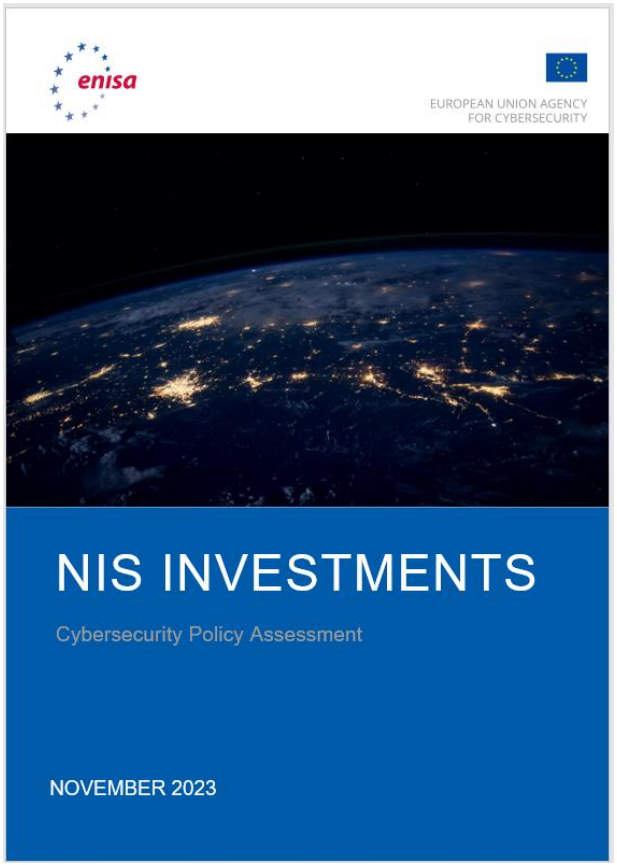
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY INVESTMENTS IN THE TRANSPORT SECTOR

Dr. Athanasios Drougkas
Cybersecurity Expert

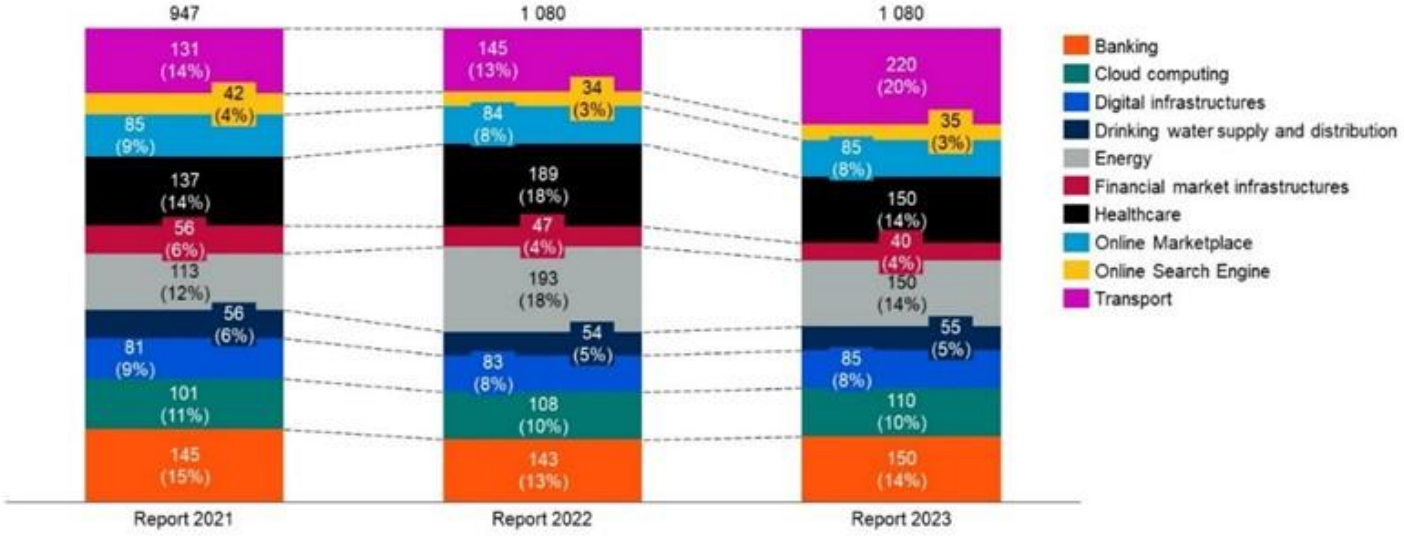
3rd ERA – ENISA Conference
08 | 11 | 2023

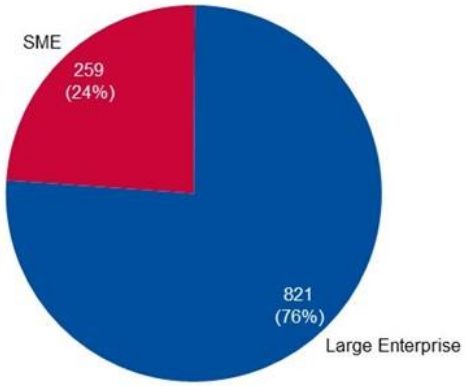
CSPA - NIS INVESTMENTS 2023

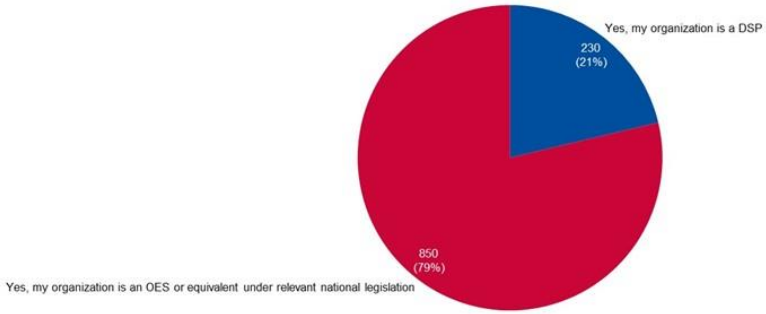


- 4th annual report (>1000 OES/DSP from 27 EU MS) adds to established **historical datasets**
- Support policy makers in the analysis of the **effectiveness of the NIS Directive**
- **Sectorial deep dive** (Transport) – supported sectorial analyses for sectorial authorities
- Focus on **skills** (European Year of Skills, Cyber Skills Academy policy initiative)
- Continued collection of data on SOC capabilities for the second year to support **CSOA** discussions

SURVEY DEMOGRAPHICS



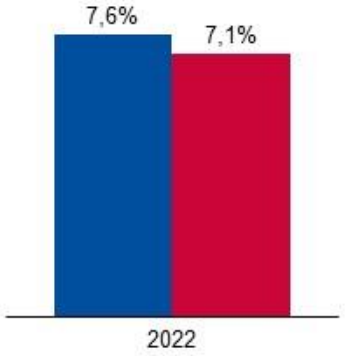


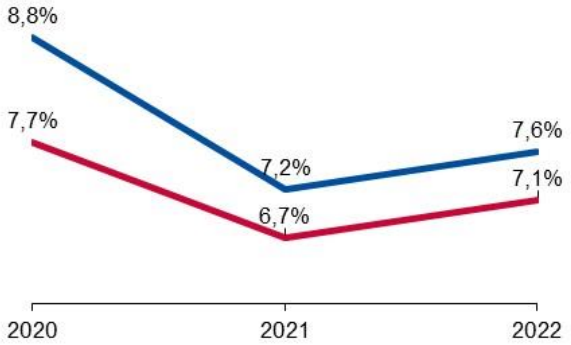


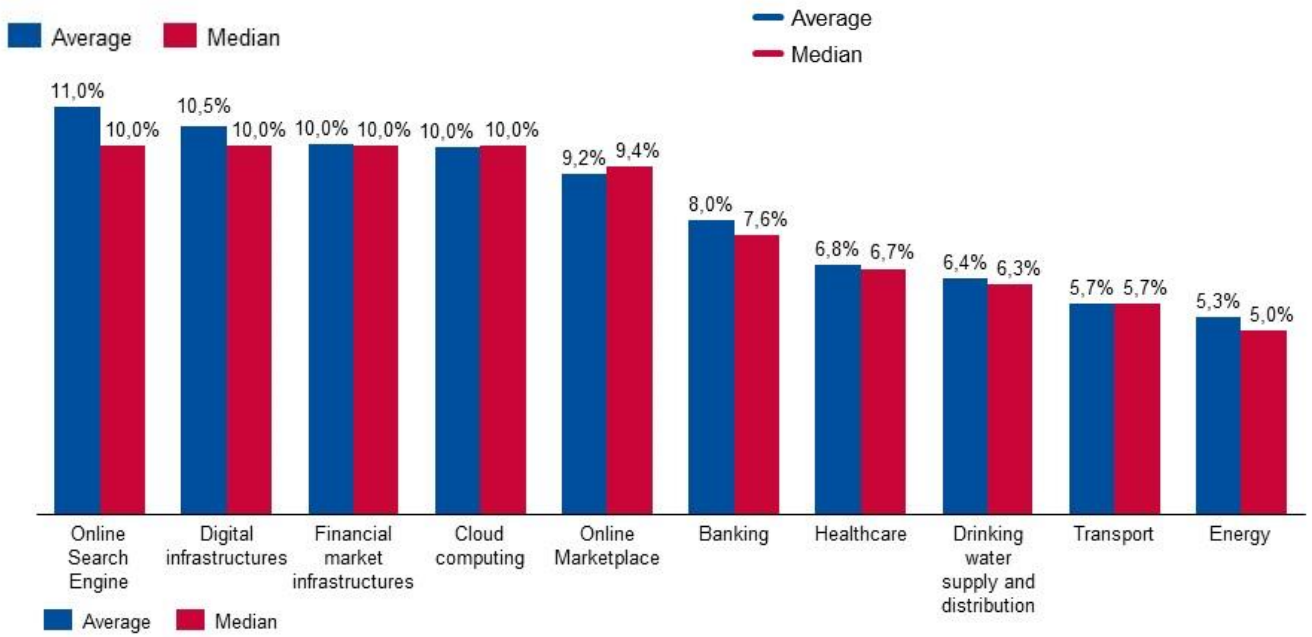
KEY FINDINGS

- OES/DSPs earmarks 7,1% of their IT investments for Information Security, an **increase of 0.4% compared to last year**.
- For 55% of OES in the transport sector the **NIS Directive is the main driver for cybersecurity investments**
- OES/DSPs allocate 11,9% of their IT FTEs for IS, a **decrease of 0,1% compared to last year, despite the overall increase in cybersecurity spending**
- OES/DSPs employ an average of 11% of women in Information Security FTEs, while the median is at zero percent, meaning that **most of the surveyed organisations do not employ any women as part of their IS FTEs**
- 83% of the surveyed organisations claim recruitment difficulties in at least one information security domain.
- 47% of the surveyed organisations declare no specific budget for information security training.
- The estimated direct costs of a major information security incident in 2022 is **250 k€, increasing from 200 k€ in 2021**.
- **30% of the organisations do not engage** in collaboration or information-sharing initiatives.

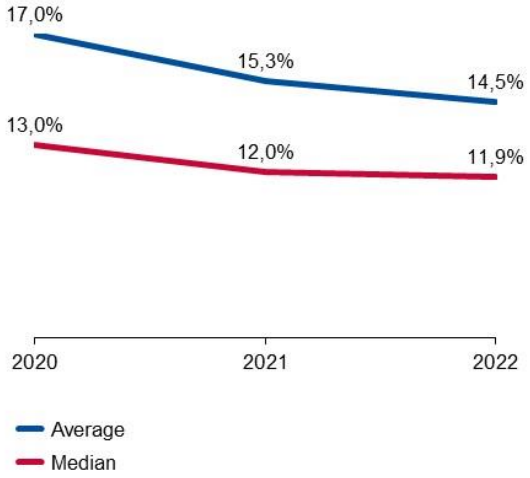
NISD IMPLEMENTATION BUDGETS



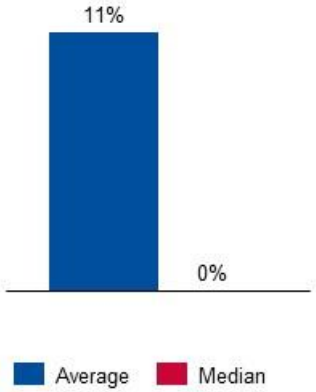




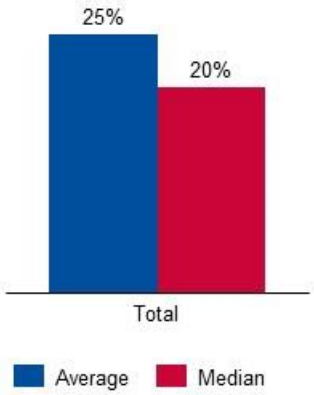
CYBERSECURITY FTES



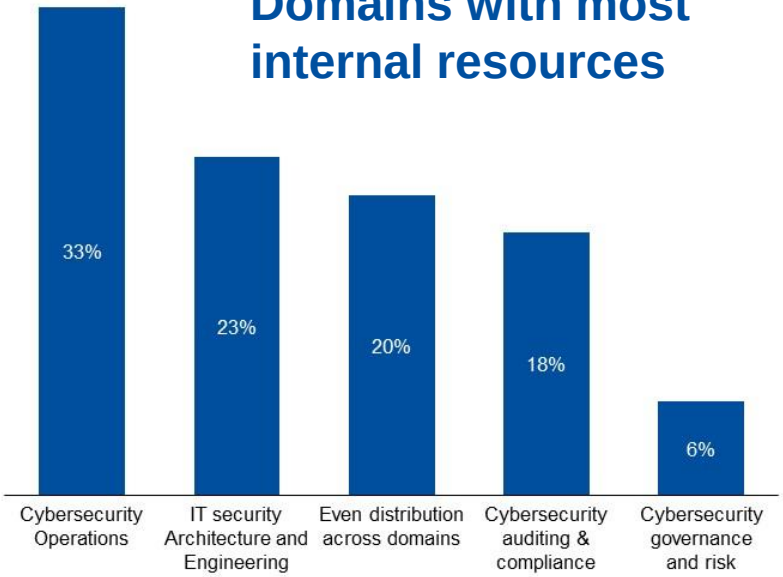
% of women in IS FTEs



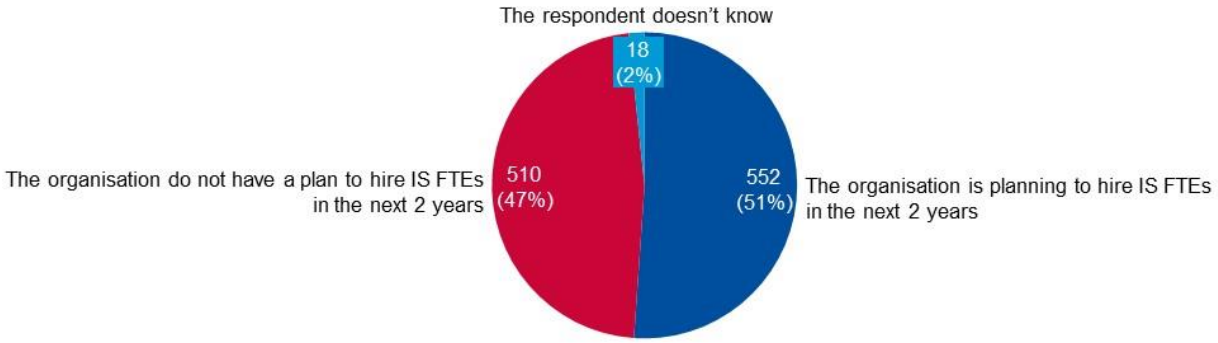
% of contractors



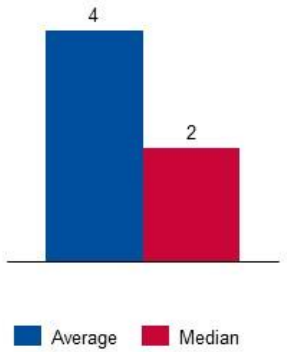
Domains with most internal resources



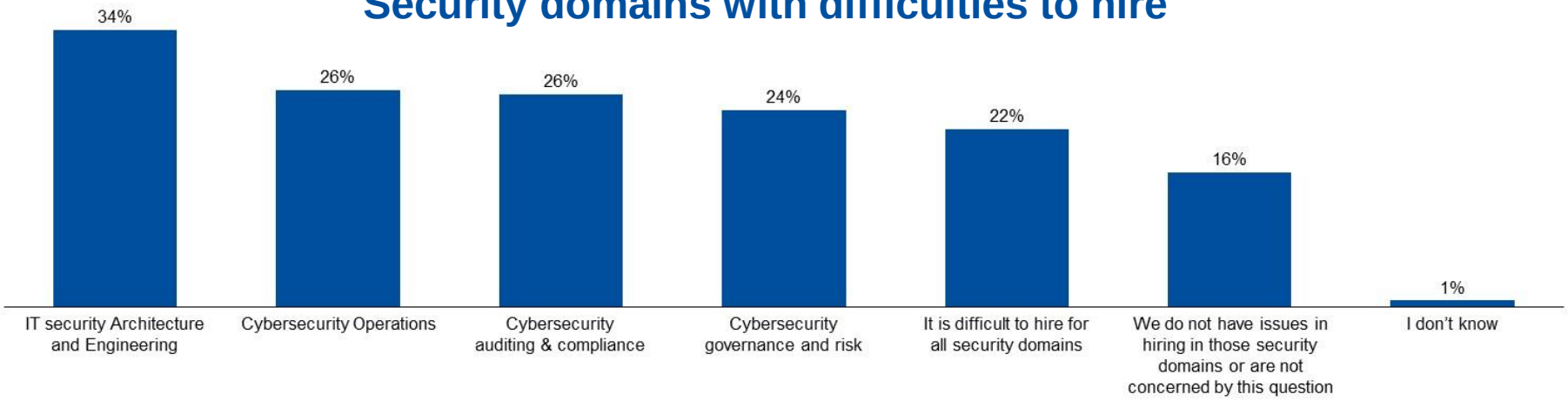
SKILLS GAP



IS FTEs hires in next 2 years

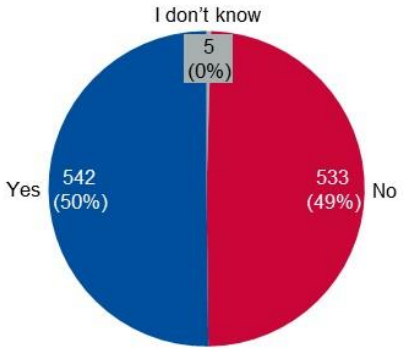


Security domains with difficulties to hire

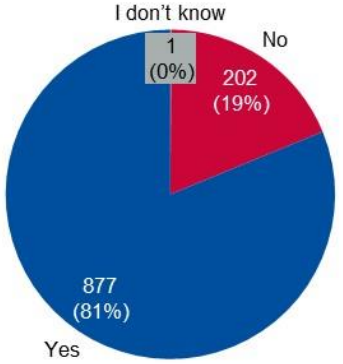


INFORMATION SECURITY GOVERNANCE

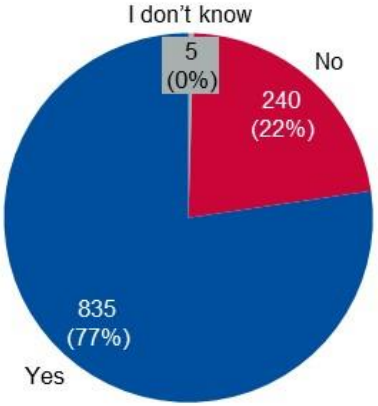
Management receives training



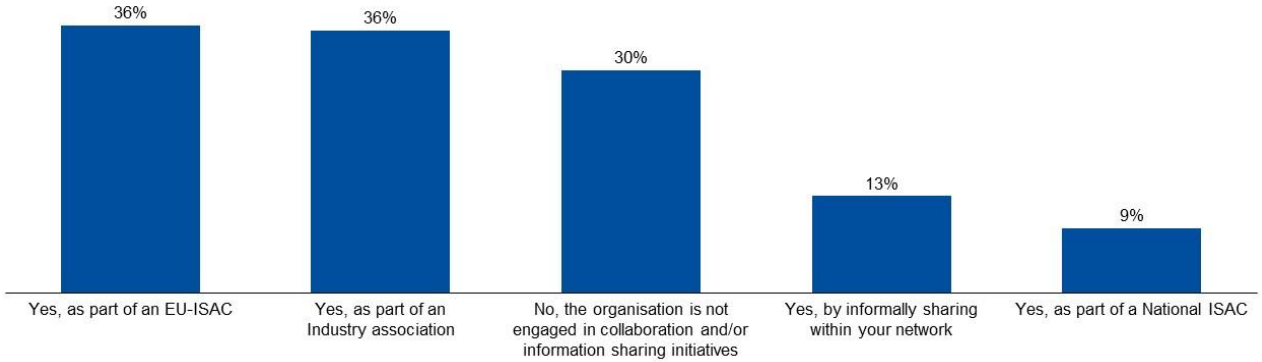
Management approves security measures



3rd party cyber risk management policy

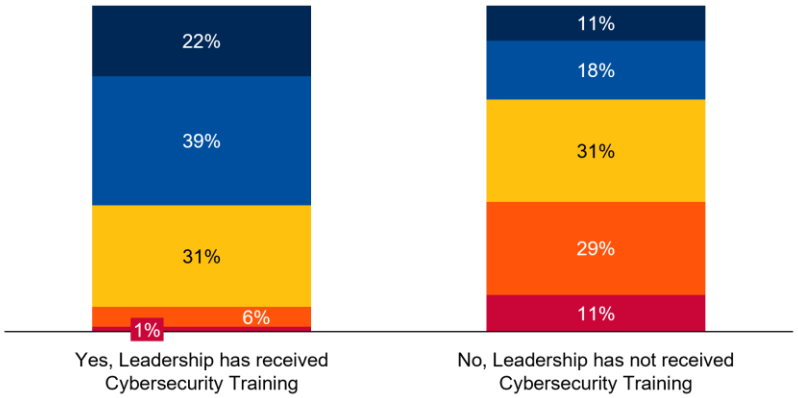


Participation in information sharing

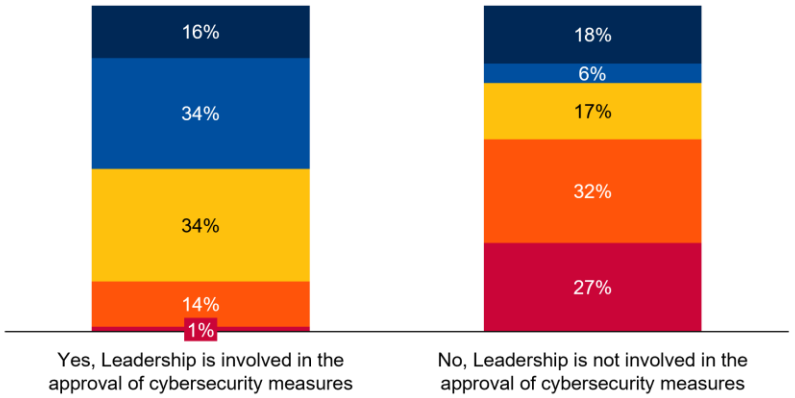


IMPACT OF LEADERSHIP INVOLVEMENT

Cyber risk management maturity depending on Leadership Training in Cybersecurity

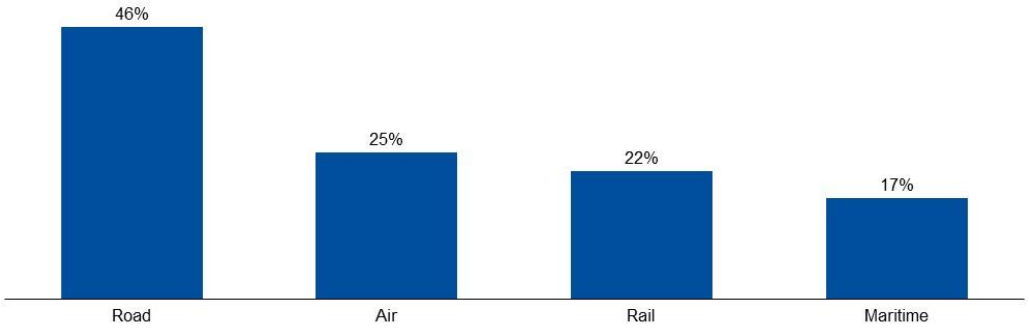


Cyber risk management maturity depending on Leadership Approval of Cybersecurity Measures

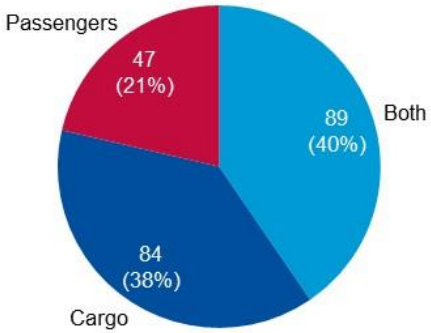


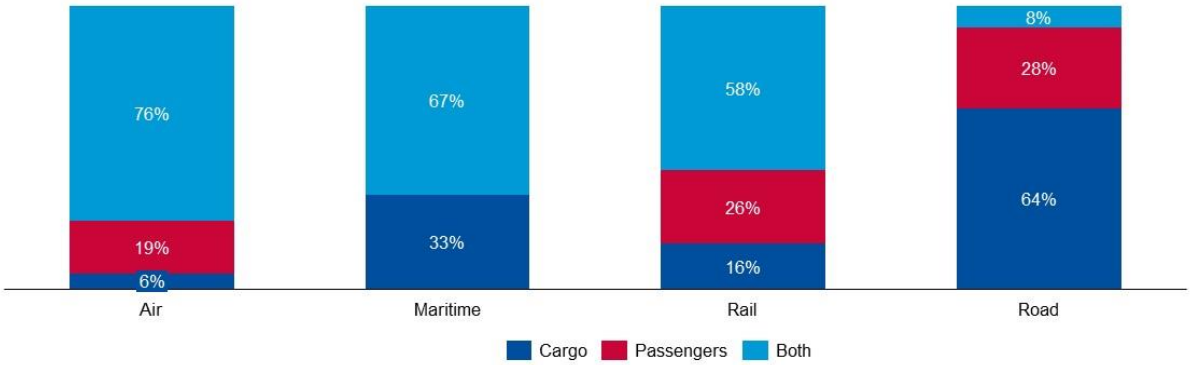
- 1 – None/Initial: We do not have any risk management capabilities.
- 2 – Developing: We have a basic understanding of our cyber risks but do not have a formal cyber risk management program.
- 3 – Defined: We have a defined cyber risk management program and have identified the key risks against our assets/processes.
- 4 – Managed: We implement a cyber risk management program and a risk-based approach in line with accepted industry standards and best practices.
- 5 – Optimized: We continuously assess and improve our cyber risk management program through regularly assessments/audits.

TRANSPORT SECTOR - DEMOGRAPHICS



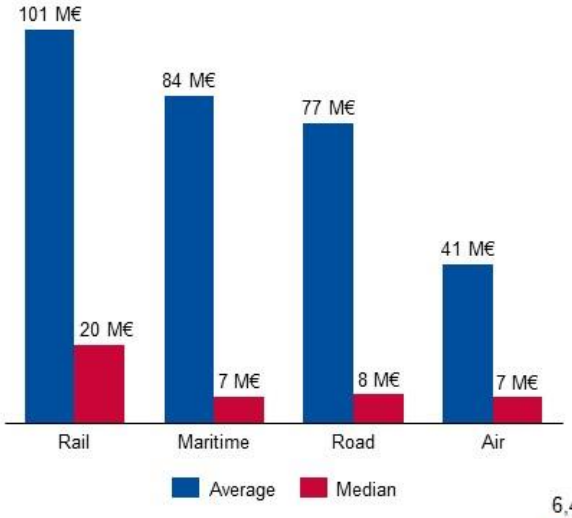
Rail sector: 48 OES
Railway undertakings: 25%
Infrastructure managers: 75%
Also OES in other sectors: 35%



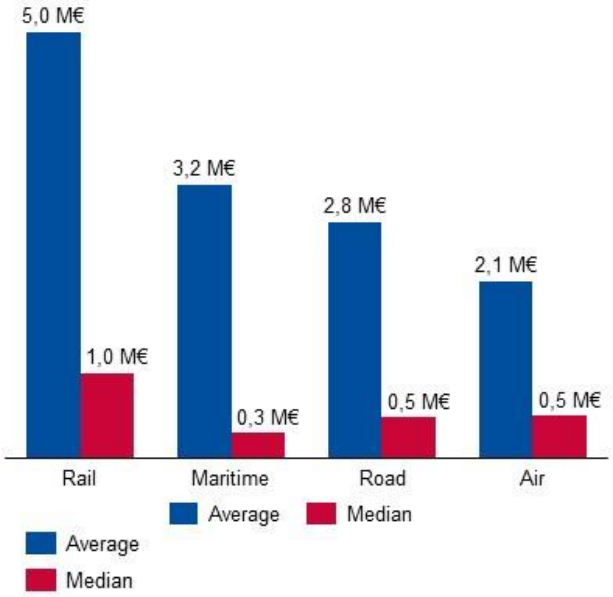


TRANSPORT SECTOR – NIS BUDGETS

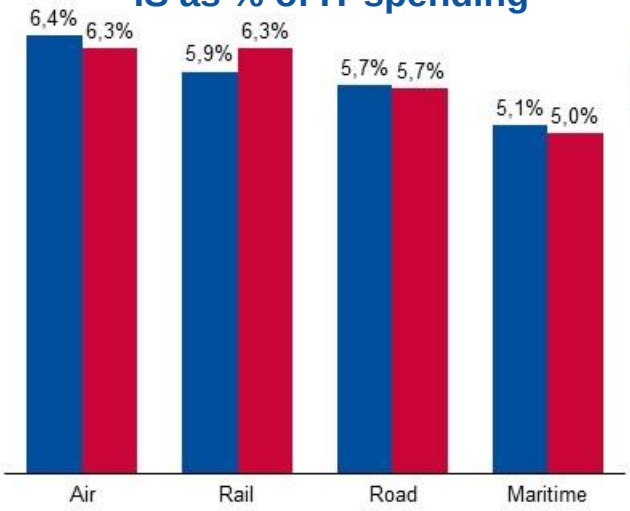
IT spending



IS spending

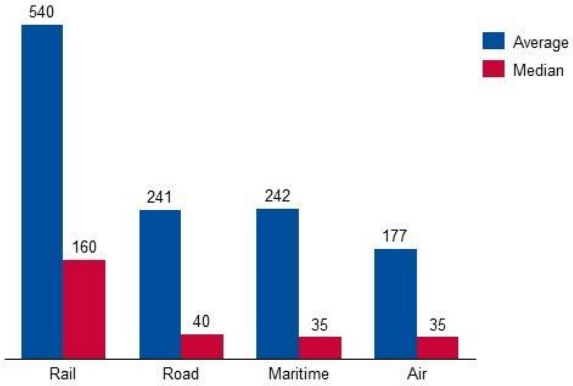


IS as % of IT spending

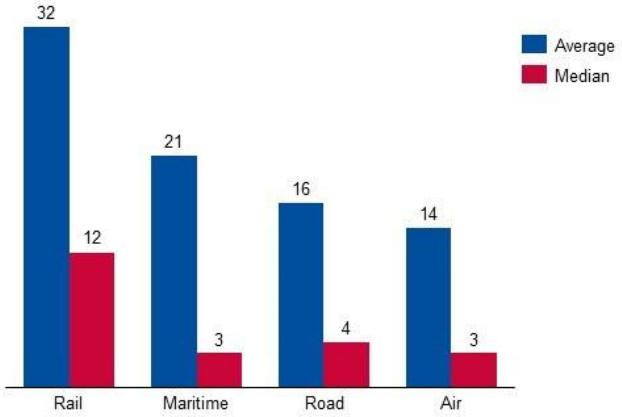


TRANSPORT SECTOR – NIS FTES

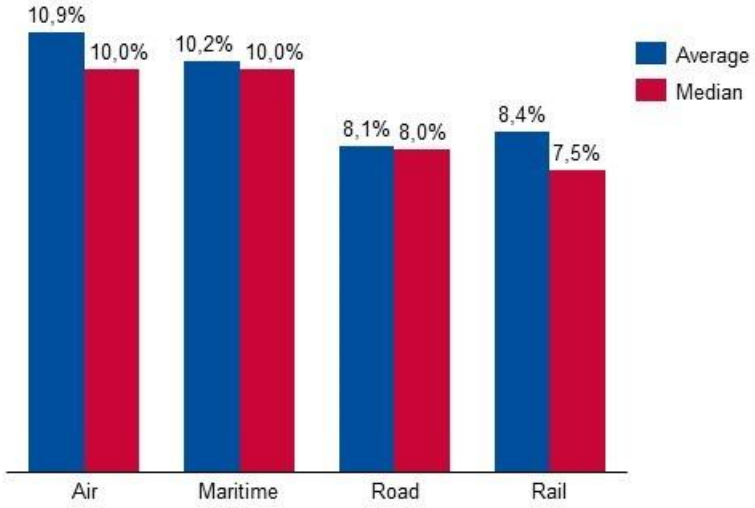
IT FTEs



IS FTEs

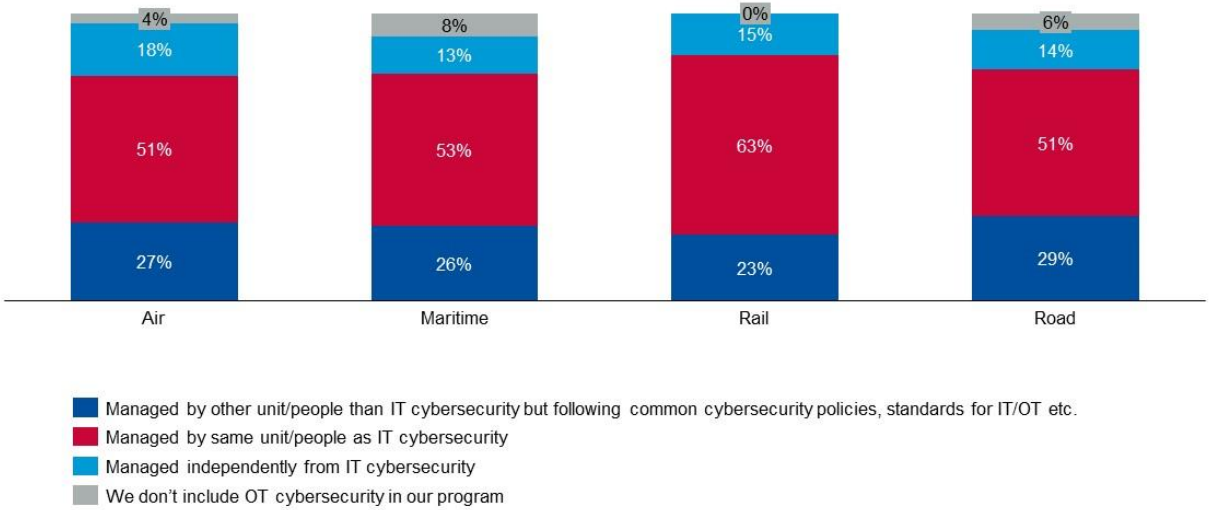


IS as % of IT FTEs

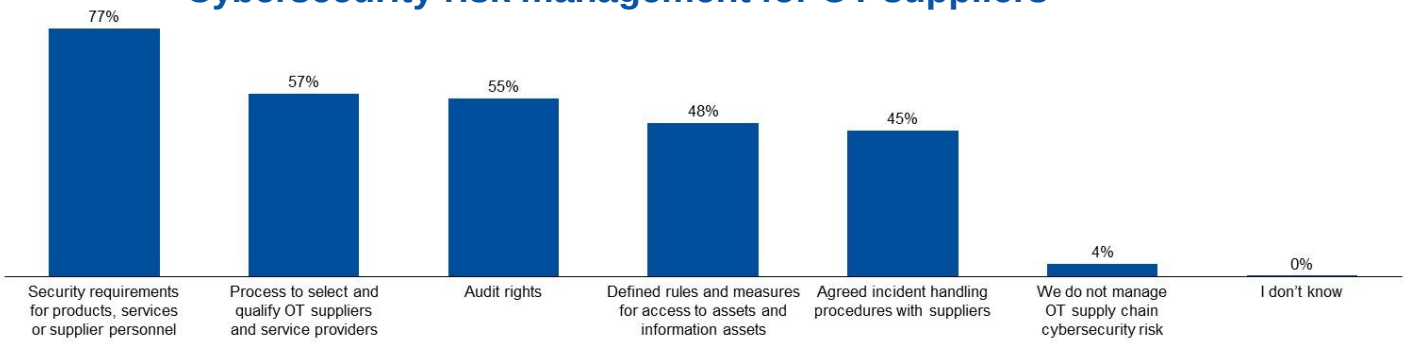


OT CYBERSECURITY

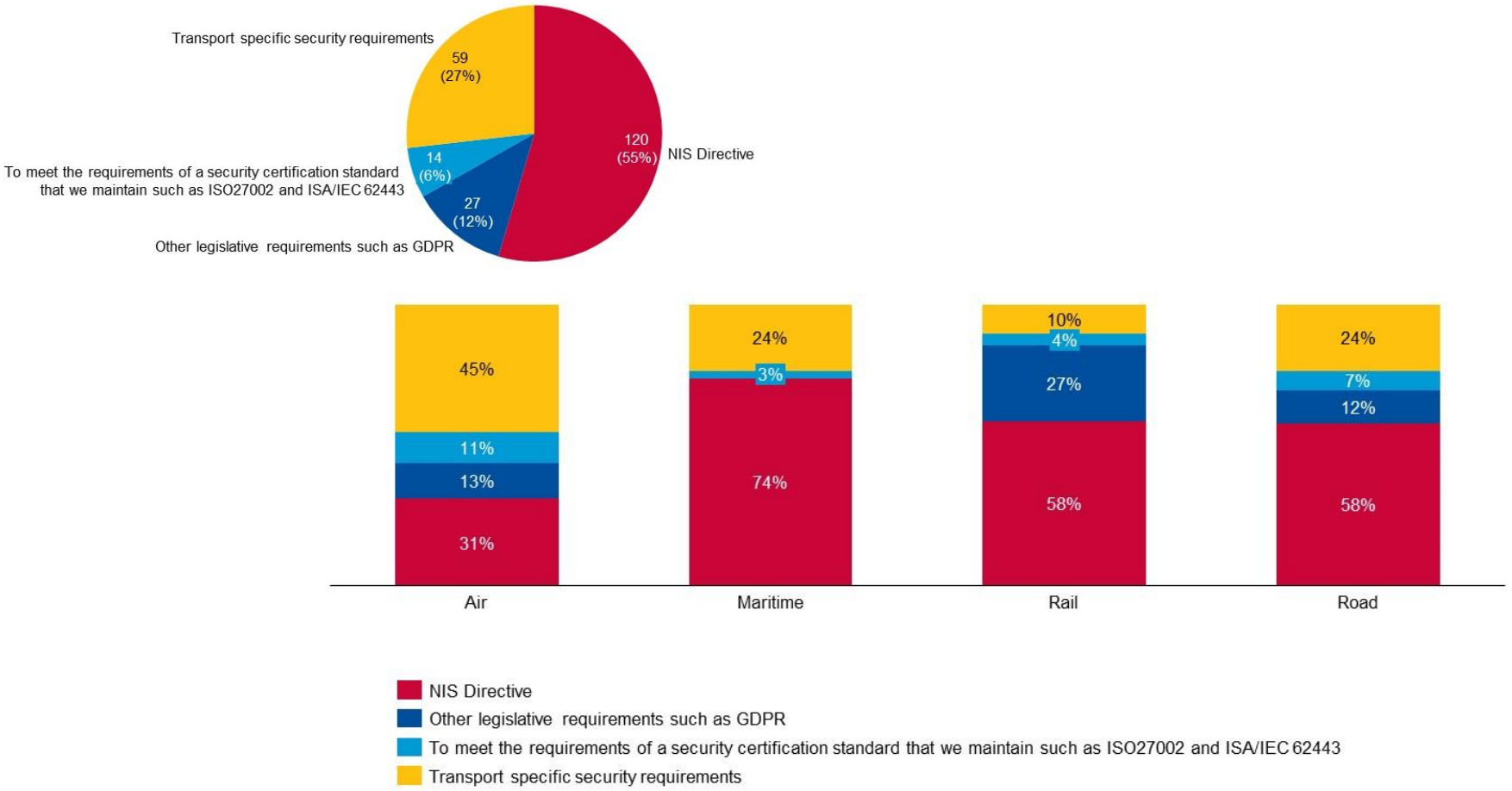
OT cybersecurity management



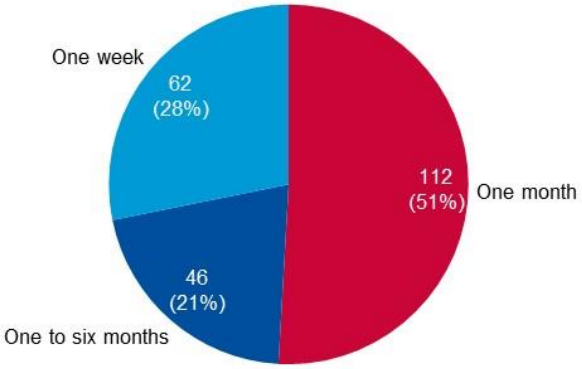
Cybersecurity risk management for OT suppliers



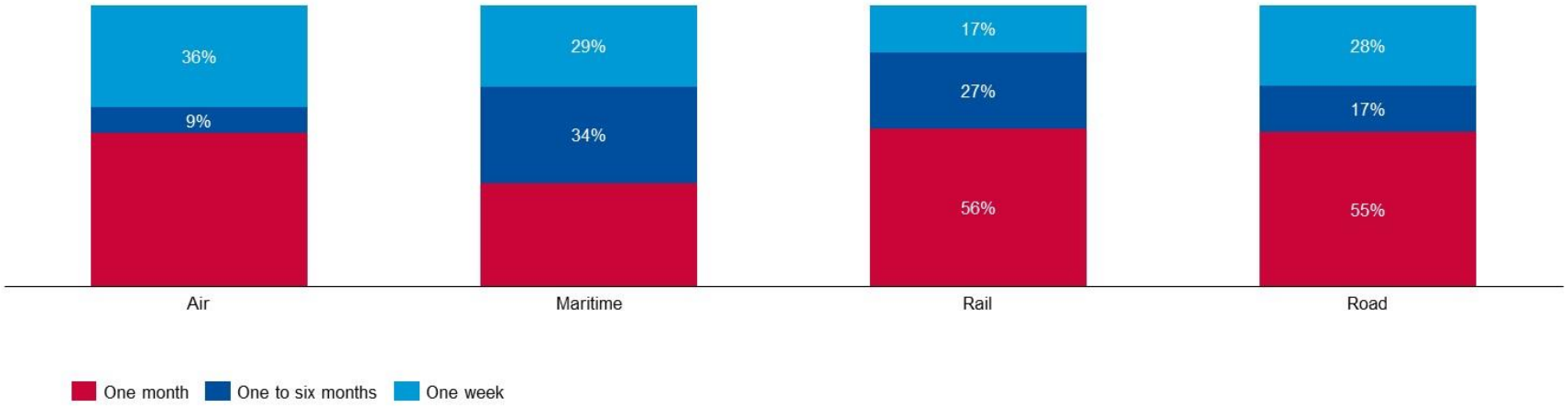
LEGAL DRIVERS FOR CYBERSECURITY INVESTMENTS



PATCHING OF CRITICAL IT/OT ASSETS

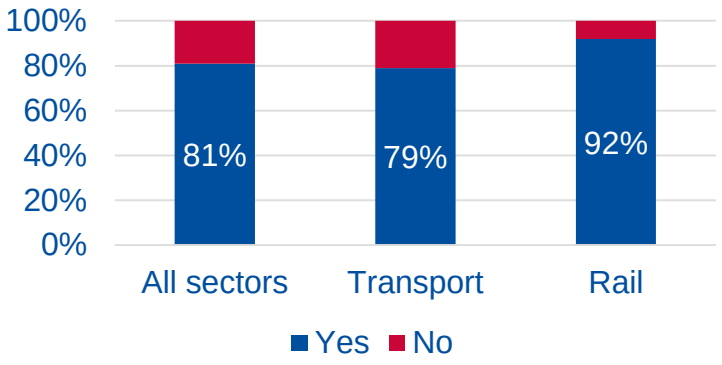


Time to patch critical vulnerabilities (IT & OT)

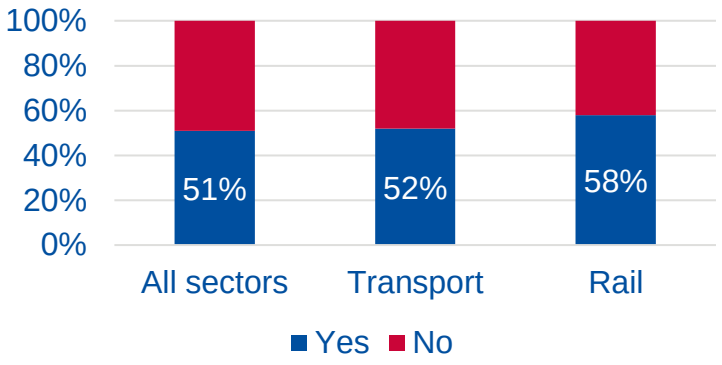


CYBERSECURITY MATURITY IN RAIL

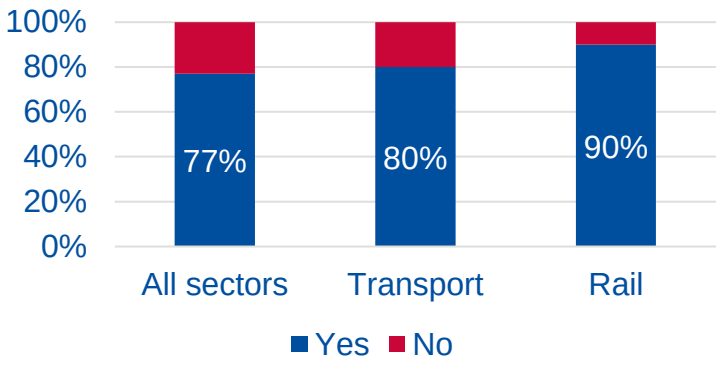
Leadership approval of security measures



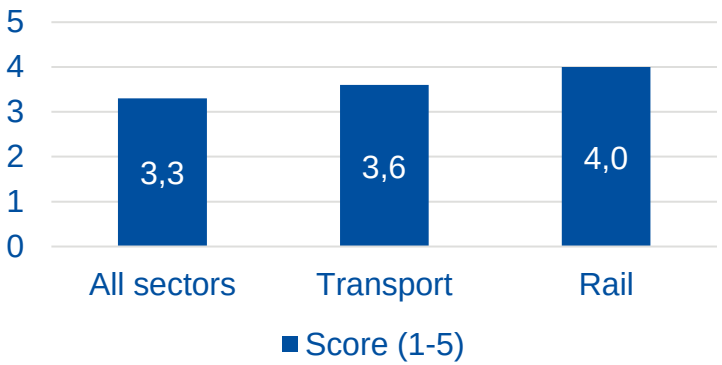
Leadership receiving cyber risk training



Cyber risk management policy for 3rd parties



Cyber risk management self-assessment score



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