EUROPEAN UNION AGENCY
FOR CYBERSECURITY

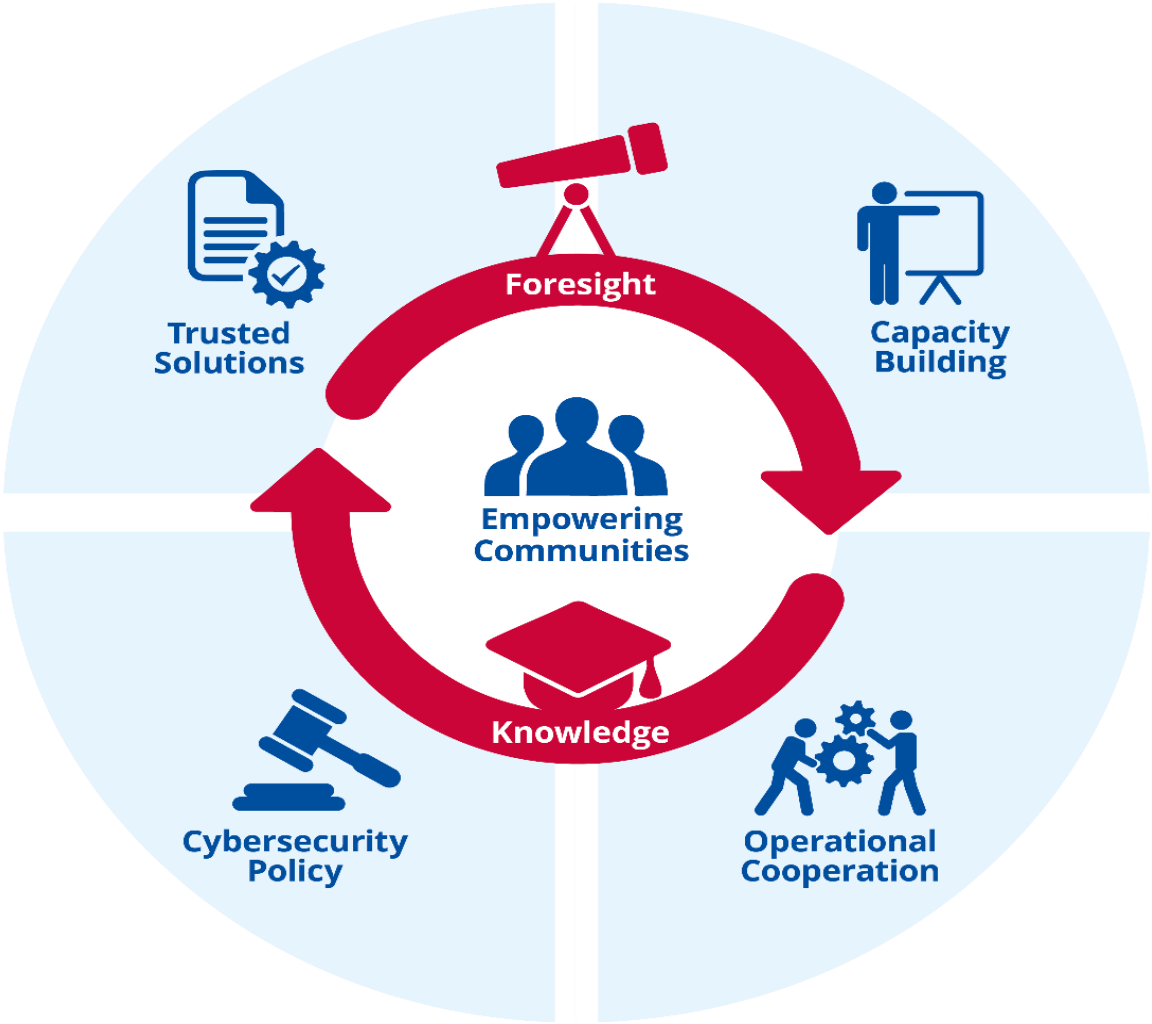
Dimitra Liveri
Marianthi Theocharidou
Secure Infrastructures & Services Unit

13 | 11 | 2020

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



NIS DIRECTIVE

GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

- NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIS-RT)
- NATIONAL NIS STRATEGY
- NATIONAL NIS AUTHORITY

COOPERATION

Increased EU-level cooperation

- EU MEMBER STATES COOPERATION GROUP (STRATEGIC)
  - EU MEMBER STATES; EUROPEAN COMMISSION; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY
- EMERGENCY TEAMS (CSIRTS) NETWORK (OPERATIONAL)
  - EU MEMBER STATES; CERT-EU; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

- SECURITY MEASURES
- NOTIFICATION OF MAJOR INCIDENTS

ENISA WORK FOR THE RAILWAY SECTOR

Support Operators of Rail Essential Services

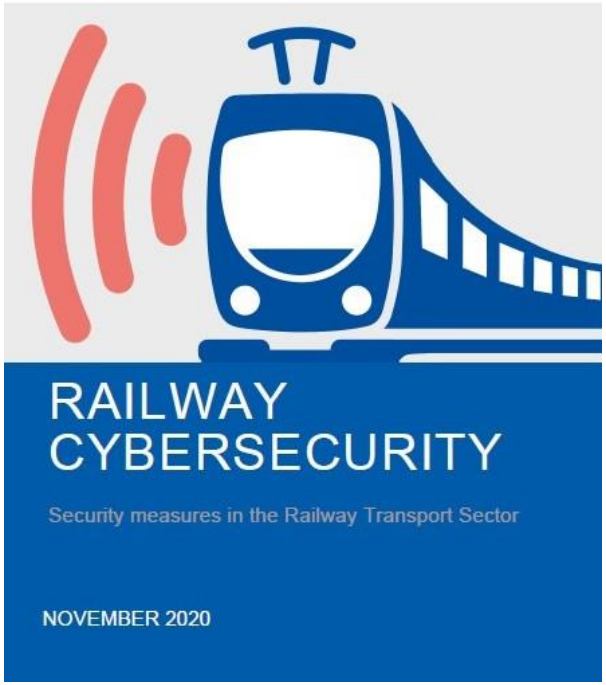
- Implementation of the **NIS Directive**
- Partner of the **European Railway ISAC**

Support standardisation and certification

- Participation in **CEN CENELEC /TC9X/WG26**
- TS **50701 on Railway applications - Cybersecurity**

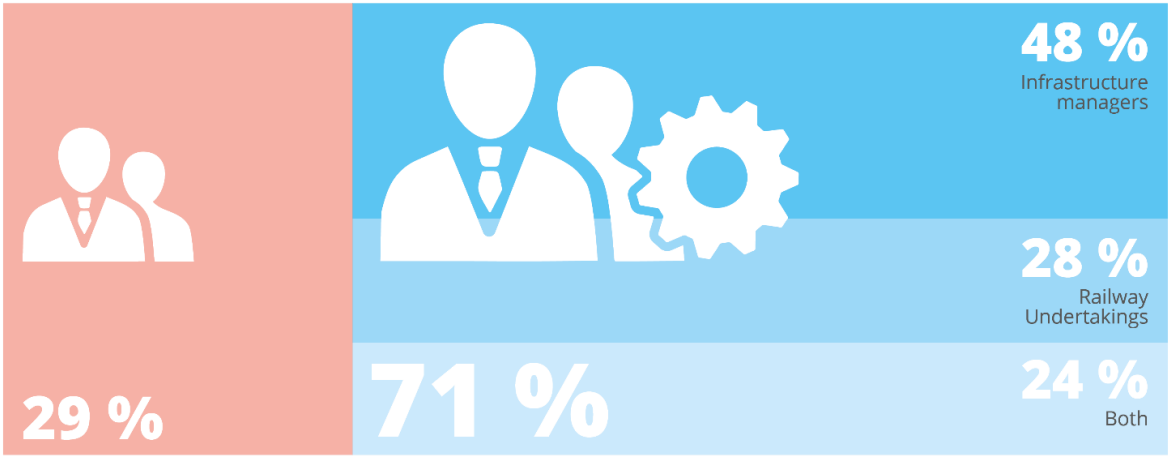
Collaborate closely with ERA

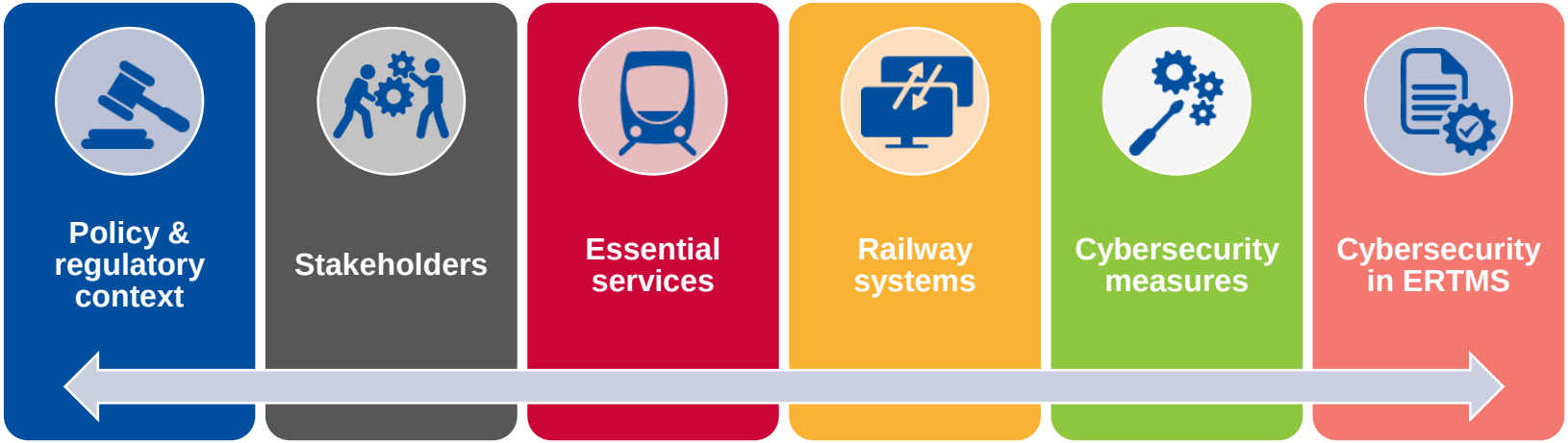
- Cybersecurity for **ERTMS**



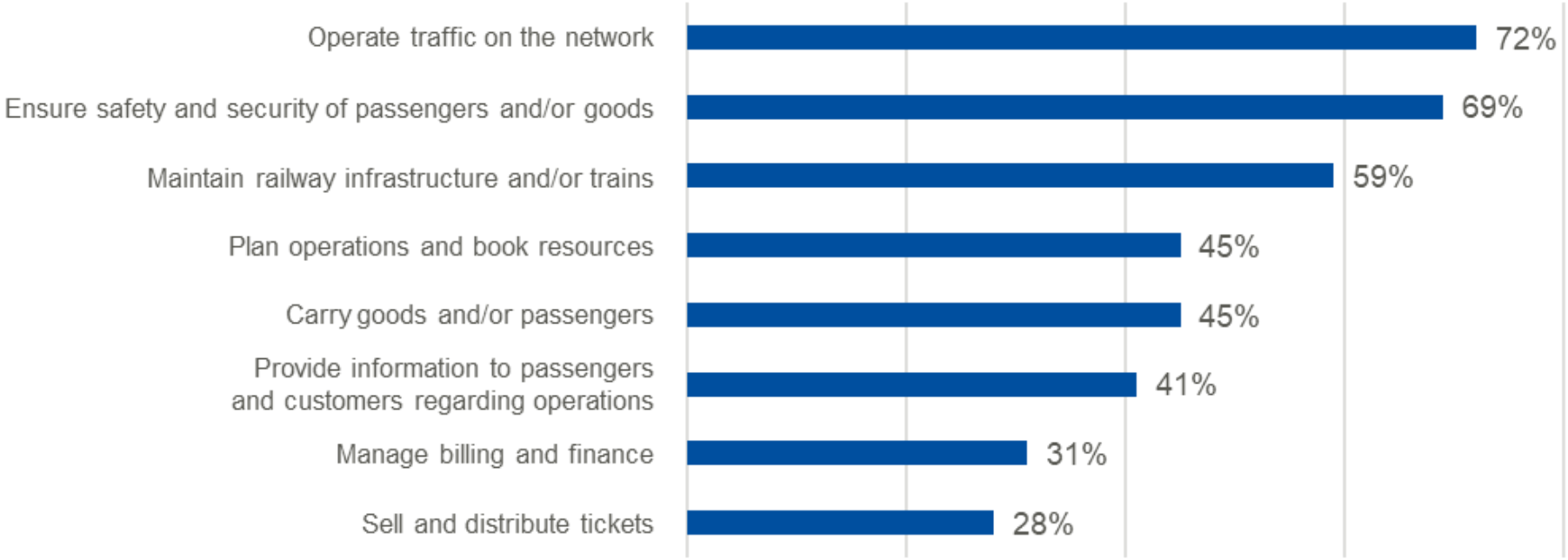
2020 Report on Railway cybersecurity
"Security measures in the Railway Transport Sector"

ENISA STUDY 2019-2020





RAILWAY SERVICES



Operating traffic on the network – IM: 71%, RU: 71%, IM/RU: 100%

Maintaining railway infrastructure and/or trains – IM: 64%, RU: 29%, IM/RU: 75%

Carrying goods and/or passengers" – RU: 57%, IM: 7%, IM/RU: 88%

Ensuring the safety and security of passengers and/or goods – IM: 64%, RU: 43%, IM/RU: 100%

RAILWAY SYSTEMS

SECURITY MEASURES

Areas of high maturity

- Security Risk Analysis
- Security Policy and Security Audit
- System Segregation
- Access Control measures
- Physical and Environmental Security
- Logging
- Incident Reporting
  Communication with authorities
- Business Continuity
  Disaster Recovery Management
- Crisis management (general)

Areas of low maturity

- Ecosystem mapping and relations
- IT Security Maintenance (for IMs)
- Security audit* and security indicators
- Accreditation
- Cryptography
- Detection
- Logs correlation and analysis
- Industrial control systems
- Crisis management (for cyber incidents)

AREAS OF IMPROVEMENT

- Digital and cybersecurity culture and awareness
- Cybersecurity standards and requirements
- Specificities of the sector: distributed infrastructure, presence of legacy systems
- Reconciling safety and cybersecurity worlds (accreditation, culture, jurisdiction)
- Costs: Security vs competitiveness and operational efficiency
- Complexity of regulatory ecosystem: Differences in national transposition of the NIS Directive

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu