EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NIS INVESTMENTS

Cybersecurity Policy Assessment

NOVEMBER 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building, and awareness raising, the Agency works with its key stakeholders to strengthen trust in the connected economy, increase the resilience of the Union's infrastructure, and, ultimately, keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use resilience@enisa.europa.eu.
For media inquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Monika Adamczyk, Athanasios Drougkas, Eleni Philippou, ENISA
Patrick Abel, François Gratiolet, Edwin Maaskant, Gartner

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-648-4, DOI: 10.2824/060928, Catalogue nr. TP-02-23-138-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report aims at providing policy makers with evidence to assess the effectiveness of the existing EU cybersecurity framework specifically through data on how Operators of Essential Services (OES) and Digital Service Providers (DSP) identified in the European Union's **directive on security of network and information systems (NIS Directive)**[1] invest their cybersecurity budgets and how the NIS Directive has influenced this investment

This fourth iteration of the report presents data from **1,080 OES/DSPs from all 27 EU Member States**. It can now provide a historical dataset that allows for year-on-year comparison and identification of trends. As 2023 is the European Year of Skills and in line with the Commission communication on a Cybersecurity Skills Academy[2], particular emphasis was placed on the topic of cybersecurity skills among the OES/DSPs. Moreover, a sectorial deep dive was conducted for OES in the Transport sector. Key findings from the report include:

- 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**
- 42% of OES/DSPs have subscribed to a dedicated cyber insurance solution in 2022, up from 30% last year, though **only 13% of SMEs subscribe to cyber insurance**.
- OES/DSPs allocate 11,9% of their IT FTEs for information security 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**
- An OES or DSP in the EU typically employs **20% contractors for his IS FTEs with Cybersecurity operations the security domain with the most contractors**
- **47% of OES or DSPs do not plan to hire IS FTEs in the next two years,**
- The organisations planning to hire information security FTEs in the next two years aim to hire 2 FTEs, with an average of 4 FTEs but **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.**
- Leadership attends **dedicated cybersecurity training for 50%** of OES/DSPs and is involved in **approving cybersecurity risk management measures for 81%** of OES/DSPs.
- **30% of the organisations do not engage in collaboration or information-sharing initiatives.**
- **51% of the transport organisations manage OT security with the same unit or people as IT cybersecurity**
- **51% of the organisations in the transport sector need one month to patch critical vulnerabilities on IT or OT assets,** and 21% need a time between 1 month and six months. Only 28% of the surveyed organisations fix critical vulnerabilities on critical assets in one week.

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148
[2] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'), COM/2023/207 final

1. INTRODUCTION

This document is the fourth edition of the NIS investments study published by ENISA to understand the impact of the **Directive on the Security of Network and Information Systems** (**NIS Directive**)[3] on Operators of Essential Services (OES) and Digital Service Providers (DSP). Specifically, the objective of this report is to support policy makers in assessing the effectiveness of the existing EU cybersecurity policy framework by providing insights into how much OESs and DSPs in cybersecurity budgets and comply with the requirements of the NIS Directive, and what impact the NIS Directive has had on these operators, as well as to collect data on various operational and organisation aspects of OESs and DSPs in the EU.

The directive on measures for a high common level of cybersecurity across the Union (**NIS 2 Directive**) [4], which adapts the previous NIS Directive to current needs has already been adopted and the transposition process is underway. The new rules cover a wider scope compared to the previous Directive and increase the number of entities that need to take measures for the management of cybersecurity risk. However, since implementation of NIS2 is still on-going, **for the purposes of this report the NIS Directive definitions and scope are taken into consideration**.

With 2023 being the **European Year of Skills** and cybersecurity skills shortage being consistently identified as a key challenge for operators in the EU, the present analysis presents data on how OES and DSPs address their cybersecurity skills needs and where the main skills gaps currently exist. This information can be used to inform follow-up actions in the context of the Cybersecurity Skills Academy presented by the European Commission[5]. Moreover, the present report provides a more **in-depth analysis of OES in the Transport sector**, examining among other topics the influence of and interplay between the NIS Directive and sectorial regulations concerning transport security and safety.

To ensure a representative account of all 27 EU Member States, **40 organisations in each Member State were surveyed making a total of 1,080 organisations surveyed across the EU**. Additional information on the demographics of the survey is available in Annex A. Moreover, available global benchmark data is presented to highlight the most relevant trends related to information security spending, cyber talent management and the cyber threat landscape

The target audience of this report is EU and National policymakers. This series of reports has been streamlined to produce historical data sets that allow for the monitoring of how specific vital indicators, such as overall cybersecurity budgets, develop over time and how policy affects these indicators, as well as allowing the collection of valuable data or evidence to inform policy decisions as part of the activities of ENISA's Cybersecurity Policy Observatory (CSPO). This report may also provide helpful information to a secondary audience, OESs and DSPs.

[3] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148
[4] https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2020:823:FIN
[5] See also https://digital-skills-jobs.europa.eu/en/latest/news/closing-cybersecurity-talent-gap-commission-launches-cybersecurity-skills-academy

2. INFORMATION SECURITY DYNAMICS AND OUTLOOK

This chapter aims to provide a high-level outline of global trends in information security and outlooks. To provide actionable insights, it leverages data and metrics collected and assessed independently of the dedicated survey. The specific data sources for the following analysis are referenced in the individual sections.

It should be noted that **the data sources for Chapter 2 are different than those for the rest of the chapters** (dedicated survey of OES/DSPs).

This data set is presented to provide a high-level overview of the market in terms of information security and to highlight a few fundamental dynamics and trends concerning cybersecurity investments in different regions, the global landscape with regards to cybersecurity skills and the respective talent gap. In addition, this chapter presents technology and cybersecurity aspects concerning operators in the transport sector and how future cybersecurity trends and threats identified by ENISA are evolving. **This broader view is complementary to the focused analysis presented in the rest of the report.**

2.1 TRENDS IN INFORMATION SECURITY SPENDING

2.1.1 Forecast spending on information security and risk management

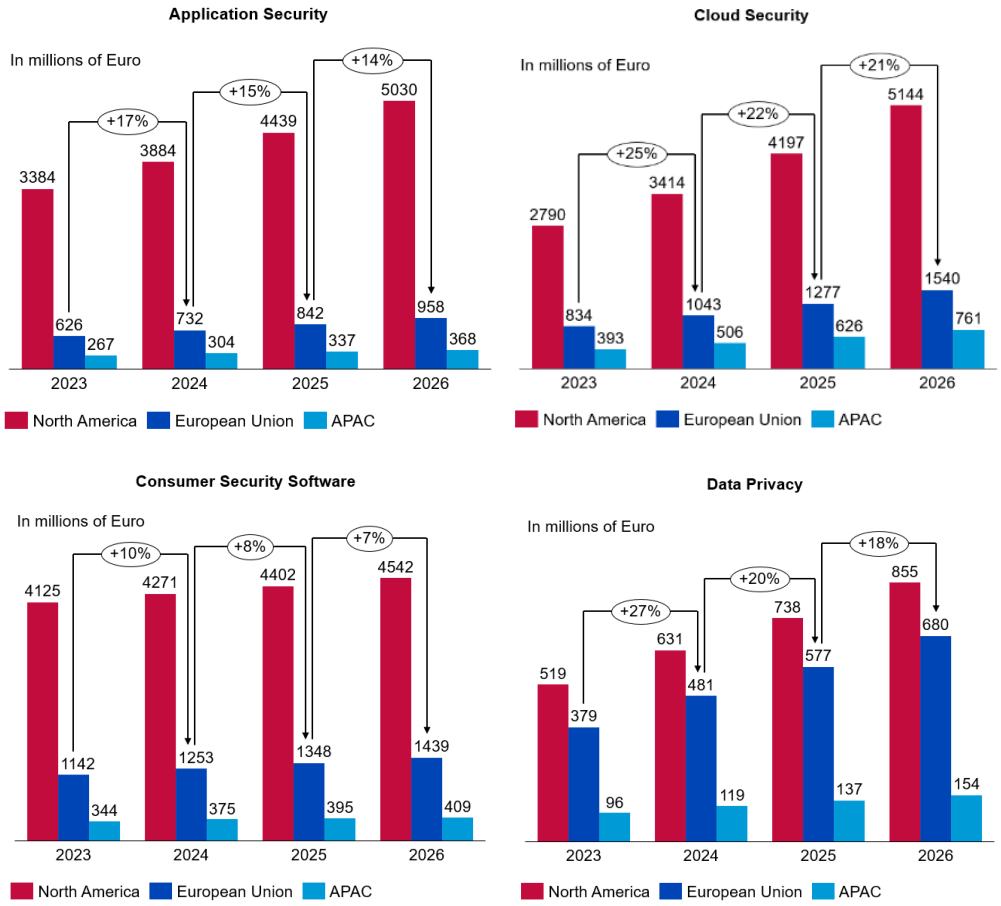
Globally, **spending on information security and risk management is set to increase to 174 billion Euros in 2023**, growing steadily at 13.9%. By 2027, **this spending will reach 267 billion Euros, showing an average annual growth of 11% from 2022 to 2027.**.

In Europe, spending on information security and risk management is expected to grow to 44 billion Euros in 2023, with a growth rate of 13.7%. By 2027, this spending will reach 71 billion Euros, with an **average annual growth rate of 10.9% from 2022 to 2027**.[6]

The subsegment experiencing the highest growth is cloud security, with an impressive average annual growth rate of over 25% from 2021 to 2026, reaching a market size of 5 billion Euros. **The largest subsegment is security services, with a market size of 92 billion Euros**.[7]

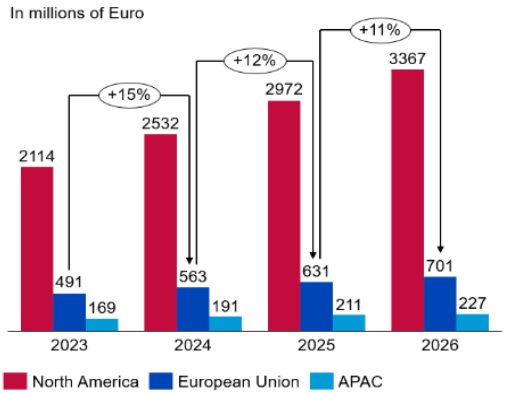
[6] Gartner, Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 2Q23 Update.
[7] Gartner, General Manager Outlook: Information Security Spending, 2H22.

Figure 1: Breakdown of information security spending per region and security segment[8]

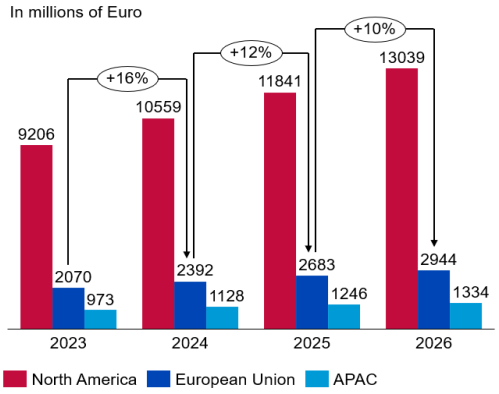


[8] Gartner, Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 2Q23 Update.

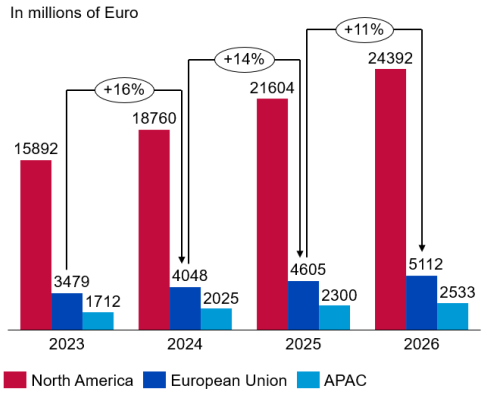
Data Security



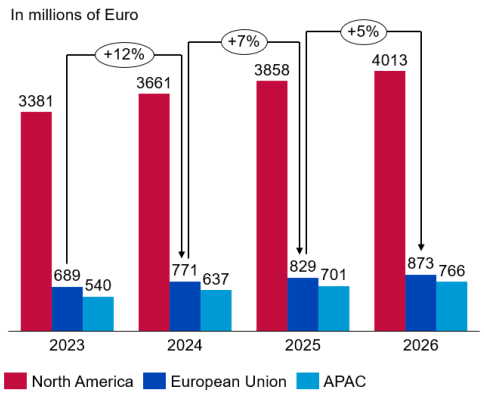
Identity Access Management



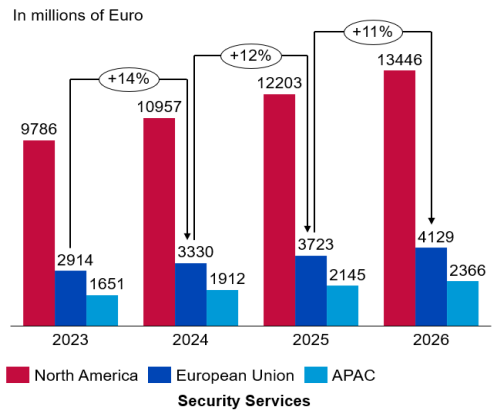
Infrastructure Protection



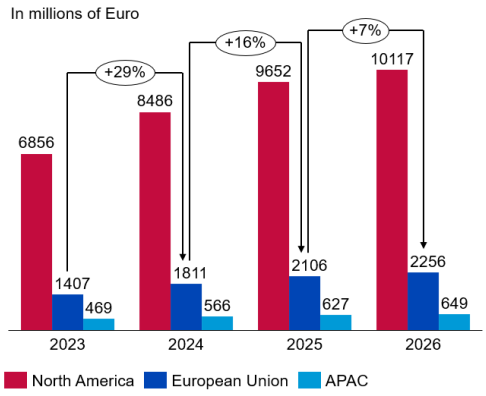
Integrated Risk Management



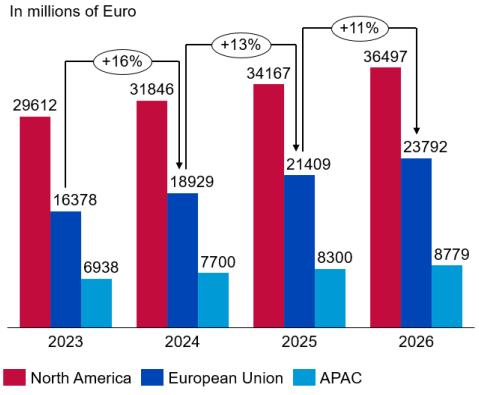
Network Security Equipment



Other Information Security Software



Security Services



While spending on information security in the EU projects to grow substantially over the next 3 years, it remains **significantly lower compared to that of North America** even when total population size and Gross Domestic Product (GDP) are factored in.

2.1.2 Information security spending key metrics by region

Information security (IS) spending as a percent of Information Technology (IT) spending is a key metric used to capture an organisation's investment level to secure its total IT environment.[9] This metric also allows a relative normalisation of information security spending between industries and organisations.

Figure 2: Information security spending as a percent of total IT spending globally

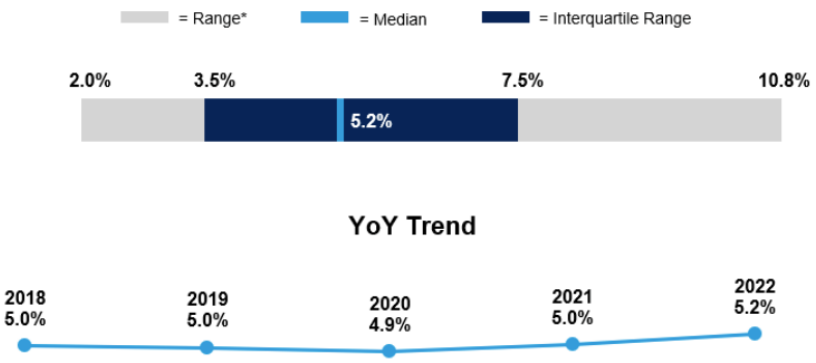


Figure 2 illustrates that the year-over-year (YoY) analysis shows that the IS spending as a share of IT spending is showing a slight increase since 2021 (+0,2 point), though relatively stable since 2018% around 5%.

In addition, Table 1 below provides insights into specific information security key metrics across different regions.[10]

Table 1: Information security spending metrics by region, 2022

Region	IS spending as % of IT spending	IS FTEs as % of IT FTEs	IS spending per employee	IS Spending as % of 2021 Revenues[11]
North America (NA)	6,4%	6,5%	1308€	3,2%
European Union*	**5,1%**	**4,5%**	**673€**	**2,1%**
Asia Pacific (APAC)	6,3%	6,3%	1050€	2,4%

*The peer group does not include Cyprus

IS spending as a share of IT spending is the lowest for the organisations in the European Union, significantly behind organisations from North America (-1,3point i.e., -20%) or Asia Pacific (APAC) with -1,2 point (i.e., -19%).

[9] Gartner, IT Key Metrics Data 2023: IT Security Measures — Analysis.
[10] Gartner, Security Spend Analytics Workbench.
[11] 2021 Revenues for commercial organisations and OPEX for government organisations

Similarly, the EU also has the lowest ratio for IS FTEs against IT FTEs with 4,5%, while organisations from North America and APAC are at 6,5% and 6,3% respectively.

Finally, IS spending per employee is also the lowest in the EU, at 673 €, while it is much higher in APAC (1050 € i.e., 56% higher) and North America (1308 € i.e., 94% higher).

2.1.3 Top investment priorities in Europe

Figure 3 illustrates the technology areas where CIO respondents of European organisations intend to spend the most significant amount of new or additional funding in 2023 compared with 2022 and technologies where they will reduce the budget. [12]

Figure 3: Top technologies for new or increased spending by Europe CIOs (including UK) in 2023 compared to 2022

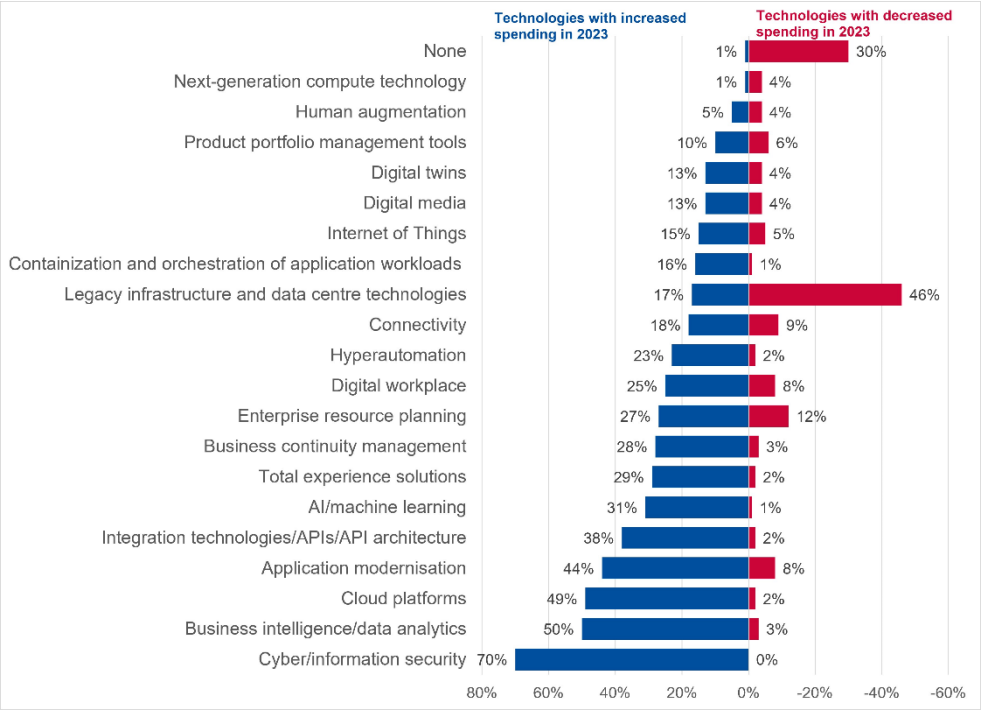


Figure 3 shows that information security, business intelligence/data analytics (BI/DA) and cloud platforms remain the top technology areas for new or increased spending among CIOs in Europe (and worldwide alike). Information security will see an increase in funding for 70% of the surveyed CIOs, showing that it is a crucial priority for most European CIOs.

2.2 SECURITY TRENDS IN THE TRANSPORT SECTOR

2.2.1 Threat landscape evolution in the transport sector

Cyber threats continually threaten to paralyze the transport sector which is increasingly dependent on technologies that enable data sharing across ecosystems. As a combination of technologies including Cloud, Internet of Things (IoT), Artificial Intelligence (AI) and Robotic Process Automation (RPA) is used to bring additional efficiencies to transport organisations, these cross-platform initiatives are also increasing cybersecurity challenges. The convergence of IT, operations technology (OT) and IoT infrastructure and services has changed the cyber risk profile of the sector. The attack surface has drastically expanded, keeping no area of the value chain safe from cyber-attacks. As an example of the fast pace of change at which the

[12] 2023 Technology Spending Priorities (Europe).

industry is adopting those new technologies, the analysis of the IoT market in the transportation sector forecasts a **14,5% CAGR[13] between 2021 and 2026**, highlighting an **impressive pace of IoT rollout** in the transport sector, and from which stems a severe challenge to the security officers of those organisations.[14]

The transport sector faces a threat landscape that continues to become increasingly menacing every year. **Cyber incidents in the transport sector have seen an increase of 25% in the monthly average number of reported incidents in 2022 compared to 2021**.[15] Cybercriminals and financial-gain-motivated hackers comprise the bulk of threat actors in the transport sector, with ransomware and data-related attacks being the most encountered threats.

ENISA's recently published Transport Threat Landscape[16] provides an analysis of the top threats in the transport sector. Ransomware which accounted for around 25% in 2022 was the most prominent, followed by DoS/DDoS/RDoS at 13%. The number of ransomware attacks almost doubled in 2022 compared to 2021 while the malware incidents almost halved. Data-related threats declined but remain significant. DDoS attacks increased substantially in 2022 owing to increased activity by hacktivists and geopolitical tensions.

2.2.2 Information security spending in the transport sector

Table 2 provides insights into critical information security metrics for the transport sector.[17]

Table 2: Information Security critical metrics for the transport sector, 2022, globally

Region	IS spending as % of IT spending	Information Security FTEs as % of IT FTEs	Information Security spending per employee	Information Security Spending as % of 2021 Revenues[18]
Global	5,9%	6,9%	527 €	2,8%

2.3 CYBER TALENT MANAGEMENT

Cybersecurity is both technology and people-centric. Hence, the cybersecurity workforce gap needs to be as minimal as possible. However, the cybersecurity talent gap is growing, with **over 3 million jobs requiring filling globally.**[19] As a result, risk assessment, oversight, strategic planning, and other critical cyber functions need more cyber professionals.[20] **Despite adding more than 464,000 workers in the past year, the cybersecurity workforce gap has grown to 3,432,476 with a 26.2% year-over-year increase**. Table 3 is a representation of the cybersecurity workforce gap across various regions.[21]

Table 3: 2022 Global cybersecurity workforce gap

Region	Workforce gap estimation	Year-over-year change in percentage
North America	436 080	+8%
LATAM	515 879	-26%
EMEA	317 050	+59%

[13] Definition available in ANNEX B
[14] TMC3, Top cyber security challenges in the transport sector.
[15] TMC3, Top cyber security challenges in the transport sector.
[16] https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape
[17] Gartner, Security Spend Analytics Workbench.
[18] Revenues for commercial organisations and OPEX for Government organisations
[19] (ISC)2 2022 Workforce Study.
[20] Forbes, The Impact of The Talent Shortage on Cybersecurity Leaders.
[21] (ISC)2 Cybersecurity workforce study.

APAC	2 163 468	+52%

The global cybersecurity talent shortage adversely affects organisations' security level and roadmaps. Cyber talent recruitment and retention continue to be pain areas for most organisations. **59% of business and 64% of cyber leaders ranked talent recruitment and retention as a critical challenge for managing cyber resilience in 2023.**[22] The challenge is even more complex for security domains requiring specialised or niche skills.

By 2026, it is estimated that 60% of organisations will shift from external hiring to upskilling their existing workforce to address systemic cybersecurity recruitment challenges.[23] Quiet hiring enables organisations to strategically address acute, immediate business needs by assigning existing employees to new roles, expanding existing employees' responsibilities through stretch and upskilling opportunities, hiring temporary workers to perform specific tasks, or any combination of the three.

2.4 2030 CYBER THREATS OUTLOOK

With rapidly accelerated digital transformations, opportunistic phishing campaigns, discontinuity of information security operations and financial constraints posing unprecedented challenges for businesses everywhere, security strategies and practices are being tested like never before. Potential financial consequences of security incidents became much more accurate to many business leaders when the Irish Data Protection Commission announced its decision to impose a €265 million fine on Meta.[24] In November 2022, Facebook's parent company received this fine for violating the General Data Protection Regulation (GDPR) following a leak of more than 500 million records in the previous years. In 2022, investment fraud was the costliest form of cybercrime, with an average of $70,811 lost per victim. In 2022, the UK had the highest number of cybercrime victims per million internet users at 4783.[25]

The impact of cybercrime is estimated to reach $10 trillion in 2023. Furthermore, the figure is estimated to increase to around $24 trillion in the next four years.[26]

The ENISA Foresight 2030[27] has identified 10 significant cyber challenges that are expected to shape the landscape for OES and DSPs over the next years. Table 4 presents data points to illustrate how these threats have been evolving in order to support the potential identification of emerging areas where policy interventions could be considered.

Table 4: ENISA foresight 2030 cyber threats

2030 Cyber Threat	Key Highlights
Supply chain compromise of software dependencies	• The most significant data breach in history started in 2019 with the SolarWinds hack and affected around 18,000 customers by installing malicious code within its software[28,29]. • By 2030, organisations would have embraced DevOps predominantly as a development and operations process.

[22] World Economic Forum, Global Cybersecurity Outlook 2023.
[23] Gartner, Top Trends in Cybersecurity 2023.
[24] Gartner, How to Respond to the 2023 Cyberthreat Landscape.
[25] Aag IT, The Latest 2023 Cyber Crime Statistics.
[26] Harvard Business Review, Human Error Drives Most Cyber Incidents. Could AI Help?
[27] https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030
[28] https://edition.cnn.com/2021/01/05/opinions/solarwinds-hack-what-should-be-done-schneier/index.html
[29] https://www.politico.com/news/2020/12/19/how-federal-hack-happened-448602

2030 Cyber Threat	Key Highlights
	• Since 80% of code in modern applications relies on open-source packages, open-source software is the backbone and weakest link in the software supply chain.[30] • **Researchers at an application security company detected at least one known open-source vulnerability in 84% of all commercial and proprietary code bases while 48% of all code bases analysed contained high-risk vulnerabilities[31].**
Advanced disinformation campaigns	• AI is being used aggressively to create political content. **If the trend of AI-generated content continues, it is estimated that around 90% of the content published on the internet in 2026 will be artificially created[32].**
Rise of digital surveillance authoritarianism/loss of privacy	• OECD research **in 10 African countries found 65 examples of digital technology being used to open civic space, but 115 examples of digital technology being used to close it[33].**
Human error and exploited legacy systems within cyber-physical	• Accounting for over 80% of incidents, human error is the most significant cyber risk[34]. • There will be a significant increase in the number of smart devices the average user has associated with them increasing the probability of human error[35]. • Skills shortages in areas such as security engineering, security assessments and industrial security operations, have made it clear that developing an effective security strategy across IT and Cyber-Physical Systems (CPS) environments is complex creating an increasing demand for tools and playbooks.[36]
Targeted attacks enhanced by smart device data	• It is predicted that around 75,4 billion IOT-connected devices will be installed worldwide by 2025, thereby increasing the cyber-attack target.
Lack of analysis and control of space-based infrastructure and objects	• It is estimated that the space segment would generate more than 500,000 petabytes of data over the next ten years, leading to increased associated data risks[37].
Rise of advanced hybrid threats	• Recent reports highlight that tools being sold and traded in underground forums can parse more than 1 billion credentials and generate password variations[38]. • Through the integrated use of AI/ML and IoT technologies, autonomous vehicles are being targeted, a trend that is likely to continue in 2030. Similarly, advanced hybrid technology-powered voice cloning tools are putting voice biometrics at risk in banks.
Cross border ICT service providers as a single point of failure	• Smart cities are an excellent example of how sophisticated the ICT chain will be by 2030. The large volume of data collected through the infrastructure of smart cities is a significant concern. By exploiting the vulnerabilities in the infrastructure and through hybrid warfare, attackers can cripple an entire region.

[30] CSO, Top 10 Open-Source Software (OSS) Risks.
[31] CSO, Top 10 open-source software risks for 2023.
[32] European Commission, CERIS FCT Event: Disinformation, Fake News and Hate Speech.
[33] https://www.oecd-ilibrary.org/sites/ce08832f-en/1/3/2/9/index.html?itemId=/content/publication/ce08832f-en&_csp_=17c2a7153f8f3e72e475ec60ee15c40c&itemIGO=oecd&itemContentType=book
[34] Harvard Business Review, Human Error Drives Most Cyber Incidents. Could AI Help?
[35] ENISA, Identifying emerging cyber security threats and challenges for 2030.
[36] Gartner, Market Guide for CPS Protection Platforms.
[37] Northern Sky Research 2022.
[38] Gartner, How to Respond to the 2023 Cyberthreat Landscape.

2030 Cyber Threat	Key Highlights
	• **Global annual smart city cybersecurity revenue is projected to reach $26 billion by 2030**[39]**.**
Artificial intelligence abuse	• **73% of organisations have hundreds or thousands of AI models already deployed** • Increased use of open AI models will create more opportunities for malicious actors to steal private data[40]. • The number of AI incidents and controversies has increased 26 times since 2012 with a notable recent incident involving a deepfake video of Ukrainian president, Zelenskyy surrendering in 2022[41].

The evolving EU cybersecurity policy framework includes a number of policy files currently under development which include provisions that can mitigate a number of the aforementioned cyber threats.

- The **Cyber Resilience Act** (CRA)[42] proposal introduces common cybersecurity rules for products with digital elements, including hardware and software, with a direct aim of minimising product vulnerabilities and ensuring vulnerability management across the lifecycle of such products. Once adopted, the CRA is expected to help mitigate the challenges posed by software dependencies and insecure products in general.
- The **AI Act**[43] proposal introduces horizontal AI rules to ensure that AI systems placed on the EU market are safe, trustworthy and respect existing law on fundamental rights and EU values.
- Space is one of the new sectors of high criticality included in Annex I of **NIS2** and sector-specific legislation might be an option for the future.

These examples involve policy files that are still under development or very early in their implementation stage so their impact vis-à-vis the 2030 cyber threats is only speculative at this stage. However, their effectiveness in mitigating these threats could be the area of focus for future ENISA work to help assess the effectiveness of the EU cybersecurity policy framework.

[39] Guidehouse Insights, Cybersecurity for Smart Cities.
[40] Gartner, How to Respond to the 2023 Cyberthreat Landscape.
[41] Stanford University, Artificial Intelligence Index Report 2023.
[42] Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
[43] https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52021PC0206&sortOrder=asc

3. INFORMATION SECURITY INVESTMENTS FOR OES AND DSPS

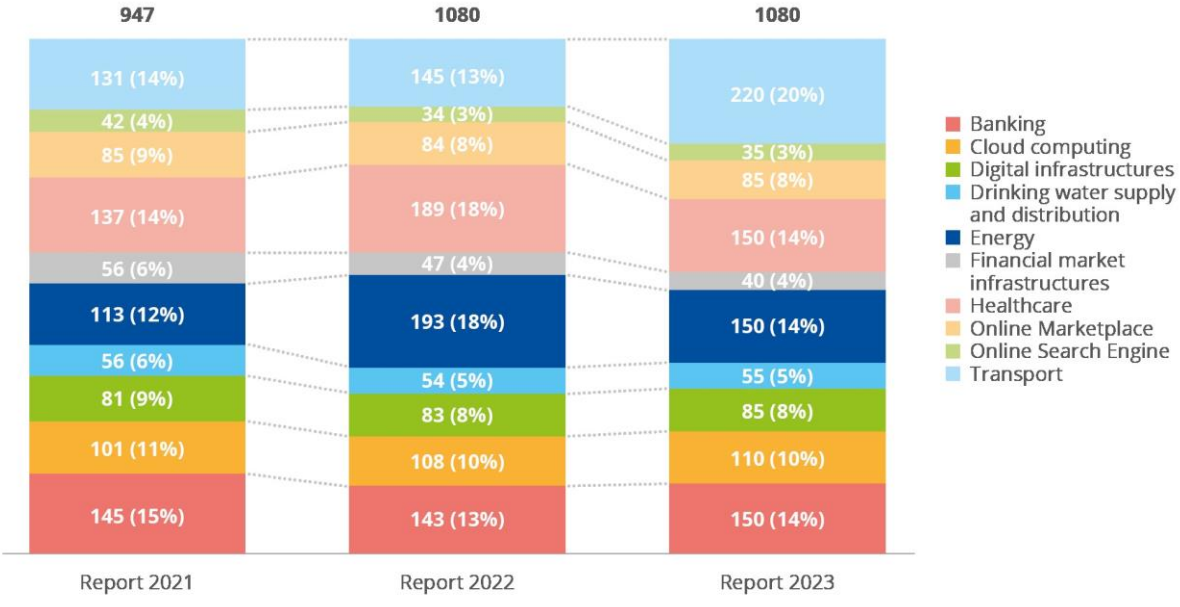
3.1 METHODOLOGY

This study is based on a dedicated market survey conducted among 1080 organisations — with 40 organisations surveyed in each Member State —identified as OESs or DSPs by the relevant national authorities. This survey data has been collected through dedicated phone interviews with cybersecurity experts and cybersecurity managers in those organisations by following a questionnaire designed specifically for the study and including both quantitative questions where ballpark figures or high-level estimates are requested and closed qualitative questions.

Some are recurring questions yearly to enable observation of NIS investment trends**. It must be noted that this study's sample is different in terms of composition and size compared to previous studies, which can influence the results and observations derived.** For more information on the design of the demographics of this year's study, please refer to ANNEX A.

A notable change in the sample composition is related to the fact that more organisations from the Transport sector were surveyed this year to perform a specific deep dive, when last year the sectoral deep dive covered Energy and Health industries. Thus, this year data was collected from 220 organisations in the Transport sector compared with 145 last year, representing a 52% increase. On the other hand, fewer data points were collected for the Energy and Health industries as they were no longer the focus industries of the report. Figure 4 illustrates the difference in sectorial distribution between this year's sample and the previous years.

Figure 4: Composition of the study sample by survey year and NIS sector



Furthermore, disparities between the historical data must be assessed in light of the macro trends and challenges that occurred in 2022 — such as, but not limited to, **increasing cost optimisation in the aftermath of the COVID-19 pandemic, the war in Ukraine and the rise of interest rates.**

The quantitative metrics collected in the survey have been analysed based on a median and average approach for the reader to appreciate both viewpoints. **When only one value is presented, this reflects the median value of the specific metric**.

Though not necessarily representing the "typical" value in a highly fragmented dataset, the median value should be regarded as the more representative value for OESs or DSPs within a specific sector or country. The average value will often be higher when it is affected by large organisations that do not necessarily reflect the populated and fragmented market of most industries and countries analysed.

By way of example:

- The median value for Information Technology spending is €10 million in 2022 (cf. Figure 5). This implies that an OES or DSP within the European Union spends around €10 million in Information Technology yearly.
- In contrast to this median value, the average Information Technology spending for OES and DSP in the European Union amounts to € 83.6 million. Still, this number is skewed by large organisations with significant budgets dedicated to Information Technology.

Regarding the qualitative metrics collected for this market study, the distribution of the organisations' answers has been calculated in percentage form to balance the weight of each solution against the others.

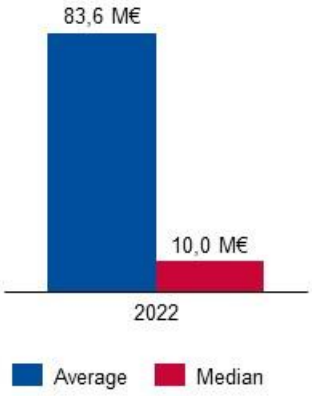
3.2 SPENDING ON INFORMATION SECURITY

Key Figures
The median Information Technology (IT) spending of an OES or DSP in the EU was 10,0 M€ million in 2022, while the average value of IT spending was 83,6 M€ over the same period.
The median spending for information security (IS) of an OES and DSP in the EU was 700 k€ 2022, while the average expenditure was 5,1 M€
An OES or DSP in the EU earmarks 7,1% of its IT investments for information security, while the average value is 7,6%. An increase of 0,4% is observed compared to the median vs IT spending in 2021
58% of the OES and DSPs surveyed this year had yet to subscribe to a dedicated cyber insurance solution in 2022. Contrary to the findings in previous years, the cyber insurance market now appears to be active/developed in all EU MS

3.2.1 IT spending

Survey Question: What was your organisation's estimated IT budget or spending in Euros for 2022 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

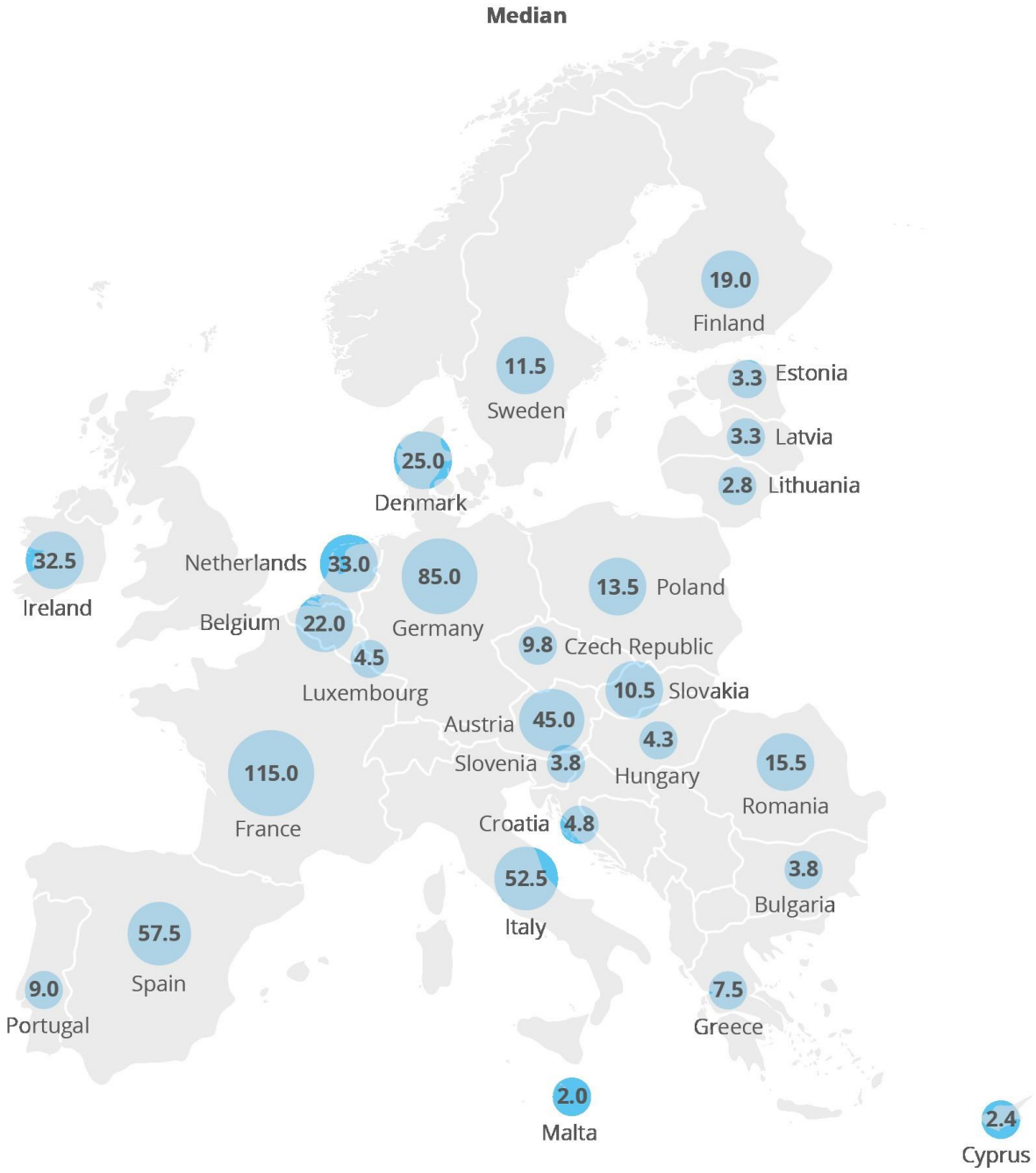
Figure 5: IT spending - all NIS sectors



The median Information Technology (IT) spending of an OES or DSP in the EU was EUR 10 million in 2022, while the average value of IT spending was EUR 83.6 million over the same period.

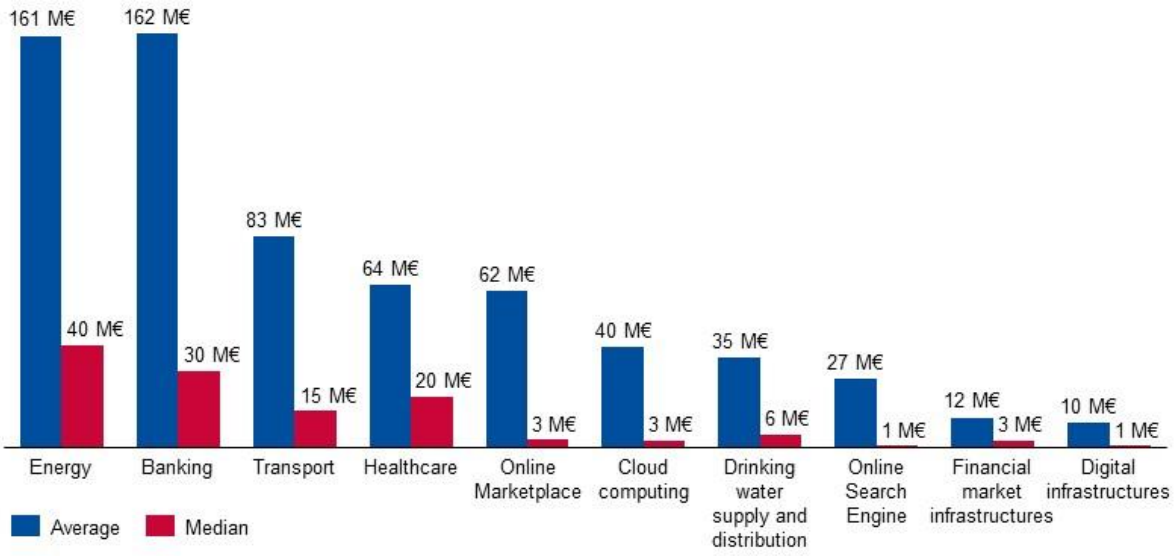
While these are absolute values that must be interpreted in light of the sector's structure and company size, a smaller budget does not necessarily imply a lower level of cybersecurity maturity. Furthermore, as detailed in the methodology section, it must be noted that the sample in this study was different in terms of composition and size compared to previous studies, which can influence the results and observations derived.

Figure 6: IT Spending of OES and DSPs surveyed in each Member State



NB: The map visualisations throughout the report depict data collected from the OESs and DSPs surveyed in each Member State. Hence, investment data refers to the average among the OESs and DSPs surveyed, not Member State's investments. In addition, when interpreting these figures, the market fragmentation or average operator size in each Member State and the criteria for identifying OESs and DSPs in each Member State — including the size of OESs and DSPs — need to be factored in.

Figure 7: IT spending by NIS sector

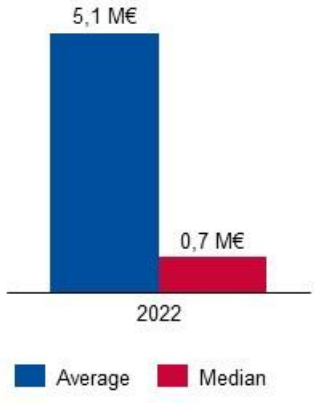


The survey data indicates that median IT spending is highest within the Energy sector (40 M€), followed by Banking (30 M€), Healthcare (20 M€) and Transport industries (15 M€). The IT spending in these industries significantly exceeds IT spending in other NIS industries, as illustrated in Figure 7. Furthermore, Online Search Engines and Digital Infrastructures have the lowest IT spending across all sectors, with a median expenditure of 1 million euro.

3.2.2 IS spending

Survey Question: What was your organisation's estimated Information Security budget or spending in Euros for 2022 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

Figure 8: Information security spending - all NIS sectors



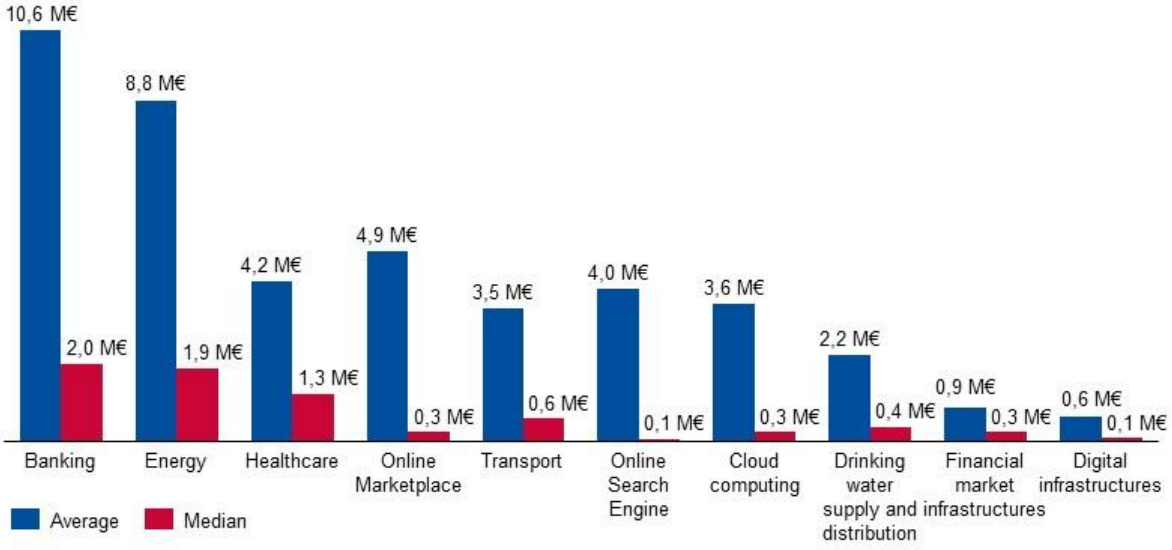
The survey data indicates that the median spending for information security (IS) of an OES and DSP in the EU was 700 k€ in 2022, while the average expenditure was 5,1 M€.

While these are absolute values that must be interpreted in light of the sector's structure and company size, a smaller budget does not necessarily imply a lower level of cybersecurity maturity.

Furthermore, as detailed in the methodology section, it must be noted that the samples in this report are different in composition and size compared to previous studies, which can influence the results and observations derived.

Figure 9: IS spending of the OES and DSPs surveyed in each Member State

Figure 10: Information security spending by NIS sector

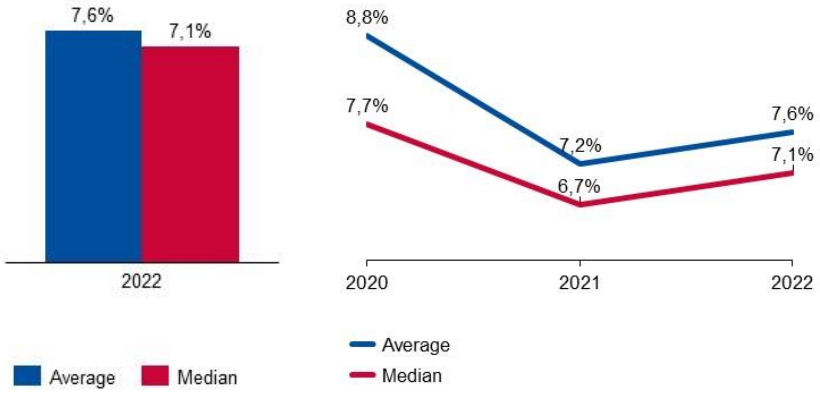


The Banking sector has the highest IS spending (2,0 M€), followed by the Energy (1,9 M€) and Healthcare sectors (1,3 M€). Furthermore, the information security spending of Digital Infrastructure organisations is the lowest, amounting to a median spending of 100 000 €.

3.2.3 IS spending as a share of IT spending

To define the importance of IS spending for an OES or DSP, the relative share of IS spending against the overall IT spending was calculated and illustrated in the figure below.

Figure 11: Information security spending as a share of IT spending - all NIS sectors



Looking at the median value, an OES or DSP in the EU earmarks 7,1% of its IT investments for information security, while the average value is 7,6%. When analysing this normalised data set with historically available data, an increase of 0,4% is observed compared to the median was vs IT spending in 2021. This is still lower than the 2020 figures where the median IS vs. IT spend ratio was 7,7%.

As detailed in the methodology section, the historical analysis must be done while considering the slight differences in the samples between the years of study and the differences in the macro environment.

Figure 12: IS spending as a share of IT spending of OES and DSP surveyed in each Member State

Figure 13: IS spending as a share of IT spending, per NIS sector

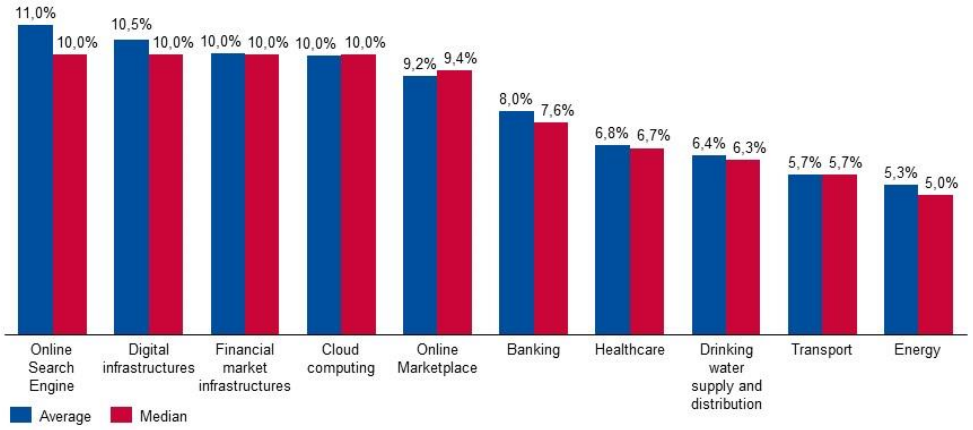


Figure 14: IS spending vs IT spending per NIS sector, using median values

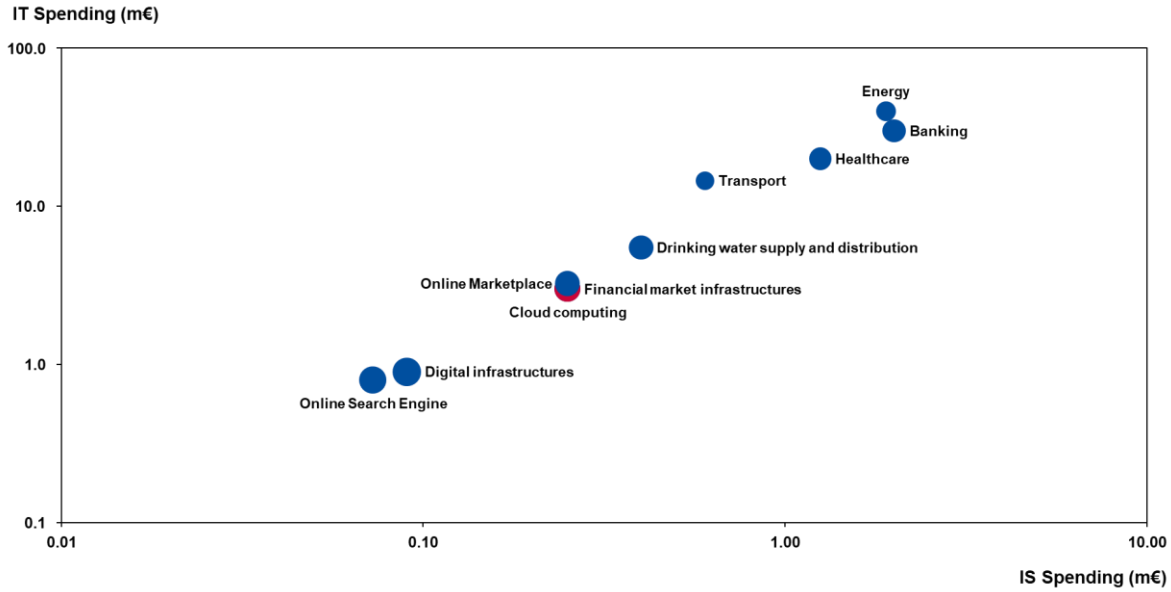
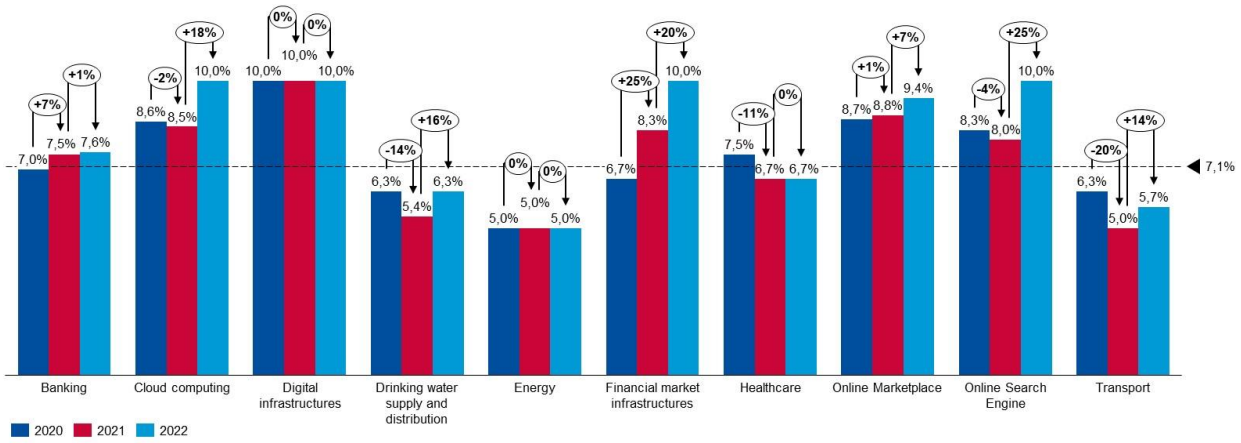


Figure 14 depicts the IS spending against IT spending for the different NIS sectors. Cloud computing and financial market infrastructures are both on the same bubble (indicated in red) with identical ratios.

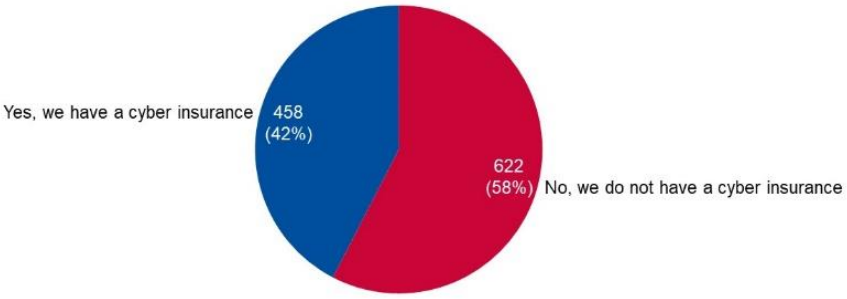
Figure 15: Year-over-year evolution of the IS vs. IT spend median ratio per NIS sector



3.2.4 Cyber insurance

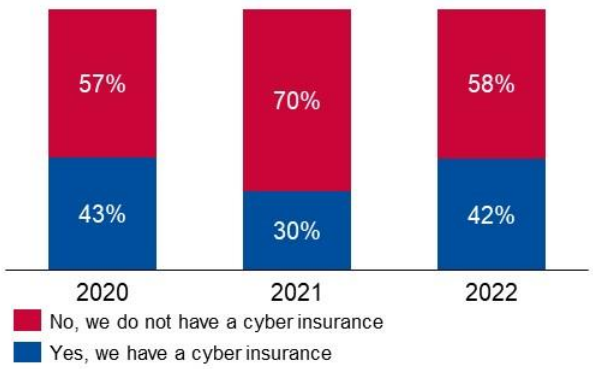
Survey Question: Did your organisation subscribe to a dedicated cyber insurance solution?

Figure 16: Did your organisation subscribe to a dedicated cyber insurance solution?



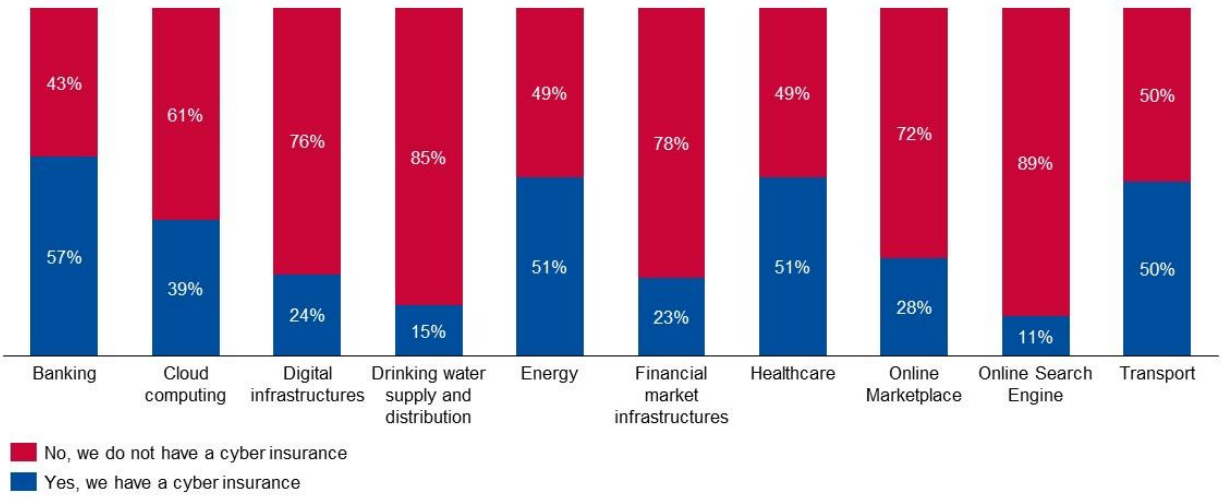
According to Figure 16, 58% of the OES and DSPs surveyed this year had yet to subscribe to a dedicated cyber insurance solution in 2022.

Figure 17: Year over-year evolution of cyber insurance subscription



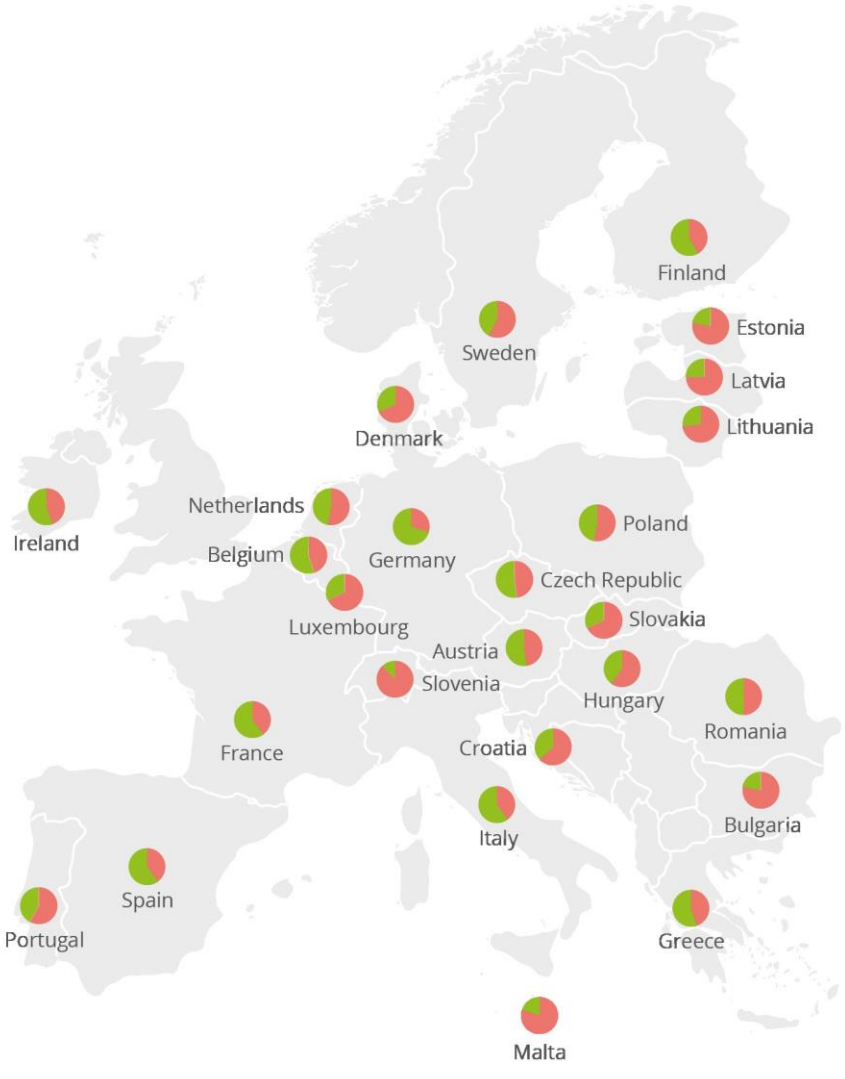
The data analysis over the years shows that the organisations surveyed this year have a subscription rate to a cyber insurance solution close to the level observed in 2020, and higher than the one captured in 2021 (42% in 2022 and 30% in 2021).

Figure 18: Cyber insurance solution subscription rate per NIS sector



The breakdown of the data per NIS industries highlights significant differences in subscription rates between sectors. Banking, Energy, Healthcare and Transport show subscription rates higher than 50% when Cloud Computing is at 39% and all the others below 28%.

Figure 19: Cyber insurance solution subscription rate for OES/DSP surveyed in each Member State



	% No, we do not have a cyber insurance	% Yes, we have a cyber insurance
Austria	47.5	52.5
Belgium	45.0	55.0
Bulgaria	77.5	22.5
Croatia	62.5	37.5
Czech Republic	47.5	52.5
Denmark	67.5	32.5
Estonia	77.5	22.5
Finland	42.5	57.5
France	40.0	60.0
Germany	30.0	70.0
Greece	45.0	55.0
Hungary	60.0	40.0
Ireland	45.0	55.0
Italy	40.0	60.0
Latvia	75.0	25.0
Lithuania	72.5	27.5
Luxembourg	67.5	32.5
Malta	80.0	20.0
Netherlands	52.5	47.5
Poland	52.5	47.5
Portugal	57.5	42.5
Republic of Cyprus	67.5	32.5
Romania	50.0	50.0
Slovakia	67.5	32.5
Slovenia	87.5	12.5
Spain	40.0	60.0
Sweden	57.5	42.5

When examining the cyber insurance subscription rate per Member State, an important finding is that, contrary to the findings in previous years, the cyber insurance market now appears to be active/developed in all EU MS.

3.3 INFORMATION SECURITY AND NIS STAFFING

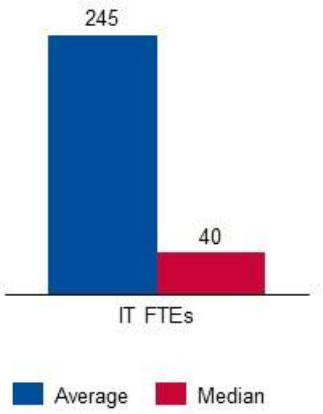
Key Figures
Looking at the median value, an OES or DSP in the EU allocates 11,9% of its IT FTEs for information security, while the average value is 14,5%. The values are slightly lower compared to 2021, despite the overall increase in information security spending.
An OES or DSP in the EU employs an 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

An OES or DSP in the EU employs a median of 20% contractors for his IS FTEs and an average of 25%.
Cybersecurity operations is the security domain with the most contractors, with 57% of the surveyed organisations selecting it, followed by IT security architecture and engineering with 18% and cybersecurity auditing and compliance with 11%.
Across all sectors, the security domain with the most IS FTEs is Cybersecurity operations with 40% of the IS FTEs, followed by IT security architecture and engineering with 23% of the IS FTEs, and cybersecurity governance and risk management with 21%. The security domain with the least IS FTEs is cybersecurity auditing and compliance with 16% of the IS FTEs.
552 out of 1080 organisations (51%) plan to hire information security personnel in the next 2 years. The median number of planned hires is 2 FTEs, with an average of 4 FTEs, meaning that larger organisations will drive even more recruitment than small ones.
Cybersecurity operations come out as the security domain with the most anticipated hires (56%), followed by IT security architecture and engineering (42%) and cybersecurity governance and risk (36%). The security domain with the least hiring expected is cybersecurity auditing and compliance with 27% of the organisations planning to hire cybersecurity resources selecting it.
83% of the surveyed organisations claim recruitment difficulties in at least one information security domain.
The security domain identified as the most difficult to hire is IT security architecture and engineering (34%). Cybersecurity operations is second (26%), closely followed by cybersecurity auditing and compliance (26% as well). Cybersecurity governance and risk come last (24%). 233 organisations (22%) have faced difficulties hiring in all cybersecurity domains.
47% of the surveyed organisations declare no specific budget for information security training. For the 573 organisations with a specific information security budget, the median training budget is 100k€, with an average of 333 k€, influenced by larger organisations with bigger budgets

3.3.1 IT FTEs

Survey Question: What was your organisation's estimated number of IT FTEs for 2022 including internal staff and contractors?

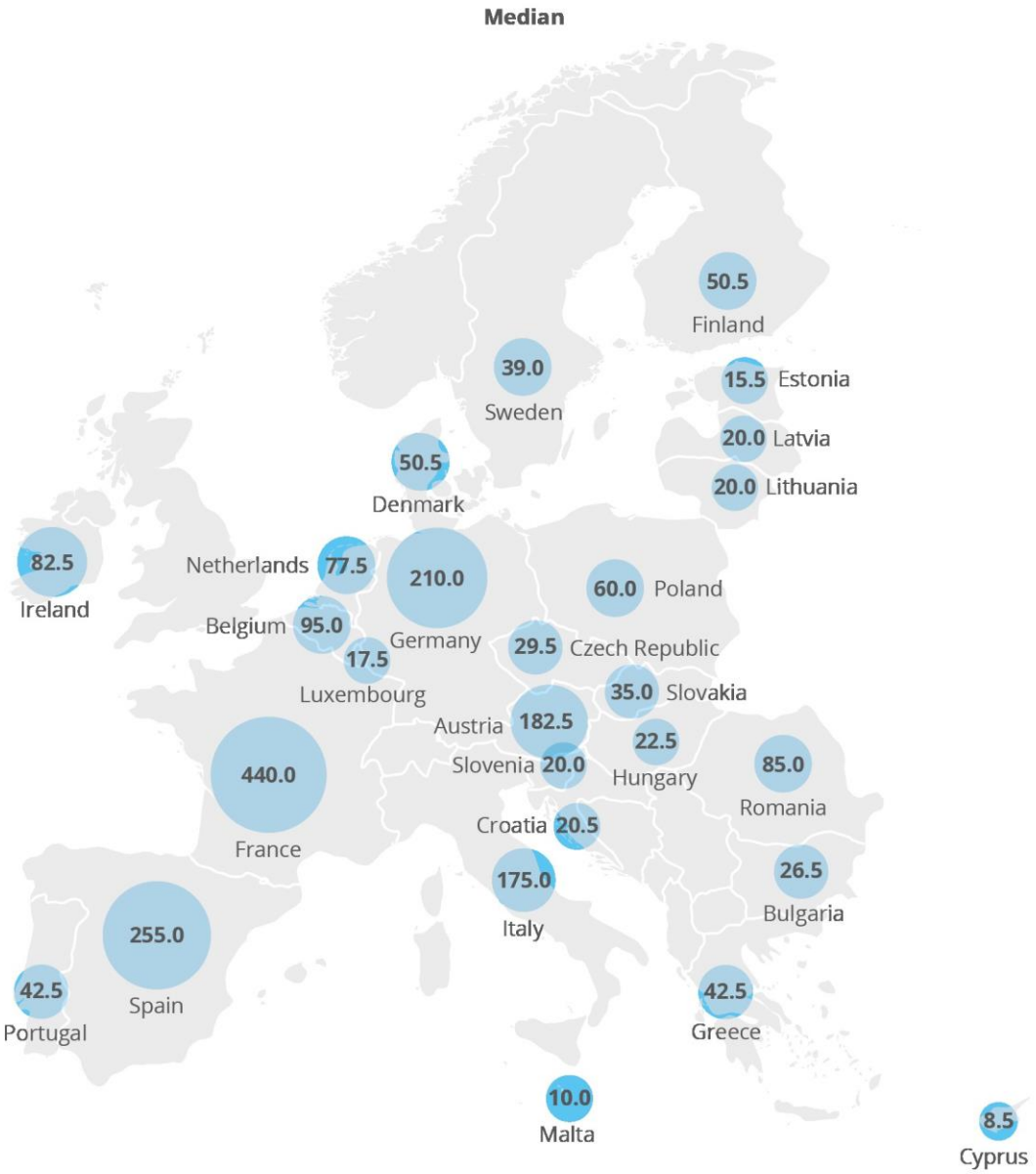
Figure 20: IT FTEs - all NIS sectors



The survey data indicates that an OES or DSP in the EU employs a median of 40 IT FTEs and an average of 245 IT FTEs. The disparity between the median and average values indicates that most organisations use a low number of IT FTEs while larger organisations engage a substantial number of IT FTEs.

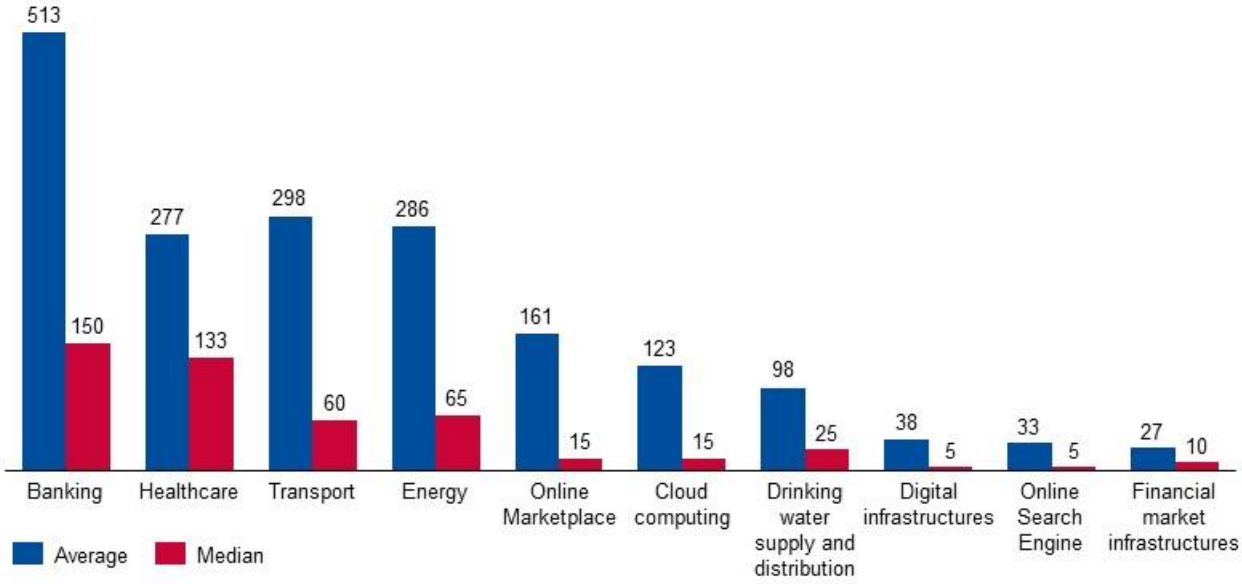
While these are absolute values that must be interpreted in light of the sector's structure and company size, a smaller number of FTEs does not necessarily imply a lower level of cybersecurity maturity. Furthermore, as detailed in the methodology section, it should be noted that this sample is different in terms of composition and size compared to previous studies, which can influence the results and observations derived.

Figure 21: IT FTEs for OESs and DSPs surveyed by Member State



Significant discrepancies exist in the total number of IT FTEs in the organisations surveyed among Member States, with median values ranging from over 400 IT FTEs in France to 9 employees in Cyprus. When interpreting these figures, the market structure and size of the organisations surveyed in each Member State must be factored in, as well as the criteria for identifying OESs or DSPs.

Figure 22: IT FTEs by sector

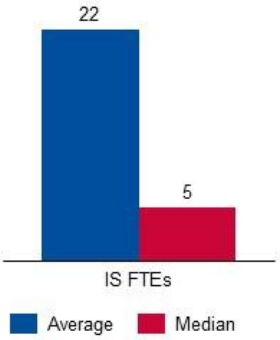


As illustrated in Figure 22 there are significant discrepancies in the number of IT FTEs across industries. For example, the Banking sector has the most considerable median value of 150 IT FTEs, which is 2,5 times higher than the median value of the Transport sector, which employs a median of 60 IT FTEs. Online Search Engines and Digital Infrastructure have the lowest median value with 5 IT FTEs.

3.3.2 IS FTEs

Survey Question: What was your organisation's estimated number of Information Security FTEs for 2022 including internal staff and contractors?

Figure 23: IS FTEs - all NIS sectors



The survey data indicates that an OES or DSP in the EU employs a median of 5 IS FTEs and an average of 22 IS FTEs. The disparity between the median and average values indicates that most organisations use fewer IS FTEs while larger organisations engage a substantial number of IS FTEs.

Figure 24: IS FTEs for OESs and DSPs surveyed in each Member State

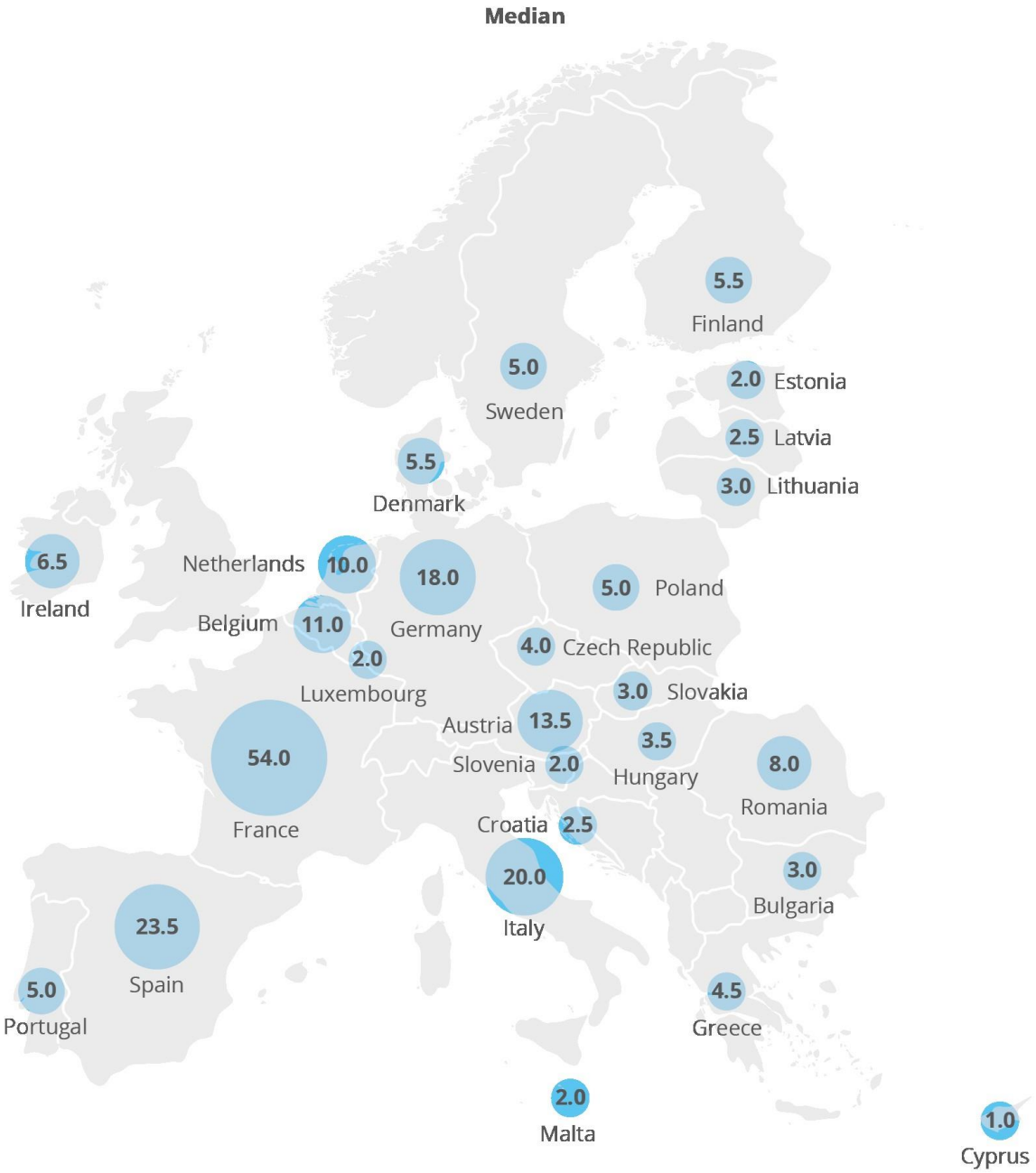
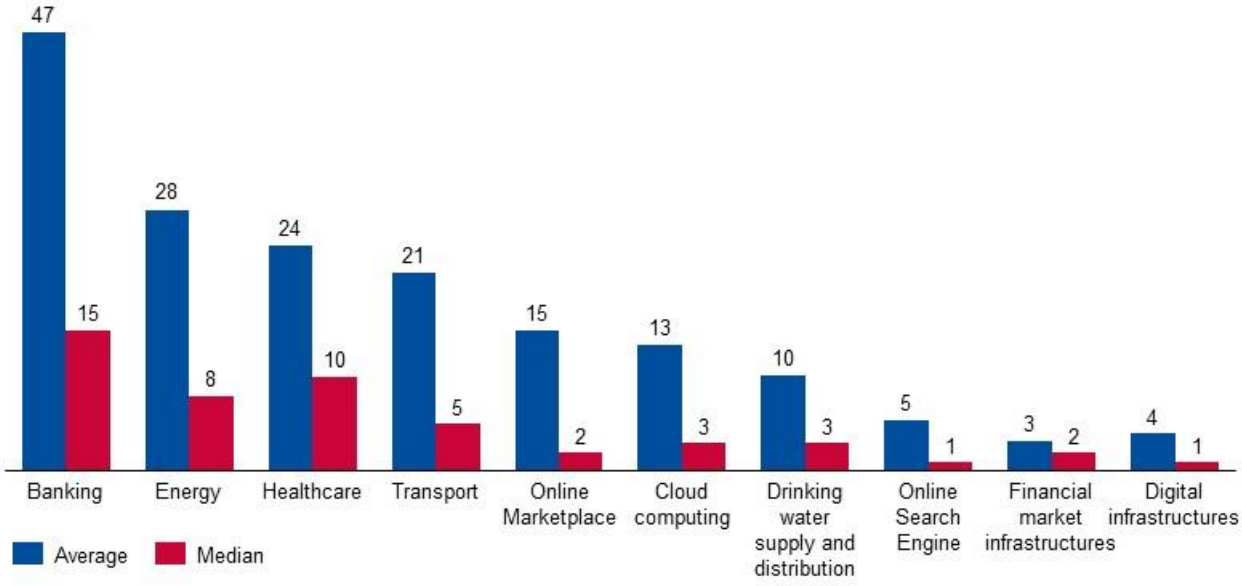


Figure 25: IS FTEs by NIS sector

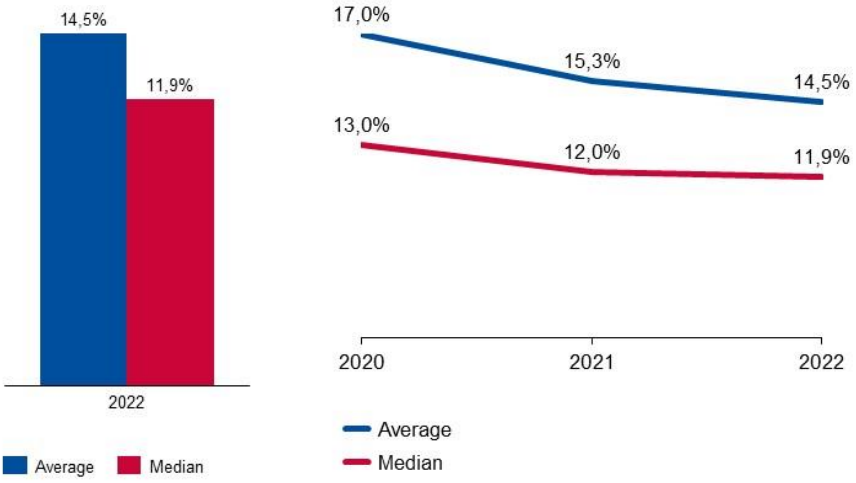


As illustrated in Figure 25, the Banking sector has the highest number of IS FTEs, with a median value of 15 FTEs in 2022, followed by the Healthcare and Energy industries, with 10 and 8 FTEs, respectively. With one FTE each, the Digital Infrastructure and Online Search Engine industries have the lowest median number of IS FTEs.

3.3.3 IS FTEs as a share of IT FTEs

To determine how cybersecurity is prioritised in terms of resources within a given organisation, the relative share of IS FTEs against the overall IT FTEs was calculated and is depicted in the figure below.

Figure 26: IS FTEs as a share of IT FTEs - all NIS sectors



Looking at the median value, an OES or DSP in the EU allocates 11,9% of its IT FTEs for information security, while the average value is 14,5%. When analysing this normalised data set with historically available data, a decrease of 0,1% is observed compared to the median IS FTEs vs. IT FTEs ratio in 2021.

As detailed in the methodology section, the historical analysis must be done while considering the slight differences in the samples between the years of study and the differences in the macro environment.

Figure 27: IS FTEs as a share of IT FTEs for OES/DSP surveyed in each Member State

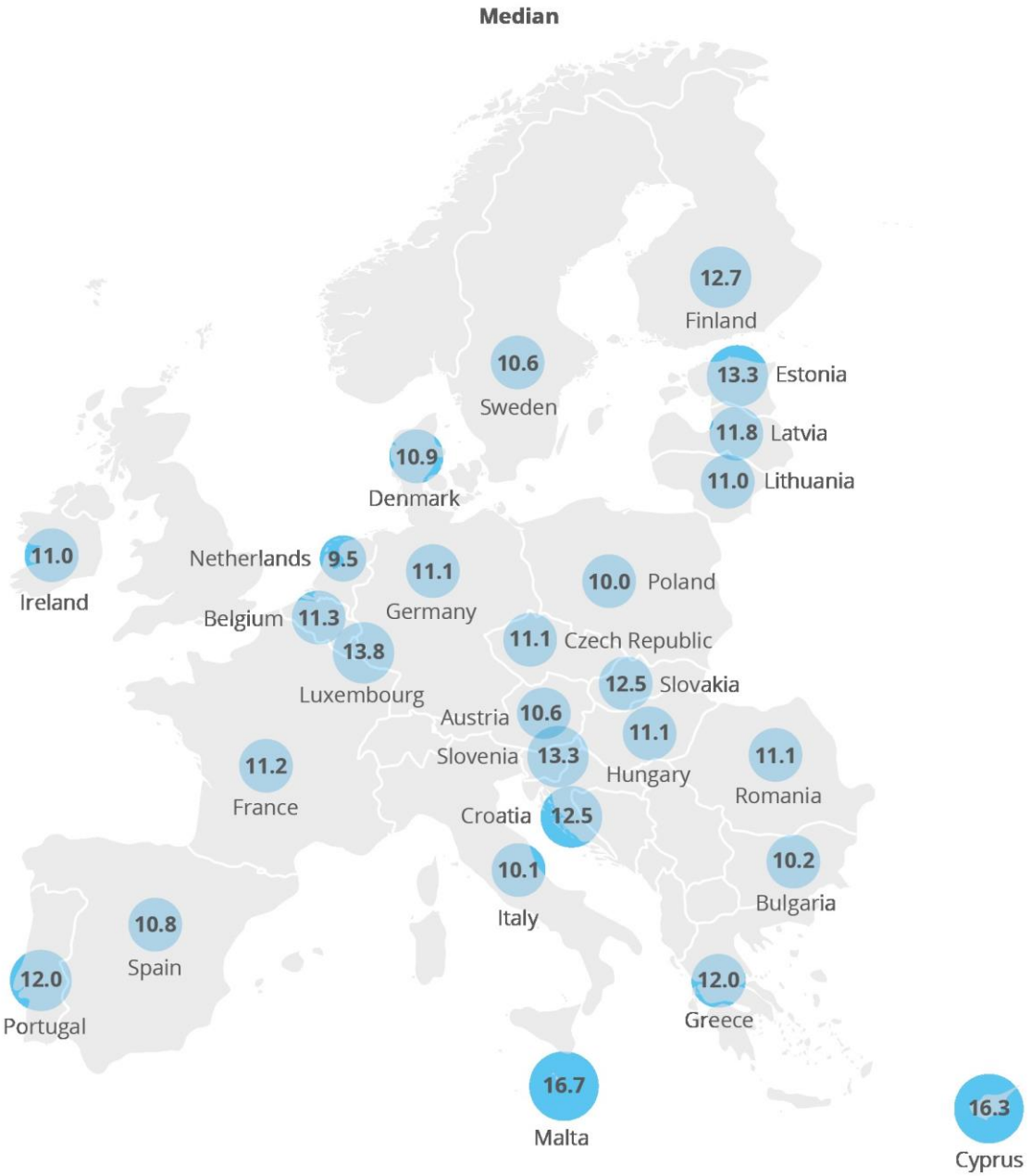


Figure 28: IS FTEs as a share of IT FTEs, per NIS sector

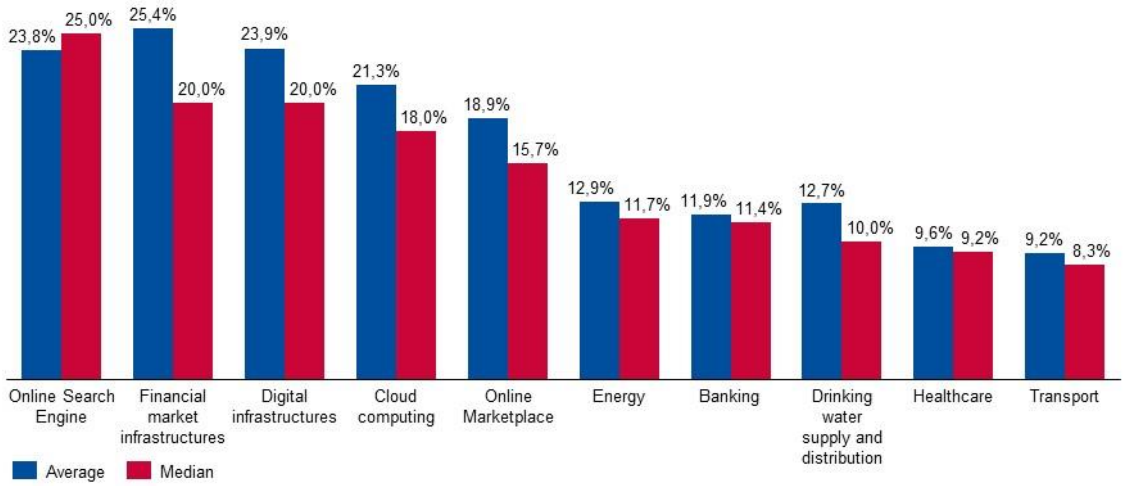
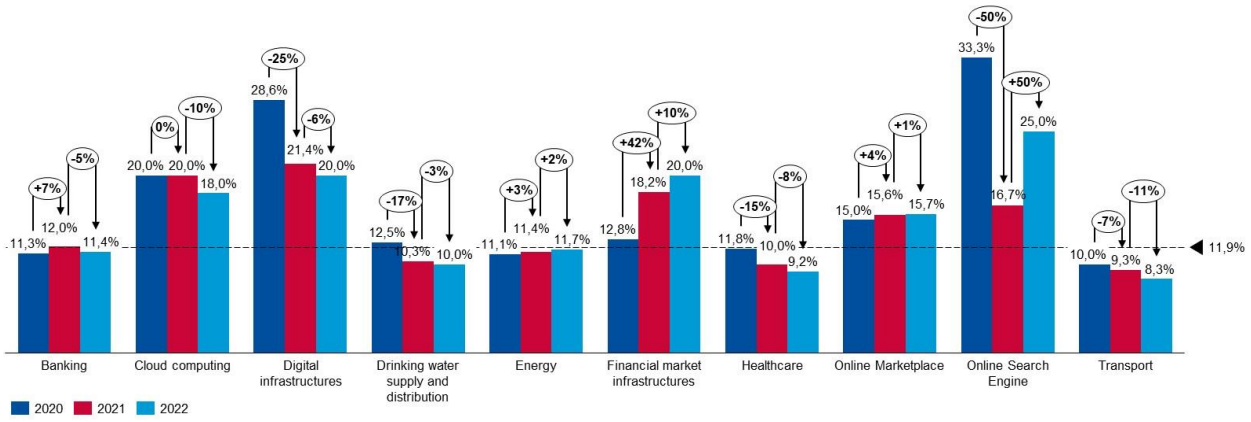


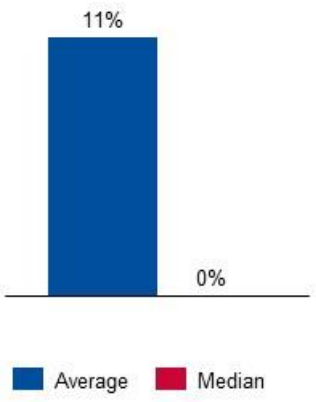
Figure 29: Year-over-year evolution of the IS FTEs vs. IT FTEs median ratio per NIS sector



3.3.4 Percentage of women in IS FTEs

<u>Survey Question:</u> Could you please indicate the percentage of women in your organisation's estimated Information Security FTEs, including internal staff and contractors?

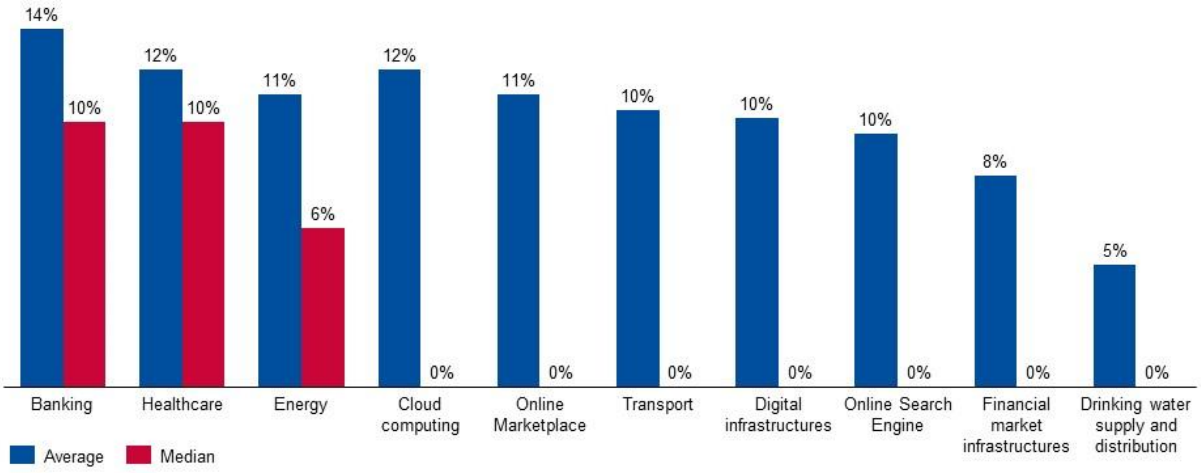
Figure 30: Percentage of women in IS FTEs, all NIS sectors



From the data collected, we can observe that an OES or DSP in the EU employs 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**.

Figure 31: Median percentage of women in IS FTEs for OES and DSPs surveyed in each Member State

Figure 32: Percentage of women in IS FTEs, per NIS sector

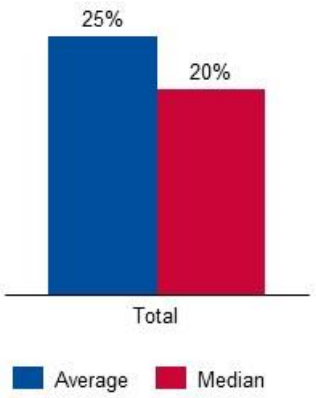


The sectoral breakdown illustrates that Banking, Healthcare, and Energy are the only industries with a positive median regarding the share of women within the IS FTEs. For all the other sectors, the median is zero, meaning that **50% or more of the surveyed organisations do not have women as part of their information security staffing**.

3.3.5 Percentage of contractors[44] in IS FTEs

Survey Question: Could you please indicate the percentage of contractors in your organisation's estimated Information Security FTEs?

Figure 33: Percentage of contractors in IS FTEs, all NIS sectors



From the data collected, we can observe that an OES or DSP in the EU employs a median of 20% contractors for his IS FTEs and an average of 25%.

[44] Contractor FTEs are defined as FTEs who are supplemental to an organisation's staff and are "operationally" managed by the in-house staff.

Figure 34: Percentage of contractors in IS FTEs for OES and DSPs surveyed in each Member State

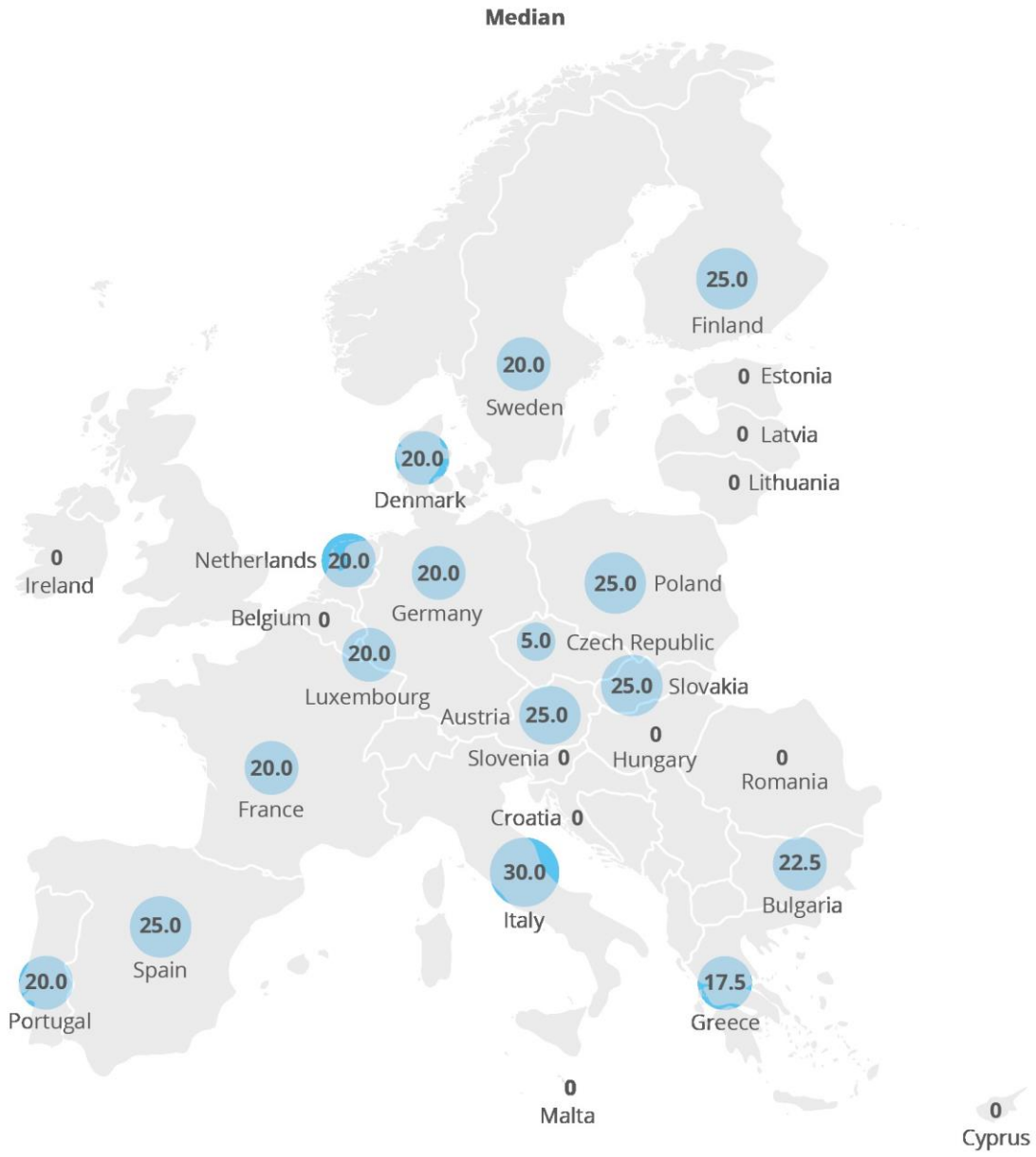
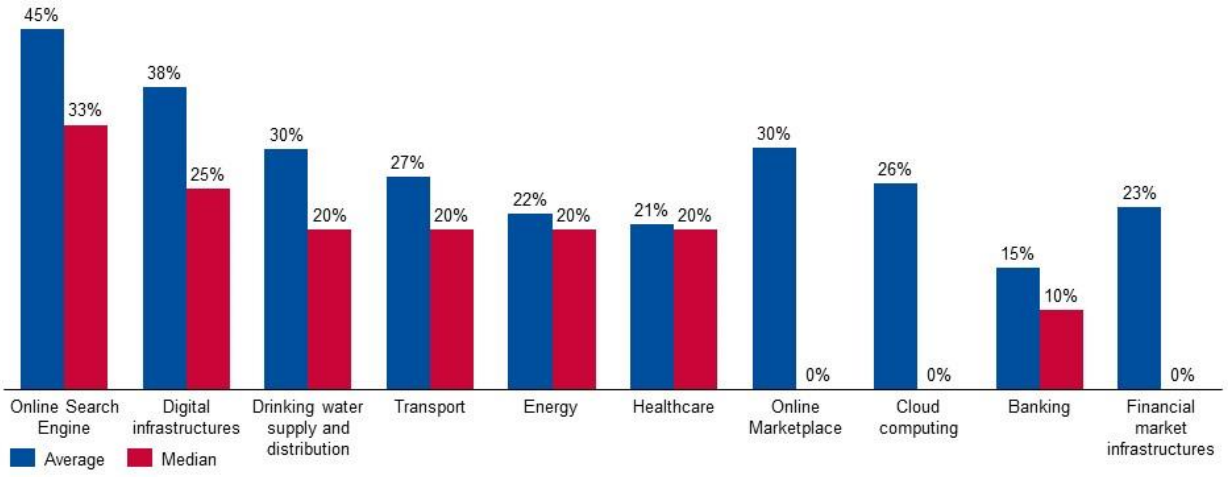


Figure 35: Percentage of contractors in IS FTEs, per NIS sector



The sectoral breakdown illustrates that Online Search Engine and Digital Infrastructures have more than one-third of their IS FTEs as contractors on average.

50% or more of the organisations surveyed in the Online Marketplace, Cloud Computing, and Financial market infrastructures industries do not employ contractors for their information security staffing.

3.3.6 Security domain with the highest share of contractors

Survey Question: In which security domain do you have the most contractors?

Figure 36: Information security domain with the highest share of contractors, per NIS sector

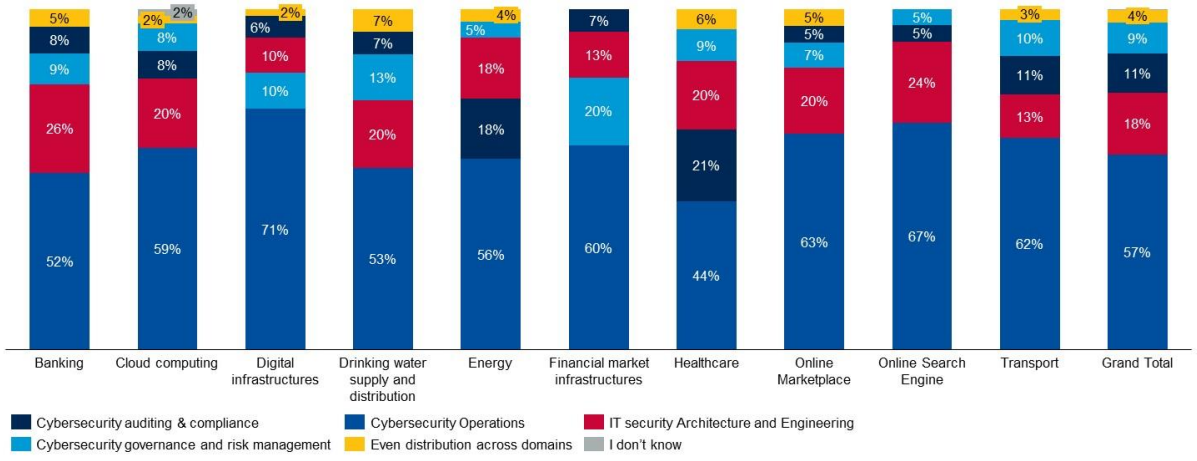


Figure 36 depicts the information security domains with the highest share of contractors per NIS sector and the average across all sectors under the Grand Total column. The defined security domains that serve as a point of reference are the following:

- Cybersecurity governance and risk (responsible for cybersecurity strategy, policies & risk management)
- Cybersecurity auditing (including internal assessor) & compliance
- IT security architecture and engineering (including IT patching)
- Cybersecurity operations (incident response & Threat intelligence)

The security domains are mapped to 10 of the 12 cybersecurity profiles defined in **the European Cybersecurity Skills Framework** (ECSF)[45]. The relevant mapping is available in ANNEX B. The profiles of Cybersecurity Educator and Cybersecurity Researcher were excluded from this mapping as they were deemed not particularly relevant for the cybersecurity organisation and operation of OES and DSPs.

Overall, cybersecurity operations is the security domain with the most contractors, with 57% of the surveyed organisations selecting it, followed by IT security architecture and engineering with 18% and cybersecurity auditing and compliance with 11%. The security domain with the fewer contractors is cybersecurity governance and risk management, with 9%. 4% of the surveyed organisations have an even distribution of contractors across disciplines.

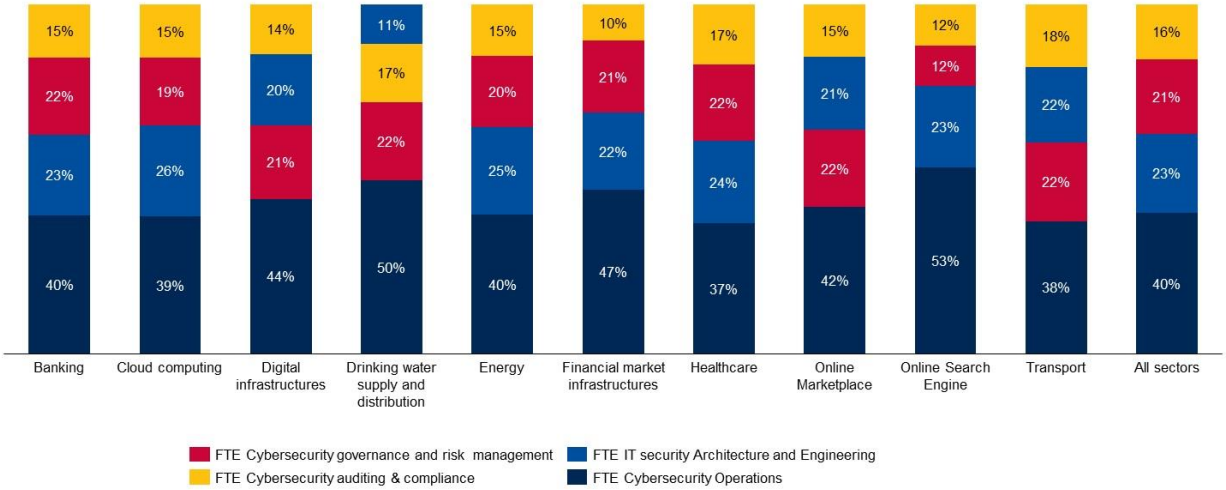
The domain with the highest share of contractors is cybersecurity operations for all NIS sectors, while the second domain may vary depending on the sector.

Indeed, banking, cloud computing, drinking water supply and distribution, online marketplace, online search engines and transport put IT security architecture and engineering second when energy and healthcare select cybersecurity auditing and compliance and financial market infrastructures and digital infrastructures identify cybersecurity governance and risk management as their second highest domain with most contractors.

3.3.7 IS FTEs distribution per security domain

Survey Question: What percentage of the IS resources in your organisation operate under each of the four significant security domains? The sum of the distribution should be 100%.

Figure 37: Distribution of IS FTEs per security domain, per NIS sector



Across all sectors, the security domain with the most IS FTEs is Cybersecurity operations with 40% of the IS FTEs, followed by IT security architecture and engineering with 23% of the IS FTEs, and cybersecurity governance and risk management with 21%. The security domain with the least IS FTEs is cybersecurity auditing and compliance with 16% of the IS FTEs.

3.3.8 Security domain with most internal resources

[45] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Survey Question (only for those that could not share the IS FTEs distribution per security domain): **Which of the following security domains has the most internal resources? (Pick one)**

Figure 38: Security domain with most internal resources

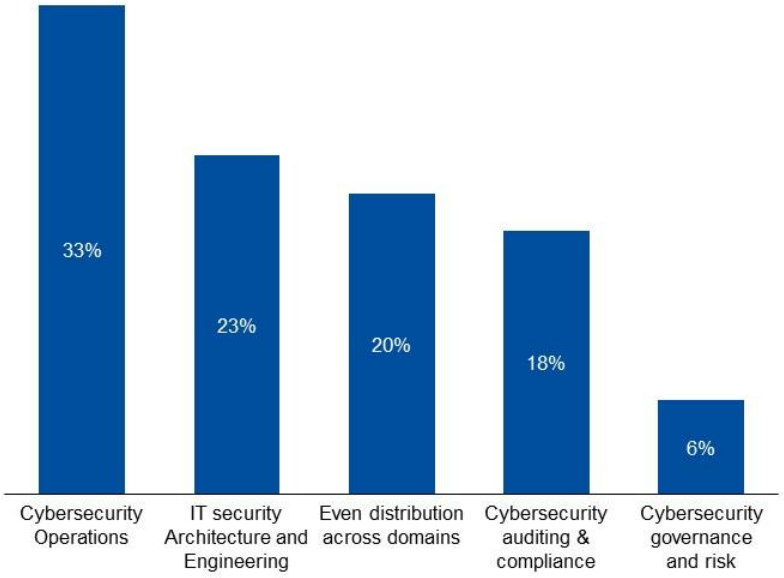
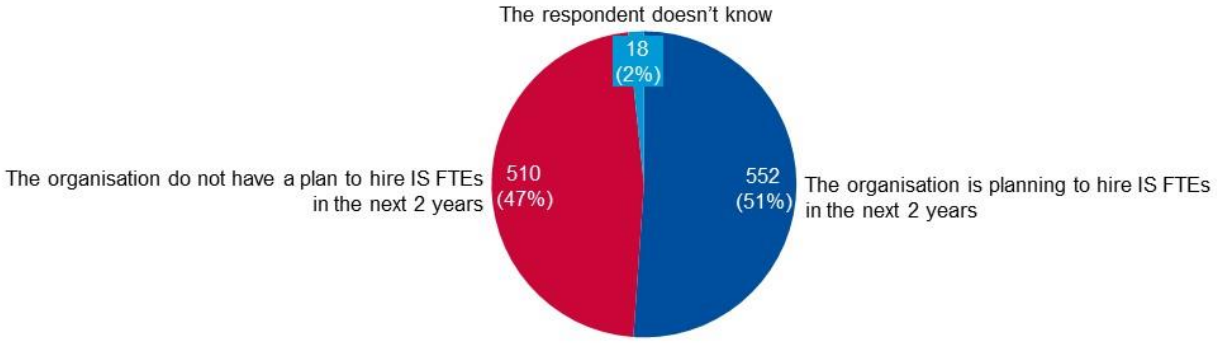


Figure 38 represents the number of times a domain was selected as the security domain with the most internal resources by the respondents that were not able to share a more accurate distribution. The overall ranking of the security domains is aligned to the previous analysis of FTE distribution done with Figure 37.

3.3.9 Hiring of Information Security FTEs in the next two years

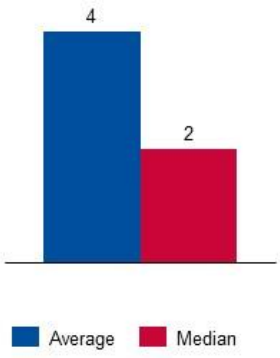
Survey Question: **How many Information Security FTEs do you expect to hire internally in the next two years?**

Figure 39: Answers to IS FTEs hiring in the next two years



Out of the 1080 organisations surveyed, 47% do not have a planning to hire IS FTEs in the next two years, and 51% were able to share their plan.

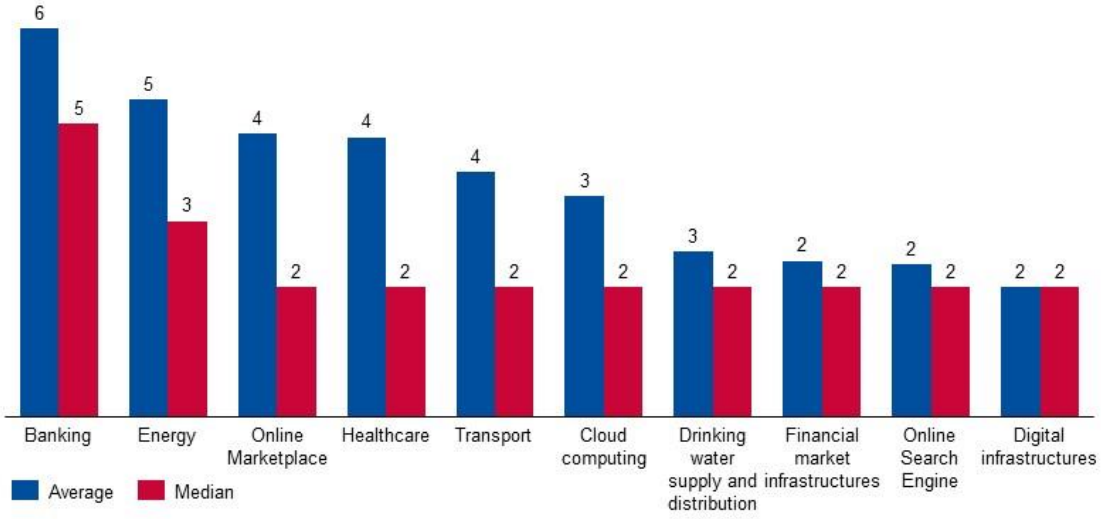
Figure 40: IS FTEs hiring all NIS sectors in the next two years.



The 552 organisations planning to hire information security FTEs in the next two years aim to hire 2 FTEs, with an average of 4 FTEs, meaning that larger organisations will drive even more recruitment than small ones.

Figure 41: IS FTEs hiring in the next two years for OES and DSPs surveyed in each Member State

Figure 42: IS FTEs hiring in the next two years, per NIS sector

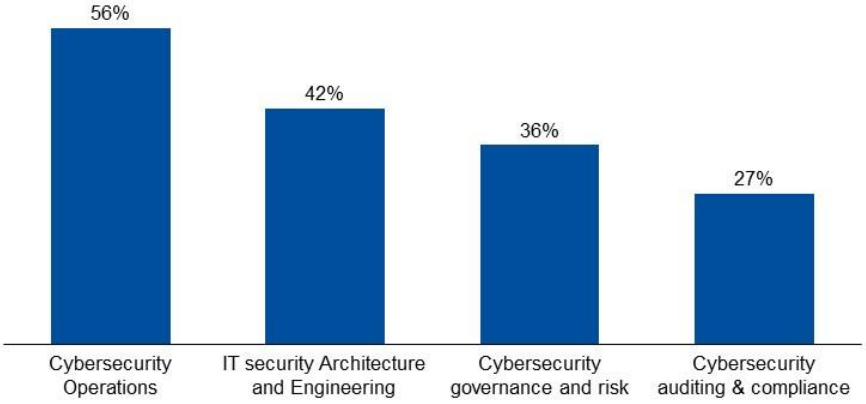


Banking is the NIS sector that anticipates the most hiring in the next two years with 5 IS FTEs planned on median per OES, followed by Energy with 3 IS FTEs planned to hire. All the other NIS industries plan to hire on median 2 IS FTEs in the next two years.

3.3.10 Information security domain with most hires expected

Survey Question: What are the security domains where you wish to hire the most security resources? (Multiple choices possible)

Figure 43: Information security domain with most hires expected



The above figure shows the **information security domains with the most hires expected for the 552 organisations having actual plans to hire** (see Figure 39). Cybersecurity operations come out as the security domain with the most anticipated hires (56%), followed by IT security architecture and engineering (42%) and cybersecurity governance and risk (36%). The security domain with the least hiring expected is cybersecurity auditing and compliance with 27% of the organisations planning to hire cybersecurity resources selecting it.

Figure 44: Security domain with most hires expected, per NIS sector

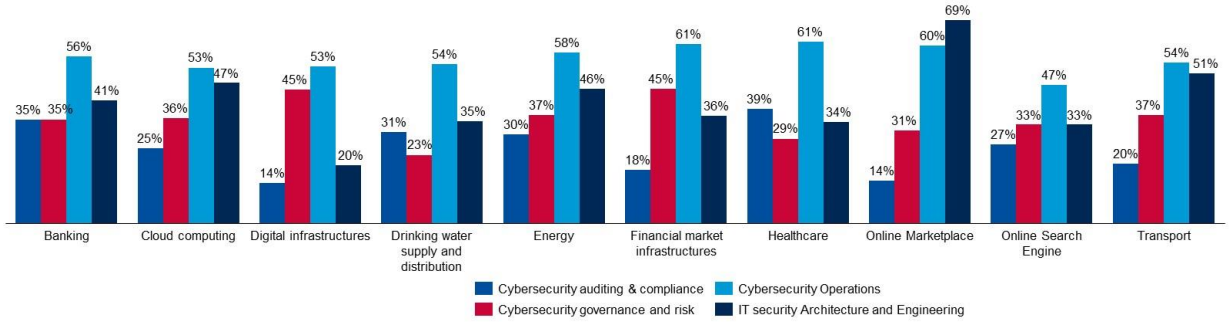
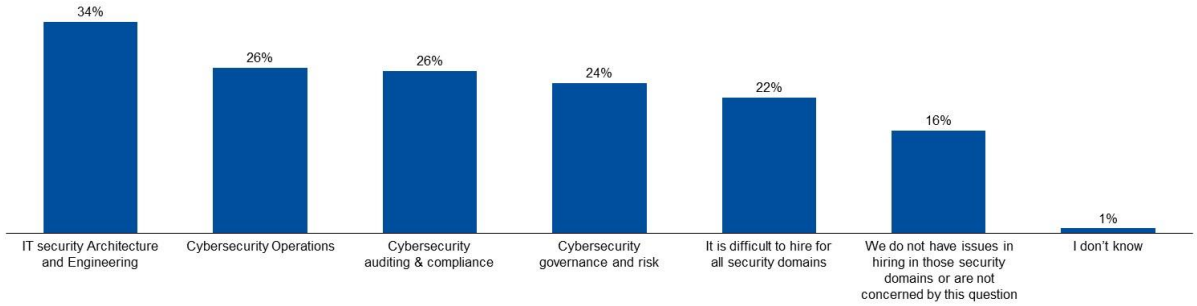


Figure 44 shows the breakdown of the answers for each of the NIS sector. The percentage is calculated based on the total number of organisations from the sector having effective plans to hire security resources.

3.3.11 Security domain with difficulties to hire

Survey Question: Are there security domains where you face hiring difficulties? (Multiple choices possible)

Figure 45: Security domains with difficulties in hiring



When asked if there are information security domains for which they face difficulties hiring resources, 176 organisations (16%) declare not having problems hiring, while 83% claim recruitment difficulties in at least one information security domain.

The security domain identified as the most difficult to hire is IT security architecture and engineering (34%). Cybersecurity operations is second (26%), closely followed by cybersecurity auditing and compliance (26% as well). Cybersecurity governance and risk come last (24%). 233 organisations (22%) have faced difficulties hiring in all cybersecurity domains.

Figure 46: Security domains with difficulties in hiring, per NIS sector

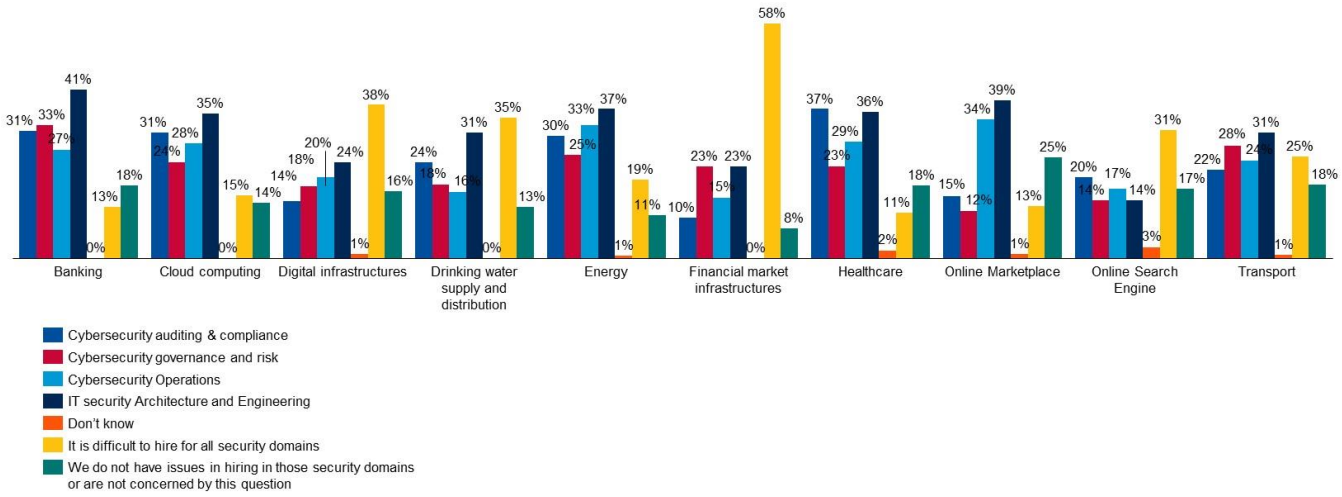
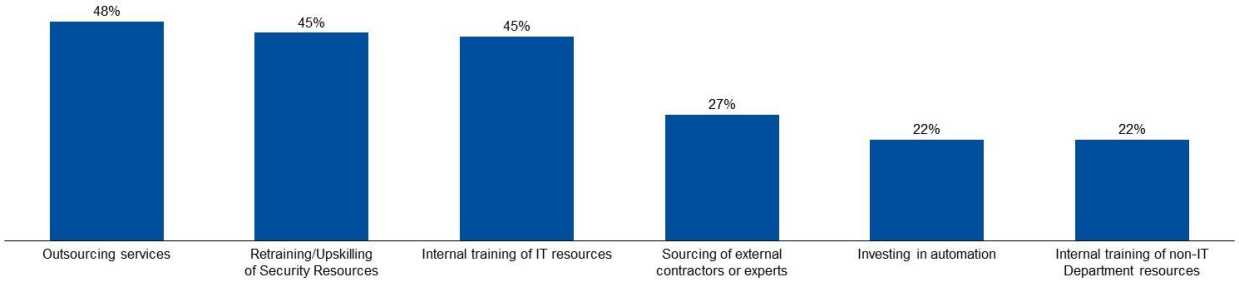


Figure 46 above illustrates the breakdown of the answers for each of the NIS sector.

3.3.12 Skill gap coverage strategy

Survey Question: How do you cover the skills gap in cybersecurity? (Multiple choices possible)

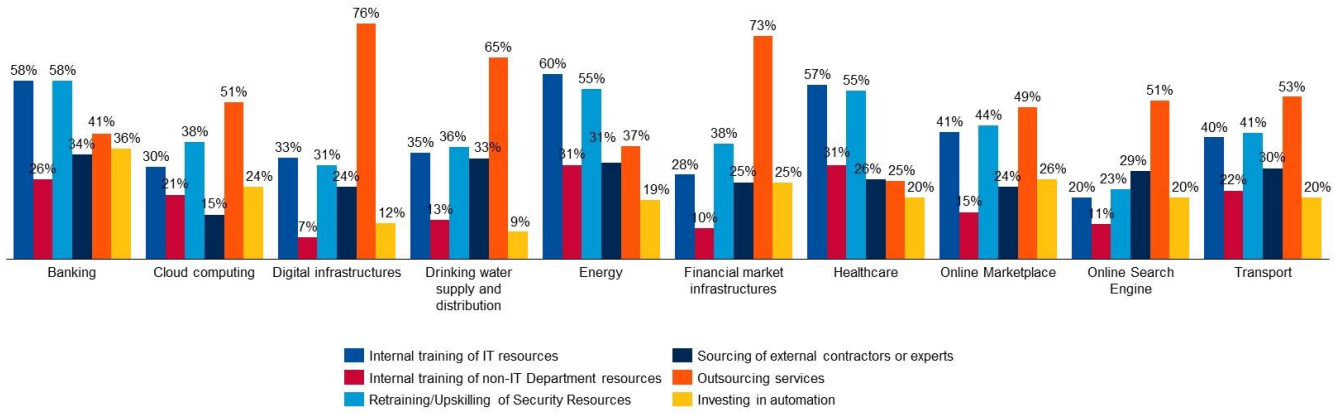
Figure 47: Strategy to cover the skills gap in cybersecurity



The three main strategies leveraged by the NIS sector organisations to cover the skills gap in cybersecurity are: outsourcing services (48%), retraining or upskilling of security resources (45%) and internal training of IT resources (45%).

Sourcing of external contractors or experts comes fourth with 27%, followed by investment in automation and internal training of non-IT resources with both 22%.

Figure 48: Skill gap coverage strategy, per NIS sector

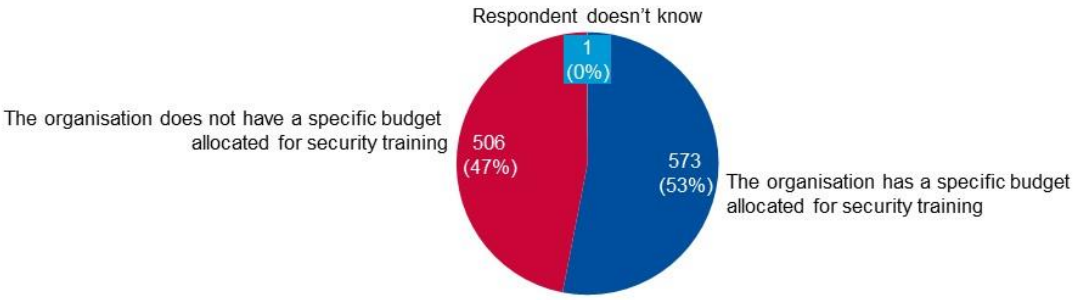


The figure above provides the details of the skill gap coverage strategy per NIS sector.

3.3.13 Cybersecurity training budget

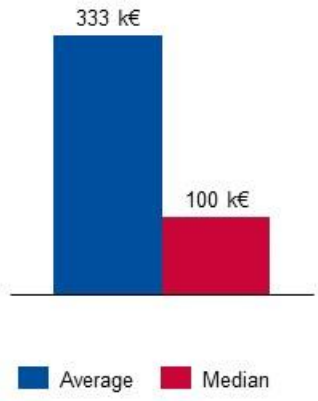
Survey Question: What is your organisation's budget for cybersecurity training in 2023?

Figure 49: Number of organisations with a specific budget for IS training



47% of the surveyed organisations declare no specific budget for information security training.

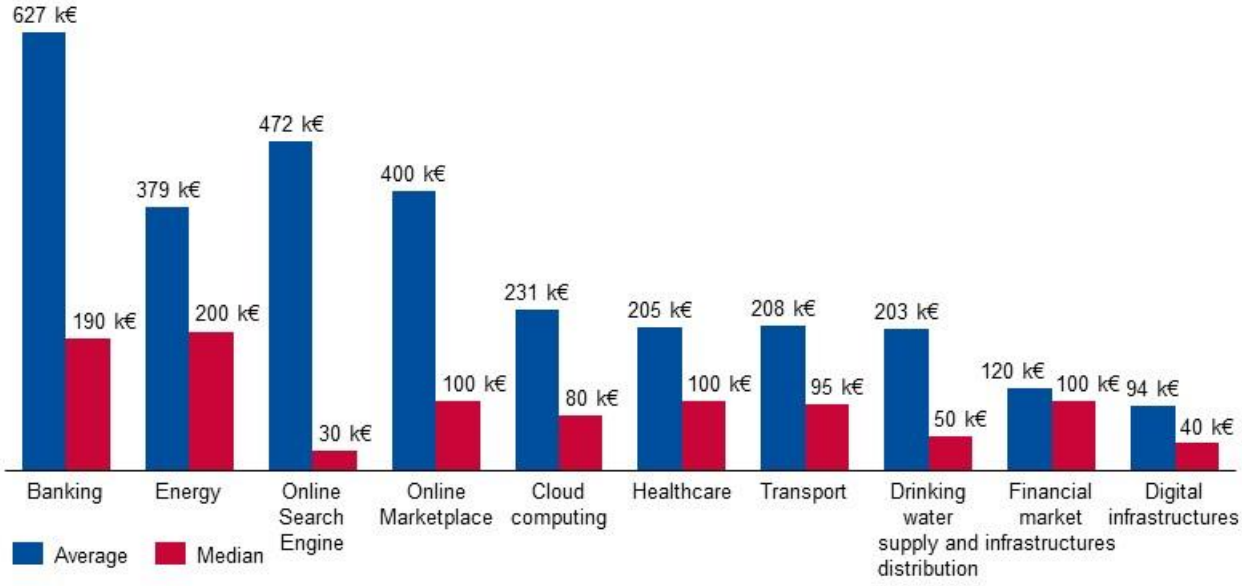
Figure 50: Cybersecurity training budget, all NIS sectors



For the 573 organisations with a specific information security budget, the median training budget is 100k€, with an average of 333 k€, influenced by larger organisations with bigger budgets.

Figure 51: Cybersecurity training budget (in k€) of OES/DSP surveyed in each Member State

Figure 52 Cybersecurity training budget, per NIS sector



The information security budget is much more critical in Energy with 200k€ and Banking with 190k€ than in the other industries, between 80k€ and 100k€. 3 NIS industries have security budgets lower than 50k€ which are drinking water supply and distribution with 50k€, digital infrastructures with 40k€ and online search engines with 30k€. Those low figures must be interpreted considering the sectorial specificities, those three industries having smaller organisations than the other industries.

Figure 53: Cybersecurity training budget as a share of IS spend, per NIS sector

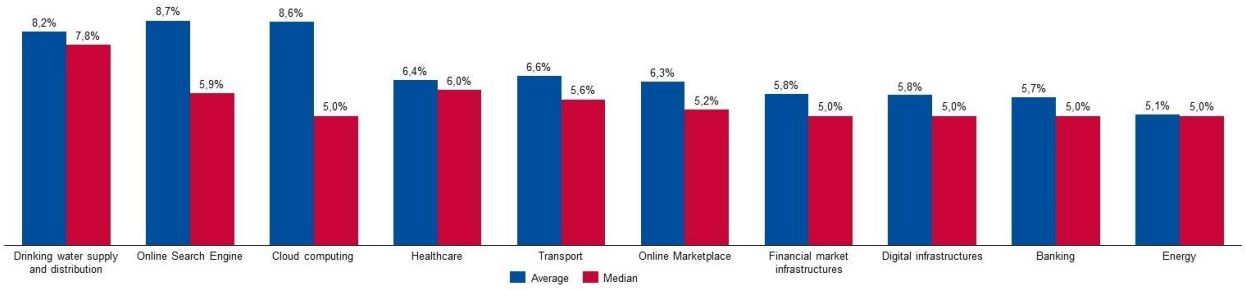
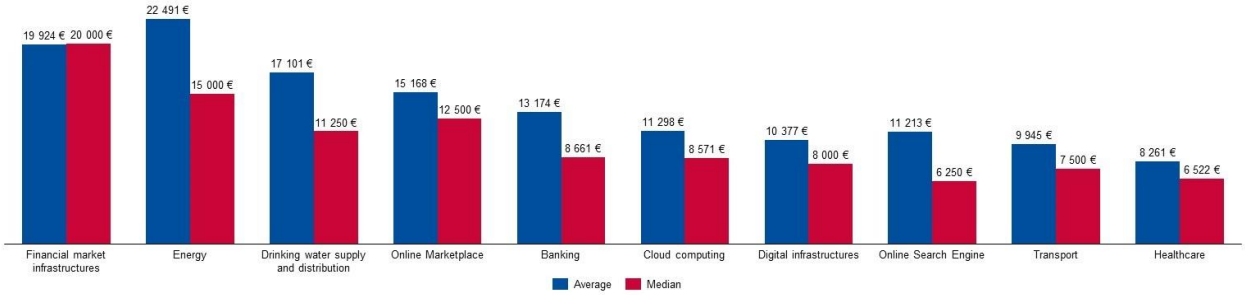


Figure 54: Cybersecurity training budget per IS FTE, per NIS sector



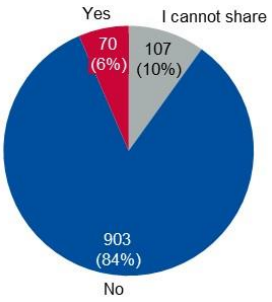
4. SECURITY INCIDENTS, DETECTION AND RESPONSE CAPABILITIES

Key Figures
The direct costs of a significant information security incident can be estimated at 250k€ according to the collected data on the 38 respondents, with an average of 365k€.
Leadership attends dedicated cybersecurity training for 50% of the organisations surveyed and is involved in approving cybersecurity risk management measures for 81% of the organisations surveyed. Both become obligations for essential and important entities under NIS2
77% of the organisations surveyed have a policy related to supply chain cybersecurity risk management from third parties.
45% of the organisations declare having good or mature cyber risk management capabilities, and 23% declare having limited to none such capabilities
30% of the organisations do not engage in collaboration or information-sharing initiatives. EU ISACs and the industry associations are the most used channels for organisations engaged in information-sharing initiatives.

4.1 SECURITY INCIDENTS

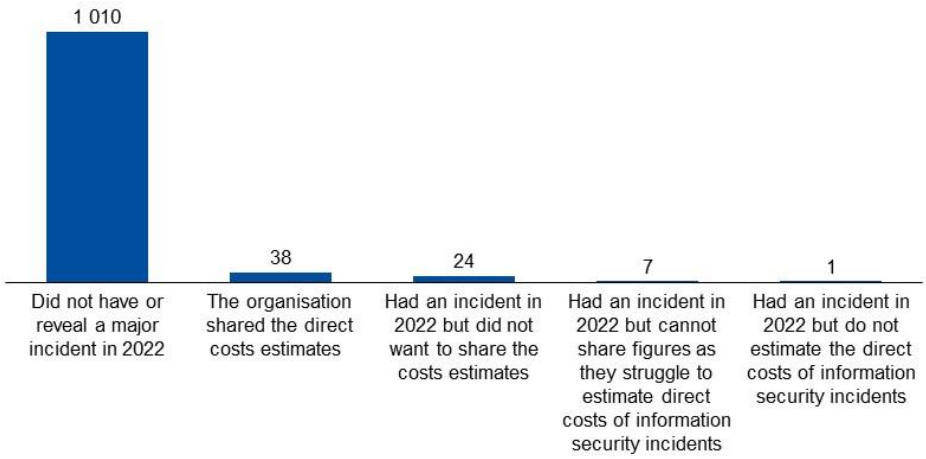
Survey Question: Did your organisation experience a significant information security incident in 2022?

Figure 55: Significant information security incident



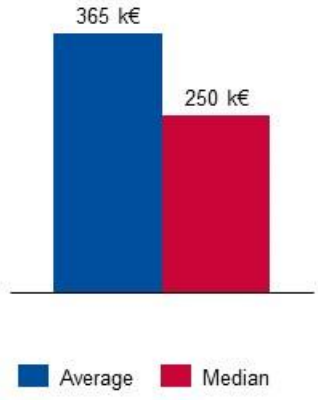
Survey Question: What were the estimated direct costs of this significant information security incident?

Figure 56: Number of NIS organisations that shared data about the direct costs of a significant IS incident



Out of the 70 organisations that have declared a significant information security incident in 2022, 38 have been able to share the estimated direct costs of such incidents. Those results are presented in the below figure.

Figure 57: Direct costs of a significant information security incident

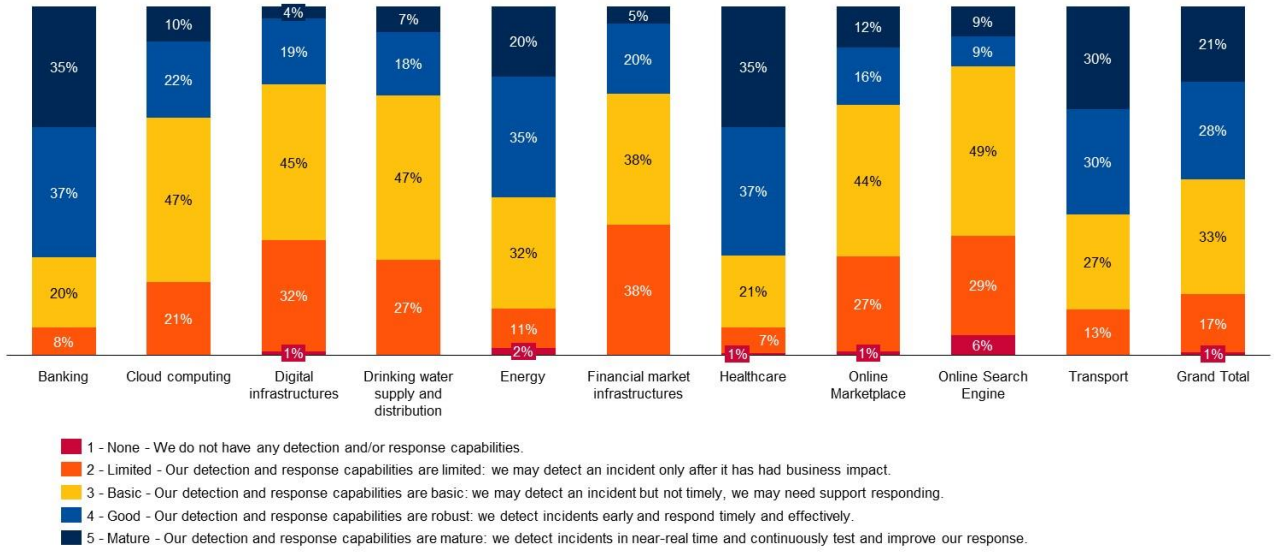


The direct costs of a significant information security incident can be estimated at 250k€ according to the collected data on the 38 respondents, with an average of 365k€. The average was influenced by immensely impacting security incidents with the maximum reported estimated at 1,5M€. The median value of the **direct costs of cybersecurity incidents continue the trend of year-on-year increase**.

4.2 INCIDENT DETECTION AND RESPONSE (IDR) MATURITY

Survey Question: Please evaluate your organisation's incident detection and response maturity on a scale from 1 to 5. Where five is the best?

Figure 58: IDR Maturity, per NIS sector



When asked for a **self-assessment** of the organisation incident detection and response maturity, 49% of the organisations declare having good or mature IDR capabilities and only 18% declare having limited to none IDR capabilities.

The sectors declaring the most mature IDR capabilities are healthcare, banking, transport and energy, with more than 50% of organisations self-assessing their IDR capabilities as good or mature.

Sectors with the most limited to none IDR capabilities are financial market infrastructures (38%), online search engines (35%) and digital infrastructure (33%).

Figure 59: IDR self-assessment maturity score per NIS sector

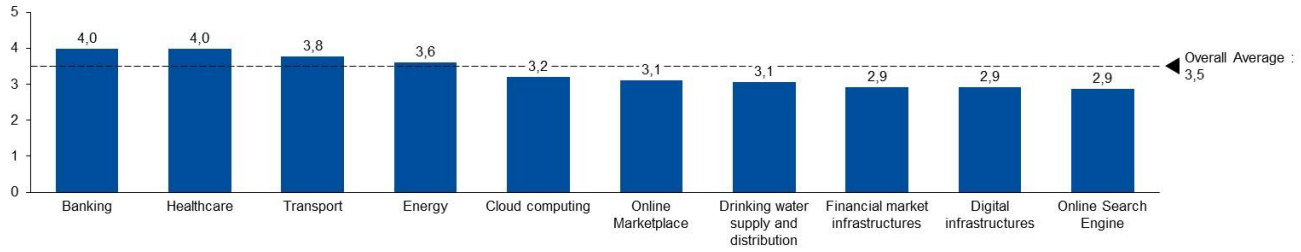


Figure 59 depicts the IDR maturity score for all NIS sectors obtained when mapping a maturity level to the corresponding score (1 for none and 5 for mature).

The average across all surveyed organisations is at 3,5 showing that the overall IDR maturity is between primary and good.

4.3 LEADERSHIP INVOLVEMENT IN CYBERSECURITY

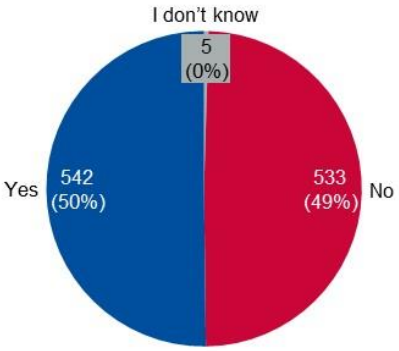
The NIS2 Directive introduces specific provisions for the management bodies of essential and important entities, specifically in relation to:

- the management bodies of essential and important entities **approving the cybersecurity risk-management measures** taken by those entities (Art. 20.1) and
- the management bodies of essential and important entities being required to **follow training** in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity (Art. 20.2)

While NIS2 is still under implementation and these measures are not necessarily mandatory in all EU MS yet, it is important to capture the current state of play concerning leadership approving cybersecurity programmes and receiving training and see how these evolve once NIS2 comes into play.

Survey Question: Is your organisation's leadership attending dedicated cybersecurity training?

Figure 60: Leadership dedicated training in cybersecurity



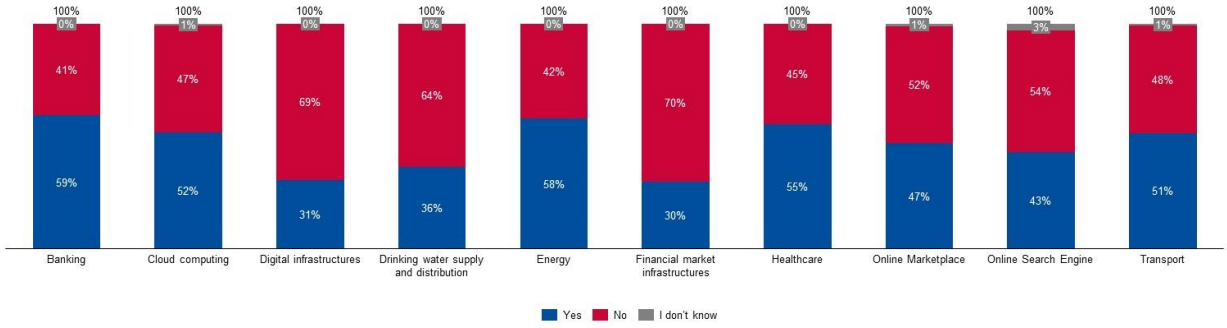
Leadership attends dedicated cybersecurity training for 50% of the organisations surveyed.

Figure 61: Leadership dedicated training in cybersecurity for OES/DSPs surveyed in each Member State

	% yes	% no	% I don't know
Austria	52.5	47.5	0
Belgium	52.5	47.5	0
Bulgaria	30	70	0
Croatia	38	63	0
Czech Republic	50	50	0
Denmark	50	50	0
Estonia	33	65	2
Finland	53	48	0
France	50	50	0
Germany	78	23	0
Greece	58	43	0
Hungary	45	55	0
Ireland	53	45	2
Italy	80	20	0
Latvia	30	70	0
Lithuania	35	65	0
Luxembourg	48	53	0
Malta	38	60	2
Netherlands	50	50	0
Poland	60	40	0
Portugal	63	38	0
Republic of Cyprus	30	70	0
Romania	63	38	0
Slovakia	53	48	0
Slovenia	43	58	0
Spain	70	25	5
Sweden	55	45	0

Italy (80%), Germany (76%) and Spain (70%) are the countries with the highest share of leadership receiving dedicated cybersecurity training.

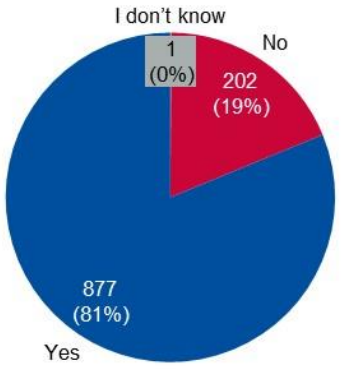
Figure 62: Leadership dedicated training in cybersecurity, per NIS sector



Leadership training in cybersecurity is highest in banking (59%), energy (58%) and healthcare (55%), and lowest in financial market infrastructures (30%) and digital infrastructures (31%).

Survey Question: Is your organisation's leadership involved in approving cybersecurity risk-management measures?

Figure 63: Leadership involvement in the approval of cybersecurity risk-management measures



Leadership is involved in approving cybersecurity risk management measures for 81% of the organisations surveyed.

The two figures below provide the underlying details per Member state and per NIS Sector.

Figure 64: Leadership involvement in the approval of cybersecurity risk-management measures for OES/DSPs surveyed in each Member State

	% yes	% no
Austria	88	13
Belgium	88	13
Bulgaria	65	35
Croatia	75	25
Czech Republic	80	20
Denmark	70	30
Estonia	65	35
Finland	85	15
France	88	13
Germany	95	5
Greece	80	20
Hungary	73	28
Ireland	88	13
Italy	93	8
Latvia	73	28
Lithuania	73	28
Luxembourg	85	15
Malta	78	23
Netherlands	83	18
Poland	93	8
Portugal	83	18
Republic of Cyprus	68	33
Romania	98	3
Slovakia	85	15
Slovenia	80	18
Spain	93	8
Sweden	75	25

Figure 65: Leadership involvement in the approval of cybersecurity risk-management measures, per NIS sector

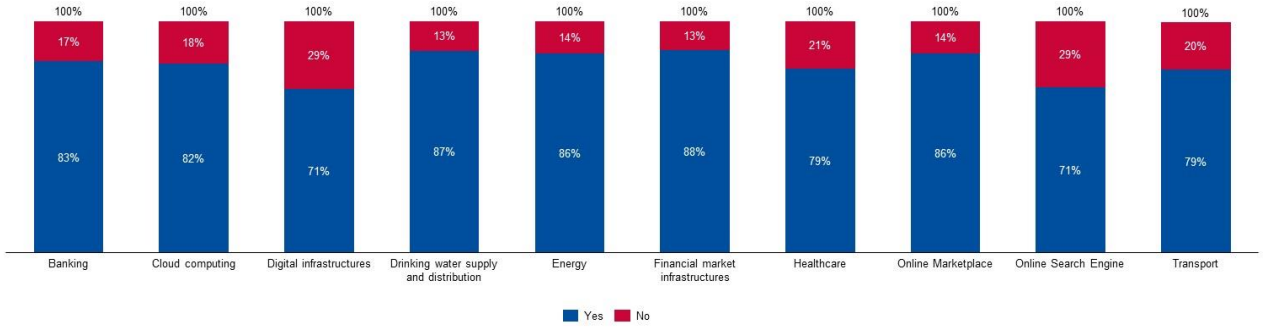
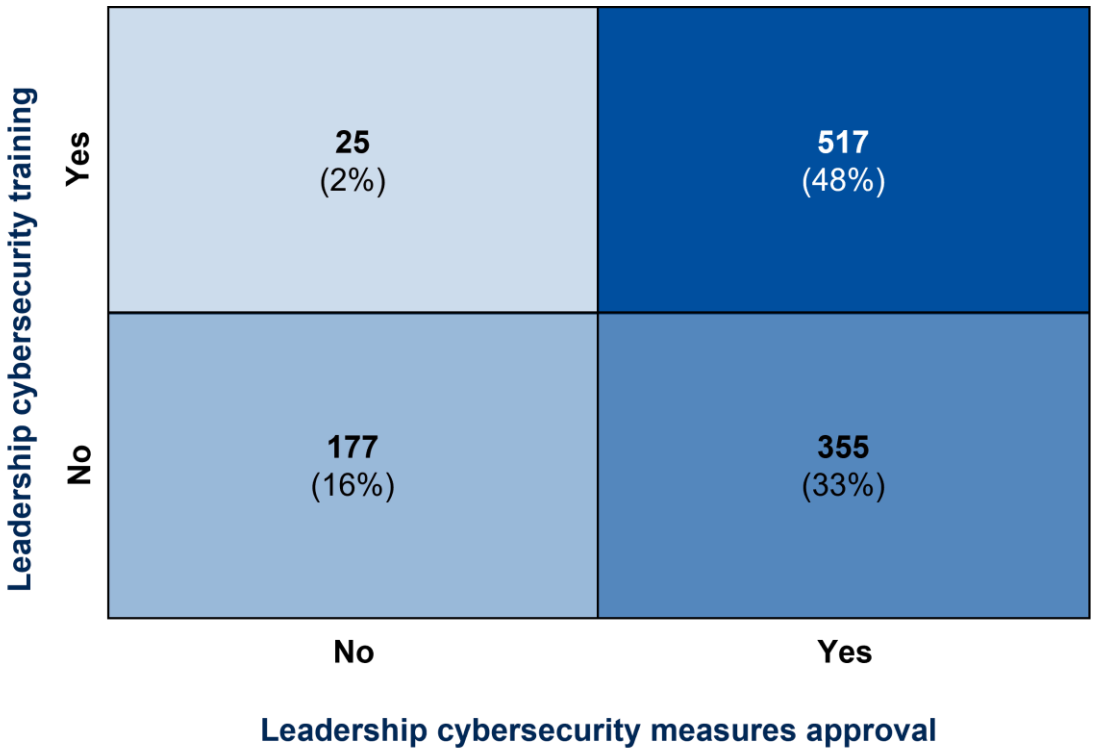


Figure 66 explores the overlap between organisation leadership receiving training on cybersecurity risks and being involved in approving the cybersecurity measures.

Figure 66: Overlap between leadership approving cybersecurity measures and receiving cyber risk training

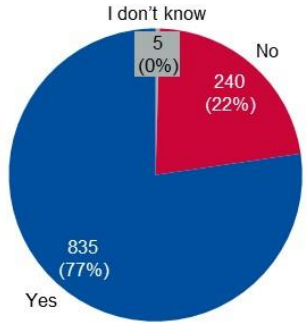


48% of the surveyed organisations have both leadership attending dedicated cybersecurity training and being involved in the approval of cybersecurity measures. On the contrary, leadership is neither involved in the approval of cybersecurity measures nor trained for 16% of the organisations.

4.4 CYBERSECURITY RISK MANAGEMENT

Survey Question: Does your organisation have a policy related to supply chain cybersecurity risk management from third parties such as partners, vendors, or suppliers?

Figure 67: Cybersecurity risk management policy for 3rd parties



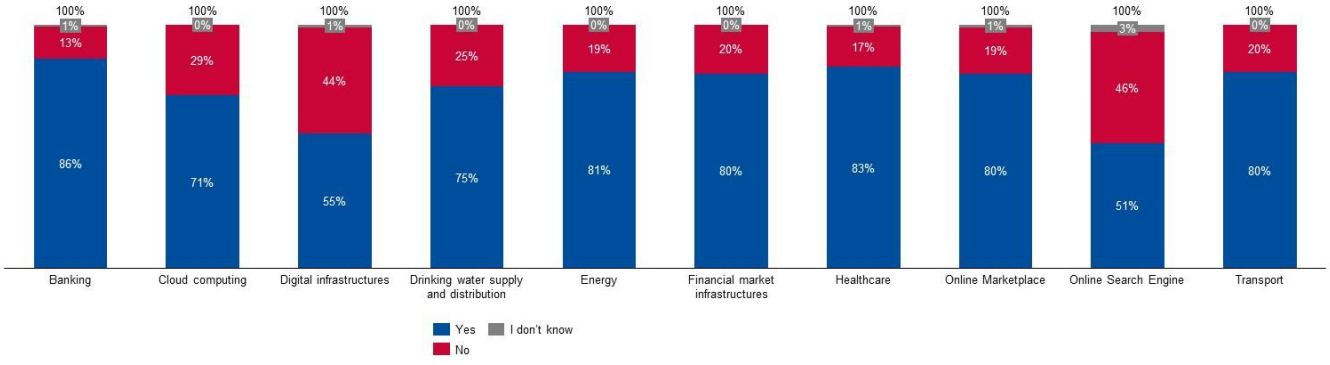
77% of the organisations surveyed have a policy related to supply chain cybersecurity risk management from third parties.

The following two figures provide the underlying details per Member state and per NIS Sector.

Figure 68: Cybersecurity risk management policy for 3rd parties for OES/DSPs surveyed in each Member State

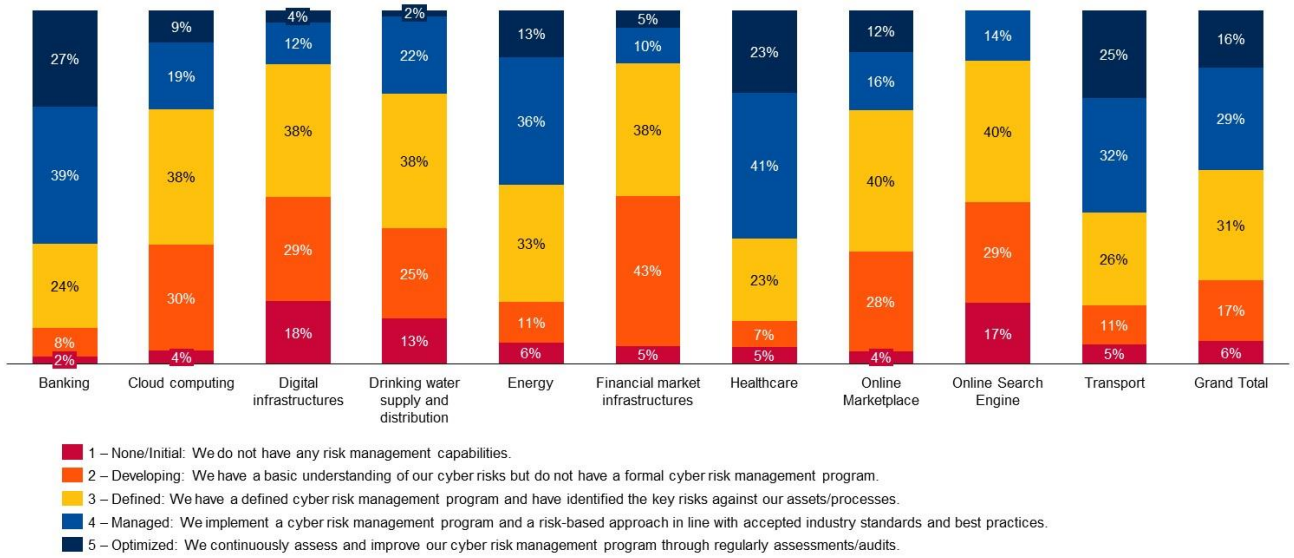
	% yes	% no	% I don't know
Austria	83	15	2
Belgium	80	20	0
Bulgaria	68	30	2
Croatia	83	18	0
Czech Republic	78	23	0
Denmark	80	20	0
Estonia	63	38	0
Finland	75	25	0
France	85	15	0
Germany	88	13	0
Greece	75	25	0
Hungary	73	28	0
Ireland	93	8	0
Italy	93	8	0
Latvia	63	33	4
Lithuania	68	33	0
Luxembourg	75	25	0
Malta	70	28	2
Netherlands	93	8	0
Poland	90	10	0
Portugal	80	20	0
Republic of Cyprus	58	43	0
Romania	88	13	0
Slovakia	78	23	0
Slovenia	65	35	0
Spain	88	13	0
Sweden	63	38	0

Figure 69: Cybersecurity risk management policy for 3rd parties, per NIS sector



<u>Survey Question:</u> Please evaluate your organisation cyber risk management maturity on a scale from 1 to 5. Where five is the best?

Figure 70: Cyber risk management maturity self-assessment, per NIS sector



When asked for a self-assessment of the organisation cyber risk management maturity, 45% of the organisations declare having good or mature cyber risk management capabilities, and 23% declare having limited to none such capabilities.

Figure 71: Cyber risk management self-assessment maturity score

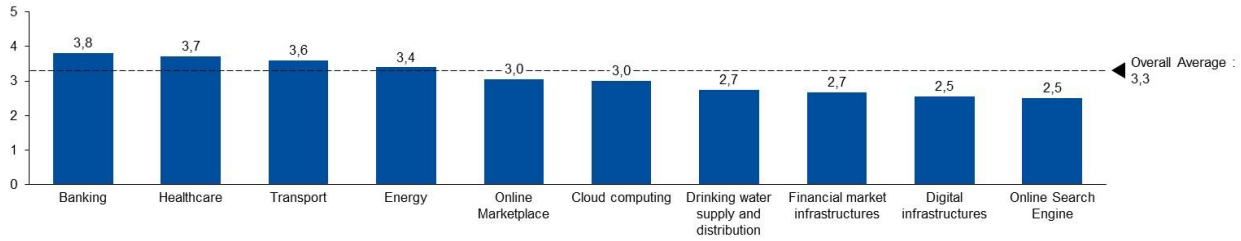


Figure 71 depicts the cyber risk management self-assessment maturity score for all NIS sectors obtained when mapping a maturity level to the corresponding score (1 for none and 5 for mature).

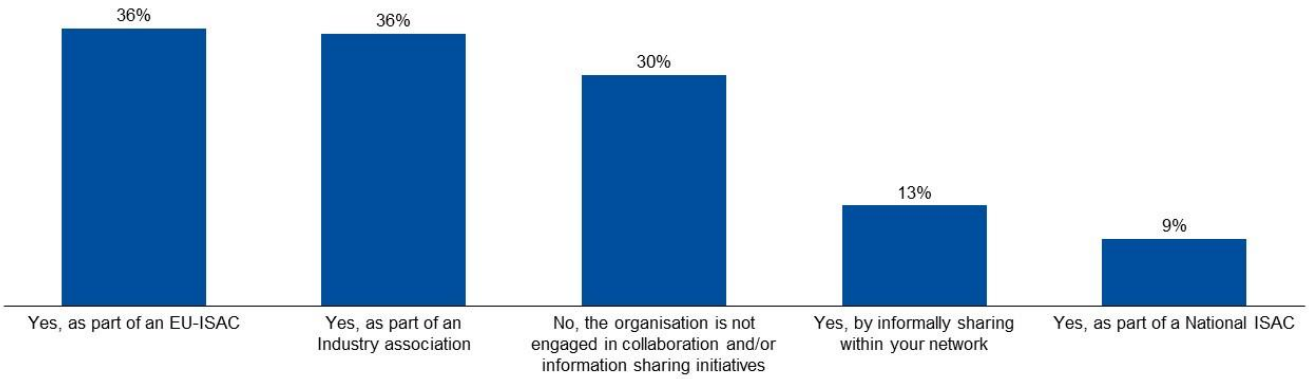
The four sectors with the most mature cyber risk management capabilities are banking, healthcare, transport, and energy. Banking and healthcare are close to an average score of 4. Digital infrastructures and online search engines have an average score of 2.5, describing more limited cyber risk management capabilities.

The average across all surveyed organisations is at 3.3 showing that the overall cyber risk maturity is slightly above “Defined”.

4.5 INFORMATION SHARING

Survey Question: Does your organisation participate in national or EU-level Information Sharing and Analysis Centres (ISACs) or other forms of information sharing? (Multiple choices possible)

Figure 72: Information Sharing and Analysis Centres



30% of the organisations (326 out of 1080) do not engage in collaboration or information-sharing initiatives.

EU ISACs and industry associations are the most used channels for organisations engaged in information-sharing initiatives.

Figure 73: Information Sharing and Analysis Centres for OES and DSPs surveyed in each Member State

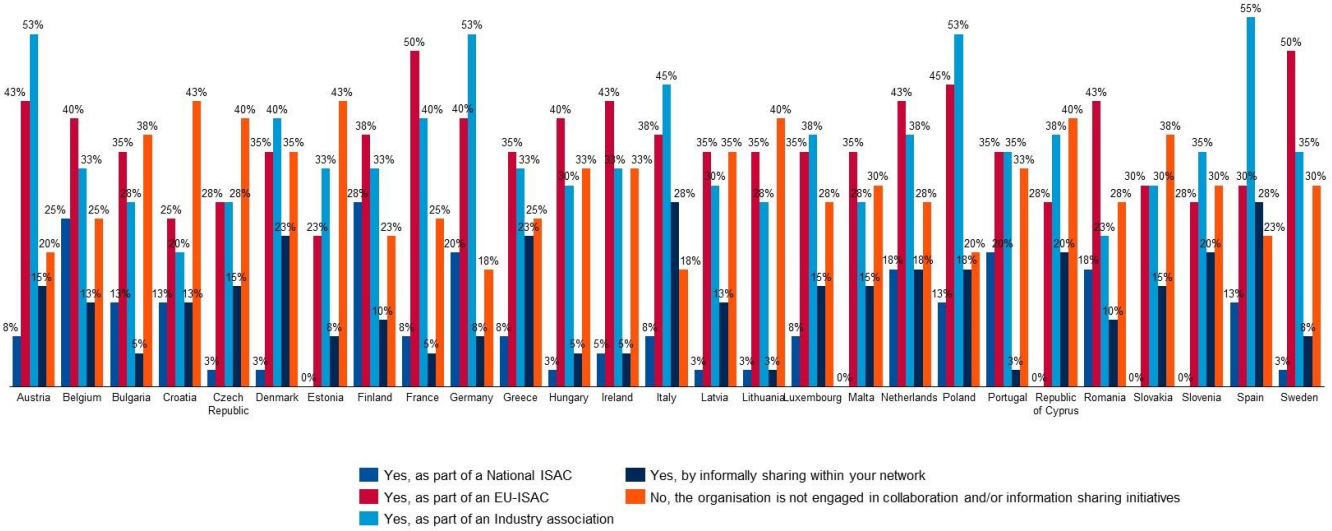
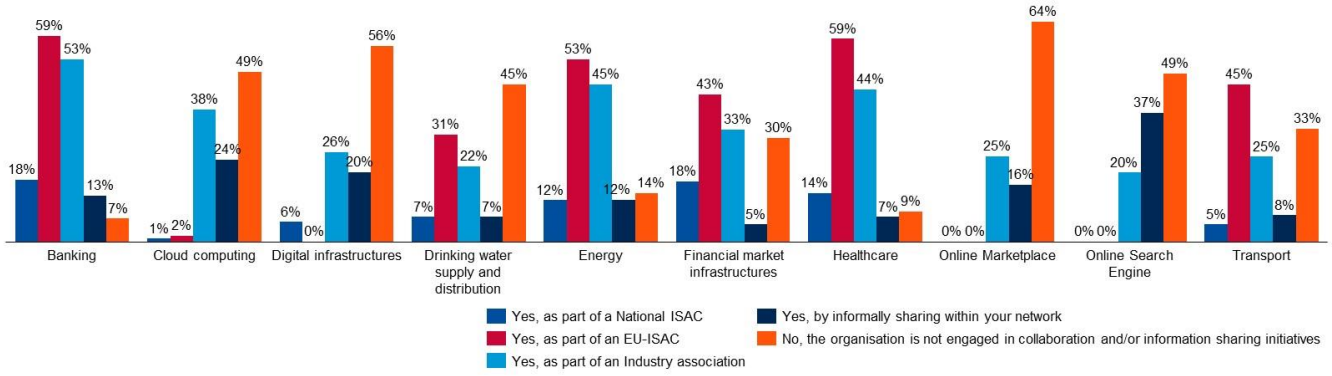


Figure 74: Participation in any information sharing activities within the sector for OES/DSP surveyed in each Member State

	% yes	% no
Austria	80	20
Belgium	75	25
Bulgaria	63	38
Croatia	58	43
Czech Republic	60	40
Denmark	65	35
Estonia	58	43
Finland	78	23
France	75	25
Germany	83	18
Greece	75	25
Hungary	68	33
Ireland	68	33
Italy	83	18
Latvia	65	35
Lithuania	60	40
Luxembourg	73	28
Malta	70	30
Netherlands	73	28
Poland	80	20
Portugal	68	33
Republic of Cyprus	60	40
Romania	73	28
Slovakia	63	38
Slovenia	70	30
Spain	78	23
Sweden	70	30

Figure 75: Information Sharing and Analysis Centres, per NIS sector



4.6 IMPACT OF LEADERSHIP INVOLVEMENT IN CYBERSECURITY ON CAPABILITIES

The following figures present the cybersecurity capabilities and maturity self-assessment of surveyed organisations depending on the involvement of their leadership in cybersecurity based on whether or not they receive dedicated training and whether or not leadership approves cybersecurity measures.

Figure 76: Organisational incident detection and response capabilities depending on leadership training and approval of cybersecurity measures

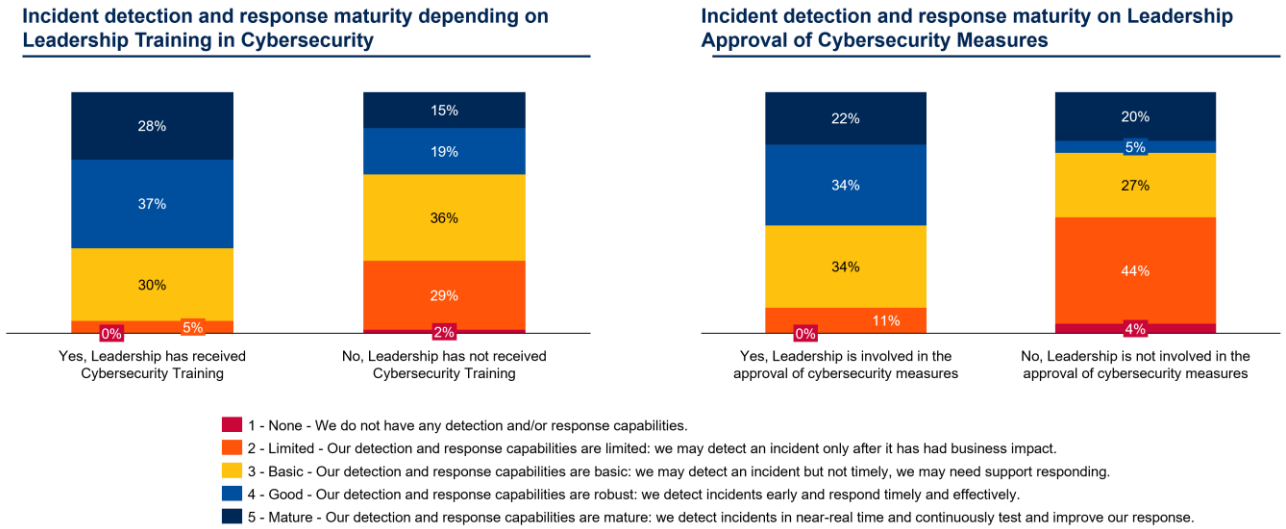


Figure 77: Organisational cyber risk management maturity depending on leadership training and approval of cybersecurity measures

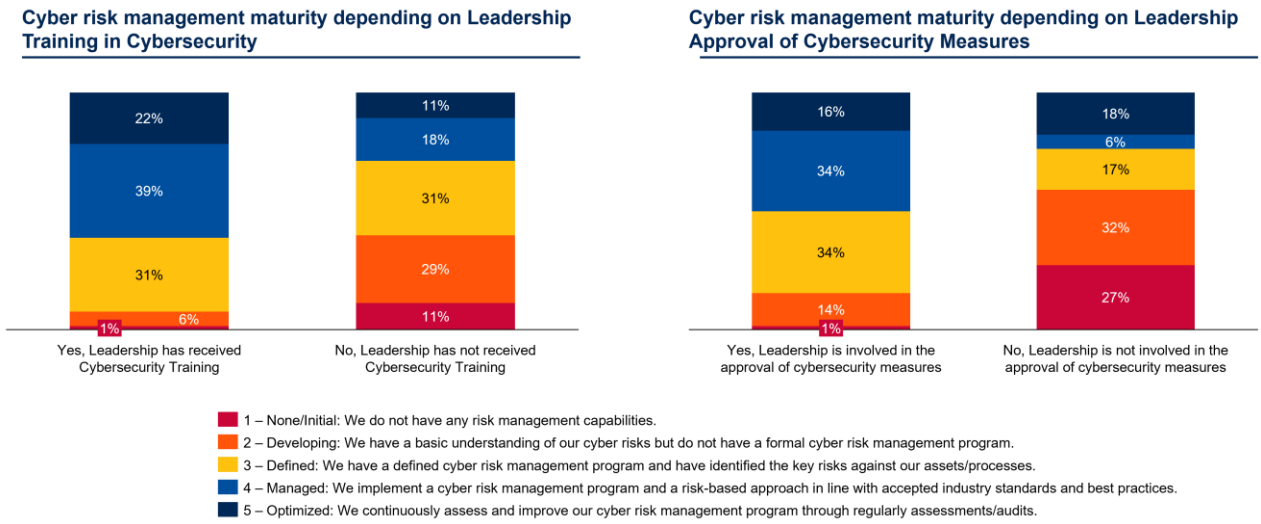
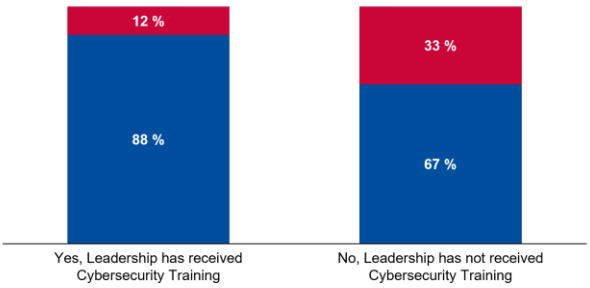


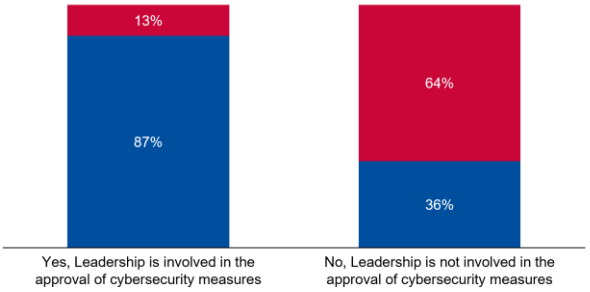
Figure 76 and Figure 77 indicate a very strong correlation between management involvement in cybersecurity and an organisation's cyber risk management maturity and incident detection and response capabilities. On both cases, **organisations whose leadership is active in cybersecurity are more than twice as likely to score above basic level in both risk management and incident detection and response**. As the respective leadership requirements become mandatory with NIS2, it would be interesting to keep monitoring how the cybersecurity maturity of essential and important entities evolve.

A similar finding concerns how organisations deal with 3rd party risk management. In this case, leadership approval of cybersecurity measures proves even more impactful as the percentage of organisations with 3rd party risk management policies increases from 36% to 87% when management signs-off on cyber risk management measures.

Cybersecurity risk management policy for 3rd parties depending on Leadership Training in Cybersecurity



Cybersecurity risk management policy for 3rd parties depending on Leadership Approval of Cybersecurity Measures



Yes, the organisation has a policy related to SC cybersecurity risk management from 3rd parties
No, the organisation does not have a policy related to SC cybersecurity risk management from 3rd parties

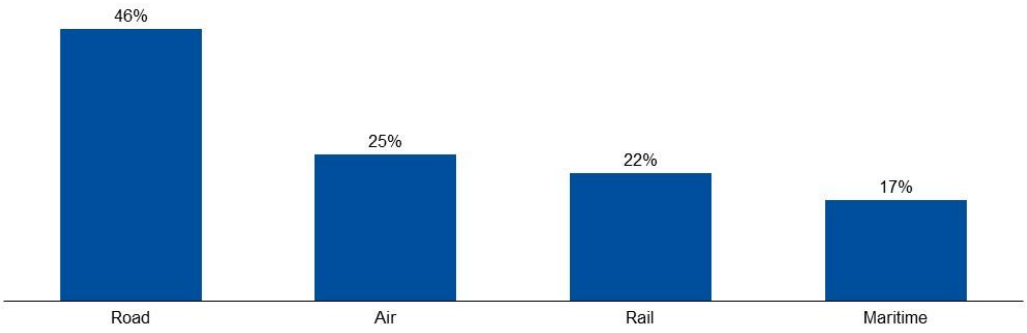
5. SECTORAL ANALYSIS: TRANSPORT

This section provides further insights into the transport sector by analysing the results of the data collected through specific questions asked to the transport sector only.

Key Figures
51% of the transport organisations manage OT security with the same unit or people as IT cybersecurity, while 15% manage OT security independently from IT cybersecurity.
The primary legal driver of cybersecurity investments in the Transport sector is the NIS Directive (55%), followed by transport industry-specific security requirements (27%) and legal requirements such as GDPR (12%). Only 6% of organisations declare security certification standards such as ISO27002 and ISA/IEC 62443 as their primary legal driver of cybersecurity investments.
51% of the organisations in the transport sector need one month to patch critical vulnerabilities on IT or OT assets, and 21% need a time between 1 month and six months. Only 28% of the surveyed organisations fix critical vulnerabilities on critical assets in one week.

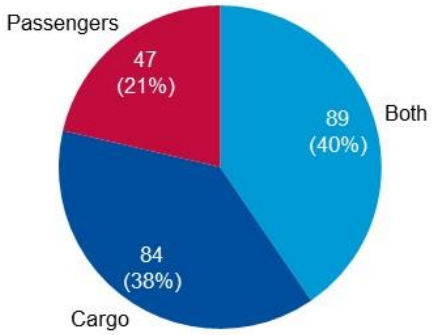
5.1 DEMOGRAPHICS OF THE SECTORAL DEEP DIVE

Figure 78: Transport sub-sectorial demographics



Out of the 220 organisations of the transport sector surveyed, 102 have road operations (46%), 55 have air operations (25%), 48 have rail operations (22%) and 38 have maritime operations (17%). The total is higher than 100% because 22 organisations (10%) have operations in multiple sub-industries of the transport industry.

Figure 79: Type of transportation



21% of the organisations in the transport sector are transporting passengers, 38% are focused on cargo transportation and 40% deal with both.

Figure 80: Type of transportation per mode of transport

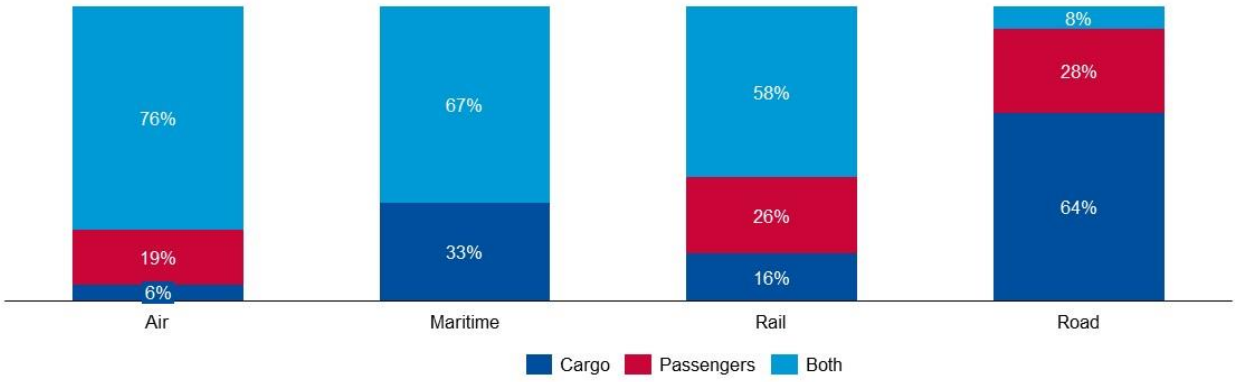


Figure 81: Transport operators' profile

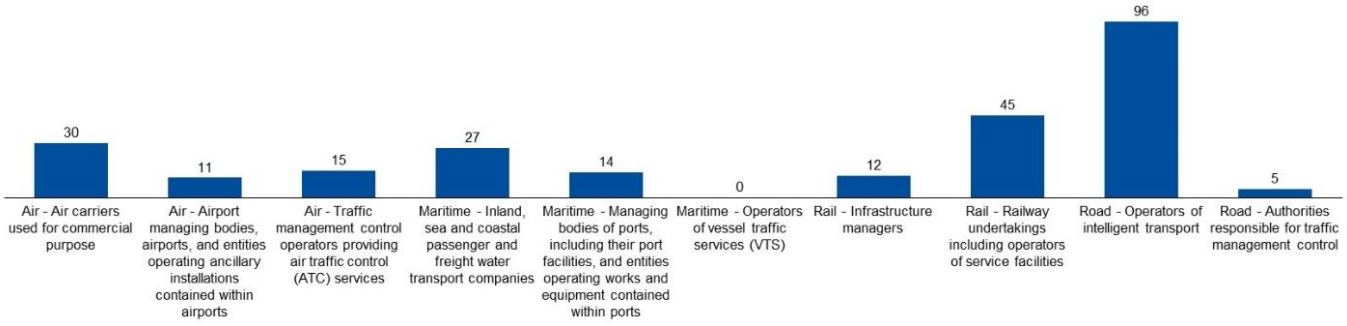
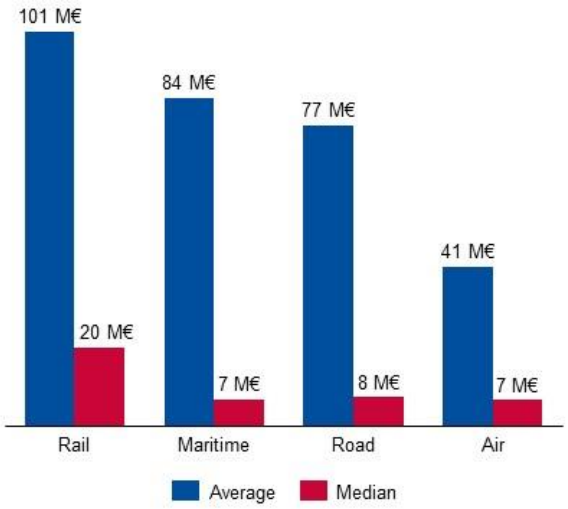


Figure 81 describes the operators' profiles as per the NIS sub-sector definition.

5.2 INVESTMENTS AND STAFFING INFORMATION PER TRANSPORT SUB-SECTOR

The following figures present key metrics on information security spending and staffing for the transport sector, focusing on a breakdown per sub-sector **for the 198 organisations operating on a single sub-sector**.

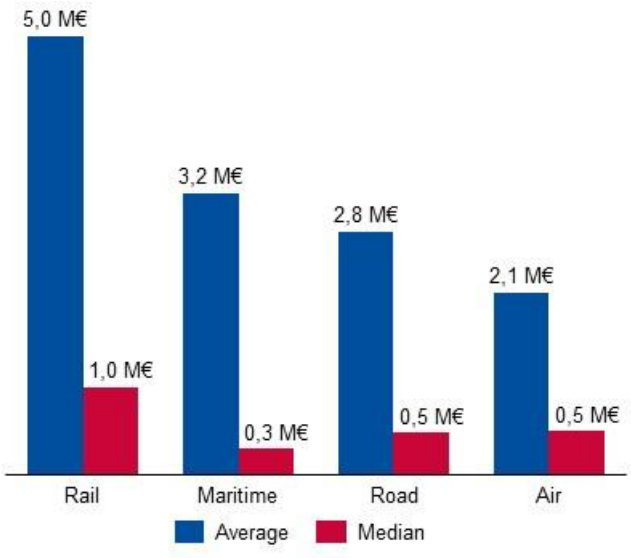
Figure 82: IT spend per transport sub-sector



In average in 2022, a rail OES has the highest IT spend amongst the transport sub-sectors with 101 M€ of IT spending. It is followed by Maritime with 84 M€ of IT spend, road with 77 M€ and last air with 41 M€ average. Those averages are much higher than the median values, indicating that the largest organisations have much larger IT budget than the smaller ones.

Median values highlight rail operators as the ones with a significantly higher IT spend with 20 M€. The other three sub-sectors being between 7 M€ and 8 M€ of IT spend.

Figure 83: IS spend per transport sub-sector



The trend analysis for the IS spend is similar to the above for IT spend. Rail operators having larger information security spending than the operators from the other sub-sectors.

Figure 84: IS spend as a share of IT spend, per transport sub-sector

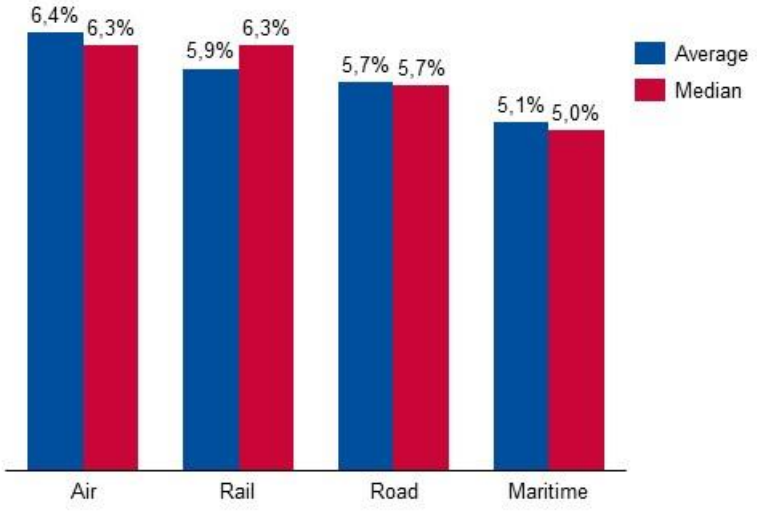


Figure 85: IT FTEs per transport sub-sector

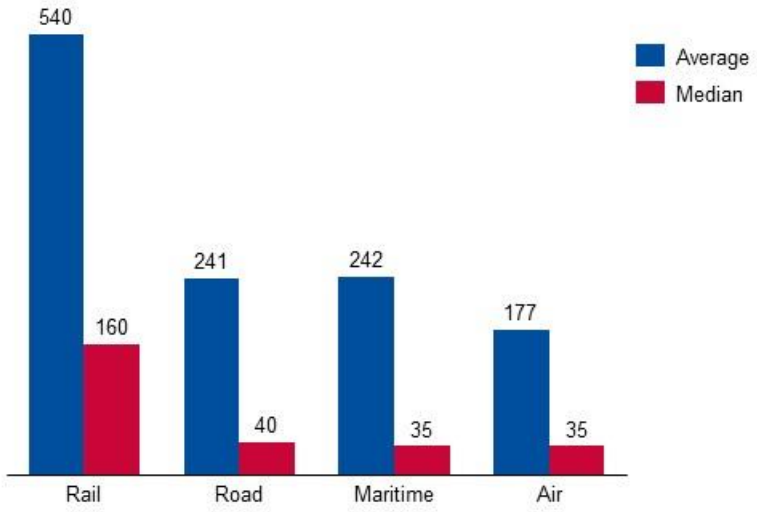


Figure 86: IS FTE per transport sub-sector

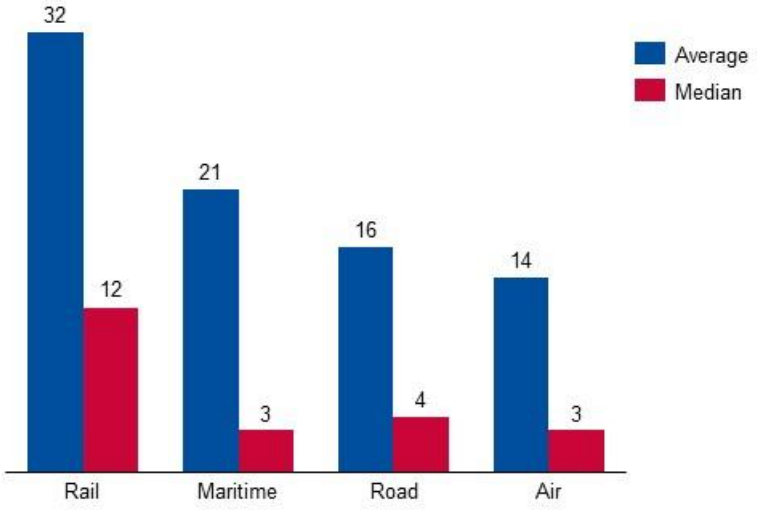
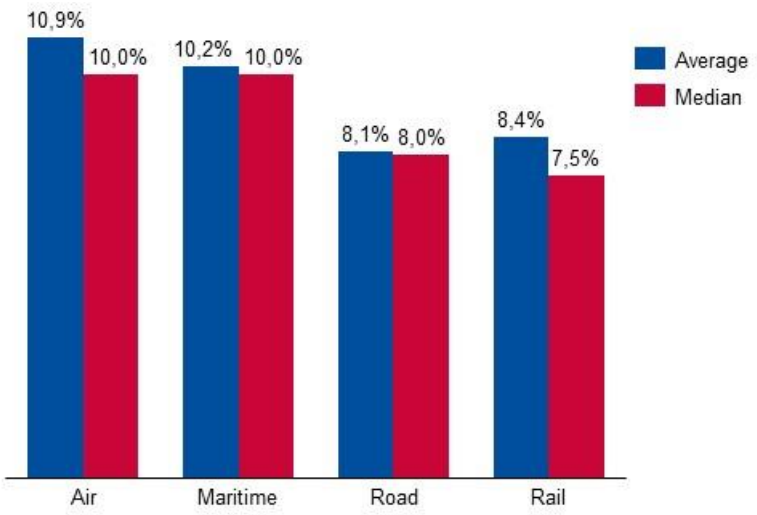


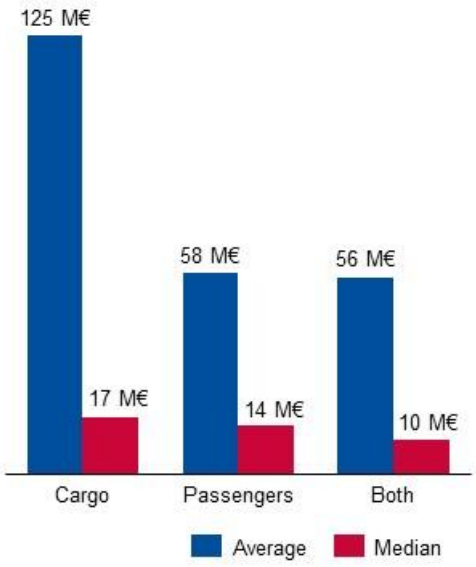
Figure 87: IS FTE as a share of IT FTE, per transport sub-sector



5.3 INVESTMENTS AND STAFFING INFORMATION PER TYPE OF OPERATIONS

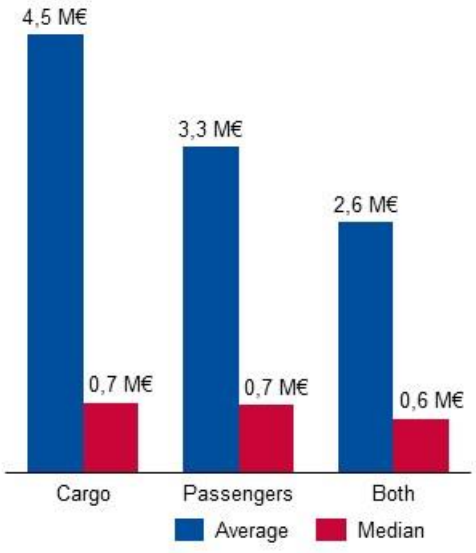
The following figures present key metrics on information security spending and staffing for the transport sector, focusing on a breakdown per type of operations

Figure 88: IT spend per transport type of operations



A typical cargo operator has a larger IT spend than a passenger only operator with 17 M€ of IT spend against 14 M€. OES that were both covering cargo and passengers had the lowest IT spend with 10 M€.

Figure 89: IS spend per transport type of operations



The 2022 IS spend amount is quite similar for all type of operations, varying between 700K€ for Cargo and Passengers only and 600k€ for both.

Figure 90: IS spend as a share of IT spend, per transport type of operations

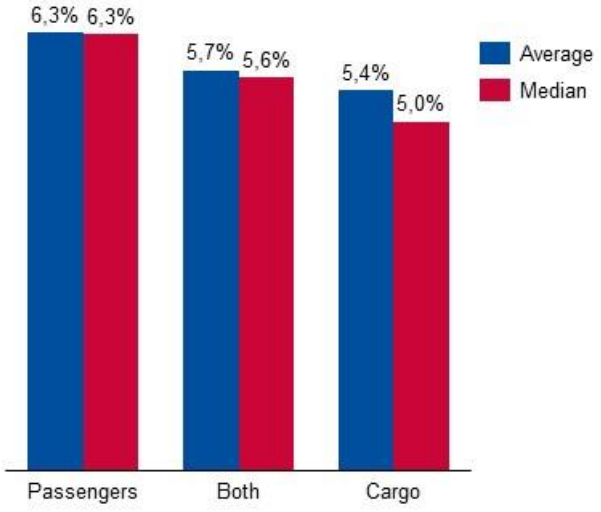


Figure 91: IT FTEs per transport type of operations

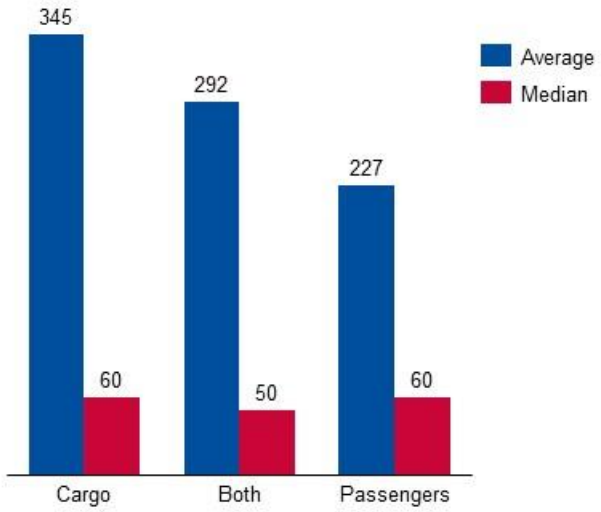


Figure 92: IS FTE per transport type of operations

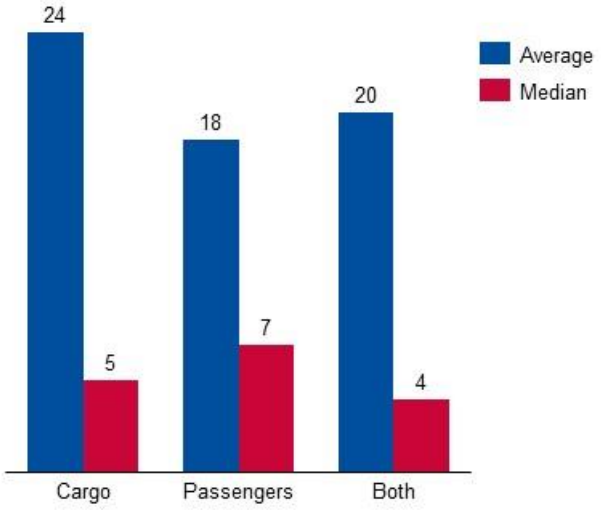
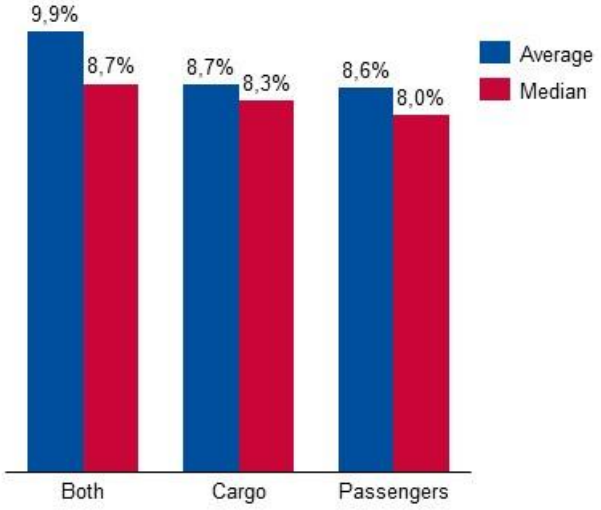


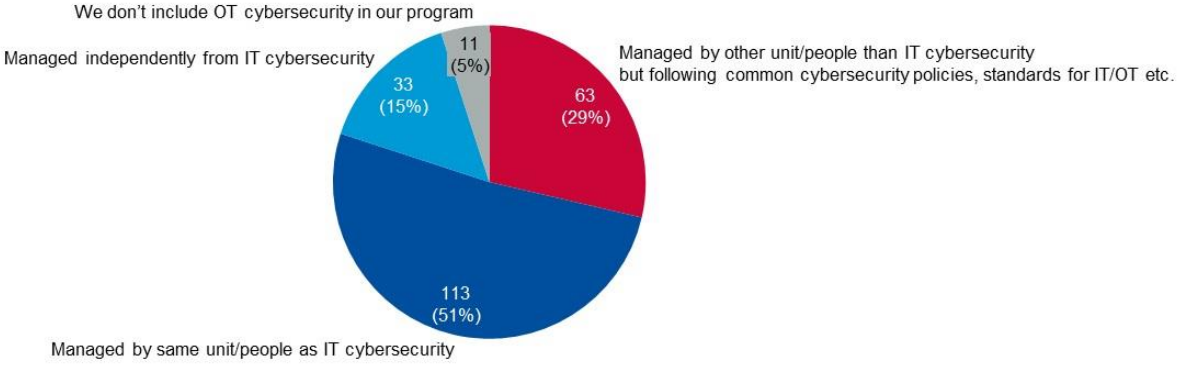
Figure 93: IS FTE as a share of IT FTE, per transport type of operations



5.4 MANAGEMENT OF OT SECURITY

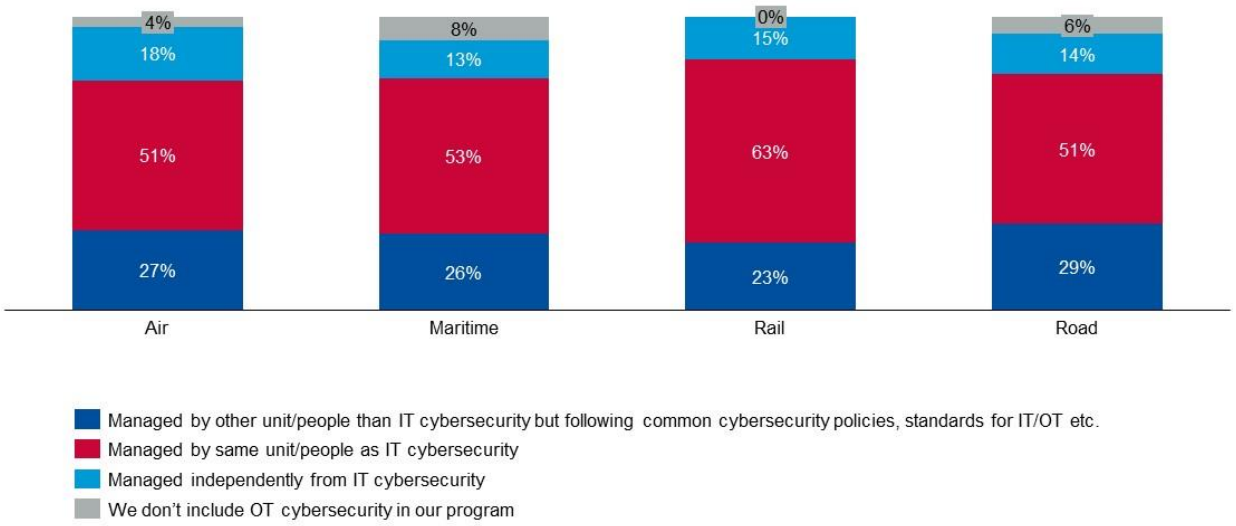
Survey Question: How is the cybersecurity of OT managed in your organisation?

Figure 94: Cybersecurity management of OT for the Transport sector



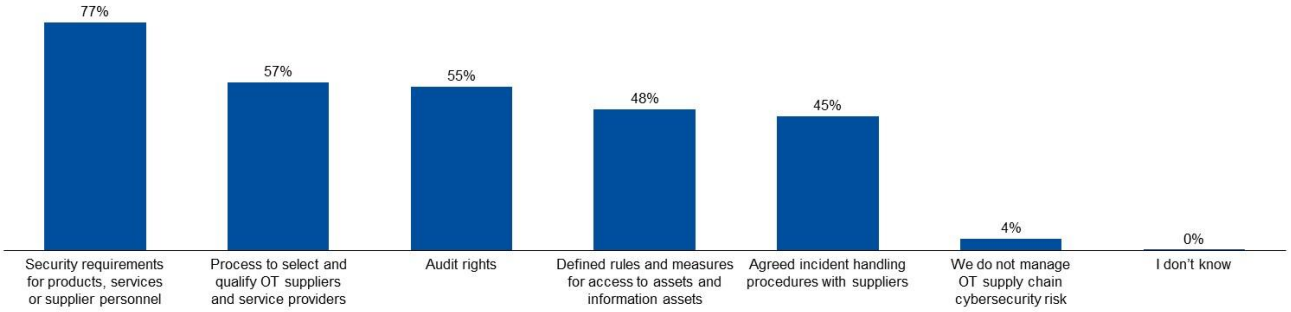
51% of the transport organisations manage OT security with the same unit or people as IT cybersecurity, while 15% manage OT security independently from IT cybersecurity.

Figure 95: Cybersecurity management of OT for the Transport sector, per mode of transport



Survey Question: How do you manage cybersecurity risks from your OT suppliers?
(Multiple choices possible)

Figure 96: Cybersecurity risk management for OT suppliers in the Transport sector

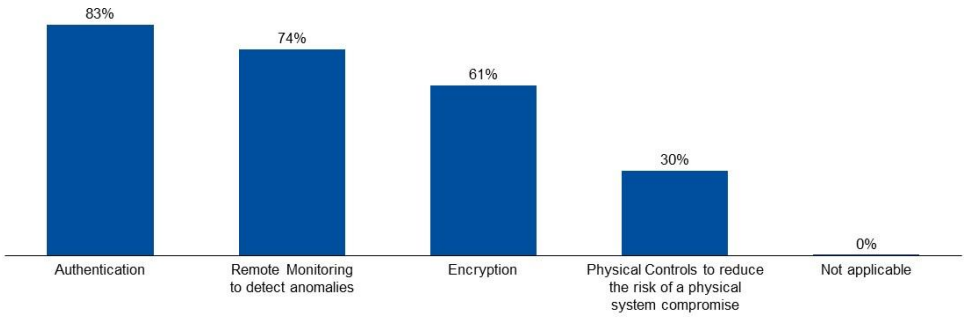


The most used method to manage cybersecurity risk for OT suppliers in the transport sector is through security requirements for products, services, or supplier personnel, with 78% of the transport organisations selecting this option. Setting eligibility criteria for OT suppliers and service providers comes second with 57%, and audit rights come third with 55%.

9 organisations (4%) do not manage OT supply chain cybersecurity risk.

Survey Question: What are the controls in place for connectivity with remote and mobile assets such as port or warehouse infrastructure, ships, lorries, aircraft, trains, etc.
(Multiple choices possible)

Figure 97: Controls in place for connectivity with remote and mobile assets in the Transport sector



The most used control for securing connectivity with remote or mobile assets in the transport sector is authentication, with 183 organisations (83%) selecting this option. Remote monitoring to detect anomalies comes second with 163 selections (74%), and Encryption comes third with 135 selections (61%). Physical controls to reduce the risk of physical system compromise are only used by 67 organisations (30%).

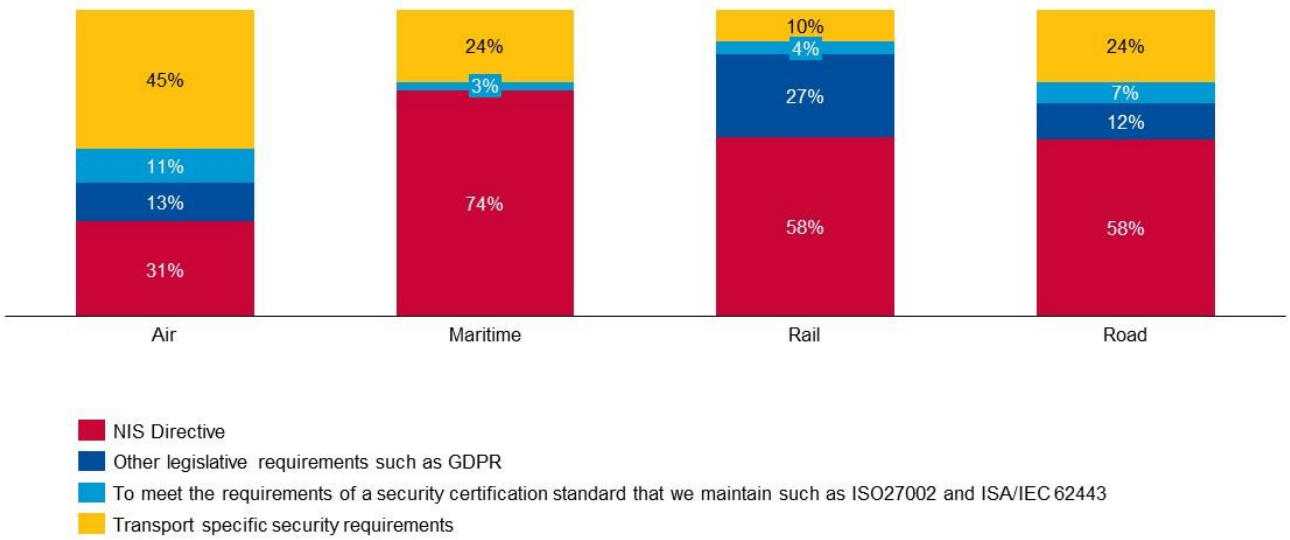
5.5 PRIMARY LEGAL DRIVER FOR CYBERSECURITY INVESTMENTS

Survey Question: Regarding the legislative requirements, what is the primary driver for your organisation's security investments?

Figure 98: Primary legal driver of cybersecurity investments in the Transport sector

According to respondents, **the primary legal driver of cybersecurity investments in the Transport sector is the NIS Directive (55%)**, followed by transport industry-specific security requirements (27%) and legal requirements such as GDPR (12%). Only 6% of organisations declare security certification standards such as ISO27002 and ISA/IEC 62443 as their primary legal driver of cybersecurity investments.

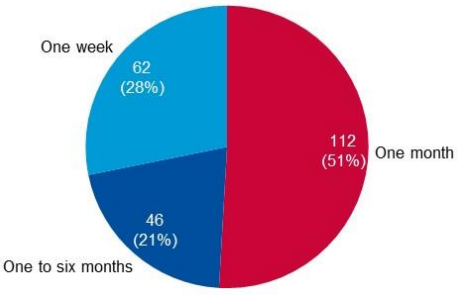
Figure 99: Primary legal driver of cybersecurity investments in the Transport sector, per mode of transport



5.6 PATCHING OF CRITICAL IT AND OT ASSETS

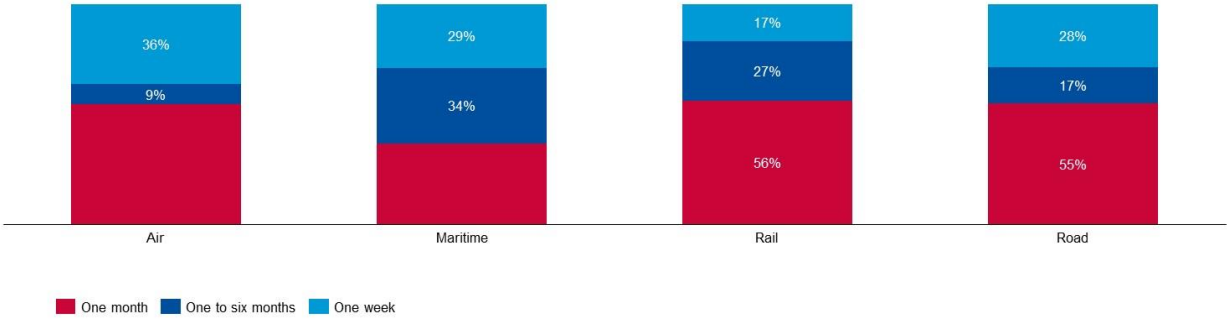
Survey Question: What is the average time to patch critical vulnerabilities on your organisation's critical assets (IT and OT)?

Figure 100: Time to patch critical vulnerabilities in the Transport sector



Based on the data collected, 51% of the organisations in the transport sector need one month to patch critical vulnerabilities on IT or OT assets, and 21% need a time between 1 month and six months. Only 28% of the surveyed organisations fix critical vulnerabilities on critical assets in one week.

Figure 101: Time to patch critical vulnerabilities in the Transport sector, per mode of transport



6. COMPARING SMES AND LARGE ENETRPRISES

This chapter aim to provide additional insights on the data collected through the lens of the organisation size, breaking down key figures for SMEs and Large Enterprises (LE).

Figure 102: SMEs and LEs distribution per NIS Sector

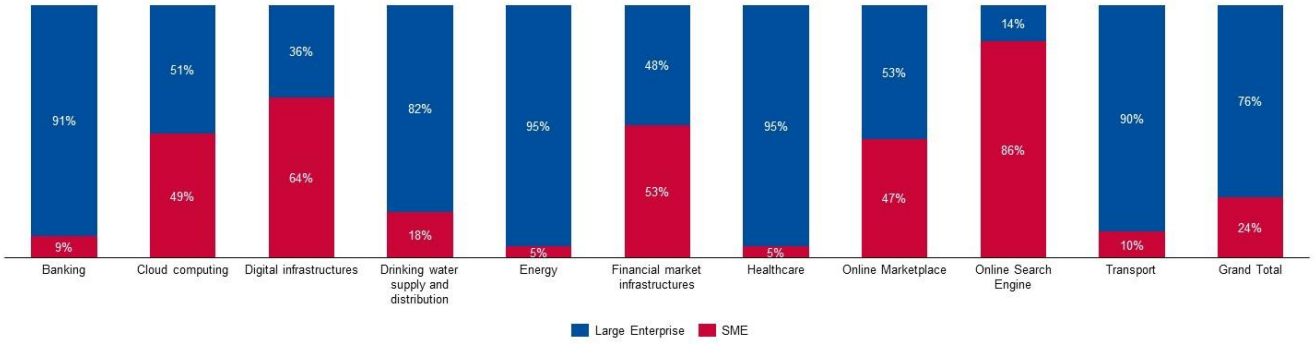
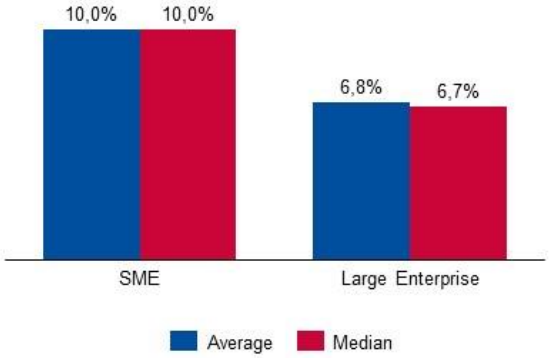
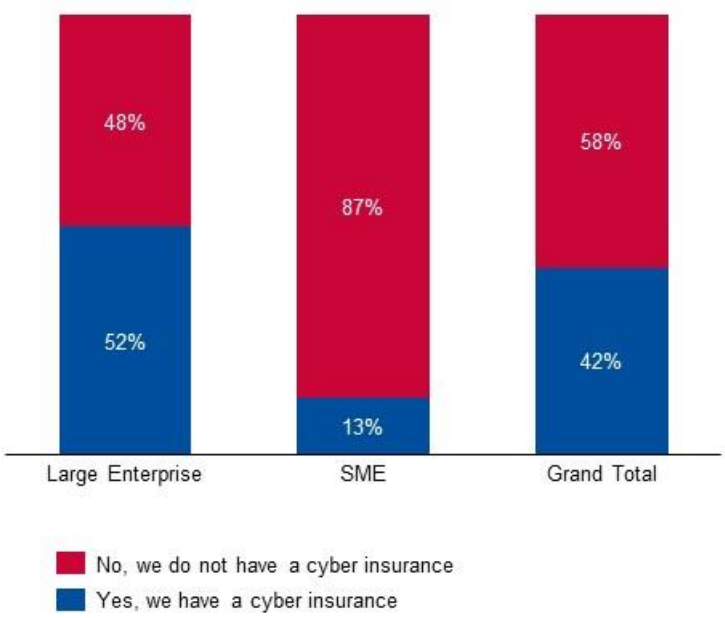


Figure 103: IS spend as a share of IT spend for SMEs and LEs



The IS spend as a share of IT spend appears larger than last year's findings for both SMEs and LEs. Consistently, the corresponding figure for SMEs appears larger than LEs, which is attributed to the need for certain baseline investments on cybersecurity – regardless of the organisation's size – which take up a substantial part of the budget. In that sense, LEs tend to benefit from the respective economies of scale.

Figure 104: Cyber insurance subscription for SMEs and LEs



The figures concerning cyber insurance subscription are substantially increased for both SMEs and LEs compared to last year, yet the big discrepancy in the percentage of respective organisations covered by cyber insurance seems to indicate that current cyber insurance offerings could benefit from tailoring to the needs of SMEs.

Figure 105: IS FTEs as a share of IT FTEs for SMEs and LEs

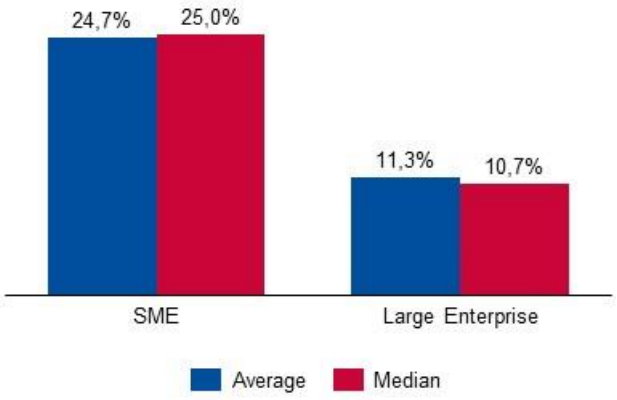
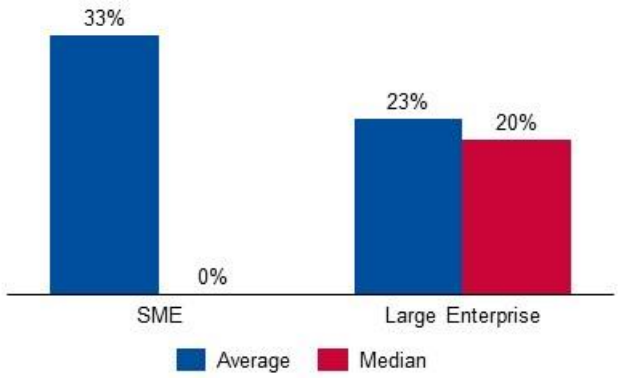
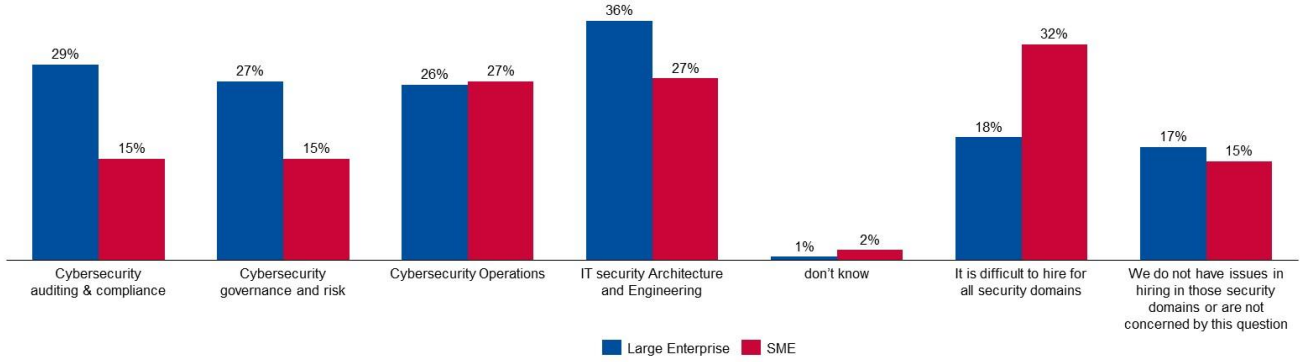


Figure 106: Percentage of contractors for SMEs and LEs



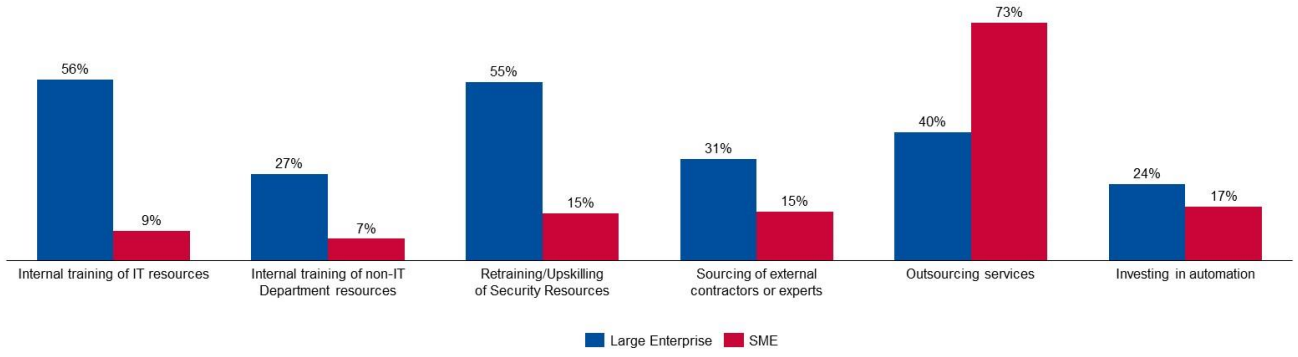
The median value of 0% for SMEs indicates that the majority of surveyed SMEs do not have any contractors among there is staff.

Figure 107: Security domains with difficulties in hiring for SMEs and LEs



A striking discrepancy in this figure concerns the difficulty for SMEs to hire cybersecurity staff in any security domain (32%) compared to LEs (18%).

Figure 108: Skill gap coverage strategy for SMEs and LEs



The data indicates that SMEs largely favour outsourcing (73%) when it comes to covering their cybersecurity skills gap, only rarely exploring other options such as internal training compared to LEs.

Figure 109: Cybersecurity training budget for SMEs and LEs

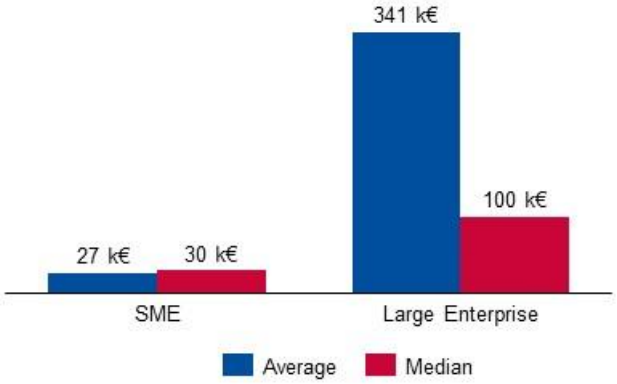


Figure 110: Cybersecurity risk management policies for 3rd parties for SMEs and LEs

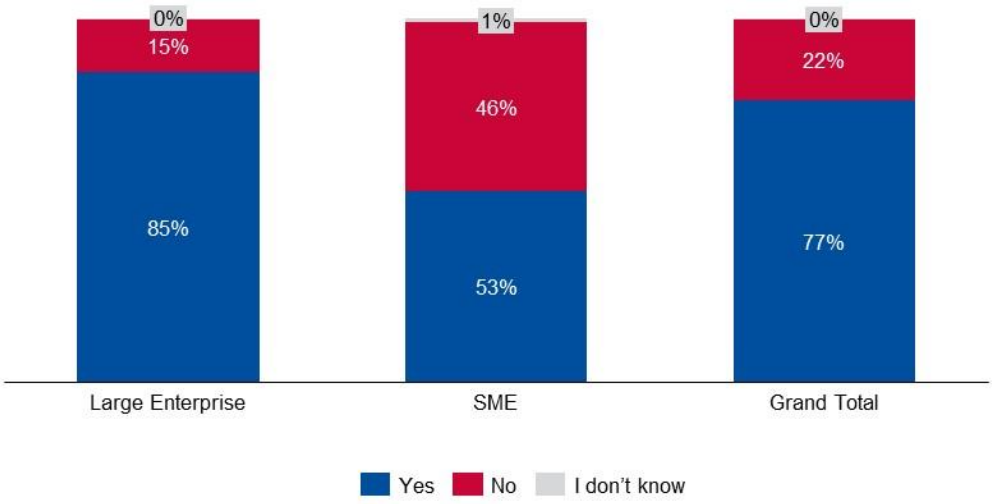
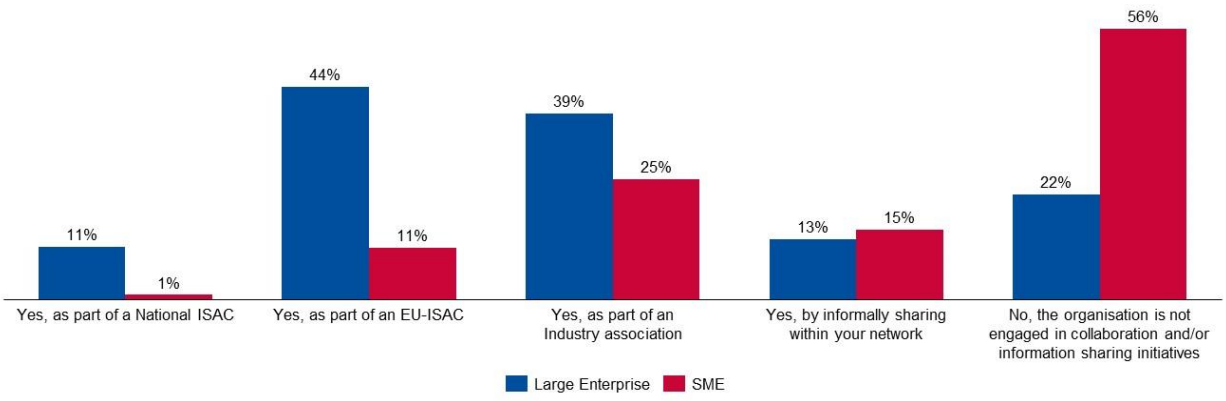
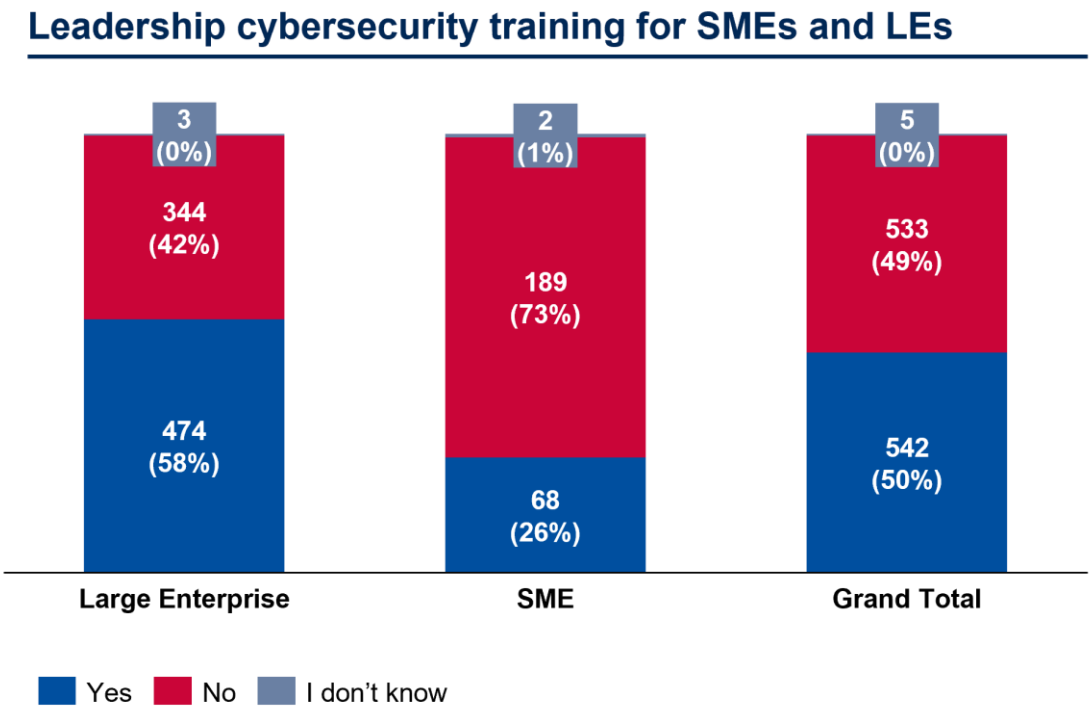


Figure 111: Information sharing for SMEs and LEs



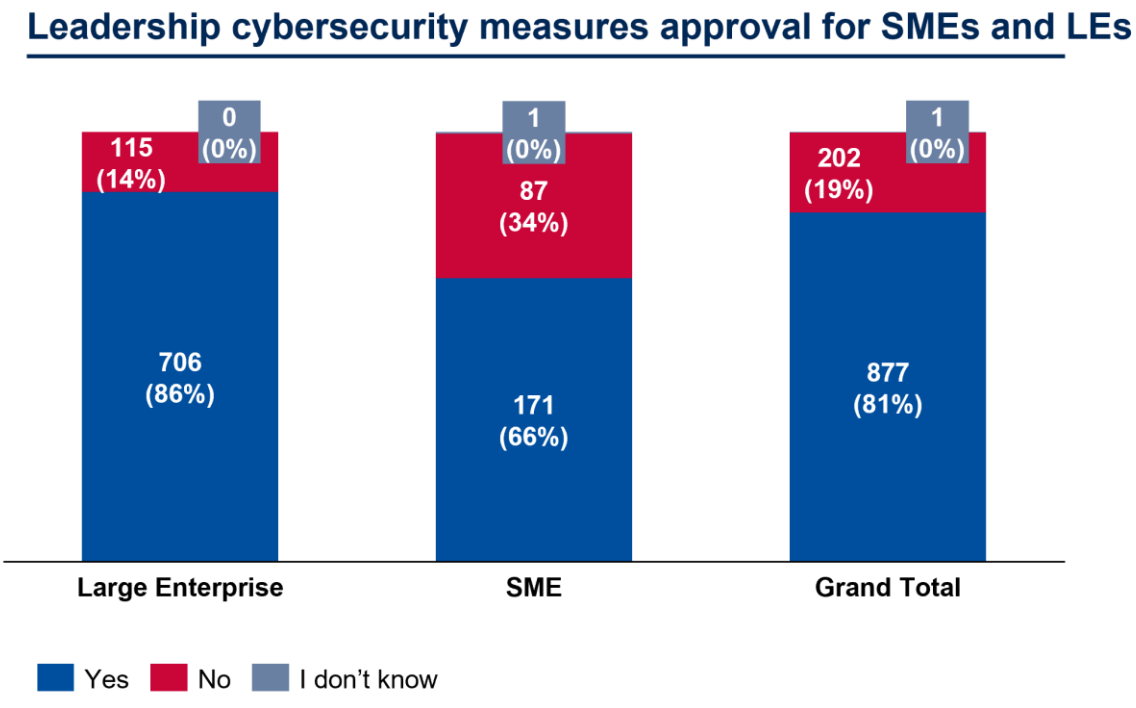
SMEs seem to have very limited access to information sharing initiatives such as ISACs (56% do not engage in similar activities) compared to LEs (only 22% do not engage in such activities).

Figure 112: Leadership attending dedicated training on cyber risks for SMEs and LEs



Leadership is attending dedicated cybersecurity training for 58% of the Large Enterprises surveyed, against 26% of the Small and Medium Enterprises, resulting in a significant 32% gap between the two categories of OES/DSPs.

Figure 113: Leadership approving cybersecurity measures for SMEs and LEs



Leadership is involved in the approval of cybersecurity measures for 86% of the Large Enterprises surveyed, against 66% of the Small and Medium Enterprises, which represents a 20% difference between the two samples. While the gap is less than the one observed for dedicated cybersecurity training, the finding still illustrates that leadership involvement in cybersecurity for SMEs is lagging behind that for LEs.

7. CONCLUSIONS

This report marks the fourth iteration of ENISA's Cybersecurity Policy Assessment (CSPA) work, which aims to provide EU and national policy makers with evidence to support them in assessing the effectiveness of the existing EU cybersecurity policy framework. For the past four years, this report has focused on the main legislative instrument, that is the NIS Directive, assesses the impact of the NIS Directive by providing an in-depth look into the investments of OES and DSPs in cybersecurity and how their cybersecurity capabilities and overall maturity have evolved over time. This year's work is based on data collected from 1080 operators from all 27 EU MS and allows for year-on-year comparison of NIS Investments data and the identification of specific trends among OES/DSPs. Moreover, this report provides additional insights into the topic of cybersecurity skills trying to identify the major challenges and skills gap projections and it also provides a sectorial deep dive for the Transport sector; for this sector additional operators were interviewed and the survey questionnaires were expanded to include additional, sector-specific questions. Due to the very large dataset, it is not practical to present all possible views and correlations of the collected datapoint so the report focuses on groupings per MS, per sector (cross-EU) and per organisation size (LEs vs SMEs). However, more granular views are possible (e.g. based on operator profiles) and can be used to support more targeted policy analysis.

A summary of the main findings and conclusions is presented below.

Compared to 2021, while the median spending on IT for OES/DSPs remained stable at EUR 10 million, the median spending on information security increased from EUR 0.6 million to EUR 0.7. The percentage of IT investments that **OES/DSPs in the EU allocate to information security was 7.1%** an increase of 0.4% compared to 2021. When comparing information security spending between EU organisations (not limited to OES/DSPs) and organisation from North America and APAC, IS spending as a share of IT spending is the lowest for organisations in the European Union at 5.1% compared to 6.4% (North America) and 6.3% (APAC). Still, entities in scope of the NIS Directive appear to outperform these values. A few conclusions can be drawn:

1. Global indicators rank **EU companies low compared to other regions in terms of IS/IT spending**.
2. However, **OES/DSPs seem to exceed these values** indicating a **positive influence of the NIS Directive** in increasing their spending
3. Still, looking at how the IS/IT ratio has developed over the past 3 years, **there does not seem to be a "race to the top"** when it comes to cybersecurity investments among OES/DSPs, meaning that more money is spent for compliance with the NIS Directive but cybersecurity is not yet perceived as a competitive advantage,

Even looking at the Transport sector specifically, despite the existence of sector-specific security and safety legislation, standards and other legislative instruments, **the NIS Directive is the main driver for cybersecurity investments for 55% among OES in Transport**.

A factor that could further drive investments are the provisions introduced with NIS2 (Art. 20) concerning the obligations that management bodies approve cybersecurity risk management measures and that they receive appropriate cybersecurity training to understand these risks. Currently – pre-NIS2 obligations –**leadership attends dedicated cybersecurity training in 50% of OES/DSPs** and is involved in **approving cybersecurity risk management measures for 81% of OES/DSPs**. When looking at how leadership involvement in cybersecurity affects a number of indicators, such as risk management maturity, incident detection and response

capabilities and 3rd party cyber risk management, the new NIS2 requirements could prove very impactful in driving overall cybersecurity maturity among essential and important entities.

70% of OES/DSPs participate in information sharing initiatives such as national or EU-ISACs industry associations or informally through their networks. However, sectors where EU ISACs exist demonstrate the highest rates of participation in any kind of information sharing activities (e.g. EE-ISAC, EM-ISAC, FI-ISAC, ER-ISAC, EH-ISAC). This shows the **impact of policy initiatives at EU level in support of ISACs**, that help create information sharing momentum in critical sectors even beyond the EU-ISACs themselves. Still, such information sharing activities often limit access to SMEs, since **56% of SMEs do not engage in similar activities**. This could be a potential area where future policy initiatives might focus.

A significant increase in the uptake of cyber insurance can be observed, as **42% of OES/DSPs subscribe to cyber insurance coverage compared to 30% in 2021**. More importantly, while in previous years the cyber insurance market appeared under-developed or not yet established in several MS, this year's findings indicate an active market in all EU MS. Still, **only 13% of SMEs subscribe to cyber insurance**, signalling that suitable products have yet to be developed tailored to the needs of SMEs. This issue may indicate a possible policy gap concerning the development of more standardised products suitable for SMEs.

The sectorial deep dive in the Transport sector revealed that 51% of the transport organisations manage OT security with the same unit or people as IT cybersecurity, while 15% manage OT security independently from IT cybersecurity. The most used method to manage cybersecurity risk for OT suppliers in the transport sector is through security requirements for products, services, or supplier personnel (78%) followed by eligibility criteria for OT suppliers and service providers (57%) and audit rights (55%). 51% of the organisations in the transport sector need one month to patch critical vulnerabilities on IT or OT assets, and 21% need a time between 1 month and six months, while **only 28% of the surveyed organisations fix critical vulnerabilities on critical assets in one week**.

Although cybersecurity investments among OES/DSPs appear on the rise, the same cannot be said about FTEs as OES/DSPs in the EU allocate 11,9% of their IT FTEs for information security a decrease of 0,1% compared to the median IS FTEs vs. IT FTEs ratio in 2021. Looking at internal FTEs, 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**. The security domain with the most IS FTEs is Cybersecurity operations with 40% of the IS FTEs, followed by IT security architecture and engineering with 23% of the IS FTEs, and cybersecurity governance and risk management with 21%.

51% of OES/DSPs plan to hire information security FTEs in the next two years aiming to hire on median 2 FTEs, with an average of 4 FTEs, meaning that larger organisations will drive even more recruitment than small ones. Most of these hires are expected in the domain of Cybersecurity operations (56%), followed by IT security architecture and engineering (42%) and cybersecurity governance and risk (36%). Still, closing this skills gap is faced with certain challenges; the cybersecurity talent gap is growing, with **over 3 million jobs requiring filling globally**. **83% of OES/DSPs claim recruitment difficulties** in at least one information security domain especially in the domain of IT security architecture and engineering (34%), followed by cybersecurity operations (26%) and cybersecurity auditing and compliance (26%), while 22% of OES/DSPs face difficulties recruiting in all domains. **32% of SMEs are facing difficulties hiring in any security domain**.

The three main strategies leveraged by the NIS sector organisations to cover the skills gap in cybersecurity are: outsourcing services (48%), retraining or upskilling of security resources (45%) and internal training of IT resources (45%). SMEs largely favour outsourcing (73%) when

it comes to covering their cybersecurity skills gap, only rarely exploring other options such as internal training compared to LEs.

47% of the surveyed organisations declare no specific budget for information security training. For the 53% of organisations with a specific information security budget, **the median training budget is EUR 100k**, with an average of EUR 333k.

8. ANNEX A – NIS DIRECTIVE SURVEY DEMOGRAPHICS

Figure 114: Sectorial distribution per Member State

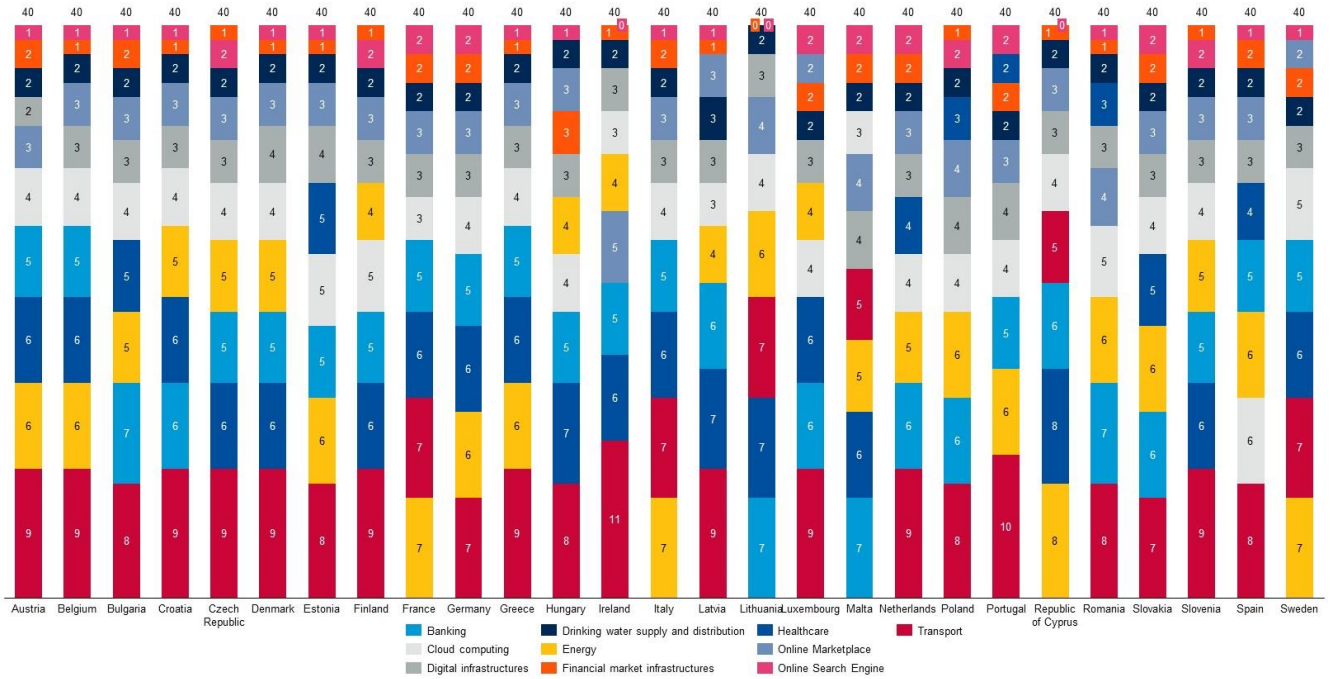


Figure 115: Revenue per NIS sector

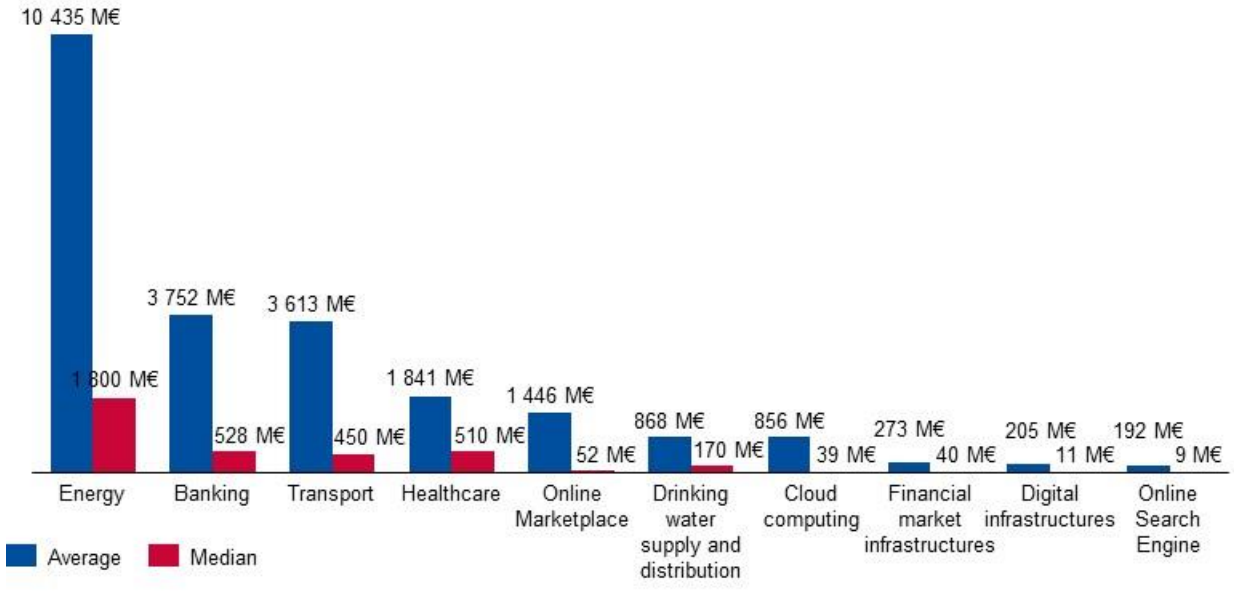


Figure 116: Employees per NIS sector

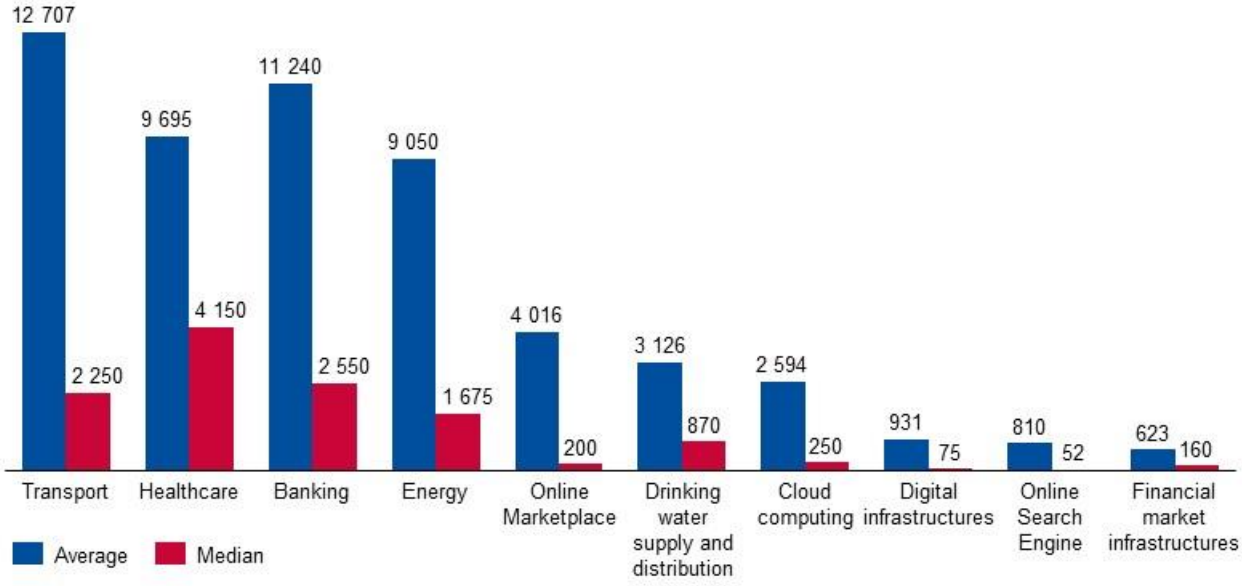


Figure 117: Function of respondent

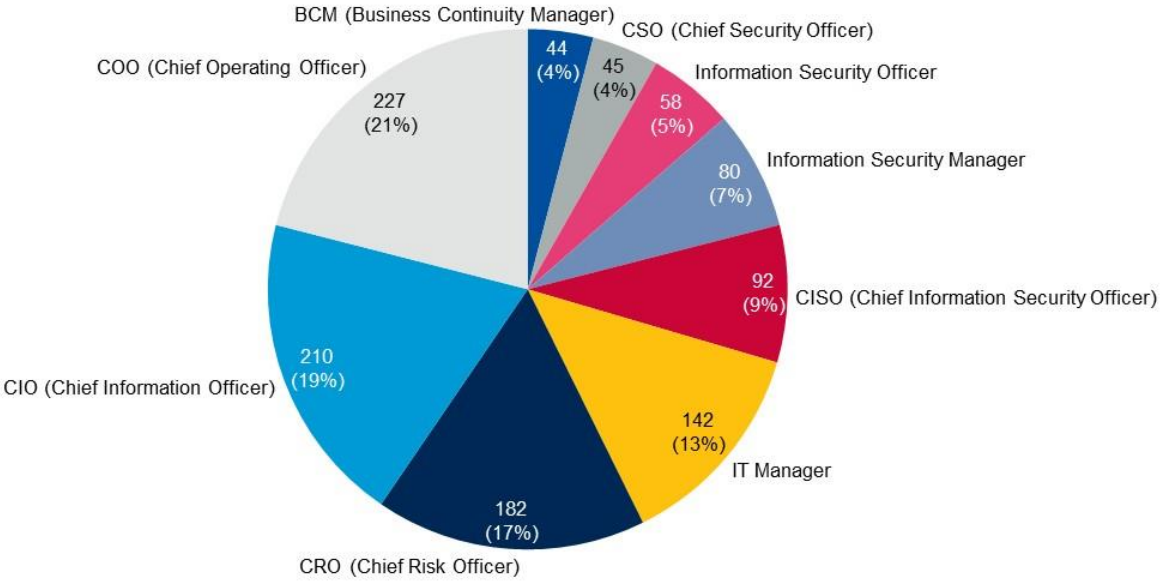


Figure 118: OES vs DSP distribution

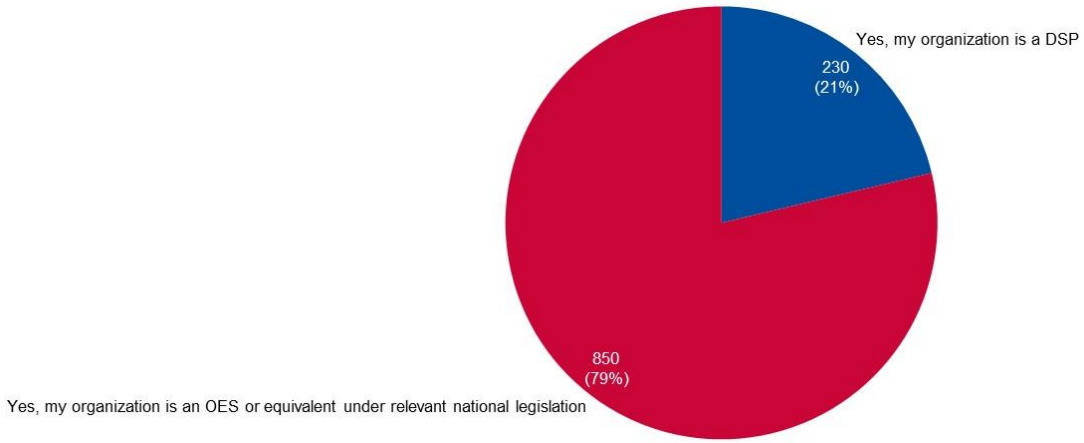


Figure 119: Small and Medium Enterprise (SME) vs Large Enterprise (LE) distribution

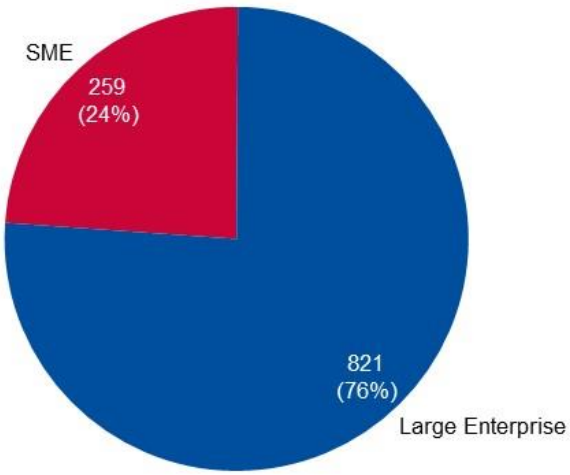
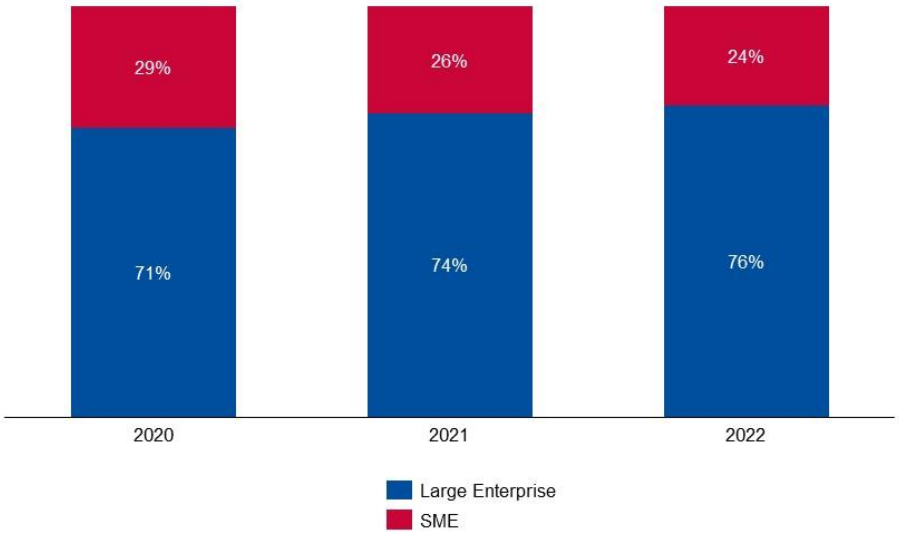


Figure 120: SME vs LE distribution year over year



9. ANNEX B: DEFINITIONS

9.1 MEDIAN AND AVERAGE DEFINITIONS

Median: the median is the value separating the higher half from the lower half of a data sample, a population, or a probability distribution. For a dataset, it may be thought of as **"the middle" value**.

The basic feature of the median in describing data compared to the mean (often simply described as the "average") is that it is not skewed by a small proportion of extremely large or small values, and therefore provides a better representation of a "typical" value.

Median income, for example, may be a better way to suggest what a "typical" income is, because income distribution can be very skewed.

Average or Arithmetic mean: the arithmetic mean is the sum of all measurements divided by the number of observations in the dataset.

Type	Description	Example	Result
Arithmetic mean	Sum of values of a dataset divided by number of values	(1 + 2 + 2 + 3 + 4 + 7 + 9)/7	4
Median	Middle value separating the greater and lesser halves of a dataset	1, 2, 2, 3, 4, 7, 9	3

9.2 CAGR DEFINITION

The compound annual growth rate (CAGR) is the annualized average rate of revenue growth between two given years, assuming growth takes place at an exponentially compounded rate. The CAGR between given years X and Z, where Z — X = N, is the number of years between the two given years, is calculated as follows:

- CAGR, year X to year Z = [(value in year Z/value in year X) ^ (1/N)-1]
- For example, the CAGR for 2006 to 2011 is calculated as: CAGR, 2006 to 2011 (X = 2006, Z = 2011, N = 5) = [(value in 2011/value in 2006) ^ (1/5)-1]

9.3 SME DEFINITION

The main factors determining whether an enterprise is an SME are defined in Recommendation 2003/361/EC[46] as follows:

- staff headcount.
- either turnover or balance sheet total

Company category	Staff headcount	Turnover	Balance sheet total
Medium-sized	< 250	≤ € 50 m	≤ € 43 m
Small	< 50	≤ € 10 m	≤ € 10 m
Micro	< 10	≤ € 2 m	≤ € 2 m

9.4 MAPPING OF ECSF PROFILES TO SECURITY DOMAINS

The table below maps the ECSF cybersecurity profiles to the security domains used in the analysis. The profiles of Cybersecurity Educator and Cybersecurity Researcher are excluded from this mapping.

Security domain	ECSF profiles
Cybersecurity governance and risk	Chief Information Security Officer (CISO) Cybersecurity Risk Manager
Cybersecurity auditing & compliance	Cybersecurity Auditor Cyber Legal, Policy and Compliance Officer
Cybersecurity operations	Cyber Incident Responder Cyber Threat Intelligence Specialist Digital Forensics Investigator Penetration Tester
IT security architecture and engineering	Cybersecurity Implementer Cybersecurity Architect

[46] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

TP-02-23-138-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-648-4
doi: 10.2824/060928