

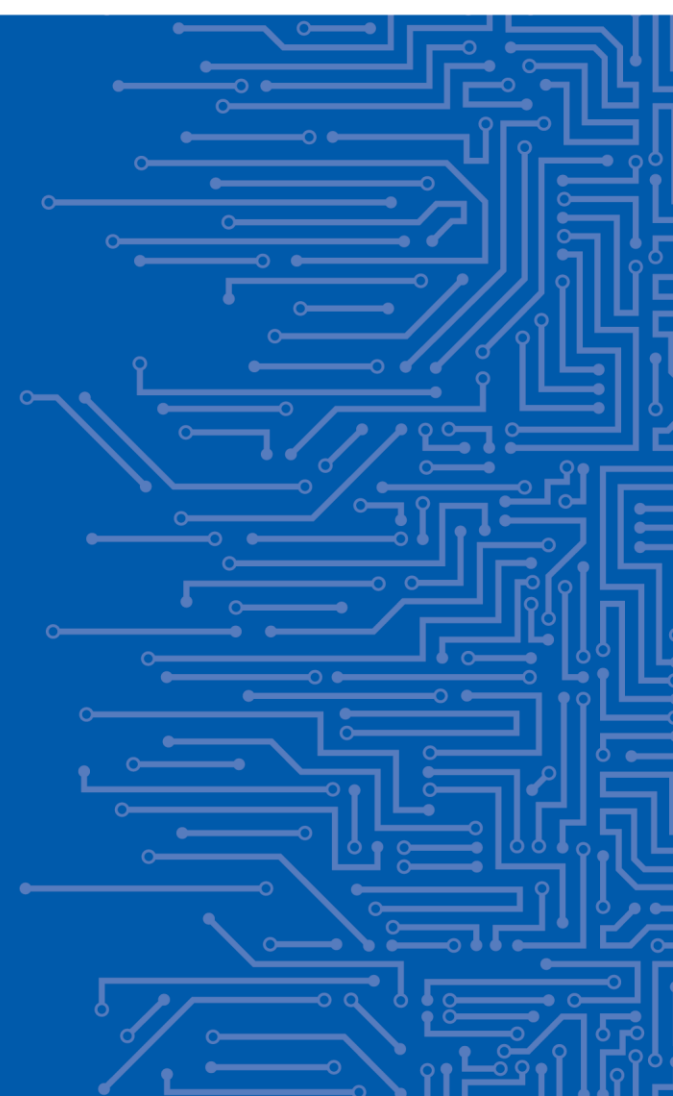


EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HIGHLIGHTS ON EU CYBERSECURITY POLICY FOR RAILWAYS

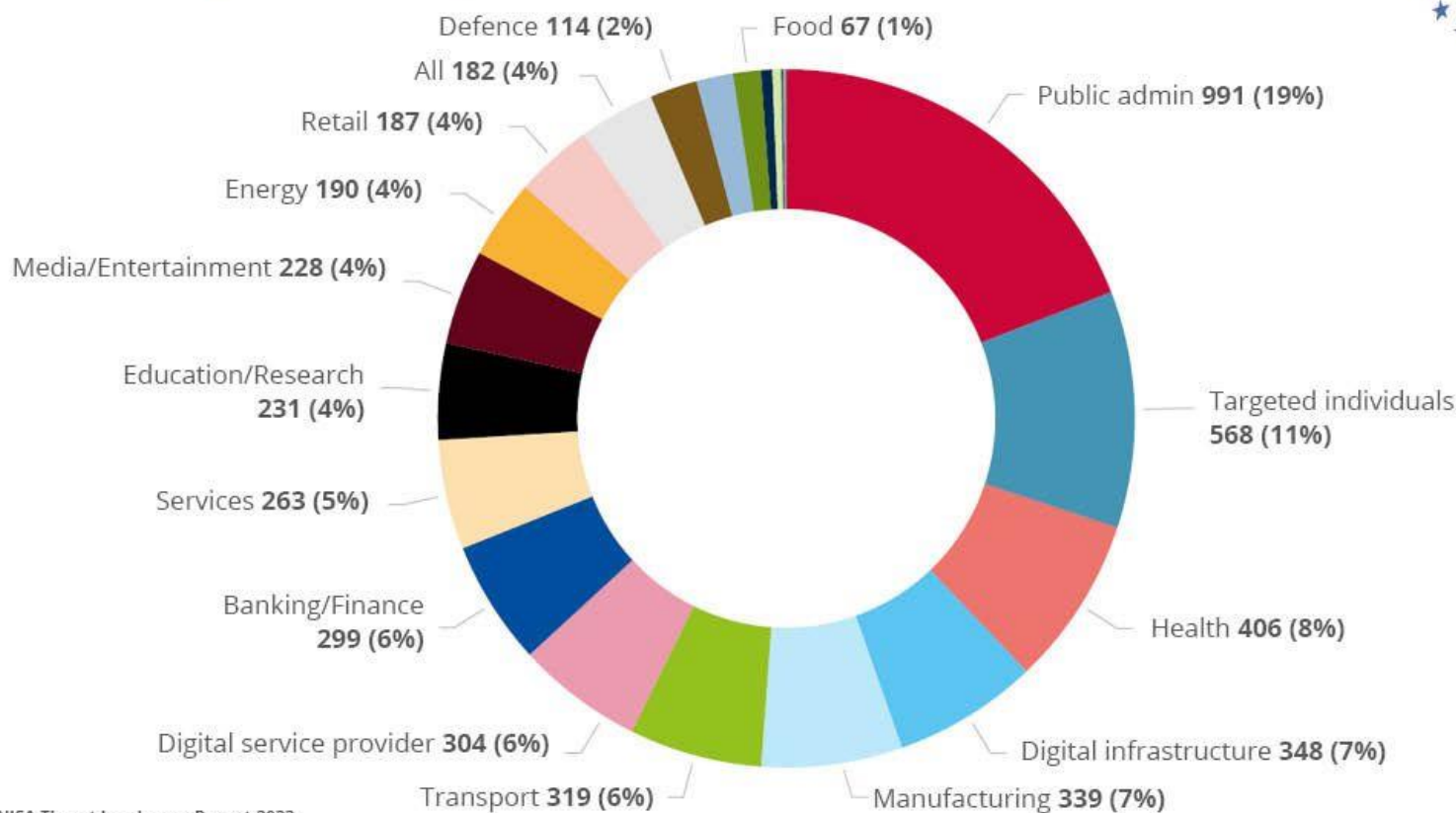
Evangelos Ouzounis

08 | 11 | 2023



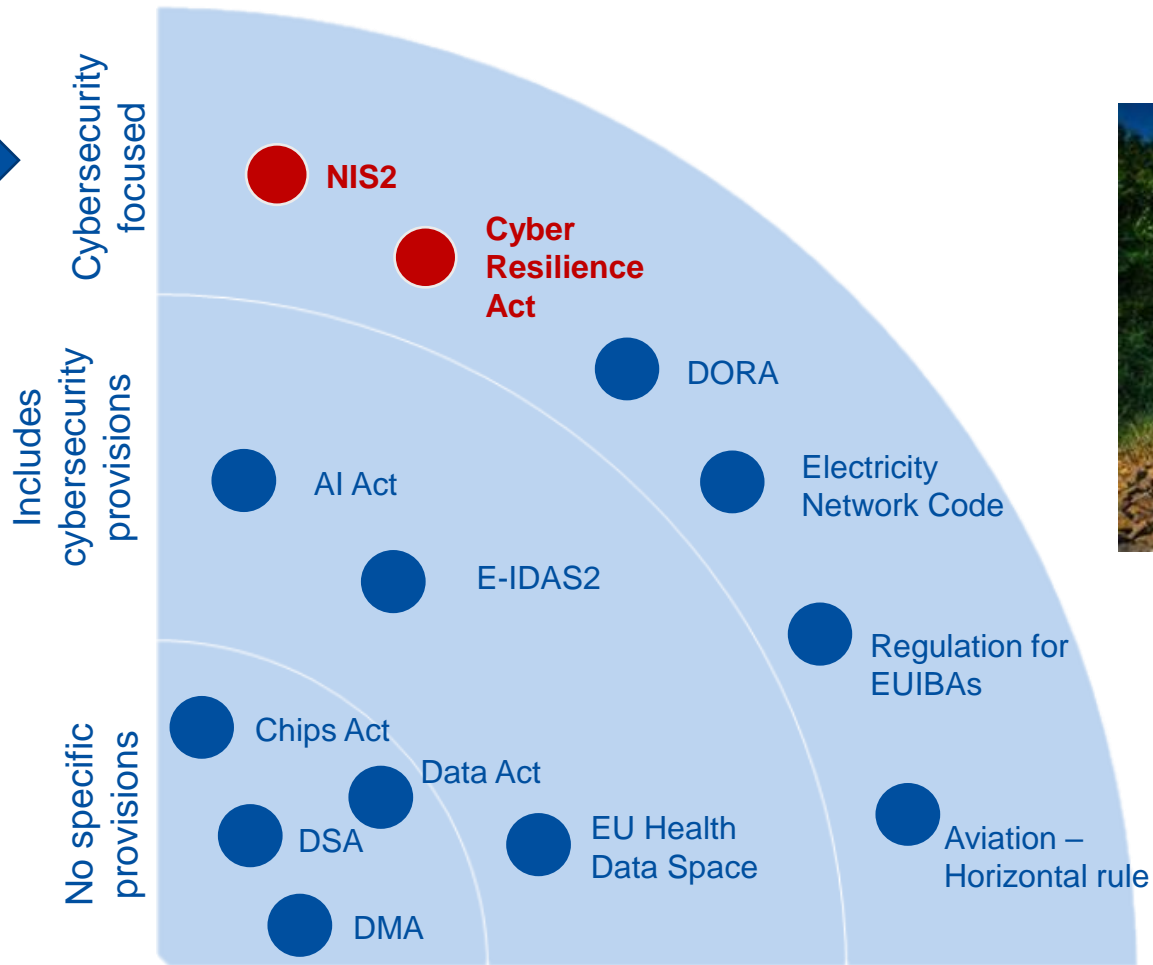
RAILWAYS UNDER THREAT

TARGETED SECTORS PER NUMBER OF INCIDENTS (JULY 2022 – JUNE 2023)







Source: ENISA Threat Landscape Report 2023.

NEW OR REVISED POLICY AREAS



NIS2: SECTORS

Sector	Subsector	Large	Medium	Small, micro
Transport 	Rail (IM and RU); <i>! Public transport: only if identified as Critical entities under CER Directive</i>	Essential	Important	-
Digital infrastructure 	Qualified trust service providers	Essential	Essential	Essential
	Non-qualified trust service providers	Essential	Important	Important
	DNS service providers (excluding root name servers)	Essential	Essential	Essential
	TLD name registries	Essential	Essential	Essential
	Providers of public electronic communications networks	Essential	Essential	Important
	Internet exchange point providers	Essential	Important	-
	Cloud computing service providers	Essential	Important	-
	Data centre service providers	Essential	Important	-
Content delivery network providers	Essential	Important	-	
ICT-Service Management 	Managed service providers, Managed security service providers	Essential	Important	-
Manufacturing 	Computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment	Important		-

https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

NIS2: MAIN PILLARS

Member State Capabilities

- National authorities
- National strategies
- Coordinated Vulnerability Disclosure frameworks
- Crisis management frameworks

Risk Management

- **Accountability for top management for non compliance**
- **Security measures for companies**
- **Incident notifications for companies**

Company responsibilities

Cooperation and Information Exchange

- Cooperation group
- CSIRTs network
- CyCLONE
- CVD and European vulnerability registry
- Peer reviews
- Biennial ENISA cybersecurity report
- EU registry for some entities (e.g. DNS service providers, Top Level Domain Name providers, cloud providers)

https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf



NIS2: RISK MANAGEMENT MEASURES

Risk analysis, information system security policies

Incident handling

Business continuity

Supply chain security

Security in network and information systems

Assessment of the effectiveness of measures

**Basic computer hygiene practices
Training**

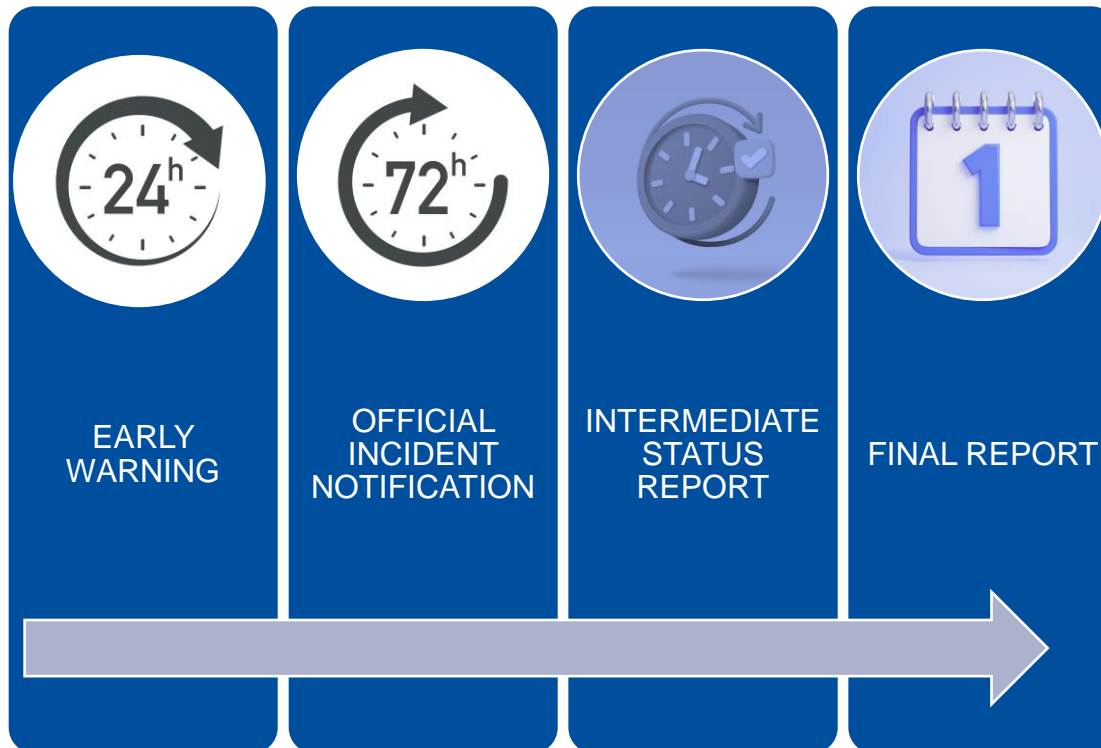
Use of cryptography

**Human resources security
Access control policies
Asset management**

**Multi-factor authentication
Secured voice, video and text communications
Secured emergency communications systems**

INCIDENT NOTIFICATION

- Notifications shall be made to the relevant national competent authority or the CSIRT in phases.
- Where appropriate, entities shall notify the recipients of their services of significant incidents.



https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

MANAGEMENT RESPONSIBILITIES



Approve the adequacy of the cybersecurity risk management measures taken by the entity



Supervise the implementation of the risk management measures



Follow training (identify risks and assess cybersecurity risk management practices and their impact)



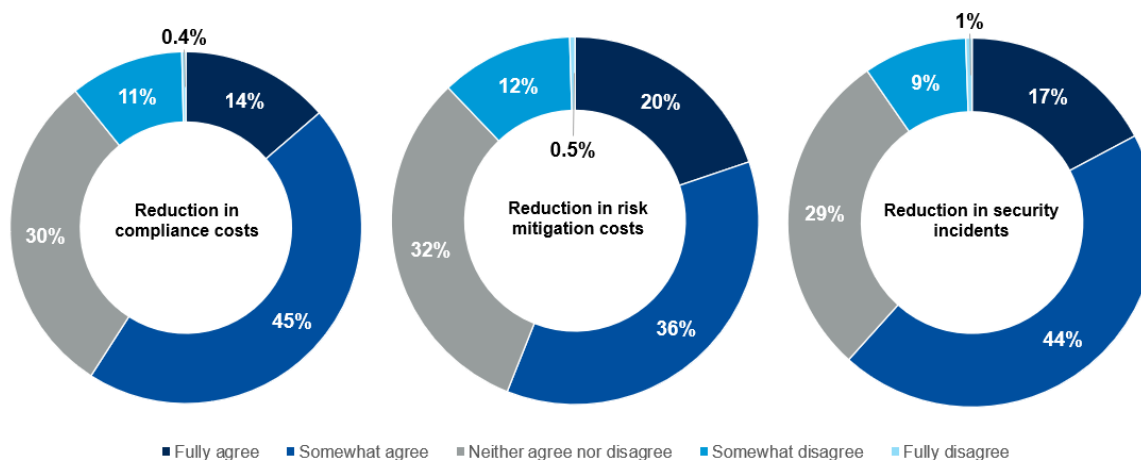
Offer similar training to their employees on a regular basis



Be accountable for the non-compliance

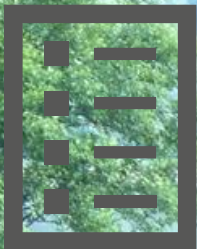
CYBER RESILIENCE ACT - CRA

- **Rules for placing on the market** of products with digital elements to ensure the cybersecurity of these products
- **Essential requirements** for product design, development and production and obligations for economic operators (manufacturers, distributors etc.)
- Essential requirements for vulnerability handling to ensure product **cybersecurity throughout the lifecycle**
- **Rules on market surveillance** and enforcement of requirements



Perceived impact of common requirements

RAILWAY CYBERSECURITY @ ENISA



Policy

- “Build” maturity to the sector
- Applicability of EU policy to the sector
- Cybersecurity Requirements (NIS 2 – TSIs alignment)

Information sharing

- Threat landscapes
- Awareness raising



Cooperation

- Collaboration with COM, national authorities and ERA
- Engagement with industry expert groups (e.g. CENELEC and IEC, LANDSEC and MOVE, EU Rail System Pillar, ISAC, UIC cybersecurity security Platform, CISO Forum)

ERA-ENISA COLLABORATION

- Implementation of NIS2
- Impact of EU certification
- Common safety methods and technical specifications for interoperability

Policy



- Awareness raising
- Skills programmes
- Trainings, exercises
- Events

Capacity and skills



THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 15231
Attiki, Greece

 +30 28 14 40 9711

 info@enisa.europa.eu

 www.enisa.europa.eu

