecurity measures taken by the organisation.*

- *Ensuring cybersecurity governance throughout the entire security supply service chain, including both physical and digital interfaces, from technology manufacturers and installers to security providers.*

- *Agreeing on activities and controls, including shared responsibilities, to manage cybersecurity risks, and ensuring that these responsibilities are sustained throughout the lifetime (e.g. by service agreements) of security solutions and services.*

- *Defining governance mechanisms (e.g. policies) in order to comply with obligations drawn from relevant regulations and directives, for example, Regulation 2019/1239 establishing a European Maritime Single Window environment (EMSWe), Regulation 725/2004 on enhancing ship and port facility security, Directive 2005/65/EC on enhancing port security, and Regulation (EC) No 336/2006 on the implementation of the International Safety Management (ISM) Code, and Resolution A.741(18) adopting the ISM Code for the Safe Operation of Ships and for Pollution Prevention. In this context, it is also relevant mentioning the Common Information Sharing Environment (CISE), an EU initiative that aims to make European and Member States surveillance systems interoperable to give all concerned authorities access to the classified and unclassified information they need to conduct missions at sea.*

Examples of services and systems in maritime transport: Examples of IT are those accessible to employees (e.g. personal computers, mobile phones, office peripherals, etc.) as well as passengers (e.g. public Wi-Fi routers and connections, etc.). Examples of OT are Supervisory Controls and Data Acquisition (SCADA) systems, heating, ventilation, and air conditioning (HVAC) systems, Global Positioning Systems (GPS) systems, access control, monitoring, surveillance, alarm response, screening technology, on-board navigation systems, SafeSeaNet, bridge systems, cargo handling and management systems, propulsion and machinery management and power control systems, access control systems, passenger servicing and management systems, passenger facing public networks, administrative and crew welfare systems, communication systems, and others.

Risk Management to Identify Cybersecurity Threats

Risk Management: Maritime organisations need to take appropriate steps to identifying, analysing, assessing, and communicating cybersecurity risks, and accepting, avoiding, transferring, or mitigating them to an acceptable level. This requires an overall organisational approach of risk management, which involves:

- *Ensuring a clear overview over the various hardware and software systems deployed for delivering different services. In the context of maritime transport, such systems involve Information Technology (IT) as well as Operational Technologies (OT), and how these systems connect and integrate with the shore side, including public authorities, marine terminals and stevedores.*

- *Identifying and evaluating key ship board operations, which are vulnerable to cyber-attacks, and performing cybersecurity risk assessments (including assessing potential operational impacts and likelihood of occurrence), which should take into account emerging threats, known vulnerabilities, and operational data in relation to the systems in scope. Where appropriate, making the link to security assessments carried out for ships (SSAs), port facilities (PFSAs), and ports (PSAs) as set out by EU maritime security legislation. These identify possible security threats to port infrastructure and security weaknesses. Additionally, maritime organisations such as the International Maritime Organisation (IMO) and maritime ISACs may provide insights on threats targeting maritime transport..*

- *Ensuring that risk assessments also cover the risks related to personnel daily activities (e.g. social media usage, personal device usage, data processing, information sharing, etc.).*

- *Identifying and implementing risk treatment measures and plans mitigating cybersecurity risks. For example, implementing a comprehensive Information Security Management System (ISMS) and a Privacy Information Management System (PIMS), aligned with other management systems such as Safety Management Systems (SMS) in accordance with the International Safety Management (ISM) Code. Such management systems (i.e. ISMS and PIMS) involve implementing security (as well as data protection and privacy) controls in order to mitigate and prevent emerging threats affecting security of maritime services and systems (including their data).*

- *Taking into account any constraints concerned with asset management and resource planning (that is, constraints that may affect the delivery, maintenance and support of critical systems for operations of essential functions in maritime transport). As for assessments, make a cross-reference where appropriate to requirements of the ISM code, Safety management Systems (SMS) and security plans carried out according to EU maritime safety and security legislation.*

Examples of risk management frameworks:
Different frameworks (e.g. the ISM Code or standards in the ISO/IEC 27000 family, NIST cybersecurity framework, MITRE ATT&CK Framework, BSI IT-Grundschutz, etc.) may inform and underpin a tailored risk management approach for maritime transport. The NIST cybersecurity framework has been also tailored to address the cybersecurity of Maritime Bulk Liquids Transfer (MBLT), Offshore Operations, and Passenger Vessel Operations. Similarly, the Baltic and International Maritime Council (BIMCO) has issued “The Guidelines on Cyber Security Onboard Ships” and the International Maritime Organization (IMO) has issued specific “Guidelines on maritime cyber risk management” (MSC-FAL.1/Circ.3). ENISA has conducted several studies concerned with good practices for maritime cybersecurity, in particular, port cybersecurity. EMSA provides services to the maritime community, including cybersecurity awareness trainings. Standards (e.g. IEC 61162-460:2018 on safety and security of maritime navigation and radio communication equipment and systems, ISO 16425:2013 on ships and marine technology, IEC 62443-4-1:2018 on security for industrial automation and control systems, etc.) define also specific security and safety requirements for systems and networks in maritime transport.

Protect against Cybersecurity Threats

Organisations in maritime transport should implement adequate and proportionate security measures in order to protect their networks and information systems – including Information Technology (IT) and Operational Security measures include:

- ***Security Policies and Processes:*** *defining, implementing, communicating, and enforcing appropriate policies and processes, which define an overall approach to securing systems and data that support operations of essential functions in maritime transport. Security measures (including cyber and physical security measures) should be included in relevant plans such as the Safety Management System (SMS) and in the Ship Security Plan (SSP). Such security policies (e.g. password and storage policies) and procedures should also cover patches and vulnerability managements of hardware and software systems (including IT and OT), Incident Management, System and Network protection.*

- ***Identity and Access Management:*** *understanding, documenting, and managing access to networks and information systems (including IT and OT) supporting the operations of essential functions in maritime transport. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised. This should take into account also the different roles and responsibilities for normal and privileged accounts.*

- ***Data and System Security:*** *protecting data (stored and transmitted electronically), critical networks and information systems (including IT and OT) from cyber-attacks. Taking into account a risk driven approach, organisations should implement security measures to effectively limit opportunities for attackers to compromise data, networks and systems. These security measures should also include the adoption of encryption and secure communication protocols in order to protect data at rest and in transit from cybersecurity threats resulting in man-in-the-middle attacks. Furthermore, it is necessary to combine such measures with physical security measures in order to protect access to systems (e.g. systems should be located in confined rooms with restricted access). This is very important for those systems that may have an impact on safety of life (e.g. navigation and radio communication systems of category II and III).*

- ***Resilience of Networks and Systems:*** *building resilience of networks and systems (including IT and OT) by designing and implementing them (and their operational procedures) in order to resist and mitigate the impact of cyber-attacks. Examples of design and implementation solutions enhancing resilience are: formally verified critical functions, redundancy of systems and networks, segregation of networks (in particular, segregation of IT and OT), multi-layer security measures and many others. Note that from an information security viewpoint, security domains implementing network and system segregations may provide a suitable security solutions. However, needs (e.g. maintenance activities, data transfers, etc.) of systems (e.g. Maritime Autonomous Surface Ships – MASS) may require bypassing or connecting different security domains (e.g. segregated systems and networks), including connecting IT and OT.*

Detect Cybersecurity Threats

Organisations should ensure that security measures remain effective, and detect any cybersecurity events affecting or with the potential to affect security controls as well as essential services and systems. In order to detect cybersecurity threats, relevant security measures are:

- ***Security Monitoring:*** *monitoring the security status of networks and information systems – including Information Technology (IT) and Operational Technology (OT) – supporting operations of essential functions in maritime transport services. This is necessary in order to detect potential security threats and to track the ongoing effectiveness of protective security measures. In order to support security monitoring, data taken into account are, for example:*
  - *security logs*
  - *virus detection logs,*
  - *intrusion detection logs*
  - *identification, authentication and authorisation logs*
  - *system and service logs*
  - *network traffic logs*
  - *data processing logs*

- ***Security Event Discovery:*** *detecting malicious activities (that is, security events) affecting or with the potential to affect the security of networks and information systems (including IT and OT) supporting operations of essential functions in maritime transport services.*

These measures may require adopting specific technologies (e.g. Security Information and Event Management, Intrusion Detection System, Intrusion Prevention System, etc.) and setting up a SOC (Security Operations Centre) or equivalent. That is, developing means to detect, analyse, respond and recover from cyber-attacks locally.

National Computer Security Incident Response Teams (CSIRTs), sectorial CERTs and commercial CERTs of maritime operators, maritime ISACs may provide Cyber Threat Intelligence (CTI) informing security monitoring and discovery.

Response and recovery planning

Organisations should define, implement, and test incident management procedures, which intend to ensure business continuity of services and systems in the event of cybersecurity incidents.
Response and recovery planning should take into account security measures, mitigating the impact of specific cybersecurity attacks, such as:

- *Network traffic redirections to redundant services during denial of service attacks.*
- *Manual procedures for operating with services and systems in degraded operational modes.*
- *Establishing programmes for drills and exercises (e.g. table top coordination, technical and response drills) to respond to cyber-attacks and emergency situations as well as to assess security measures, procedures and organisational resilience to deal with cyber incidents.*
- *Access to archived or backup storage locations in case of compromised integrity and availability of data storages.*
- *Coordination and collaboration with National CSIRTs, (public and commercial) CERTs and ISACs during cybersecurity incidents, coordination of incidents and crises at Pan-European level.*
- *Information sharing with other organisations, including providers in the supply chain of services in maritime transport.*
- *Security playbooks with detailed procedures for managing cybersecurity incidents, and bringing back services and systems to normal operational conditions.*
- *Define procedures in order to deal with data breaches, including procedures for dealing with data breaches affecting personal data in compliance with the General Data Protection Regulation (GDPR) and any other relevant sectorial regulation or directive.*
- *Acquire cyber insurance in order to outset partially the risk associated with severe cyber incidents.*
- *Contract an incident response retainer with one or more specialised firm(s) for extra capacity and expertise.*
- *Define procedures for information sharing of cybersecurity incidents (including non-conformities, accidents and hazardous situations) with relevant stakeholders, including procedures for incident notification in compliance with the NIS Directive (EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union).*