CYBERSECURITY IN RAILWAYS – POLICY DEVELOPMENTS

ENISA-ERA CONFERENCE

16 March 2021

Rail cybersecurity: Legislative framework

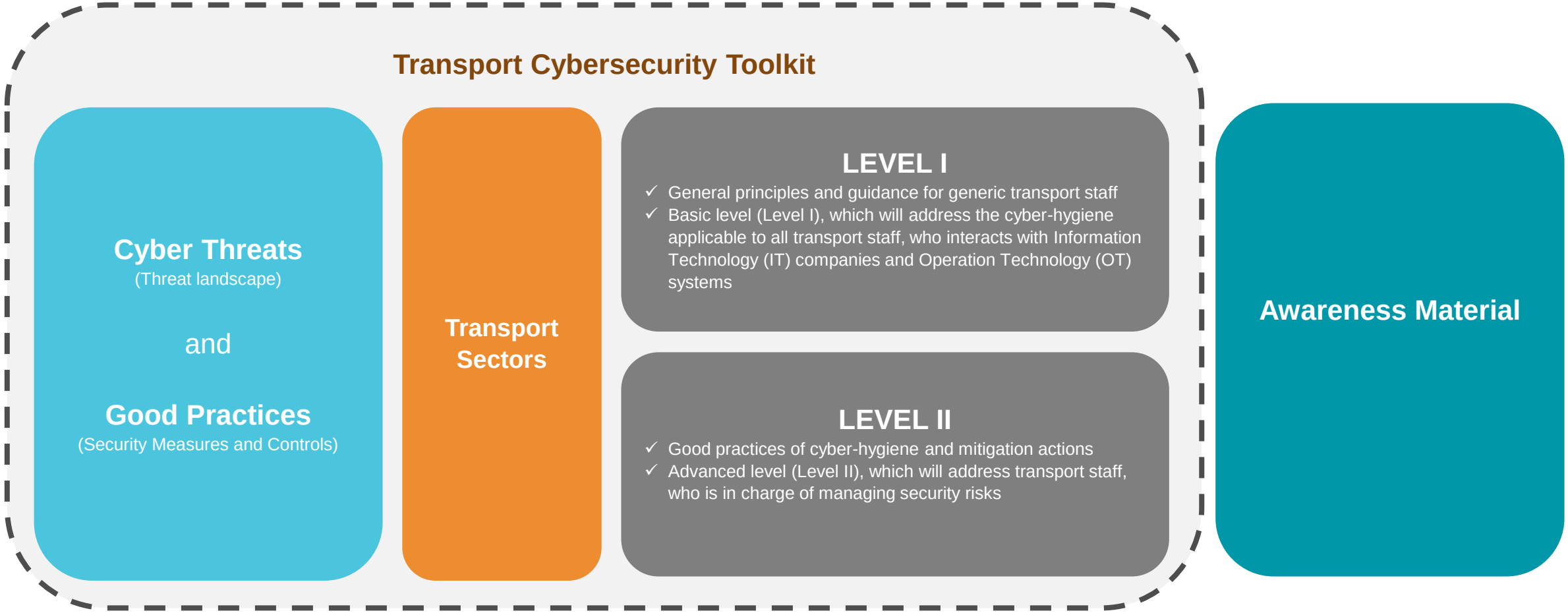
- Rail transport is covered by the Directive on Security of Networks and Information Systems (NIS Directive) and its proposed revision
  - By December 2020, 73 Operators of Essential Services had been designated in the rail sector
- In October 2019, the Commission organised a sectoral workshop to discuss NIS implementation:
  - NIS was found to be an appropriate framework for rail; although differences of implementation among Member States were noted
  - Time to be given for ongoing sectoral initiatives to deliver (in particular TS 50701)
  - Importance of cyber-awareness, cyber-skills and exchange of information, etc.

Cybersecurity awareness

- The “human element” tends to be the weakest in the cybersecurity chain…
  - People see cybersecurity as an IT issue only
  - They do not know or do not always adhere to corporate cybersecurity policies
- … And the attackers know how to exploit this vulnerability
- DG MOVE’s contribution: the development of a **Transport Cybersecurity Toolkit**
  - Provide transport staff with a knowledge base of good principles of cyber-hygiene
  - Strengthen cyber-awareness in transport companies

European Commission

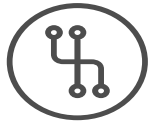
Architecture of the cybersecurity toolkit



European Commission

Cybersecurity toolkit: Level I

- ‘Basic level’
- Targeted audience: all transport staff across all modes
- Four main threats are identified:



Top Threat no.1 – Malware Diffusion
The dissemination of a software designed for intentionally damaging computers, servers, clients or networks.

Top Threat no.2 – Denial of Service
Flooding the targeted host or network with traffic until it crashes preventing users from accessing, due to the actions of a malicious cyber threat actor.

Top Threat no.3 – Unauthorised Access and Theft
Unauthorised access, appropriation and exploitation of critical assets

Top Threat no.4 – Software manipulation
The process of changing software data for malicious reasons.

European Commission

European Commission

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).*

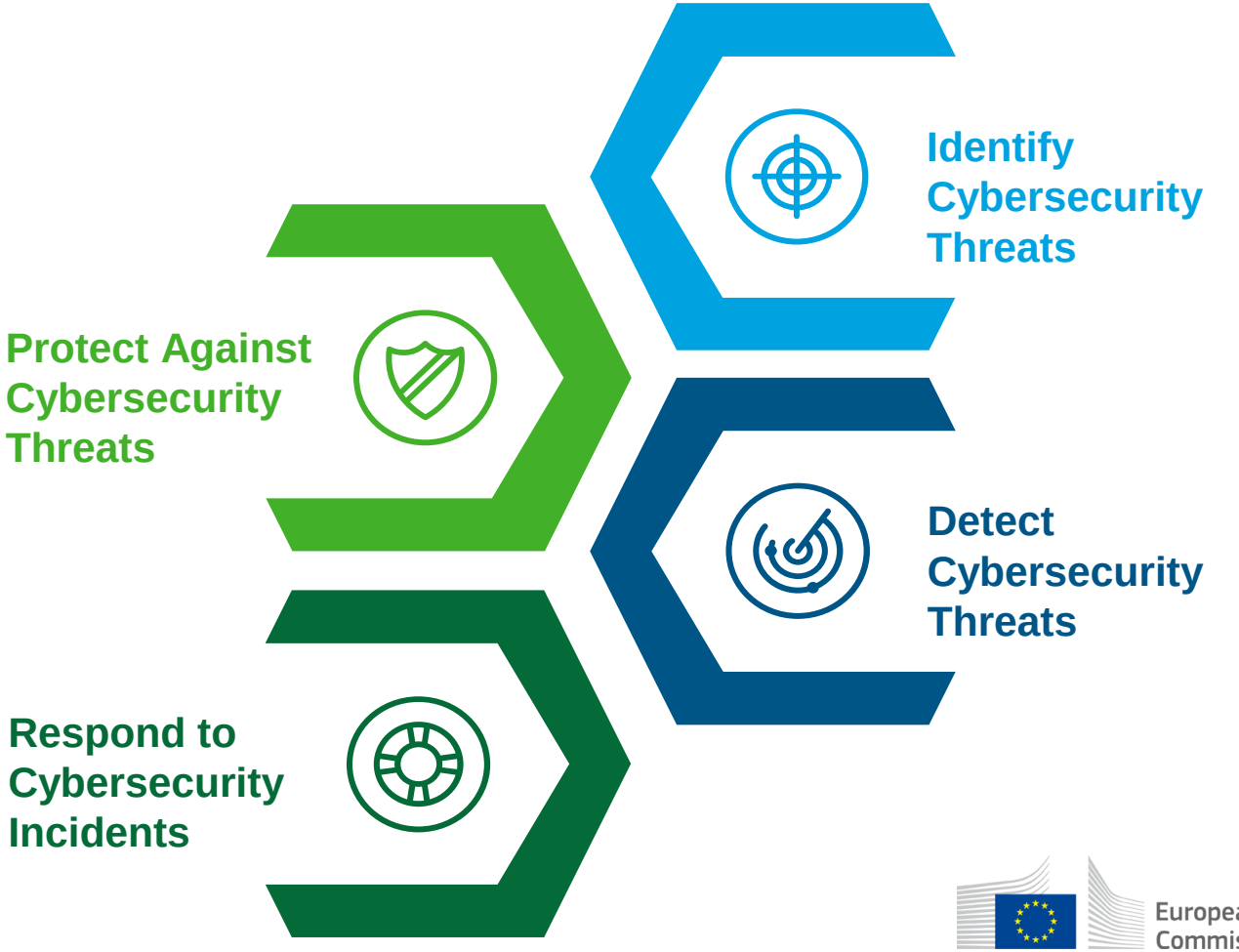
- *Avoid using privileged (e.g. administrator-level) accounts and credentials for regular activities and operations.*

- *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.*

Cybersecurity toolkit: Level II

- ‘Advanced level’
- Modules specific to different modes of transport: aviation, maritime and land
- Targeted audience: (cyber)security practitioners
- Identify, Protect, Detect, Respond



European Commission

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).*

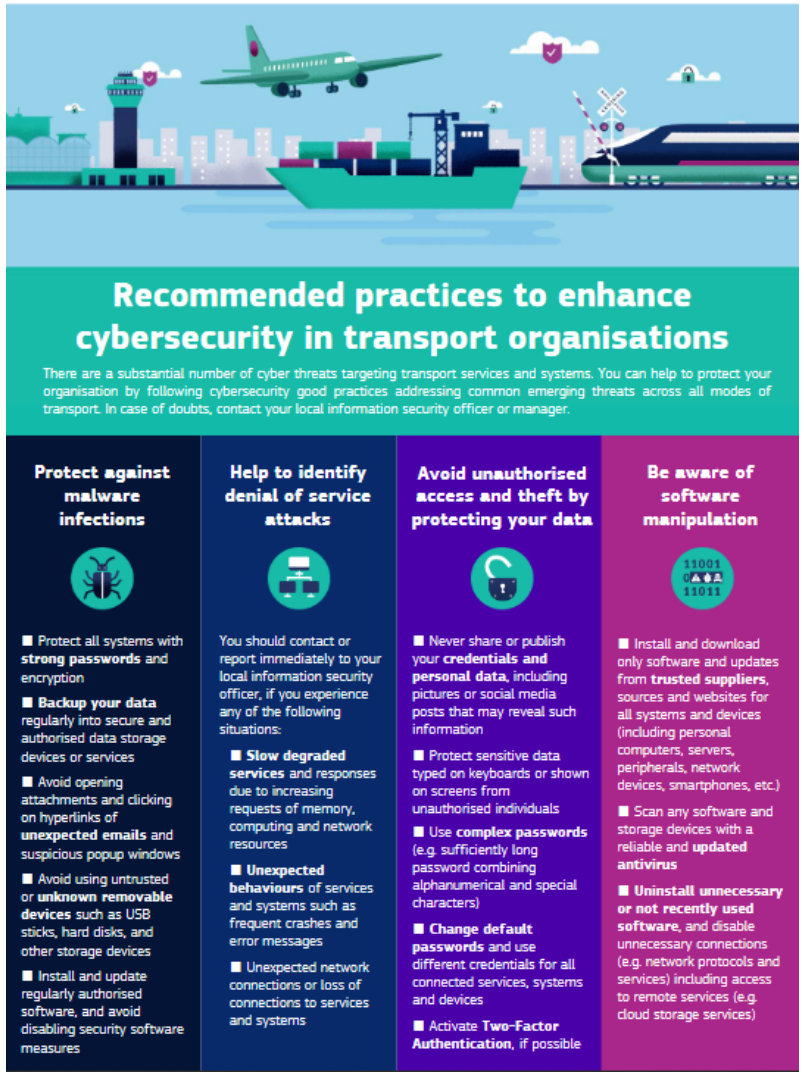
- *Ensuring cybersecurity governance throughout the entire security supply service chain, including both physical and digital interfaces, from technology manufacturers and installers to security providers.*

- *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).*

Cybersecurity toolkit: status & next steps

- Toolkit published on 16 December 2020 (available here) together with an awareness poster (available here)
- Diffusion through the Commission groups on transport security
- Translations planned for 2021 so as to facilitate widest dissemination possible



Thank you

alexis.perier@ec.europa.eu

European Commission