EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NIS INVESTMENTS

NOVEMBER 2022

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 the 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.

CONTACT

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

AUTHORS

Athanasios Drougkas, Viktor Paggio, Javier Gomez Prieto, ENISA
Patrick Abel, François Gratiolet, Edwin Maaskant, Gartner

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-585-2, ISSN 2600-4712, DOI: 10.2824/433214, Catalogue nr. TP-AM-22-001-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report marks the third iteration of ENISA's NIS Investments report, which collects 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 this investment has been influenced by the NIS Directive. In addition, global cybersecurity market trends are presented through Gartner security data and insights observed globally and in the EU, in order to provide a better understanding of the relevant dynamics.

This year's report presents data collected from **1080 OES/DSPs from all 27 EU Member States** and can now provide a historical dataset that allows for year-on-year comparison and identification of trends. Moreover, sectorial deep dives were conducted for the Energy and Health sectors.

Overall, a number of absolute values, such as **IT and Information Security (IS) budgets or % of IT budgets spent on IS seem to be significantly lower compared to last year**. This can be attributed to the composition of the survey sample and to the higher representation of OES from the Energy and Health sectors due to the sectorial deep dives, but also to the macroeconomic environment, such as the COVID-19 impact on the respective budgets.

Other key findings of the report include:

- The median percentage of IT budgets spent on IS is 6.7 %, **1 percentage point lower compared to last year's findings**.
- The **NIS Directive and other regulatory obligations**, as well as the threat landscape are the main factors **influencing IS budgets**.
- **Large operators invest significantly more on CTI compared to smaller ones** with the median spend on CTI across OES/DSPs being EUR 50 000. Internal SOC capabilities seem to be very closely correlated with CTI spending, even though CTI is useful outside the context of SOC operations likely indicating the **need to facilitate access to CTI for smaller operators**.
- The estimated direct cost of a major security incident is EUR 200 000 on median, **twice as large as last year**, indicating an increase in the cost of incidents. **Health and Banking remain the top two sectors** in terms of incident cost.
- 37% of the OESs and DSPs in the EU do not operate a dedicated SOC.
- 30% of OES/DSPs possessed cyber insurance in 2021, a **decrease of 13% compared to 2020**, with **only 5% of SMEs subscribing to cyber insurance**.
- 86% of OES/DSPs have implemented third-party risks management though only 47% have a dedicated TRM budget and only 24% have a dedicated TRM role.
- 32% of the OESs within the Energy sector indicate that none of their critical OT processes are monitored by a SOC.
- Only 27% of surveyed OES in the Health sector have a dedicated ransomware defence programme and **40% of surveyed OES have no security awareness programme for non-IT staff**.

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148

1. INTRODUCTION

This document is the third edition of the NIS investments study published by ENISA with the aim of understanding the impact of the **Directive on Security of Network and Information Systems** (**NIS Directive**)[2] on Operators of Essential Services (OES) and Digital Service Providers (DSP). Specifically, the objective of this report is to provide insights into how OESs and DSPs invest their 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.

Table 1: Categories of OES and DSPs as Defined in the NIS Directive

Categories of OESs and DSPs	
OES	**DSPs**
• Energy (electricity, oil and gas) • Transport (air, rail, water and road) • Banking • Financial market infrastructures • Health • Drinking water supply and distribution • Digital infrastructure	• Online marketplaces • Online search engines • Cloud computing services

So as to ensure a representative account of all 27 EU Member States, 40 organizations in each Member State were surveyed making a total of 1,080 organizations surveyed across the EU as a whole. Additional information on the demographics of the survey is available in Annex A. In light of the COVID-19 pandemic and recent geopolitical developments this report provides **two specific sectoral analyses**, focused on the Energy and Health sectors, respectively.

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

On 13 May 2022 the Council of the European Union and the European Parliament agreed on a directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), which adapts the previous NIS Directive to current needs. 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.

As such, this report could provide additional input and key lessons-learned during the transition phase from NIS to the NIS 2 Directive, as well as the future transposition and implementation of the second Directive.

[2] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148.

2. INFORMATION SECURITY DYNAMICS AND OUTLOOK

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

It should be noted that **the source of the data for Chapter 2** (Gartner databases and ENISA foresight) is **different than the source of the data for the rest of the chapters** (survey).

This data set is presented in order to provide a high-level overview of the global market in terms of information security investments and to highlight a few key dynamics of the market for information security. **This broader view serves as complementary information to the focused analysis presented in the rest of the report on OES/DSP in the Member States**.

2.1 TRENDS IN INFORMATION SECURITY AND SPENDING ON THREAT INTELLIGENCE

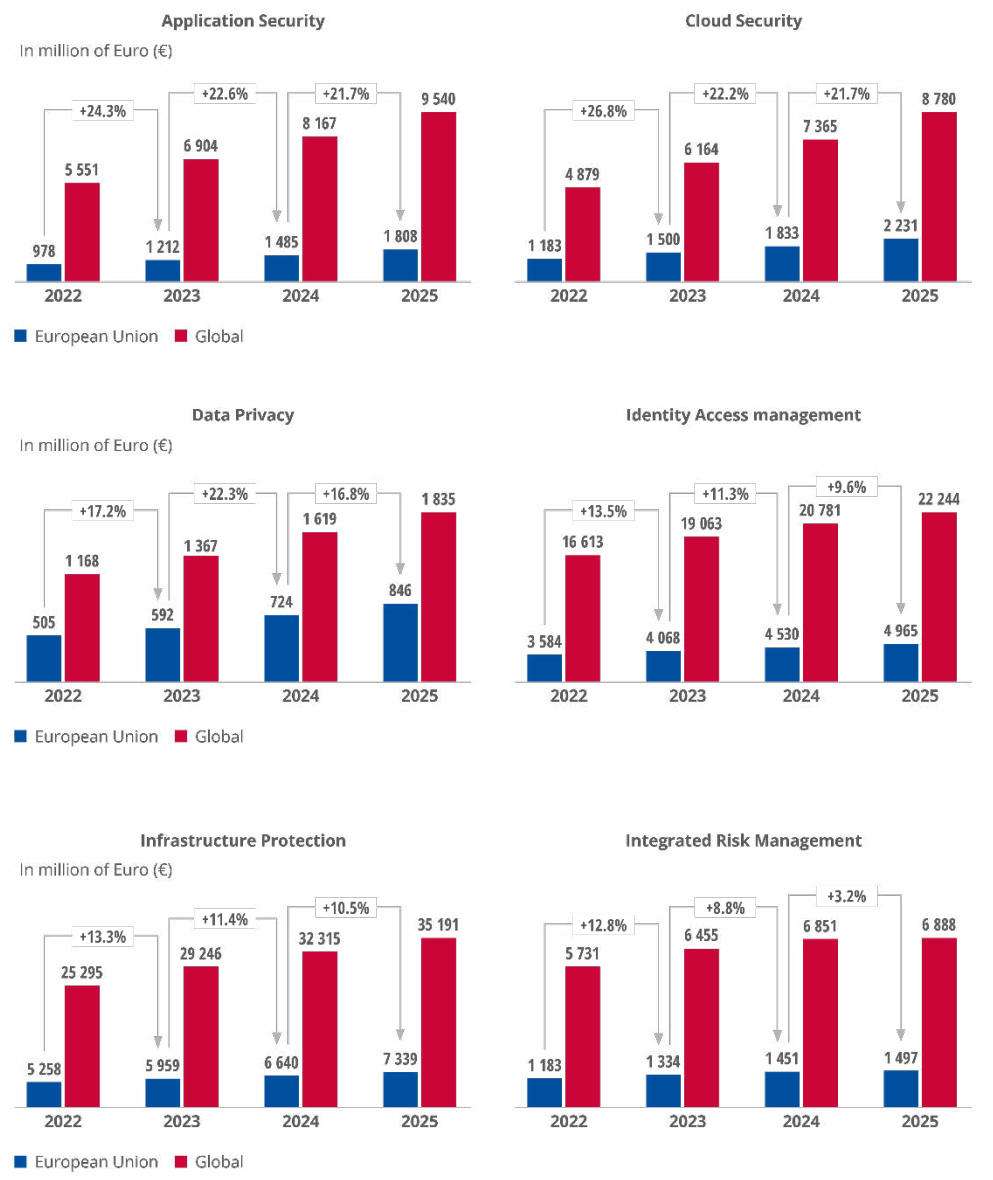
2.1.1 Forecast spending on Information security

In 2022, the market for information security and risk management will reach EUR 170 billion, with an estimated global growth of 6.5% by 2025[3]. This growth is driven by the reinitiating of projects that were put on hold at the beginning of 2020, an increase in remote and hybrid working and an increase in incidences of data breaches. The uncertainties at macroeconomic level caused by geopolitical conditions, inflation and the talent crunch will be at play as well, dampening growth in information security.

As illustrated in Figure 1, the total end-user spending on Information Security and Risk Management (ISRM) – both within the EU and worldwide – is expected to evolve among the following lines:

[3] Gartner, Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 2022.

Figure 1: ISRM End-User Spending Forecast

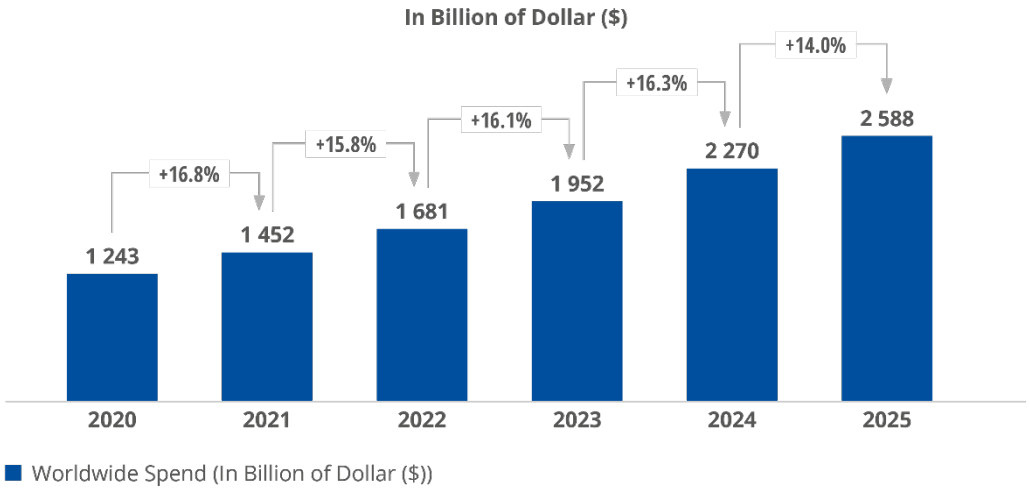


2.1.2 Spending forecast on cyber threat intelligence

The market for cyber threat intelligence (CTI) continues to benefit from relatively high demand coming from multiple organisations, ranging from small to large enterprises. The increasing awareness of the importance of cybersecurity and the realisation of the need to support decision-making and processes with operationalised threat intelligence are driving spending in this area[4].

[4] Gartner, Emerging Technologies: Critical Insights for Threat Intelligence Demand, 2022.

Figure 2: Worldwide CTI Spending Forecast



Regardless of these increased spending priorities, the CTI market remains fairly fragmented with an increasing number of established providers acquiring and driving CTI market consolidation, and the presence of vendors offering differing sets of focused specialisations and capabilities[5].

The market variation is characterised by differences in demand between more mature and better staffed security teams contrasted by less mature adopters. The more mature security teams tend to require more technical-focused CTI, while the less mature organisations are more likely to prefer less extensive, tactically oriented solutions rather than strategic intelligence that offers too much information that is difficult to leverage due to limited resources.

Small and midsize enterprises (SMEs) often opt for solutions that deliver prioritised and contextualized TI information that is more closely integrated with other security controls versus enterprise-specific CTI offerings such as dedicated threat intelligence platforms.

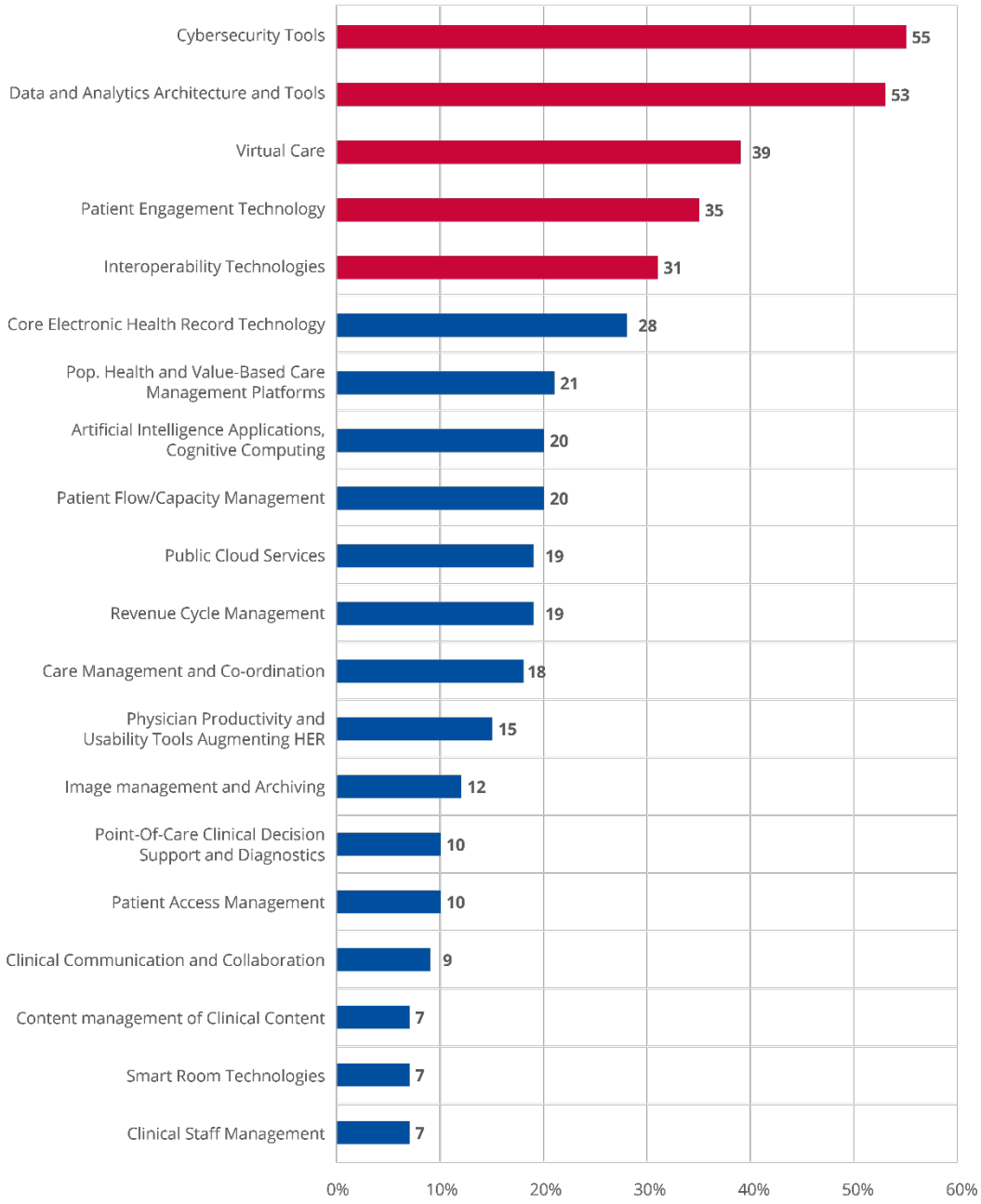
2.2 SECTOR SPECIFIC TRENDS IN SPENDING ON TECHNOLOGY

2.2.1 Technology investments in the Health sector

Figure 3 depicts the industry-specific technologies that are a top priority for increased investment in 2022[6]. Moreover, dedicated Gartner research indicates that COVID-19 continues to impact investment priorities within the Health sector, with many providers expanding care delivery outside the hospital's four walls.

[5] Gartner, Market Guide for Security Threat Intelligence Products and Services, 2021.
[6] Gartner, CIO and Technology Executive Survey, 2022.

Figure 3: Sector-specific solutions targeted for increased funding (%)



In light of the aforementioned, it may be noted that cybersecurity remains a top category for new spending in 2022, driven by unrelenting attacks on healthcare providers such as ransomware related intrusions[7]. Data and analytics ranked second in CIO priority for spending on solutions, which is related to the platform solutions for population health and value-based care management[8].

Virtual care remains one of the top priorities but is no longer the most commonly selected top five technology as it was in 2021. This likely reflects the slight maturing of this market segment,

[7] Gartner, Top 5 Technology Investments for Healthcare Providers in 2022.
[8] Gartner, Population Health Management Framework for Healthcare Provider CIOs, 2022.

where providers have already acquired what they need to fill the emergent needs of the pandemic to replace face-to-face patient visits[9].

Patient engagement remains solidly in the top five and includes CRM, portals and consumer-facing applications[10,11]. Furthermore, interoperability technologies have increased in priority, with 31% of CIOs selecting this in their top five compared to only 19% a year ago. Timely, relevant and accurate health data and insights about patient context are increasingly important to improving healthcare decisions and driving the adoption of health IT[12].

2.2.2 Technology investments in the Energy sector

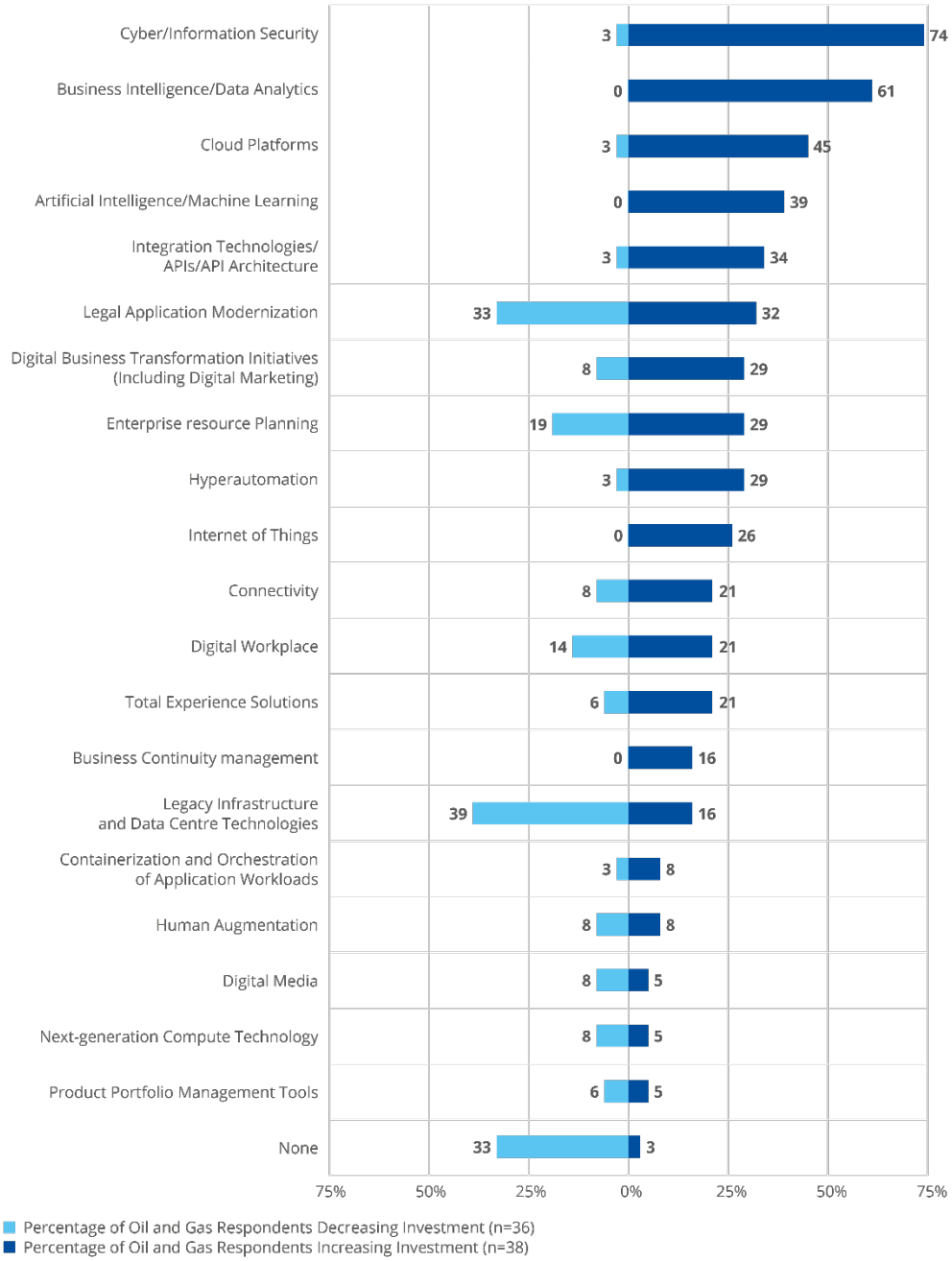
Prompted by increasing asset connectivity and rising cyber threats, oil and gas companies have moved to modernise and address legacy gaps in cybersecurity. As in recent years, cybersecurity tops the list of technologies for investment in 2022, with the highest percentage yet seen of organisations (74%) increasing spending[13].

The sector's enthusiasm for analytics technologies is undimmed; 61% of organizations will increase investment in business intelligence or data analytics, while 39% will increase investment in AI or machine learning. Moreover, the augmentation of the sensor networks of installed control systems with IoT sensors and data aggregation to support analytics has been a major theme of digitalization in the sector[14].

Notably, cloud platforms have increased in priority with 45% of companies increasing investment. In that same context it may be noted that a significant 39% of companies are planning on decreasing spending on legacy infrastructure and data centres. A change in stance based on proven provider capabilities has led many oil and gas companies to prioritise cloud services when seeking efficiency and improvements in productivity[15].

[9] Gartner, Market Guide for Virtual Care Solutions, 2021.
[10] Gartner, Market Guide for Digital Health Platform for Healthcare Providers, 2021.
[11] Gartner, Hype Cycle for Consumer Engagement with Healthcare and Wellness, 2021.
[12] Gartner, 7 Critical Domains of a Successful Healthcare Provider Interoperability Strategy, 2022.
[13] Gartner, Top 10 Trends Driving the Oli and Gas Industry in 2022.
[14] Gartner, Market Guide for Advanced Distribution Management Systems, 2021.
[15] Gartner, Emerging Technologies and Trends Impact Radar: Enabling Power and Energy Technologies, 2022.

Figure 4: Sector-specific solutions targeted for increased or decreased funding (%) – Oil and Gas sector



2.3 TOP STRATEGIC TRENDS IN CYBERSECURITY

As a result of the COVID-19 pandemic, hybrid working and the cloud-based digitalization of business operations have both expanded, resulting in new security issues. This situation has led to ransomware attacks, intricate attacks on the digital supply chain, deeply ingrained vulnerabilities and an increase in attacks on identification systems. Additionally, a lack of trained security personnel makes these mounting security issues even worse.

Against this backdrop, Gartner predicts that cybersecurity practices in the EU will be impacted in two primary ways as outlined below[16].

2.3.1 Reframing the security practice

The centralised approach to cybersecurity controls will become obsolete due to significant changes in the scope, scale and complexity of the modern digital organisation. As such, cybersecurity leaders are increasingly being placed in various parts of the organisation to decentralise security decisions.

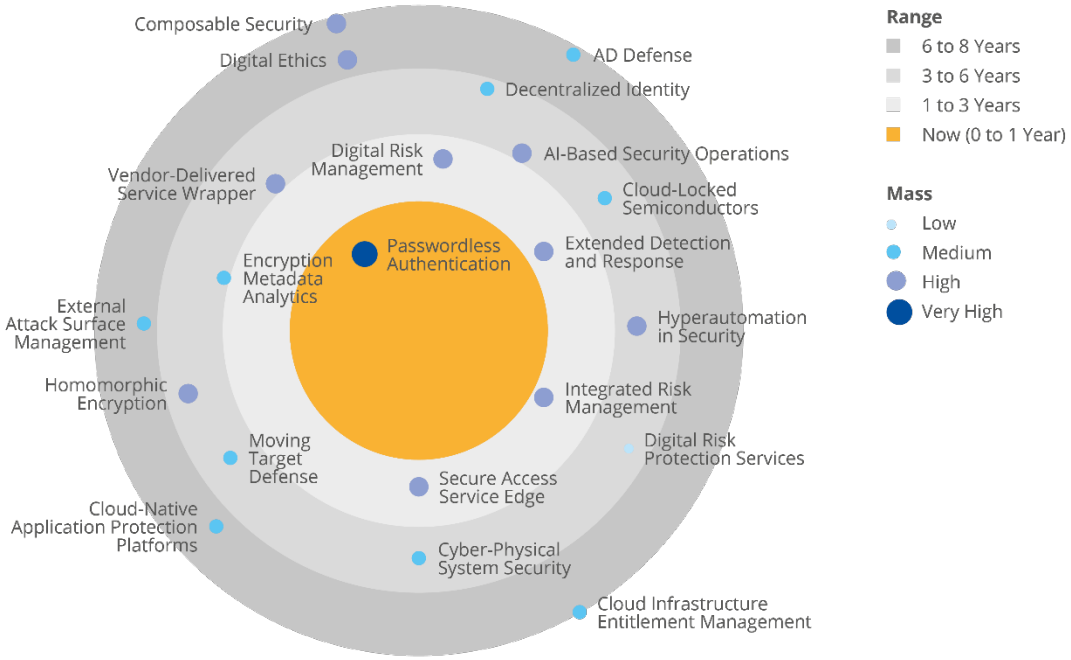
However initiatives to rethink and refocus security awareness are necessary to enable more sophisticated thinking about security and distributed responsibilities for security. Therefore, forward-thinking leaders in security and risk management should invest in security behaviour and culture-changing programmes that foster new ways of thinking and embed new security behaviours within organisations.

2.3.2 Rethinking technology

Given the shortage of human resources and the lack of skilled experts, most organisations are still unable to implement effective, all-encompassing cybersecurity. As a result, there is a growing need to combine security products into multifunctional solutions that can address a variety of related security problems.

There are several trends that characterise the emergence of security technologies, represented in Figure 5 and further elaborated below[17].

Figure 5: Emerging security technologies & trends



At a basic level, **passwordless authentication** is a means of authenticating users without using passwords. Passwordless authentication is considered to be in the 'now' range, with estimated adoption around 30% to 40% of the way towards an early majority target.

[16] Gartner, Top Trends in Cybersecurity 2022.
[17] Gartner, Emerging Technologies: Top Trends in Security for 2022.

Integrated risk management (IRM) is defined as practices and processes supported by a risk-aware culture and enabling technologies that improve decision-making and performance through an integrated view of how well an organisation manages its unique set of risks. IRM is believed to be one to three years from adoption by an early majority because — although the technology is ready — it is taking some time for organisations to embed IRM into their operations.

Secure access services edge (**SASE**) delivers multiple converged network and security 'as a service' capabilities, such as software-defined wide-area network (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), firewall and zero trust network access (ZTNA). SASE is estimated to be about one to three years away from adoption by an early majority, whereas several vendors offer complete SASE solutions today and those solutions are maturing quickly.

Digital risk management (DRM) technology integrates the management of risk specifically associated with digital products and services enabled by cloud, mobile, social and big data, as well as third-party technology such as artificial intelligence (AI), machine learning (ML), operational technology (OT) and the Internet of Things (IoT). DRM adoption is estimated to be one to three years out as the capabilities of IRM solution providers and market consolidation begin to address the complete scope of the DRM use cases of organisations.

Extended detection and response (XDR) is a threat detection and incident response (IR) tool that unifies multiple security products. The IR capability can change the state of individual component security products as part of the recovery process. XDR is considered to be a short-range technology that will gain rapid adoption and acceptance in the market, enabling less mature organisations to deliver genuine threat detection and response capabilities[18].

2.4 THE CHANGING CYBER THREAT LANDSCAPE

An expanding digital footprint introduces gaps in inventory and data collection, which inevitably weakens preventative controls, business continuity plans, data protection, monitoring and incident response capabilities. The lack of visibility across the expanding environment of an organisation leads to more enterprise blind spots, some of which are exploited by attackers[19].

2.4.1 Attack surface expansion

Traditional approaches to security monitoring, detection and response need to shift significantly to address the risks posed by new technologies and business initiatives. Organisations should begin to look at the value placed on areas that may currently seem inconsequential, such as increases to the attack surface brought about by users connecting to new applications and services outside the corporate purview.

Digital risk protection services (DRPS), external attack surface management (EASM) technologies and cyber asset attack surface management (CAASM) can help visualise the external and internal parts of the business that enable systems and thus automate the discovery of some of the gaps in coverage[20]. As such, organisations must begin to think about security strategies beyond the traditional 'castle-keep' scenarios and take action to increase the visibility of security and mitigation of risk of critical business functions.

Furthermore, IBM's X-Force Threat Intelligence Index 2022 assessment[21] indicates that threat actors targeted various sectors in 2021 and will continue to do so.

[18] Gartner, Emerging Technologies: Top Trends in Security for 2022.
[19] Gartner, Top Trends in Cybersecurity 2022.
[20] Gartner, How to Respond to the 2022 Cyberthreat Landscape.
[21] IBM, X-Force Threat Intelligence Index 2022.

Table 2: Top 10 sectors affected in 2021

Sector	% of Attacks
Manufacturing	23.2%
Finance and Insurance	22.4%
Professional and Business Services	12.7%
Energy	8.2%
Retail and Wholesale	7.3%
Healthcare	5.1%
Transportation	4.0%
Government	2.8%
Education	2.8%
Media	2.5%

2.4.2 Identity threat detection and response (ITDR)

The misuse of credentials is continuing to accelerate, increasing the number of security incidents in consequence. What is worse is that sophisticated attackers are trying to exploit the identity system more frequently. This can provide a successful attacker with unprecedented levels of access while making detection and response significantly more difficult.

Although organisations have already spent considerable effort on improving IAM capabilities, much of it has been spent on technology to improve user authentication. Although this represents an important security advance, somewhat ironically, it has also increased the attack surface for a foundational part of the cybersecurity infrastructure. Consequently, more needs to be done to protect identity systems, detect when they are compromised, and enable rapid investigations and efficient remediation. Although the need for better prevention and detection is clear, ensuring the highest levels of IAM fabric resilience also requires the ability to quickly revert to a known good state.

The IAM teams of many organisations spend too much of their time protecting other group's digital assets, and not enough time protecting their own IAM infrastructure. ITDR is not yet a consolidated product offering. Instead, several tools can assist organisations in building a defensive IAM capability. Many IAM tools are however still operating in silos that are not visible to incident responders. Organisations must re-evaluate their IAM infrastructure with the goal of identifying opportunities for detecting compromise and immediately investigating and responding. Currently, best practice is to use a layered approach (defence-in-depth strategy) that leverages complementary IAM and security controls.

2.4.3 Digital supply chain risks

Digital supply chain security is another noteworthy emerging cyber threat. Vulnerabilities that are deeply embedded in the digital supply chain are often extremely difficult to detect, and thousands of applications or devices may be impacted simultaneously.

These risks are becoming significant enough to demand new approaches to mitigation that involve more deliberate risk-based vendor or partner segmentation and scoring, more requests for evidence of security controls and secure best practices and a shift to resilience-based thinking. As a result, security and risk management teams need to partner with other departments to prioritise and manage risks to digital supply chains. Although the overall level of risk transparency remains disappointingly low, regulatory frameworks are emerging for organisations that support public sector and critical infrastructure related markets, and adherence to these new rules will increasingly become mandatory[22].

Moreover, these efforts can provide a blueprint for new approaches to managing supply chain risks in non-regulated entities. Although it is certainly desirable to ascertain a critical partner's susceptibility to attack, current approaches are only partially successful in identifying and remediating supply chain attacks. Today's organisation can never hope to entirely avoid security failure, and effective leaders focus on the organisational resilience of mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios[23].

2.5 THE ONGOING CYBERSECURITY TALENT CRUNCH

Accelerated digital transformation of information and services has rendered the cybersecurity teams of many organisations unable to handle the increased demand for cybersecurity services. Cybersecurity leaders are experiencing challenges with sourcing talent, developing teams of skilled specialists, retaining talent, preparing for future demands for talent and improving leadership in cybersecurity[24].

The labour market for IT employees has been tightening throughout 2021, a trend that exacerbates hiring challenges for leaders in cybersecurity. The job market for IT professionals is tightening increasingly, with the number of IT employees seeking employment having decreased by 3.3% compared to Q1 2021. At the same time optimism among specialists about job opportunities and their expectations of high rewards upon switching employers continue to increase (14.7% increase in compensation). The combination of decreasing numbers of active job seekers and high expectations for new jobs makes it more challenging for organisations to compete for talent.

To address these challenges and achieve long-term strategic objectives, CISOs should evolve their talent sourcing and development tactics by sourcing staff from less conventional channels. By expanding cybersecurity talent pipelines and employing progressive team development practices, cybersecurity leaders can meet demands for increased cyber talent despite the lack of conventionally qualified hires. CISOs should also anticipate emerging cyber threats and create new corresponding roles and skills training to address increased demand and growing threats[25].

2.5.1 Leverage non-traditional labour pools and profiles

Organisations have traditionally hired computer science or science, technology, engineering and math graduates from technical universities and then backfilling those who leave with lateral hires of similar experience. Many organisations have in the past confined their recruitment to the cities in which the firms have delivery centres, often partnering with local universities to attract new graduates.

These strategies must now be rethought. The COVID-19 pandemic has proved that many consulting and software engineering services can be delivered by people working remotely. There is no longer any benefit in restricting recruitment to the cities where organisations have delivery centres. Moreover, the flexible staffing market has experienced the same high demands

[22] Gartner, Top Trends in Cybersecurity 2022.
[23] Gartner, How to Respond to the 2022 Cyberthreat Landscape.
[24] Gartner, Cybersecurity Talent Strategies for CISOs.
[25] Gartner, IT Services Talent Crunch: 5 Urgent Levers for Tech CEOs to Attract and Retain Staff.

as the rest of the service market, making resources scarcer and daily billing rates higher than usual.

2.5.2 Prioritise and implement relevant technology

Used properly, technology and automation can be used to improve work by automating highly repetitive tasks, which frees up talent that can then be focused on higher-value-added work. The higher-value-added work in turn is something that talent desires and will be important for attracting and retain talent.

It is critical to note that, for all their usefulness, technology, automation, ML and AI are not friction-free and come with a host of challenges themselves, such as reinforcing bias and scaling bad practices. There needs to be proper governance and sponsorship by multidimensional stakeholders to ensure proper execution of the advantages of technology to address the talent crunch.

2.5.3 Strengthen employee value propositions

The employee value proposition is the set of attributes that potential and current employees perceive as the value they gain through employment with the organization. While compensation is very important, job opportunity, career development and respect are equally powerful factors that employees value.

Employee value propositions are notoriously difficult to build or change, even in the aftermath of the COVID-19 pandemic. The primary reason for that inability to realise greater value is that the majority of organisations are focused on an outdated concept of employee value propositions that focuses on work and not on the human element. These strategies must now be rethought.

2.5.4 Redesign work

Successfully addressing the talent crunch will require organisations to rethink and redesign the way work is done and measured. The highest prioritisation should be on improving processes and making work easier as these have the most impact on workforce health, while also making the process environment more effective.

Organisations now have an opportunity to take a fresh look at basic assumptions about the work that goes into producing and delivering their products and services. This analysis should start at the business process level. It should include job categories behind each product or service, and typically may need to extend to the level of individual tasks and job roles. Critically, it needs to include a strong focus on metrics — for example, the fixation on utilisation as a primary measure of IT service performance can detract from a more value-oriented focus. Today's unprecedented talent crunch demands a review and often a reordering of the metrics being used[26].

2.6 ENISA FORESIGHT

ENISA recently published its first report on the topic of foresight with the aim of defining a comprehensive framework that will allow the identification of emerging and future cybersecurity challenges[27].

[26] Gartner, Cybersecurity Talent Strategies for CISOs.
[27] https://www.enisa.europa.eu/publications/foresight-challenges

The Foresight Challenges report presents ENISA's primary use cases and proposes an appropriate methodological framework for each use case. The identified key use cases, which are expected to be key drivers in future cybersecurity dynamics are the following:

- **Future and emerging challenges** that will impact security over the next 3-5 years;
- **Strategic decision-making development** so that leadership can design a strategy that can manage future challenges over the next 3-5 years;
- **Evolution of the threat landscape** and foreseen changes of cybersecurity emerging threats and drivers over the next 1-3 years;
- **Needs and priorities for cybersecurity R&D** to assess the gap between existing research focus and required future focus based on landscape evolution over the next 5 years;
- **Evolution of operational cooperation** to consider shifting factors in cooperation mechanisms and relationships;
- **Identification of future policy priorities** based on emerging challenges that may warrant a policy response;
- **Disruptive events** that necessitate envisioning future states following events such as mass ransomware incidents or wide-reaching APTs.

As ENISA builds its knowledge around these key foresight use cases, the present report will keep monitoring their influence on the global cybersecurity dynamics and outlook.

3. INFORMATION SECURITY INVESTMENTS FOR OESs AND DSPs

3.1 METHODOLOGY

This study is based on a dedicated market survey conducted among 1,080 organisations — with 40 organisations surveyed in each Member State — that were 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.

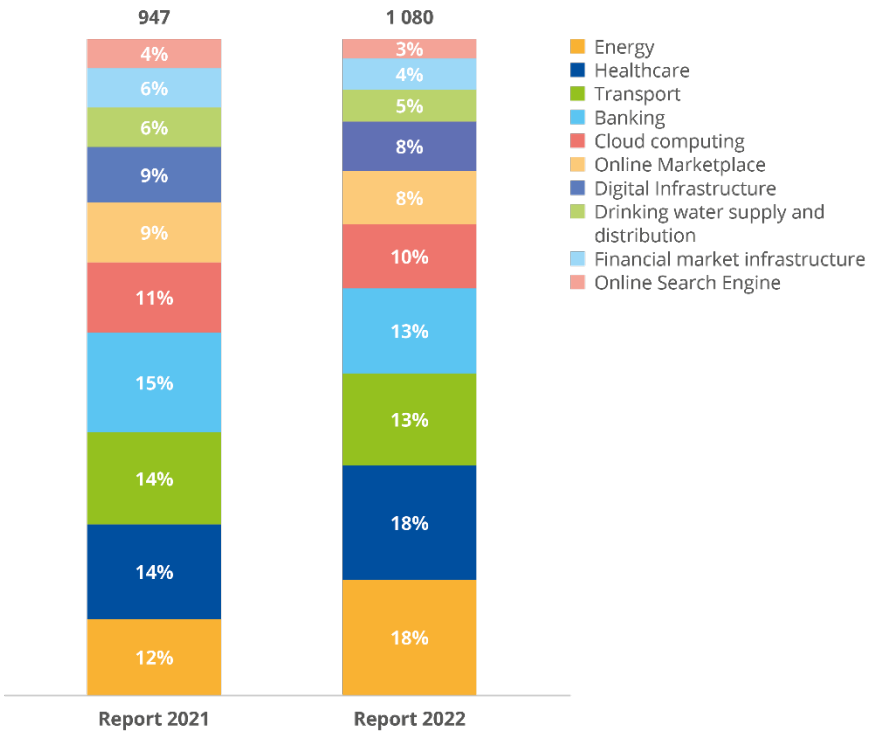
Some questions are recurring questions year over year in order to enable observation of NIS investment trends. It must however be noted that **the sample of this study is different in terms of composition and size compared to previous studies, which can influence the results and observations derived**. For more information on the composition of the demographics of this year's study, please refer to chapter 8 and ANNEX A.

A critical change in the sample composition is related to the fact that more organizations from the Energy and Healthcare sectors were surveyed this year in order to perform specific deep dives on those two sectors of interest. Thus, this year data was collected from 193 organisations in the Energy sector compared with 113 last year, which represent an additional 80 energy organisations surveyed (+70%). Similarly, data was collected from 189 organizations in the Health sector compared with 137 last year.

Figure 6 illustrates the difference in sectorial distribution between this year's and last year's samples. An example of the impact this change can have is that the Energy sector is the sector with the lowest IS spend as a share of IT spend both in last year's study (5%) as well as in this year's study (5%), therefore the increase of Energy sector organizations surveyed from 12% to 18% of the total sample will lower the overall median IS spend as a share of IT spend.

The specific market composition of each sector in terms of company size has also been analysed by categorizing the organisations in terms of SMEs or Large Enterprises, based on the EU definition.

Figure 6: Composition of the study sample by year and by sector



Furthermore, disparities between the historical data have to be assessed in light of the macro trends and challenges that occurred in 2021 — such as, but not limited to, **increasing cost optimisation in the aftermath of the COVID-19 pandemic**.

The quantitative metrics that were collected in the survey have been analysed on the basis of a median and average approach in order for the reader to appreciate both viewpoints.

The median value, though not necessarily representing the "typical" value in a highly fragmented dataset, 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 where it is affected by large organisations that do not necessarily reflect the populated and fragmented market of most of the sectors and countries that were analysed.

By way of example:

- The median value for Information Technology spending amounts to €10 million in 2021 (cf. §3.2.1) which 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 €60 million, but this number is skewed by large organisations that possess significant budgets dedicated to Information Security.

With regard to the qualitative metrics that were collected for this market study, the distribution of the organisations' answers has been calculated in percentage form so as to balance the weight of each answer against the others.

Finally, additional information and insights on the Energy and Health sectors have been derived from the overall data set and are represented within two deep dives in chapters 6 and 7 respectively. Although sub-sectoral information has been collected for those two deep dives, the

data collected does not allow for sub-sectorial comparison in this year's survey as most organisations operate in multiple sub-sectors which means that the figures collected are not representative of a single sub-sector.

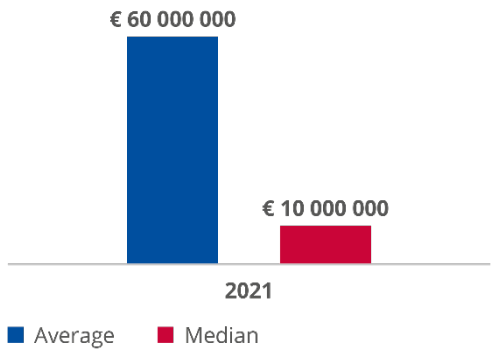
3.2 SPENDING ON INFORMATION SECURITY

Key Figures
The median Information Technology (IT) spending of an OES or DSP in the EU was EUR 10 million in 2021, while the average value of IT spending was EUR 60 million over the same period.
The median spending for information security (IS) of an OES or DSP in the EU was EUR 600 000 in 2021, while the average spending was EUR 4 million.
Regarding median values, an OES or DSP in the EU earmarks 6.7% of its IT investments for information security, while the average value is 7.2%.
On median, an OES or DSP in the EU spends EUR 50 000 on CTI, while the average spending amounts to EUR 399 000.

3.2.1 IT spending

Survey Question: What was your organisation's estimated IT budget or spending in Euros for 2021 (including CAPEX and OPEX for hardware, software, internal personnel, contractors and outsourcing spend)?

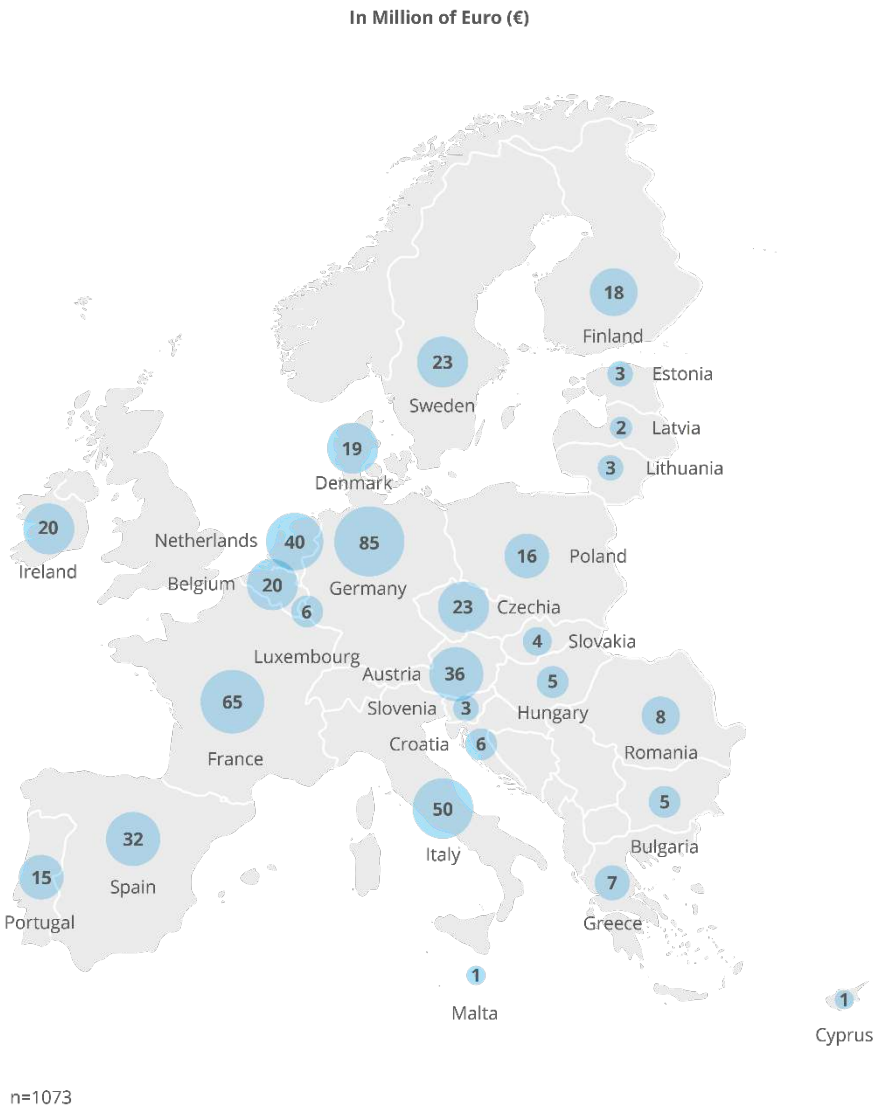
Figure 7: IT spending – all sectors



The median Information Technology (IT) spending of an OES or DSP in the EU was EUR 10 million in 2021, while the average value of IT spending was EUR 60 million over the same period.

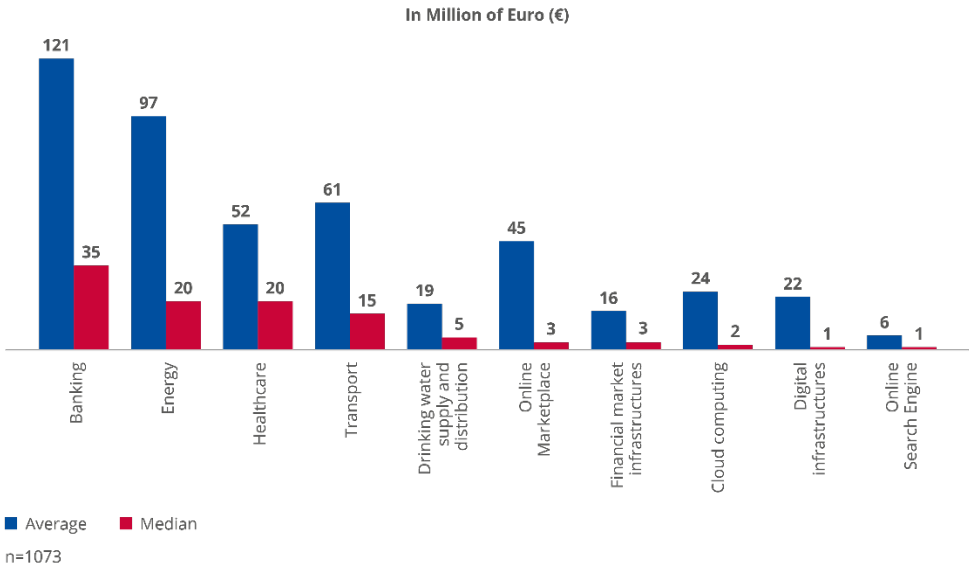
While these are absolute values that have to be interpreted in light of the sector's structure and company size, a smaller budget does not necessarily imply a lower level of cybersecurity maturity. Furthermore, as detailed in the methodology section, it must be noted that the sample in this study was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

Figure 8: IT spending of OESs 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, data on investments refers to the average among the OESs and DSPs surveyed and not Member State's investments. In addition, when interpreting these figures, the market fragmentation or average operator size in each Member State, as well as the criteria for identifying OESs and DSPs in each Member State — including the size of OESs and DSPs — need to be factored in.

Figure 9: IT spending by sector

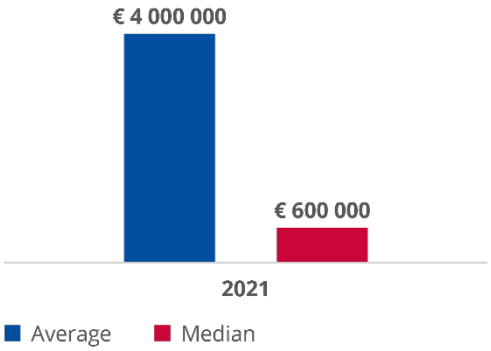


The survey data indicates that median IT spending is highest within the Banking sector (EUR 35 million), followed by the Energy, Healthcare (EUR 20 million) and Transport sectors (EUR 15 million). The IT spending in these sectors significantly exceeds IT spending in other sectors, as illustrated in Figure 9. Furthermore, Online Search Engines and Digital Infrastructures have the lowest IT spending across all sectors, with a median spending of EUR 1 million.

3.2.2 IS spending

Survey Question: What was your organization's estimated Information Security budget or spending in Euros for 2021 (including CAPEX and OPEX for hardware, software, internal personnel, contractors and outsourcing spend)?

Figure 10: Information security spending



The survey data indicates that the median spending for information security (IS) of an OES and DSP in the EU was EUR 600 000 in 2021, while the average spending was EUR 4 million.

While these are absolute values that have to 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 terms of composition and size compared to previous studies, which can influence the results and observations derived.

Figure 11: Information security spending of the OESs and DSPs surveyed in each Member State

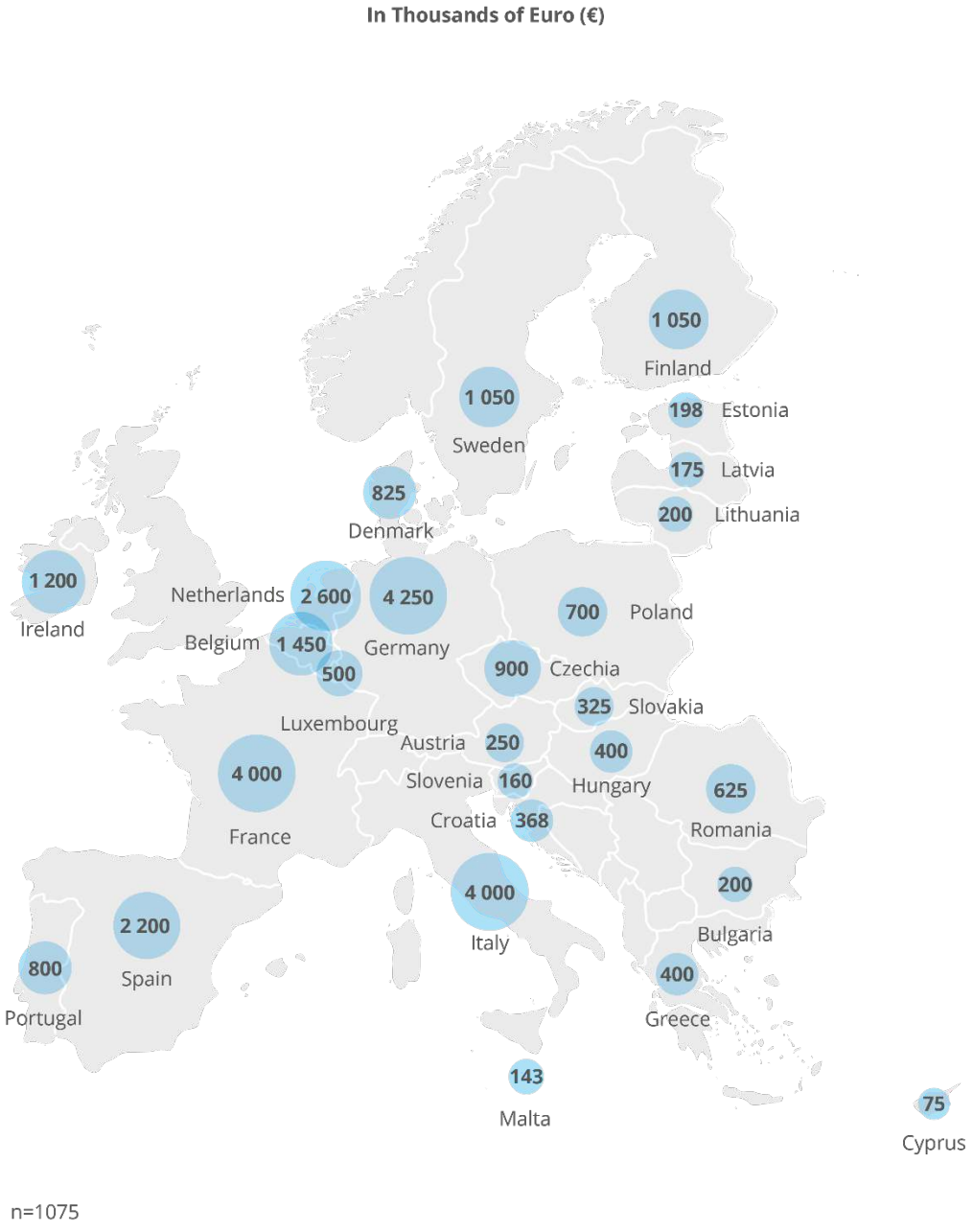
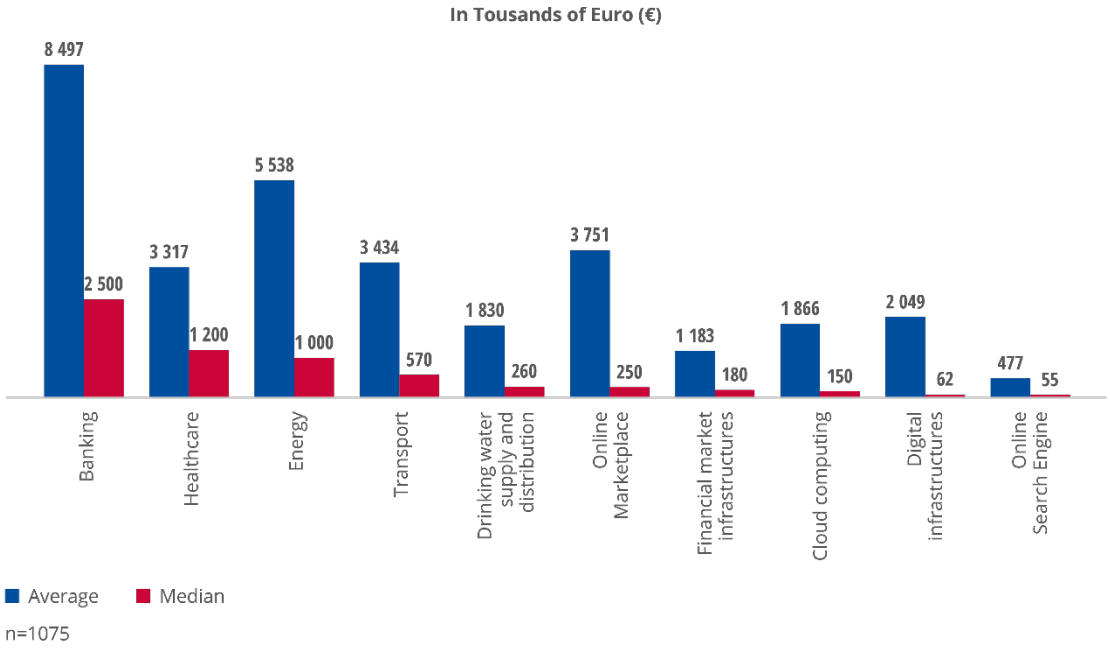


Figure 12: Information security spending by sector

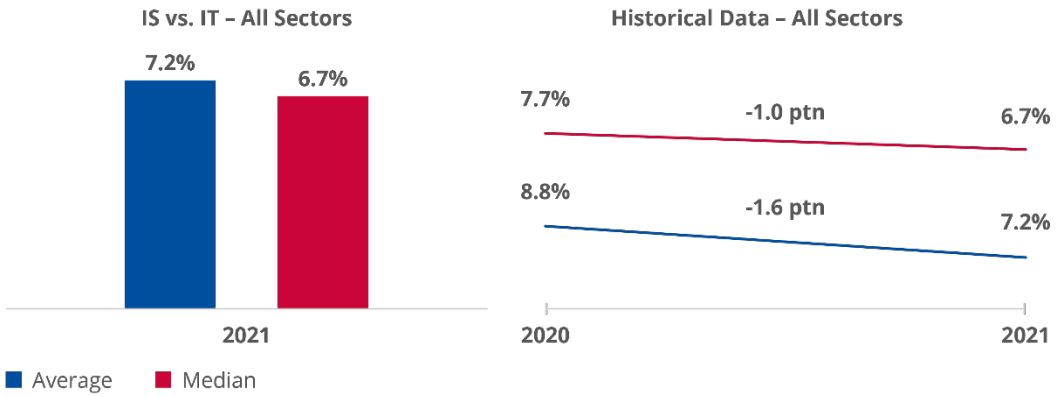


In a manner similar to the total IT spending, the Banking sector (EUR 2.5 million) has the highest IS spending, followed by the Healthcare (EUR 1.2 million) and Energy sectors (EUR 1.0 million). Furthermore, the information security spend of Digital Infrastructure and Online Search Engine companies is the lowest, amounting to a median spending of EUR 100 000.

3.2.3 IS spending as a share of IT spending

In order 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 is illustrated in Figure 13.

Figure 13: Information security spending as a share of IT spending – all sectors



As regards the median value, an OES or DSP in the EU earmarks 6.7% of its IT investments for information security, while the average value is 7.2%. When analysing this normalised data set with historically available data, a decrease of one percentage point is observed in comparison to the median IS vs IT spending in 2020. As detailed in the methodology section, the historical

analysis has to be done while keeping in mind the slight differences in the samples between the years of study and the differences in the macro environment.

Figure 14: Median information security and IT spending – all sectors

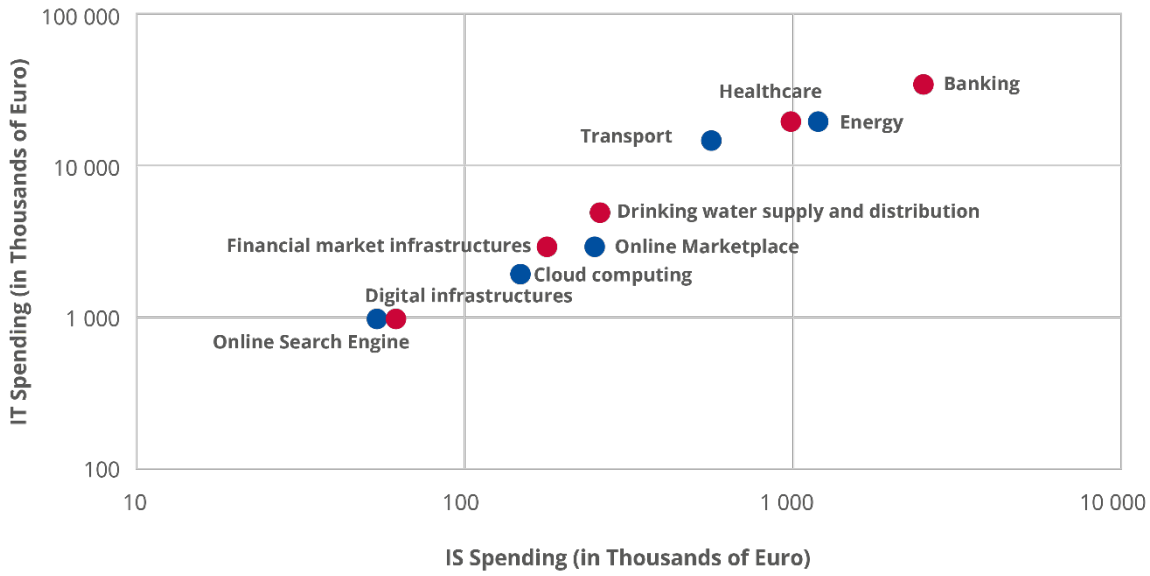


Figure 15: Information security spending as a share of IT spending of OES or DSP surveyed in each Member State

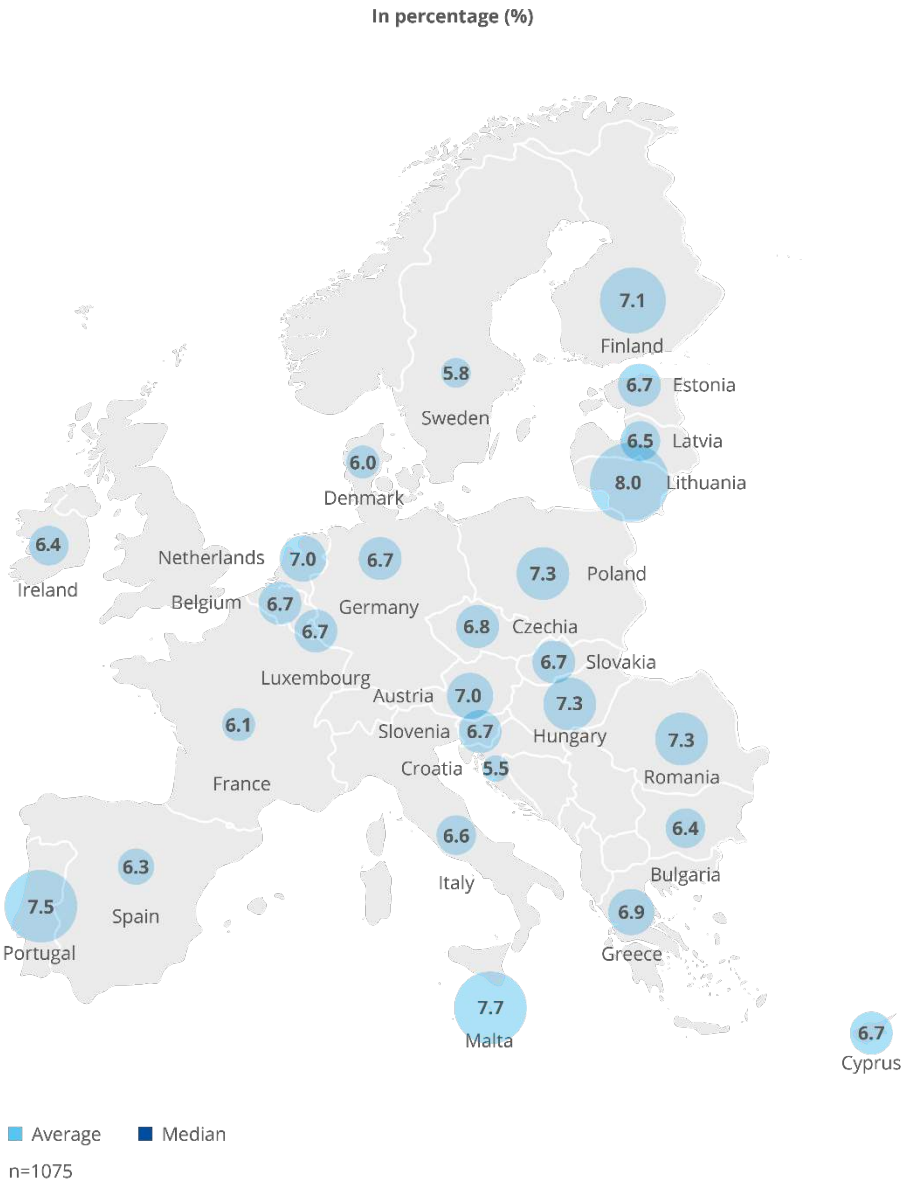
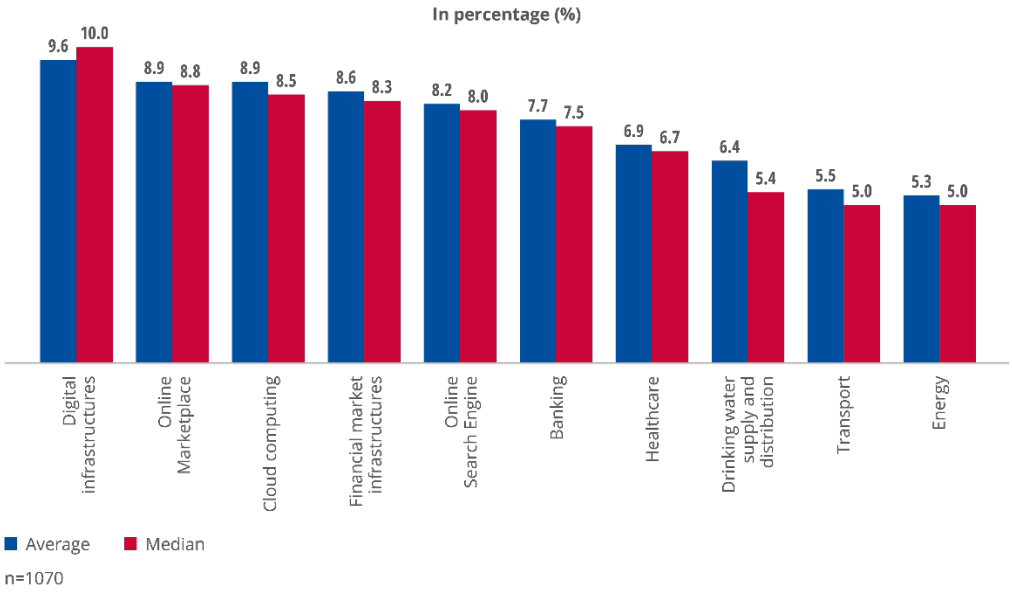


Figure 16: Information security spending as a share of IT spending by sector

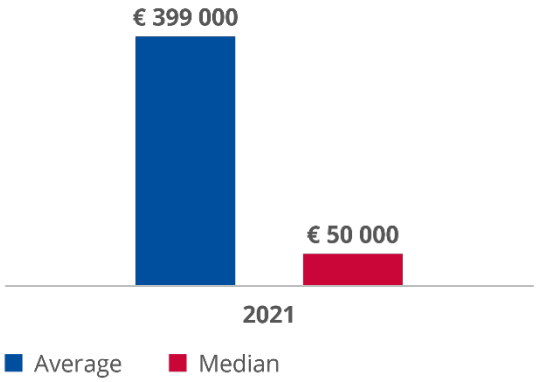


In line with the 2020 data, Digital Infrastructures maintain the highest IS vs IT spending (10%) in 2021, followed closely by Online Marketplaces (8.8%) and Cloud Computing (8.5%). Drinking water supply and distribution, Energy and Transport bring up the rear, with an IS vs IT spending that is lower than 5.5%.

3.2.4 Cyber threat intelligence (CTI) spending

Survey Question: What was your organisation's estimated security budget or spending in Euros for cyber threat intelligence (CTI) and/or information sharing for 2021?

Figure 17: CTI spending – all sectors



The survey data indicates that an OES or DSP in the EU spends on median EUR 50 000 on CTI, while the average spending amounts to EUR 399 000. The disparity between the median and average values indicates that most organisations do not earmark vast budgets for CTI, while some (larger) organisations — specifically within the Banking and Energy sectors — do invest significantly in CTI.

Figure 18: CTI spending for each OES or DSP surveyed in each Member State

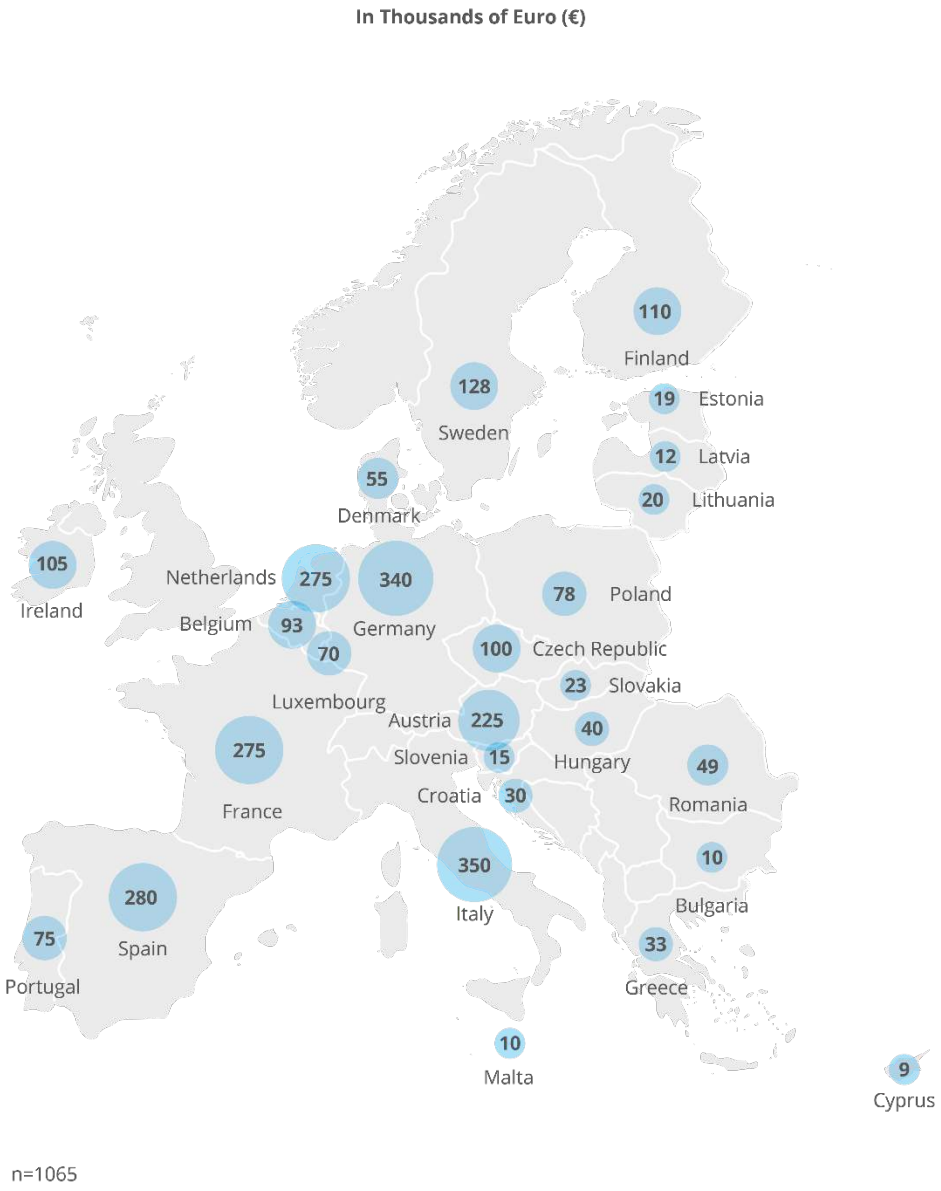
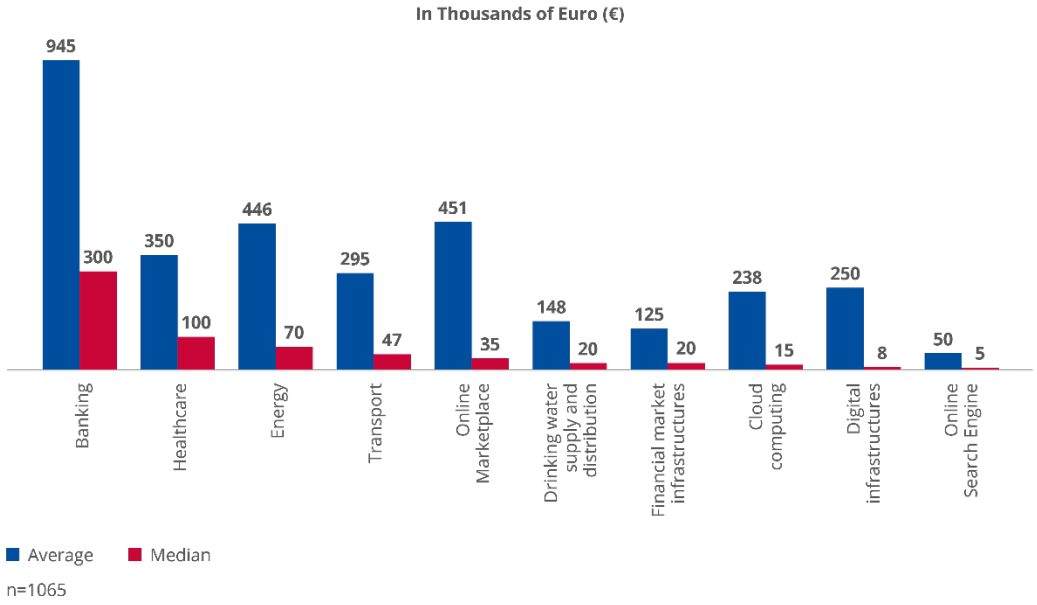


Figure 19: CTI spending in each sector



The survey data indicates that median CTI spending is the highest (EUR 300 000) in the Banking sector, significantly exceeding the other sectors as illustrated in Figure 19. Furthermore, Online Search Engines and Digital Infrastructures have the lowest CTI spending across all sectors, with a median spending of EUR 6 000 and EUR 8 000 respectively.

3.2.5 External factors impacting cybersecurity investment strategies

Survey Question: Which external factor(s) had the most impact on your organisation's cybersecurity investment strategy? ***Rank the three factors with the most impact, where 1 indicates the most important one***

Figure 20: External factors impacting cybersecurity investment strategies

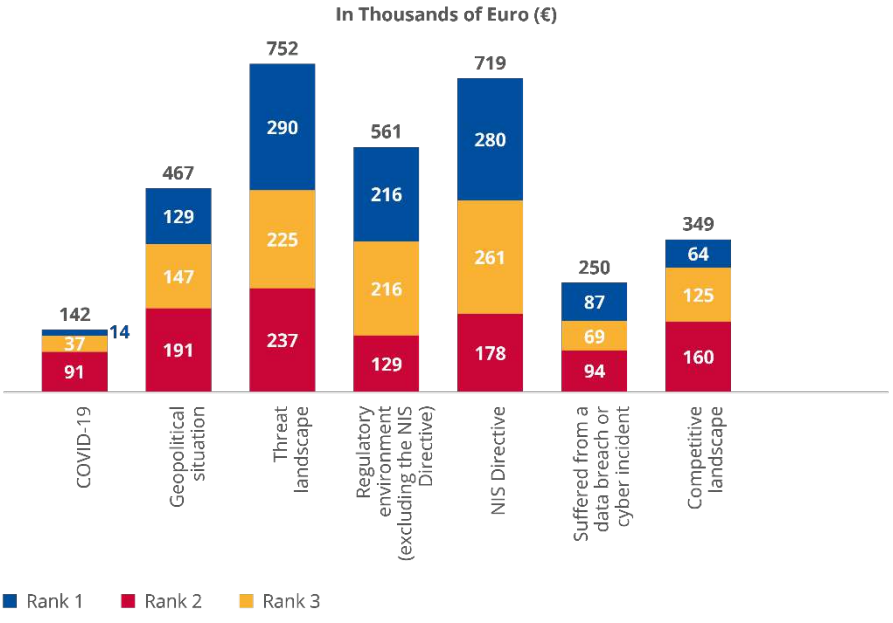
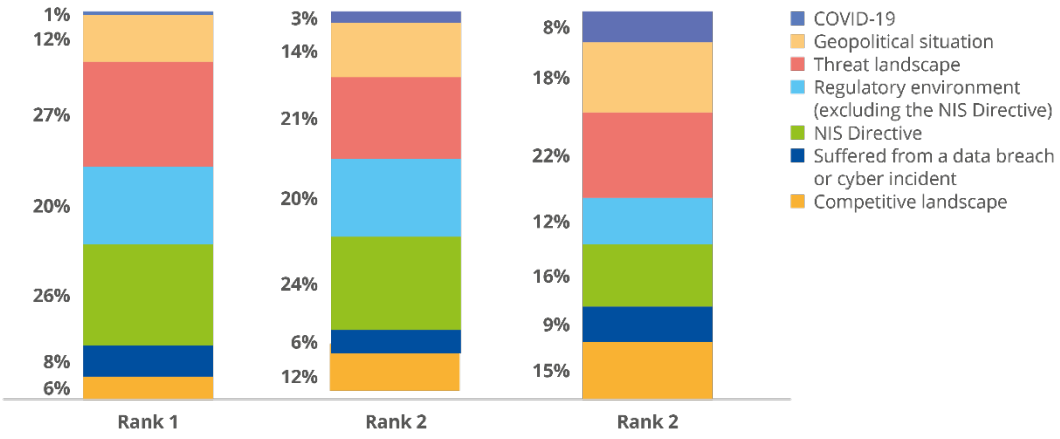


Figure 20 details the major external factors affecting investments in cybersecurity, ranking them in importance from one to three with rank one being the most important factor.

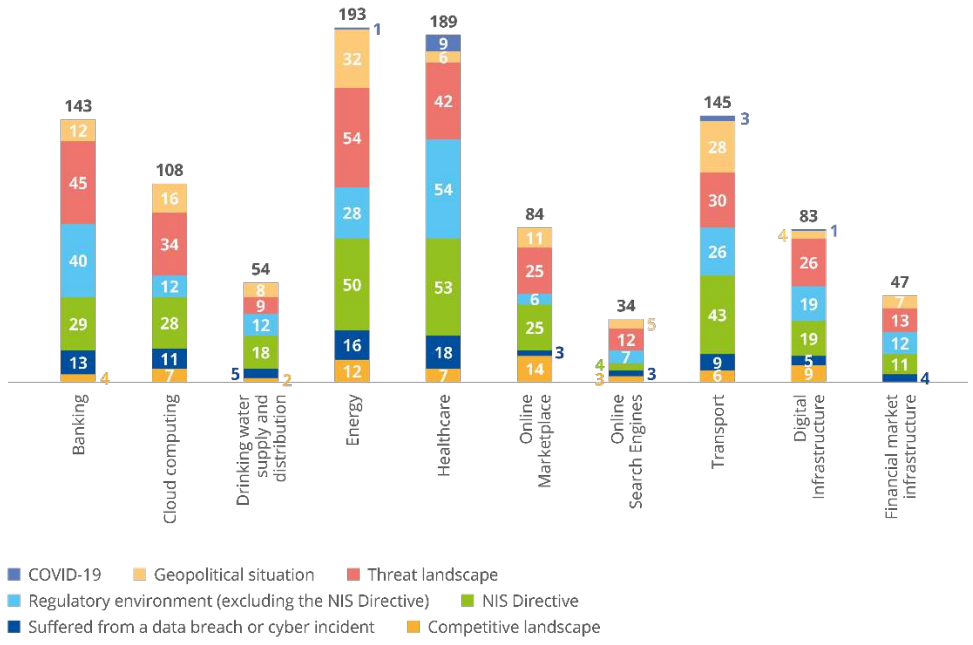
The survey data indicates that the cybersecurity investment strategy of 69% of the OESs and DSPs in the EU was mostly influenced by the threat landscape, closely followed (66%) by obligations under the NIS Directive. Furthermore, the regulatory environment and the current geopolitical situation are taken into consideration as determinants of investments by 52% and 43% respectively of the organisations surveyed.

Figure 21: External factors impacting cybersecurity investment strategies by rank



The ranking analysis shows that although COVID-19 may be an external factor impacting cybersecurity investments for a small portion of the organisations surveyed, it comes mostly in the third rank in the importance of external factors.

Figure 22: Most important external factor (ranked 1) impacting cybersecurity investment strategies in each sector



The sectorial analysis of the most important external factors impacting spending on information security shows that behind the Threat Landscape and the NIS Directive, the Geopolitical situation had a very high impact in the Energy and Transport sectors while the impact was much lower for Digital Infrastructures and Online Search Engines. For Healthcare, the overall regulatory environment was as important as the NIS Directive in driving cybersecurity investments.

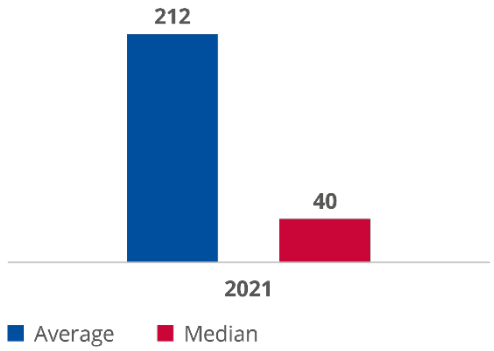
3.3 INFORMATION SECURITY AND NIS STAFFING

Key Figures
For an OES or DSP in the EU, the median number of employees is 40 IT FTEs and the average is 212 FTEs.
The median number of employees in an OES or DSP in the EU is 5 IS FTEs and the average is 21 FTEs.

3.3.1 IT FTEs

Survey Question: What was your organisation's estimated number of IT FTEs for 2021 including internal staff and contractors?

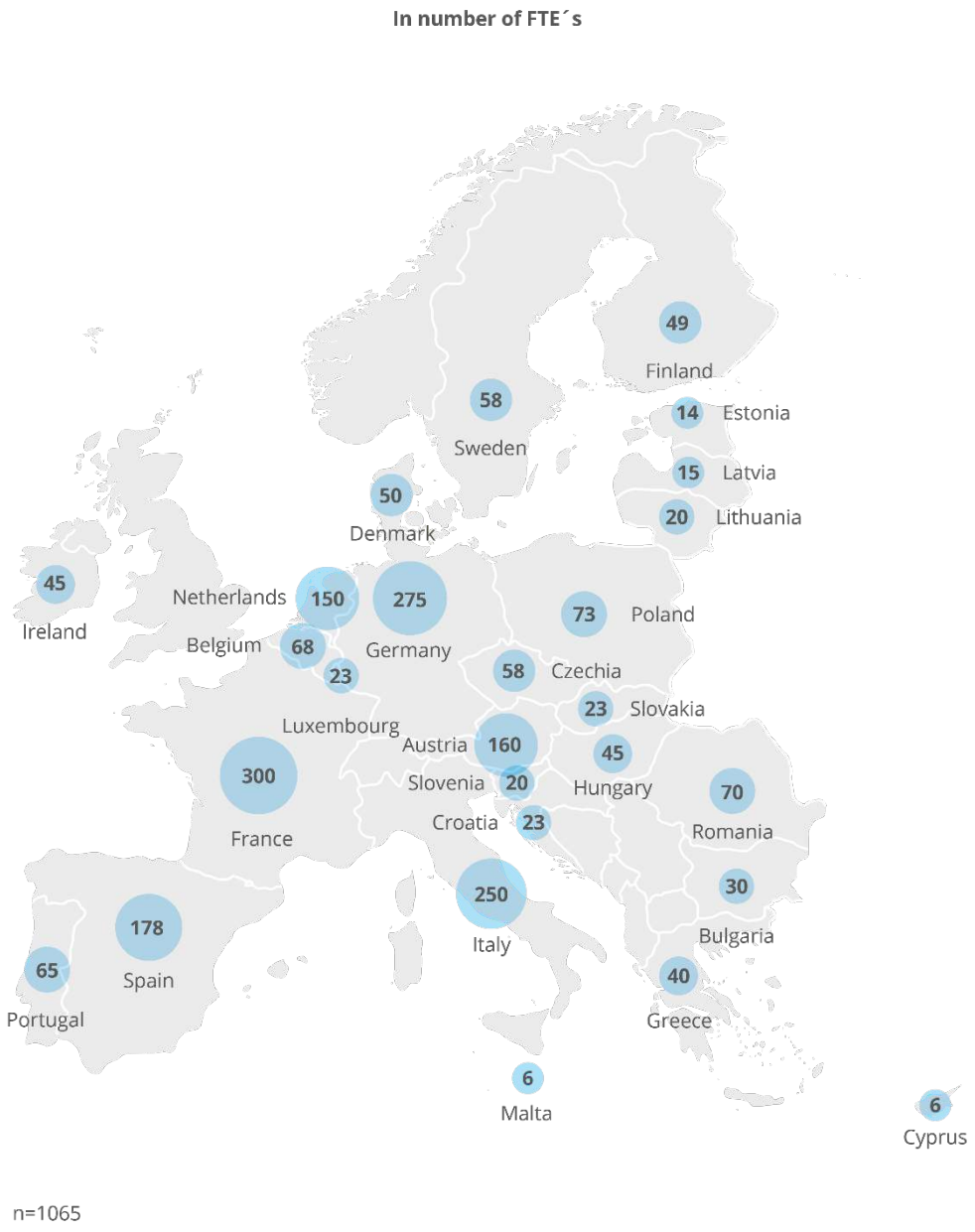
Figure 23: IT FTEs – all sectors



The survey data indicates that an OES or DSP in the EU employs a median of 40 IT FTEs and an average of 212 FTEs. The disparity between the median and average values indicates that most organisations employ a low number of IT FTEs while larger organisations engage a substantial number of IT FTEs.

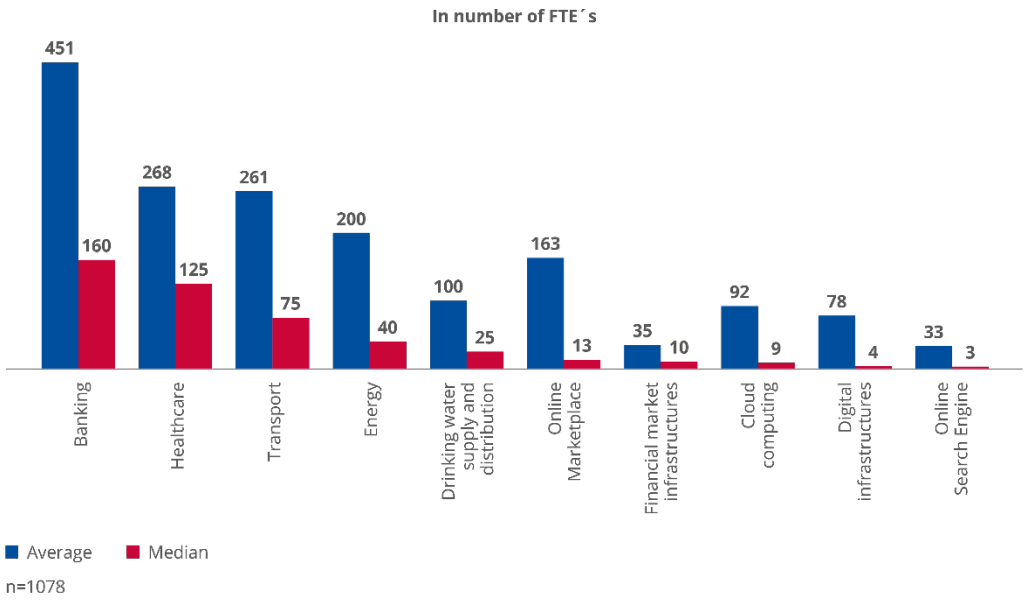
While these are absolute values that have to be interpreted in light of the sector's structure and company size, a smaller number of FTEs does not necessarily imply a lower level of cybersecurity maturity. Furthermore, as detailed in the methodology section, it should be noted that this sample is different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

Figure 24: IT FTEs for OESs and DSPs surveyed by Member States



There are large discrepancies in the total number of IT FTEs in OESs and DSPs among Member States, with median values ranging from over 300 IT employees in France to 6 employees in Malta or Cyprus. When interpreting these figures, the market structure and size of each Member State needs to be factored in, as well as the criteria for identifying OESs or DSPs in each Member State.

Figure 25: IT FTEs by sector

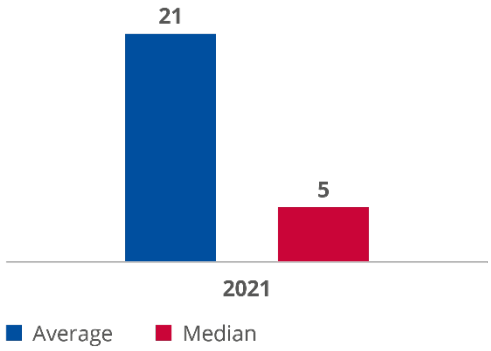


As illustrated in Figure 25, there are large discrepancies in the number of IT FTEs across sectors. For example, the Banking sector has the largest median value of 160 FTEs, which is approximately 115% higher than the median value of the Transport sector, which employs a median of 75 IT FTEs. However, Online Search Engines and Digital Infrastructure have a significantly lower median value of 3 and 4 IT FTEs respectively.

3.3.2 IS FTEs

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

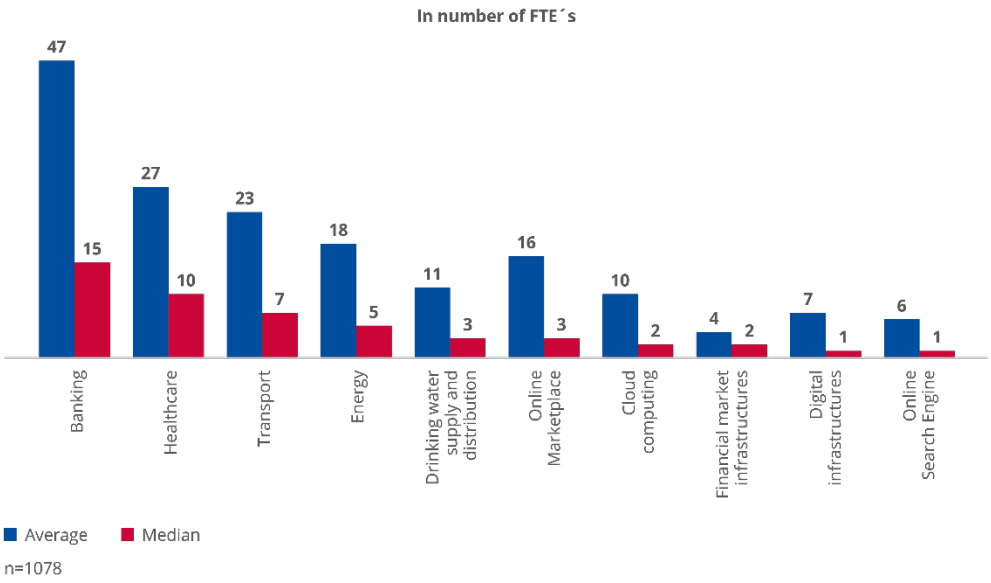
Figure 26: Information security FTEs – all sectors



The survey data indicates that an OES or DSP in the EU employs a median of 5 IS FTEs and an average of 21 FTEs. The disparity between the median and average values indicates that most organisations employ a low number of FTEs while larger organisations engage a substantial number of IS FTEs.

Figure 27: Information security FTEs for OESs or DSPs surveyed in each Member State

Figure 28: Information security FTEs by sector

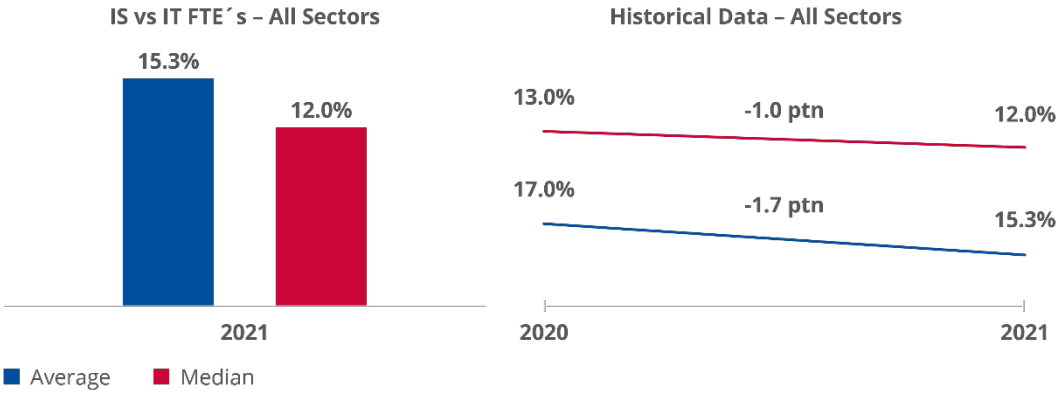


As illustrated in Figure 28, the Banking sector has the highest number of IS FTEs, with a median value of 15 FTEs in 2021, followed by the Healthcare and Transport sectors, with 10 and 7 FTEs respectively. With one FTE each, the Digital Infrastructure and Online Search Engine sectors have the lowest median number of IS FTEs.

3.3.3 IS FTE as a share of IT FTEs

In order to determine the importance of IS FTEs in an OES or DSP, the relative share of these FTEs against the overall IT FTEs was calculated and is depicted in Figure 29. When analysing this normalised data set with historically available data, a decrease of one percentage point is observed in comparison to the median IS vs IT FTE ratio in 2020.

Figure 29: Information security FTEs as a share of IT FTEs – all sectors



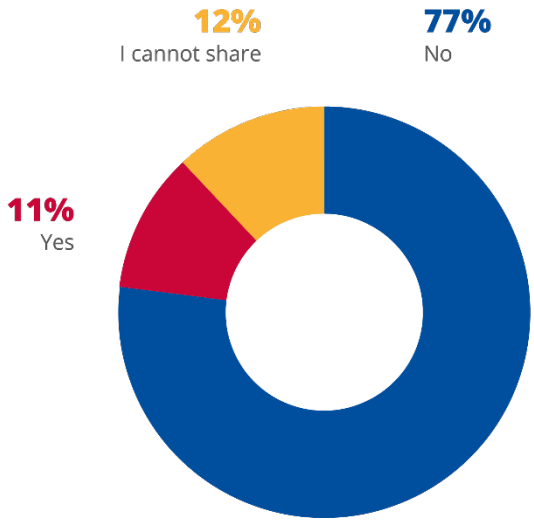
4. SECURITY INCIDENTS AND CYBERSECURITY CAPABILITIES

Key Figures
Of the OESs and DSPs that opted to disclose incident information, 28% experienced a ransomware attack, 22% malicious code and 19% unauthorized access in 2021.
Of the OESs and DSPs that opted to disclose incident information, the highest median costs of major security incidents are found in the Banking and Healthcare sectors (EUR 300 000), followed closely by the Energy (EUR 270 000) and Transport (EUR 225 000) sectors.
The average cost of a ransomware attack on OESs and DSPs in 2021 amounted to EUR 541 500.
62% of the OESs and DSPs in the EU believe that the implementation of the NIS Directive has had a direct positive impact on their detection capabilities. Moreover, 21% are of the opinion that the implementation of the NIS Directive has had a positive influence on their recovery capabilities.
Of the OESs and DSPs that opted to disclose incident information, 33% indicated that incident response costs and costs related to data recovery and business continuity management (22%) are the top two components of direct cost, followed closely by a loss of productivity (19%).
37% of the OESs and DSPs in the EU do not operate a dedicated SOC.
Most OESs and DSPs within the EU (69%) indicate that a majority of their information security incidents are caused by the exploitation of vulnerabilities in software or hardware products.
A majority of OESs and DSPs in the EU (52%) have a patching policy, in which less than 20% of their assets are not covered.
46% of the OESs and DSPs in the EU patch critical vulnerabilities in less than a month, and 92% does this in less than 6 months.
30% of the OESs and DSPs in the EU were covered by cyber insurance in 2021.
48% of the OESs and DSPs in the EU have implemented a risk-based vulnerability management process, with 26% covering only internet-facing assets and 22% only covering critical assets.
73% of the OESs and DSPs in the EU aim to further enhance incident response skills and talent, closely followed by cyberthreat intelligence (54%) and risk management (53%).

4.1 CYBERSECURITY INCIDENTS

Survey Question: Did your organisation experience a major information security incident in 2021?

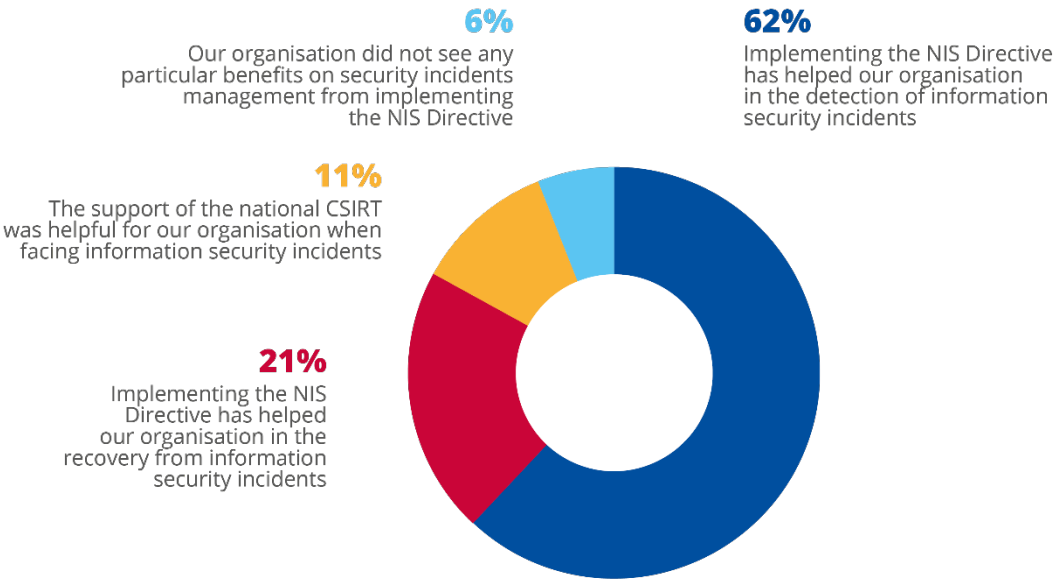
Figure 30: Did your organisation experience a major information security incident in 2021?



As indicated in Figure 30, 77% of the organisations surveyed declared that they had not experienced a major security incident in 2021 (837). Moreover, 11% of the of the organisations surveyed (118) indicated they had experienced a major information security incident in 2021 and 12% of the organisations (125) refused to disclose this information.

Survey Question: To what extent did the implementation of the NIS Directive help your organisation mitigate the impact of information security incidents?

Figure 31: Impact of the NIS Directive in mitigating the impact of information security incidents



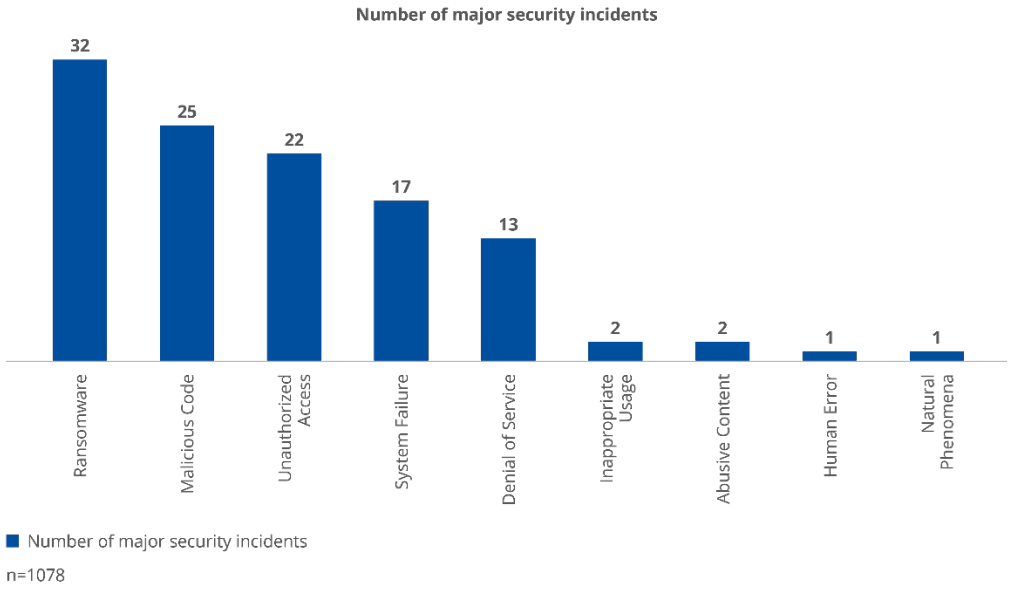
As indicated in Figure 31, the survey data indicates that 701 organisations (62%) believe that the implementation of the NIS Directive has had a direct positive impact on their detection capabilities.

Furthermore, 235 organisations (21%) are of the opinion that the implementation of the NIS Directive has had a positive influence on their recovery capabilities.

4.2 NATURE AND COSTS OF MAJOR SECURITY INCIDENTS

Survey Question: What was the nature of the major security incident that you experienced in 2021?

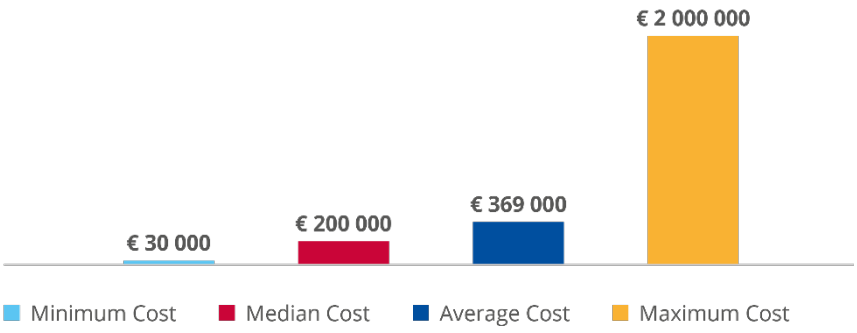
Figure 32: Nature of the last major information security incident experienced in 2021 – all sectors



For the 118 organisations that opted to disclose the details of their most recent major information security incident in 2021, the survey data indicates that 28% experienced a ransomware attack, 22% malicious code and 19% unauthorized access.

Survey Question: What were the estimated direct costs of this major information security incident in 2021?

Figure 33: Estimated direct costs of latest major security incident – all sectors

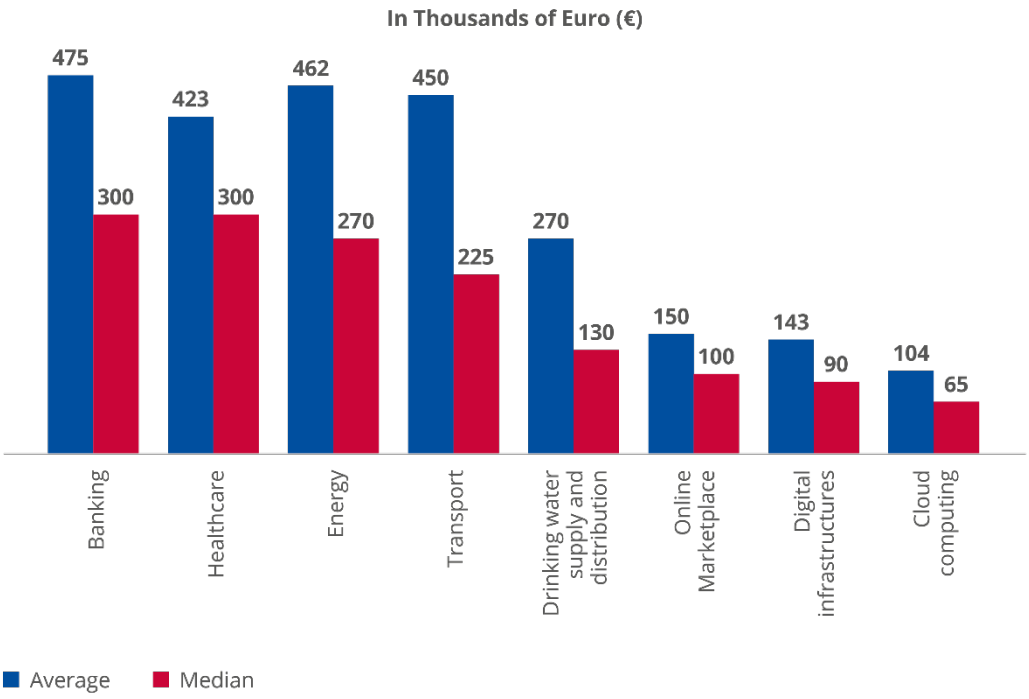


Of the 118 organisations that disclosed in this study that they faced a major security incident in 2021, 57 organisations did not share any financial information related to their latest major security incident and 61 organisations agreed to disclose the estimated direct costs of such an incident in 2021.

The median direct cost of a major security incident in 2021 based on the answers collected from all NIS sectors is 200 000 euros. It may also be noted that the highest direct cost a cybersecurity incident reported in this study is EUR 2 million for an organisation within the financial market infrastructure.

As there is no standard definition of a major security incident shared across the organisations surveyed, we can observe that the minimum direct cost for a cybersecurity incident as reported is EURO 30 000.

Figure 34: Estimated direct costs of major security incidents by sector



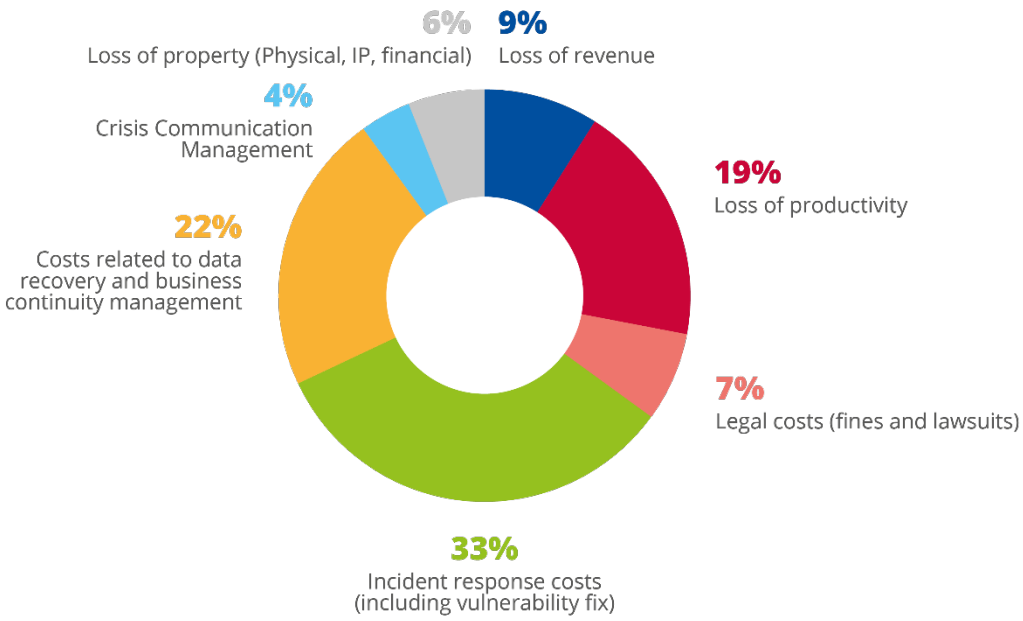
The survey data indicates the highest median costs of major security incidents is found within the Banking and Healthcare sectors (EUR 300 000), followed closely by the Energy (EUR 270 000) and Transport (EUR 225 000) sectors.

As illustrated in Figure 35, a further breakdown was made of the statistically relevant incidents where the average direct cost was offset against the reported minimum and maximum cost of major security incidents in 2021. While the average direct costs of ransomware are the highest, the spread between average and maximum cost are the highest for Denial of Service and Unauthorized Access attacks.

Figure 35: Estimated direct costs by type of incident

<u>Survey Question</u>: What were the top two components of the direct costs associated with major information security incidents in 2021?

Figure 36: Top two components of direct incident costs – all sectors

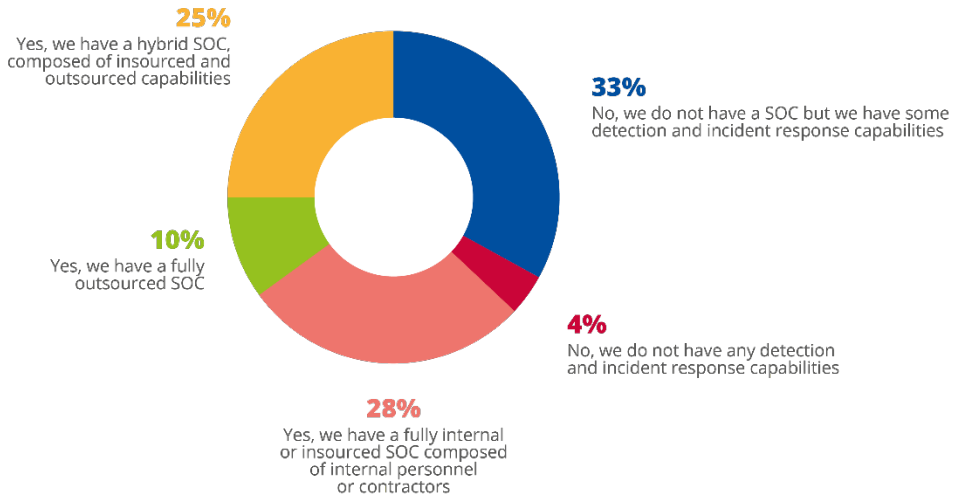


For the 118 organisations that chose to disclose the details of their latest major information security incident in 2021, the survey data indicates that incident response costs (33%) and costs related to data recovery and business continuity management (22%) are the top two components of direct cost, followed closely by a loss of productivity (19%).

4.3 SECURITY OPERATIONS CENTRES (SOC)

Survey Question: Does your organisation run a Security Operations Centre (SOC)?

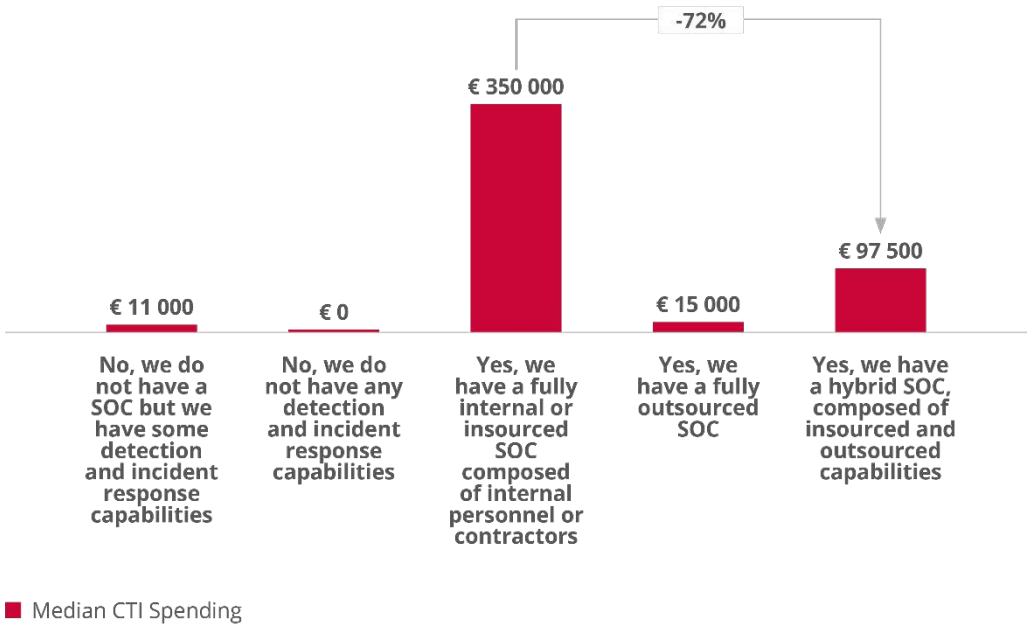
Figure 37: Security operations centres – all sectors



The survey data indicates that 37% of the OESs and DSPs in the EU do not operate a dedicated SOC. Of these 4% do not possess any detection and/or incident response capabilities.

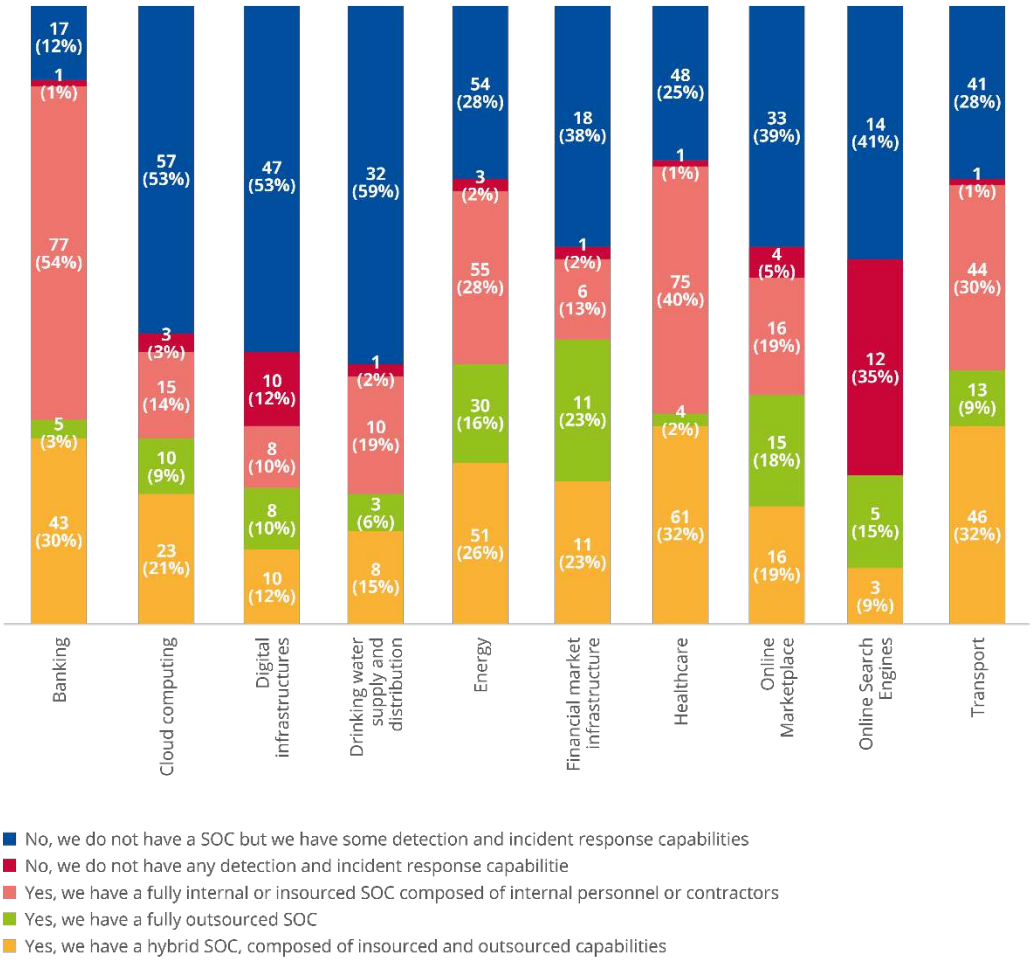
Moreover, the survey data indicates a slight preference for completely internal SOCs (28%) over hybrid solutions (25%) which combine insourced and outsourced capabilities.

Figure 38: Security operations centres compared to CTI spending – all sectors



Fully internal or insourced SOCs spend around EUR 350 000 on CTI, which is 72% more than a hybrid SOC. At the same time, the median CTI spending for organisations with a fully outsourced SOC is very close to that of organisations with limited SOC capabilities. CTI is probably expected from the outsourcing service provider though it must be noted that such values have to be interpreted in light of the individual outsourcing agreements of the respective OESs and DSPs, which may or may not include CTI services from the SOC provider. Regardless, CTI is useful for information security outside the context of SOC, such as conducting risk assessments, though from an investment standpoint organisations primarily focus on CTI if they have in-house SOC capabilities.

Figure 39: Security operations centre by sector

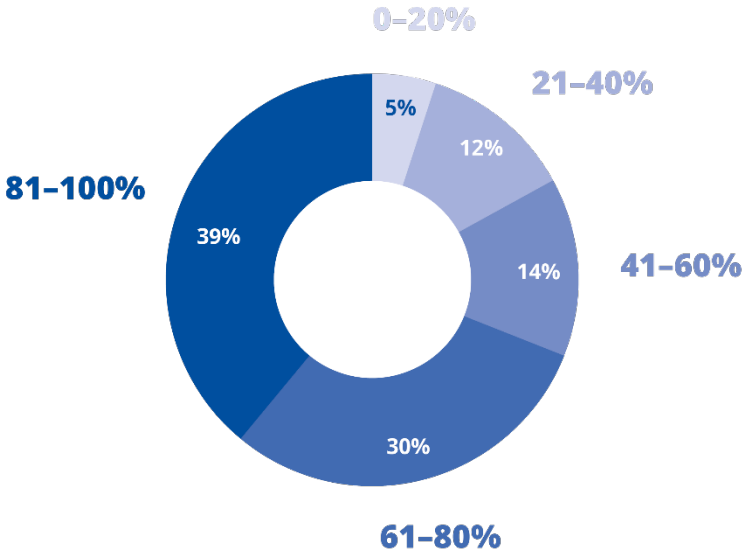


The sectorial view of this information shows a very large difference between sectors. For instance, Banking has only 13% of its organisations without a formal SOC while the respective figure is 76% for the Online Search Engine organisations.

4.4 PATCHING

<u>Survey Question</u>: As regards having experienced a major security incident in 2021, what percentage of incidents involved the exploitation of a vulnerability in software or hardware products?

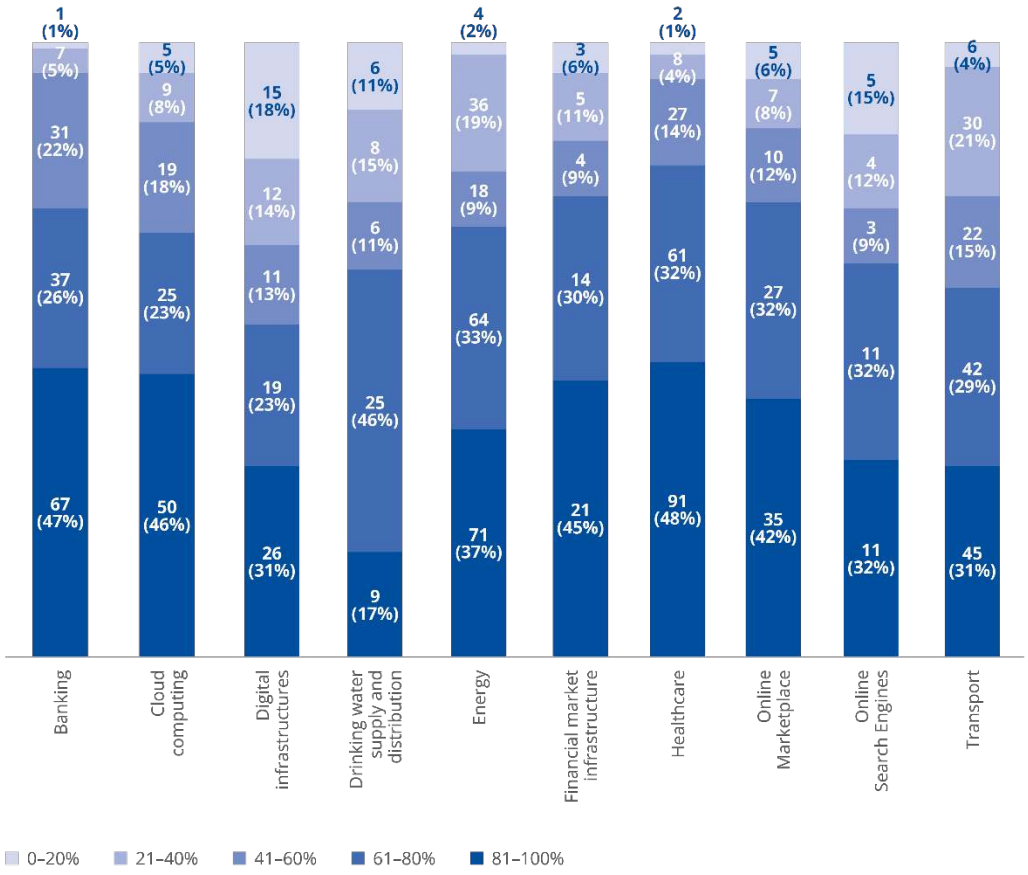
Figure 40: Percentage of incidents attributed to vulnerabilities in software or hardware products



With regards to having experienced a major information security incident in 2021, most OESs and DSPs within the EU (69%) indicated that a majority of their information security incidents are caused by the exploitation of vulnerabilities in software or hardware products.

Furthermore, only 17% of the surveyed organisations indicated that less than 50% of their incidents involve the exploitation of such vulnerabilities.

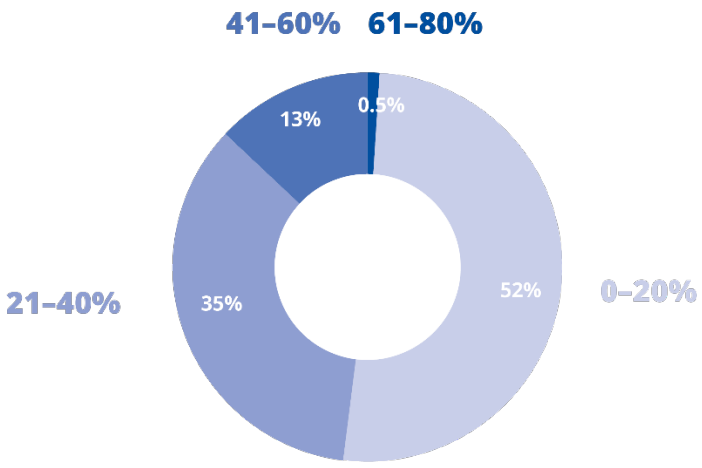
Figure 41: Percentage of incidents attributed to vulnerabilities in software or hardware products per sector



When looking at the detailed data for each sector, Healthcare is the sector that declared the most security incidents related to vulnerabilities in software or hardware with 80% of the Healthcare organisations declaring a share of those vulnerabilities higher than 61%. 18% of respondents in Digital Infrastructures and 15% of the respondents in Online Search Engines have declared a share of incidents related to vulnerability in software or hardware lower than 20%.

<u>Survey Question</u>: What is the percentage of assets over which you have no visibility regarding patching?

Figure 42: Visibility over the patching of assets – all sectors

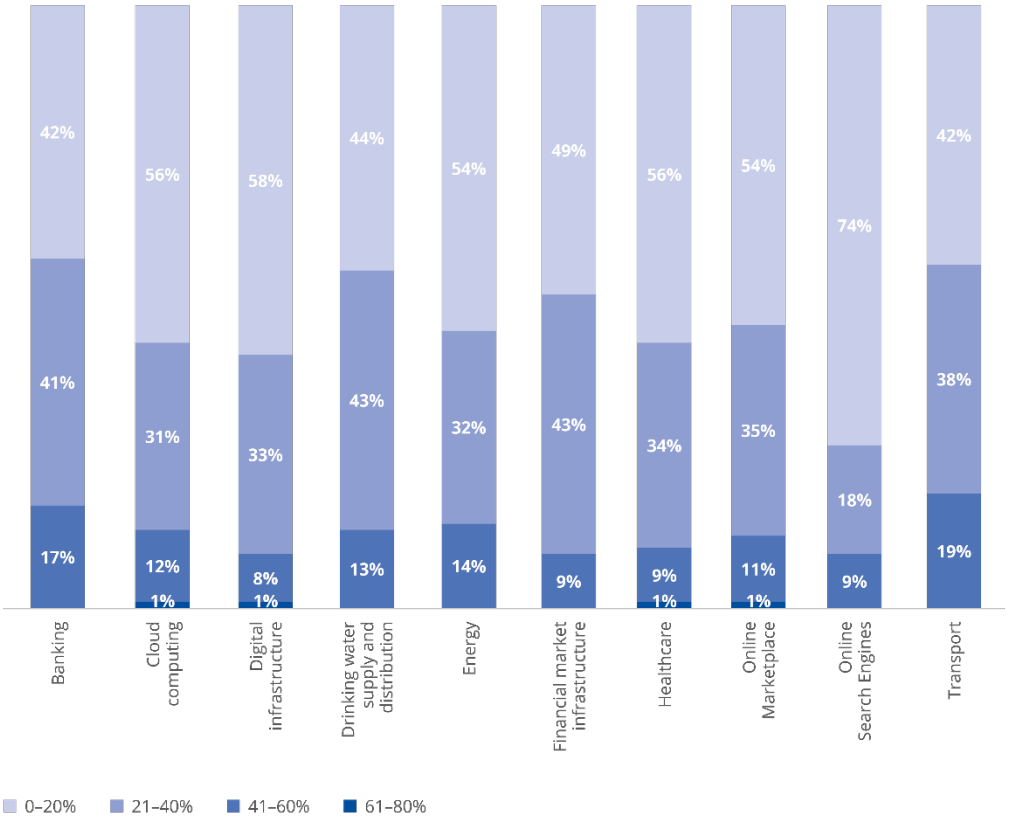


1 organization answered "do not know"

Despite the strong interconnection between vulnerabilities and security incidents — as illustrated in Figure 42 — the survey data indicates that a majority of OESs and DSPs in the EU (52%) have a rigid patching policy, in which only 20% or less of their assets are not covered.

On the other hand, 13.5% of the organisations surveyed have no visibility over the patching of 40% or more of their information assets.

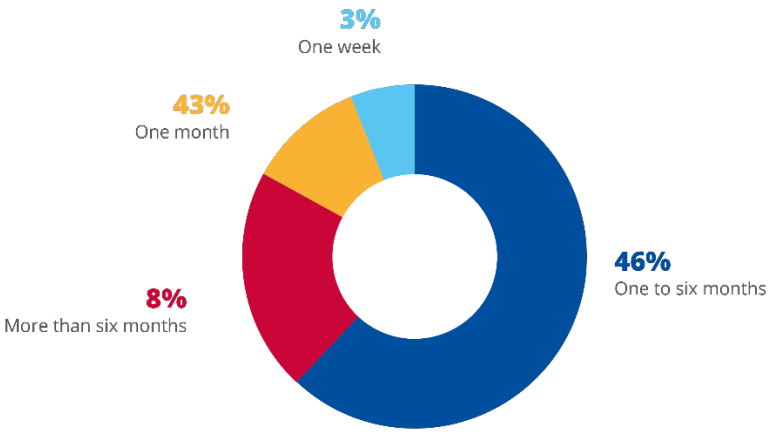
Figure 43: Visibility over the patching of assets by sector



As illustrated in Figure 43, a further breakdown by sector indicates similar trends across the various sectors — without any significant outliers. On the basis of the survey data, it must be noted that Online Search Engines have the best visibility over the patching of their information assets.

<u>Survey Question</u>: What is the normal time taken to patch critical vulnerabilities on IT assets within your organisation?

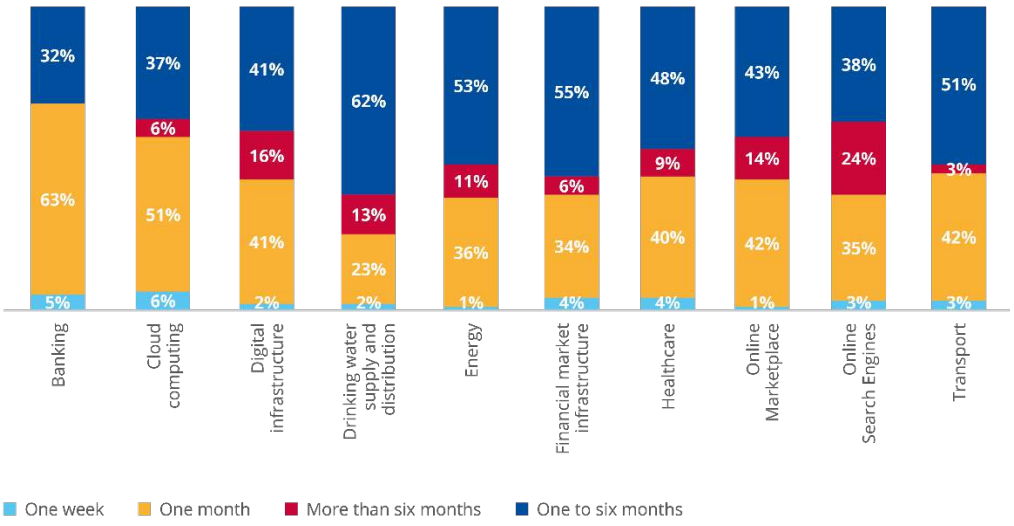
Figure 44: Duration of patching – all sectors



The survey data indicates that 46% of the OESs and DSPs in the EU patch critical vulnerabilities in less than a month. Furthermore, an equal percentage of the organisations surveyed indicate that they patch critical vulnerabilities within six months or less. As such, one may reasonably conclude that 92% of the OESs and DSPs in the EU patch critical vulnerabilities within at least six months after their discovery.

Only 8% of the organisations surveyed indicate that they exceed this time and take longer than six months to patch critical vulnerabilities in their systems.

Figure 45: Duration of patching by sector

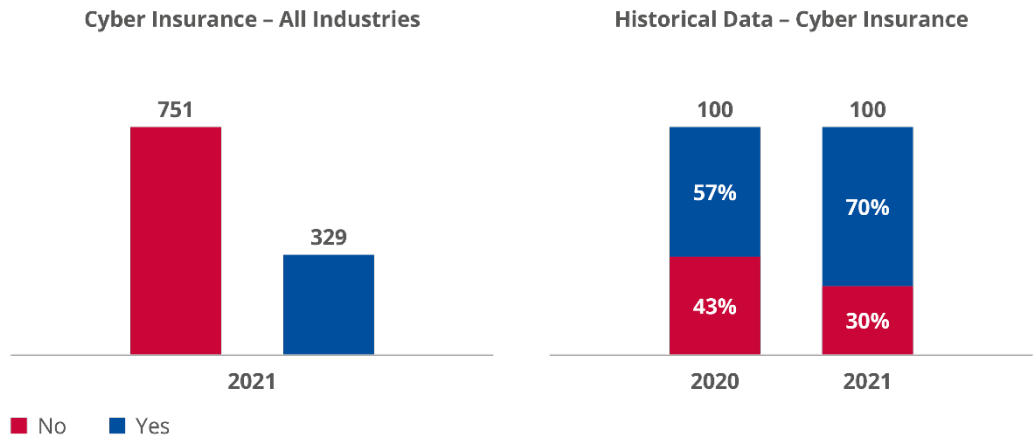


As illustrated in Figure 45, a further breakdown by sector indicates that the Banking sector can be considered as the best in class with regards to the time taken to patch while Drinking Water and Online Search Engines have the longest patching times across sectors.

4.5 CYBER INSURANCE

<u>Survey Question</u>: Has your organisation subscribed to a dedicated cyber insurance policy?

Figure 46: Cyber insurance – all sectors



The survey data indicates that 30% of the OESs and DSPs in the EU possessed cyber insurance cover in 2021. When analysing this normalised data set with historically available data, a decrease of 13% is observed in comparison to the OESs and DSPs in the EU that possessed cyber insurance in 2020.

The detail on the answer is provided in the figure below and shows that although 70% of the organisations surveyed did not have cyber insurance cover in 2021, 40% of the organisations overall actually plan to subscribe to one.

Figure 47: Cyber insurance detailed view – all sectors

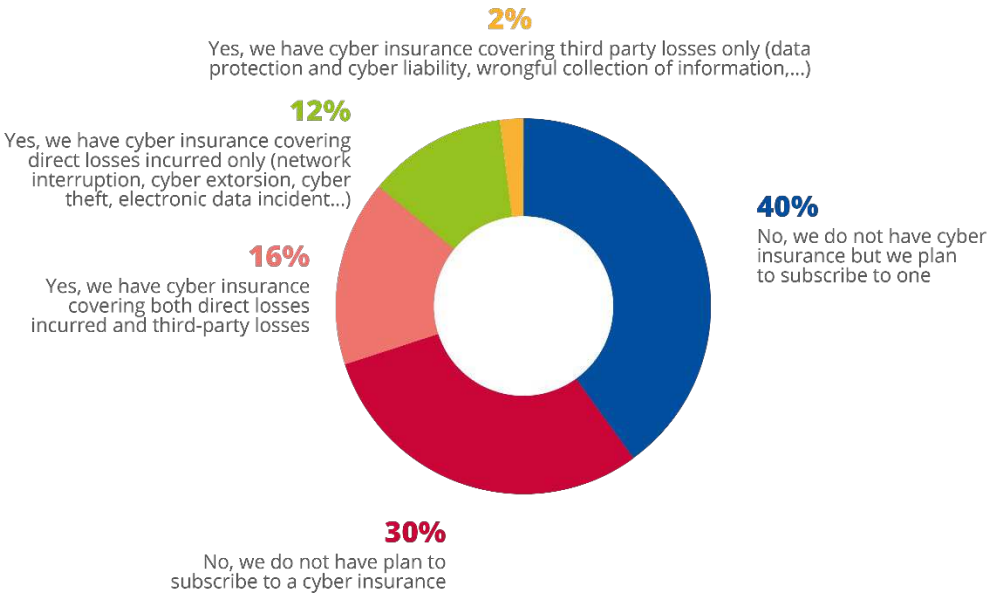
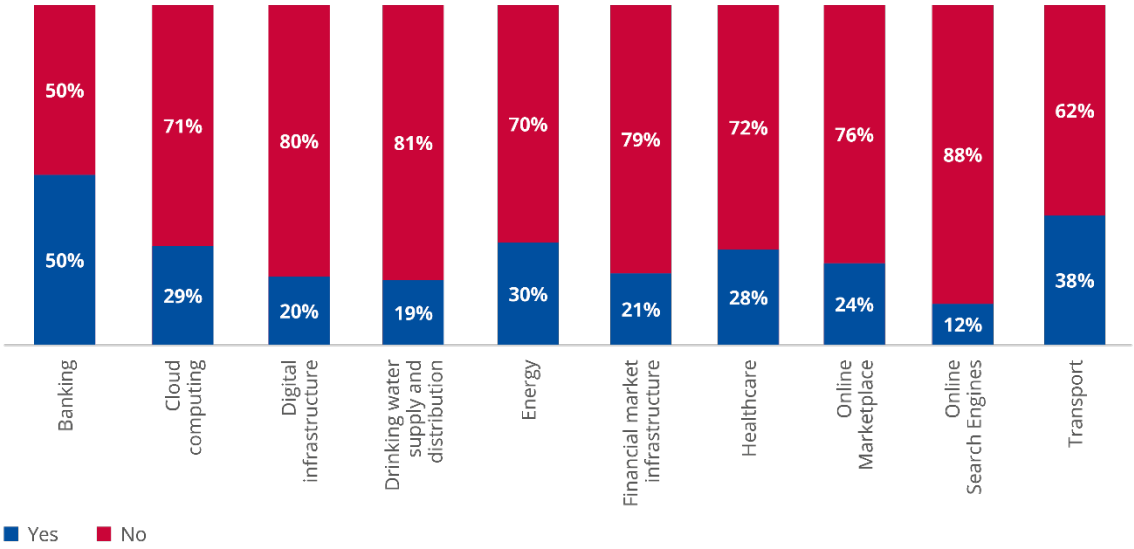
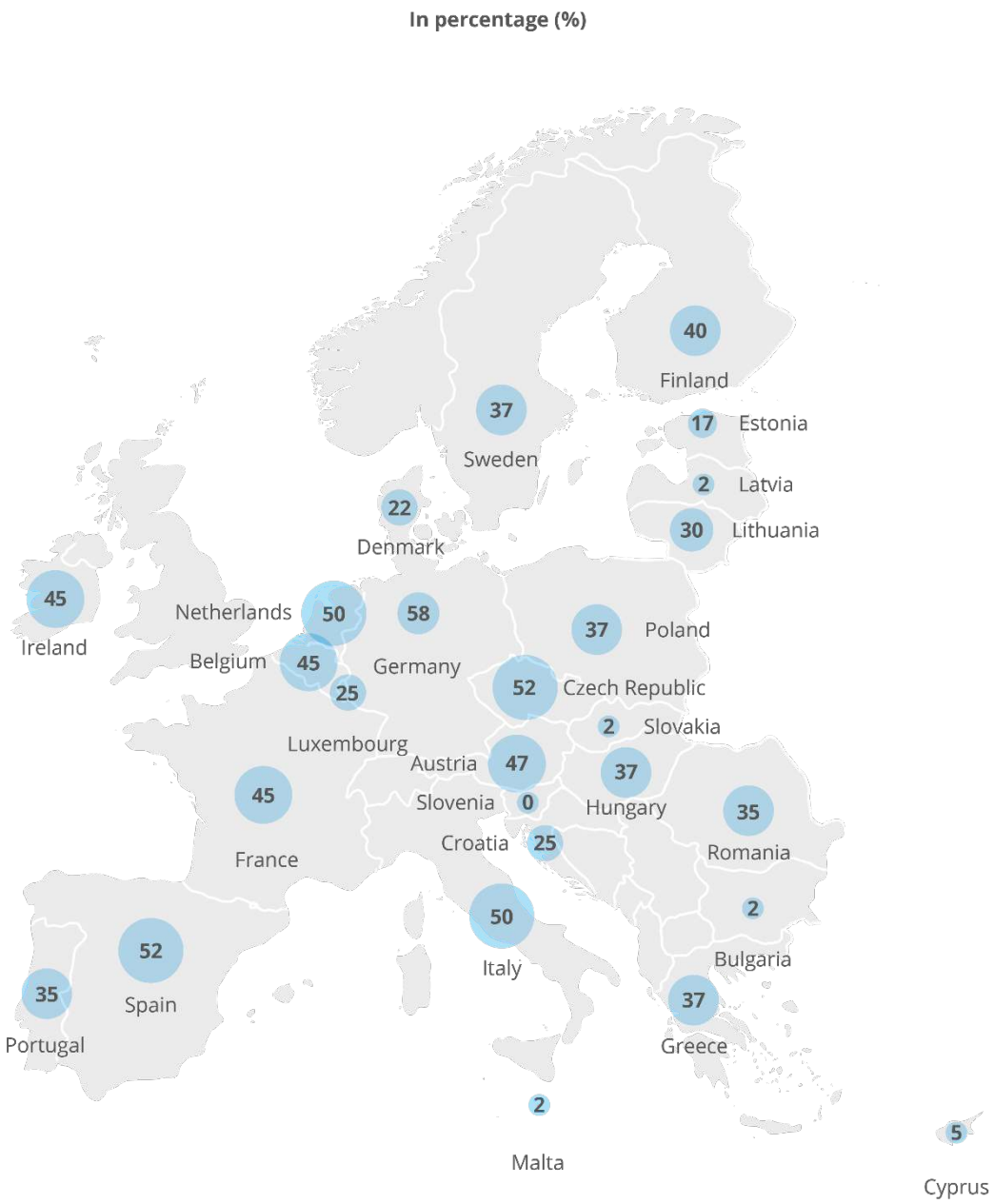


Figure 48: Cyber insurance by sector



As depicted in Figure 48, similar trends across the various sectors are observed. On the basis of the survey data, it must however be noted that half of the OESs and DSPs in the Banking sector possess cybersecurity insurance.

Figure 49: Cyber insurance for OESs and DSPs surveyed in each Member State



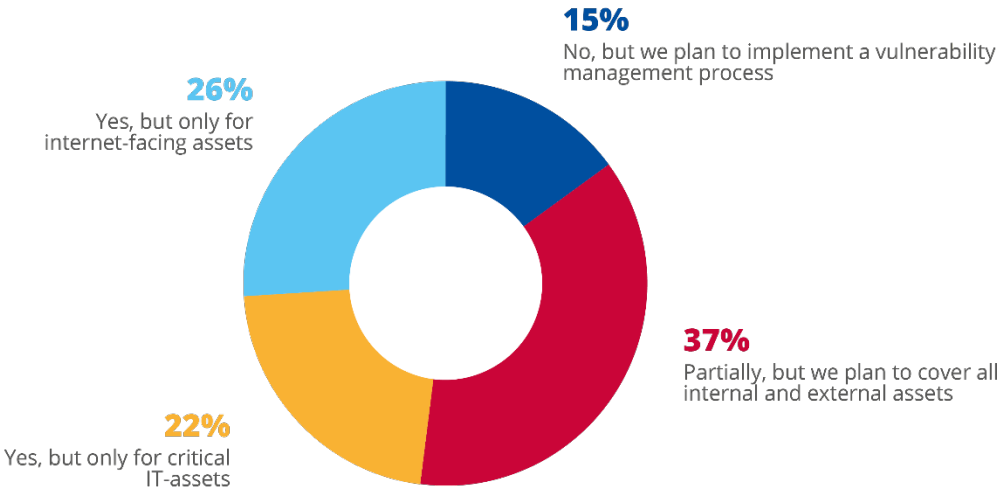
As illustrated in Figure 49, a further breakdown by Member States indicates that there are significant outliers. On the basis of the survey data, it may be noted that OESs and DSPs in Bulgaria, Latvia, Malta, Slovakia and Slovenia hardly possess any cybersecurity insurance. This could imply the cybersecurity market has yet to be established or materialise fully within these Member States.

Furthermore, around 50% of the OESs and DSPs in Austria, Czech Republic, Italy, the Netherlands and Spain possess cybersecurity insurance.

4.6 VULNERABILITY MANAGEMENT

Survey Question: Has your organisation implemented a risk-based vulnerability management process?

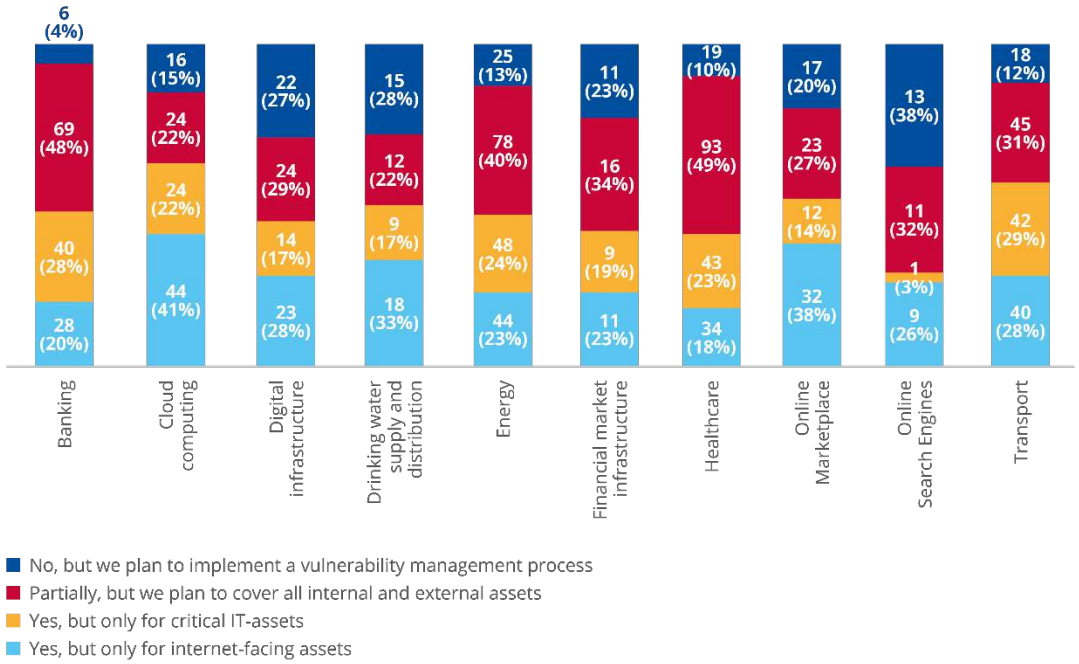
Figure 50: Vulnerability management – all sectors



The survey data indicates that 48% of the OESs and DSPs in the EU have implemented a risk-based vulnerability management process, with 26% covering only internet-facing assets and 22% only covering critical assets.

Whereas 37% of the surveyed organisations have partially implemented a risk-based vulnerability management process, it may be noted that only 15% of the OESs and DSPs within the EU currently do not possess such processes.

Figure 51: Vulnerability management by sector

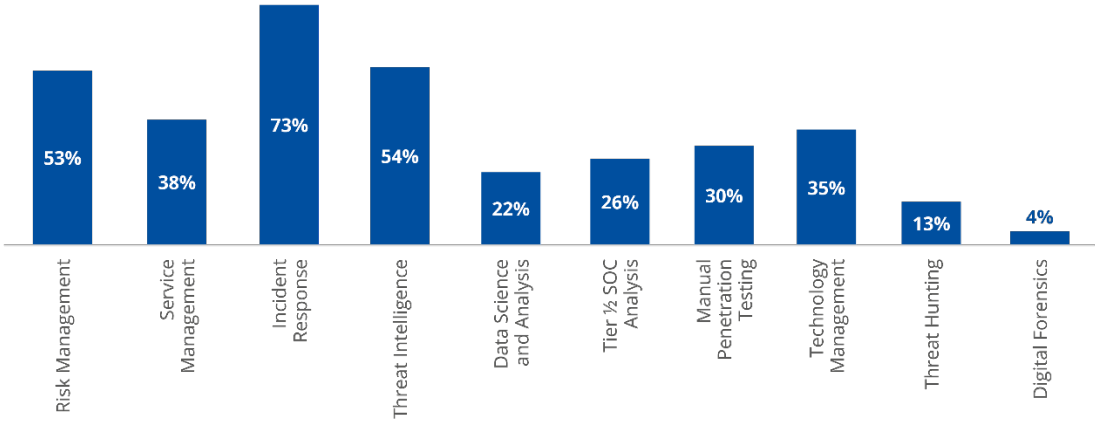


The sector with the highest share of organisations without a risk-based vulnerability management process is Online Search Engines (38%), while only 4% of the organisations in the Banking sector do not have such processes in place.

4.7 CYBERSECURITY SKILLS

Survey Question: What are the top skills and talents related to security that your organisation aims at hiring or developing internally (e.g. training)? Please select all that apply

Figure 52: Cybersecurity skills prioritised for internal development – all sectors



The survey data indicates that 73% of the OESs and DSPs in the EU aim to further enhance incident response skills and talents, closely followed by cyberthreat intelligence (54%) and risk management (53%). Threat hunting and digital forensics have the lowest priority, with less than 15% of the surveyed organisations indicating they will further develop these skills and talents.

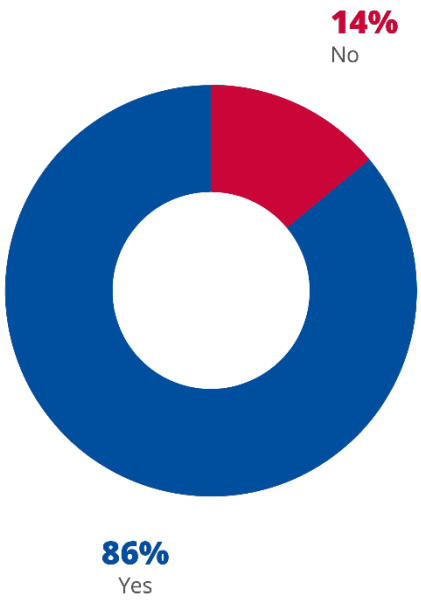
5. SUPPLY-CHAIN SECURITY

Key Figures
86% of the OESs and DSPs in the EU have implemented third-party risk management (TRM) policies.
Only 47% of the OESs and DSPs in the EU have earmarked a dedicated budget for third-party risks management (TRM).
Only 24% of the OESs and DSPs in the EU have dedicated employees for third-party risks management (TRM).
61% of the OESs and DSPs in the EU have a preference for security certificates, followed closely by security risk rating services (43%) and due diligence or risk assessments (37%) when assessing their third-party risks. Moreover, an OES or DSP in the EU focuses predominantly on the type of product or service (59%), the volume of spending with the provider (47%) and whether or not the provider is subject to the NIS Directive (42%), when assessing supply chain security concerns.
59% of the OESs and DSPs in the EU agree that common requirements would lead to a reduction in compliance costs for users as regards their supply chain.
56% of the OESs and DSPs in the EU agree that common requirements would lead to lower costs of risk mitigation for users.
61% of the OESs and DSPs in the EU agree that common requirements would reduce the number of security incidents and, as a result, the cost of managing and recovering from such incidents.

5.1 THIRD-PARTY RISK MANAGEMENT (TRM) POLICIES

Survey Question: Has your organisation approved security policies related to third parties such as partners, vendors or suppliers?

Figure 53: Existence of third-party risk management policies – all sectors

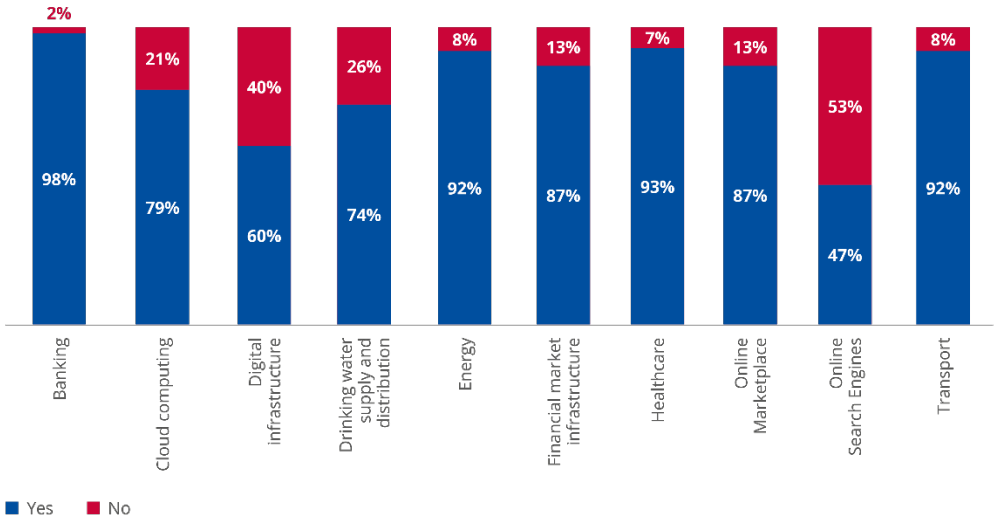


The survey data indicates that 86% of the OESs and DSPs in the EU have implemented third-party risks management (TRM) policies.

Only 14% of the organisations surveyed have no approved security policies related to third parties — i.e. partners, vendors or suppliers.

As illustrated in Figure 54, a further breakdown was made by sector, indicating that the Banking sector can be considered as the best in class with regards to TRM policy, while over 50% of Online Search Engines do not address TRM concerns in a formal policy.

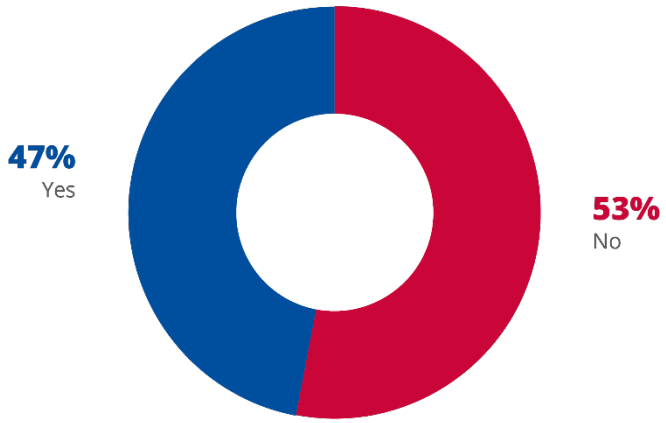
Figure 54: Third-party risk management policies by sector



5.2 TRM BUDGET

<u>Survey Question</u>: Does your organisation have a dedicated budget or budget line for Supply Chain Security?

Figure 55: Dedicated TRM budget – all sectors

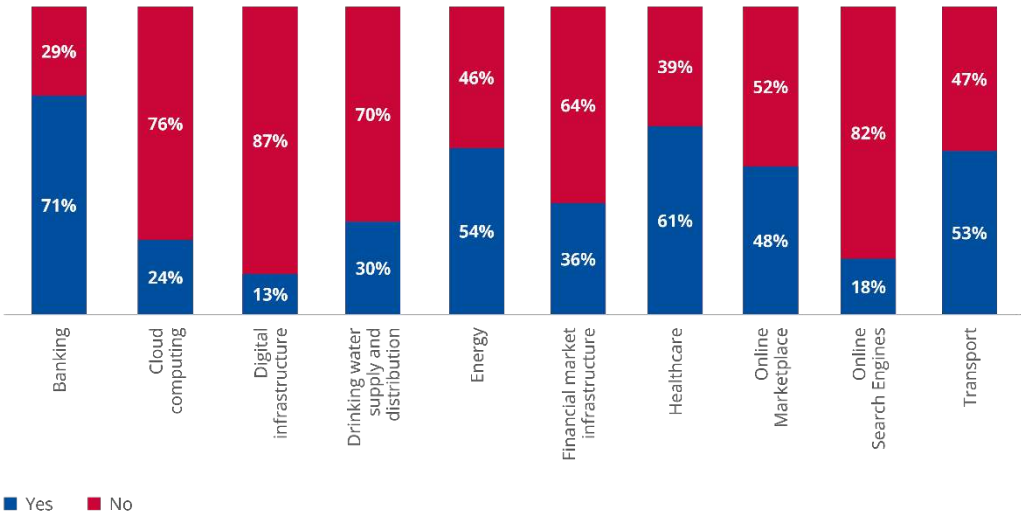


As indicated in Figure 55, the survey data indicates that only 47% of the OESs and DSPs in the EU have earmarked a dedicated budget for third-party risks management (TRM).

The majority of the organisations surveyed (53%) have no approved budget for these matters.

As illustrated in Figure 56, a further breakdown was made by sector. This indicates that the Banking sector has the highest percentage of dedicated TRM budgets, while most Online Search Engines and Digital Infrastructures do not earmark any specific budget for TRM concerns.

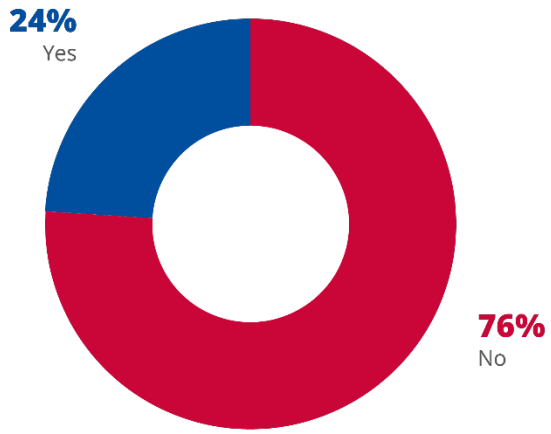
Figure 56: Dedicated TRM budget by sector



5.3 TRM ROLES AND RESPONSIBILITIES

Survey Question: Is there a dedicated role for Supply Chain Security in your organisation?

Figure 57: Dedicated TRM role in the organisation – all sectors



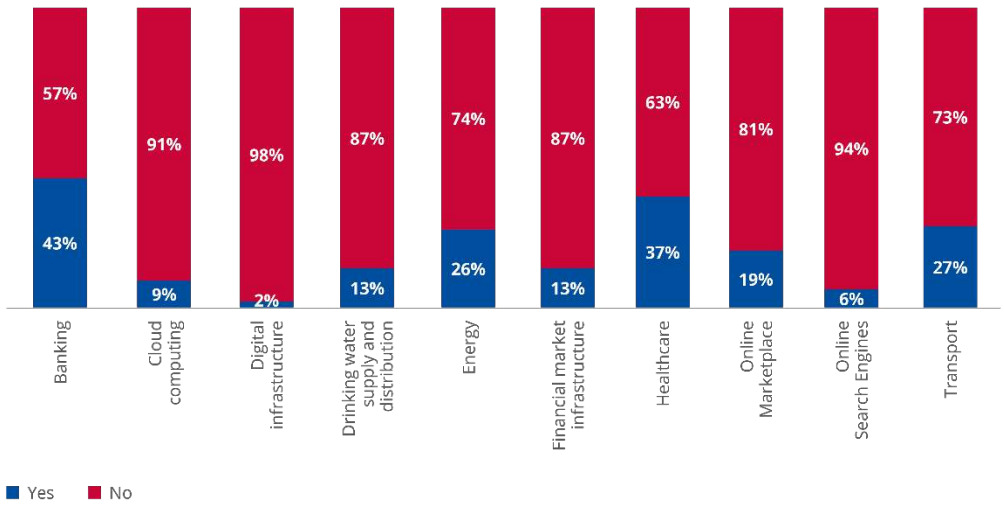
The survey data indicates that only 24% of the OESs and DSPs in the EU have employees dedicated to the management of third-party risks.

The majority of the organisations surveyed (76%) have no dedicated FTEs for these matters. Of the 274 organisations that indicated they have dedicated employees for TRM, the Banking

sector has the highest number of TRM FTEs, with a median value of 5 FTEs in 2021, followed by the Transport and Digital Infrastructure sectors with 4 and 3.5 FTEs respectively.

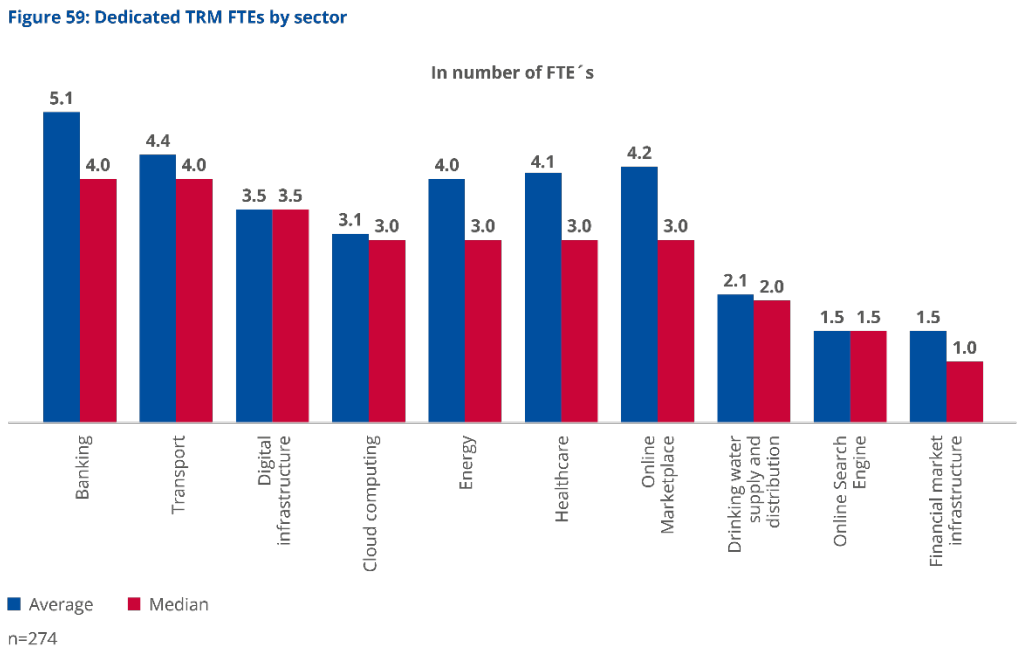
As illustrated by Figure 58, a further breakdown was made by sector. This indicated that the majority of OESs and DSPs within the EU — regardless of the sector — do not have dedicated TRM roles. That having been said, OESs in the Banking and Healthcare sectors appear to be more likely to have such dedicated roles.

Figure 58: Dedicated TRM role by sector



***Survey Question*: How many FTEs are dedicated to supply chain security activities in your organisation?**

Figure 59: Dedicated TRM FTEs by sector

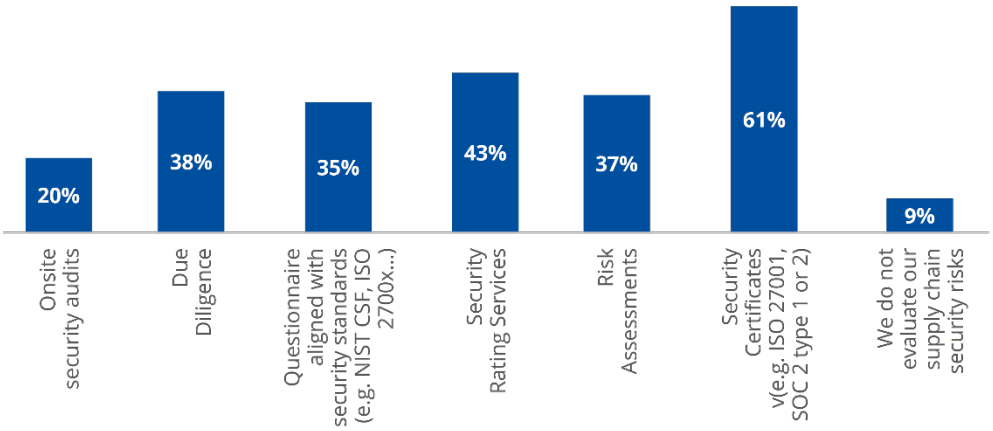


As illustrated in Figure 59, Financial Market Infrastructures (1 FTE) and Online Search Engines (1.5 FTEs) have the lowest median number of TRM FTEs.

5.4 RISK MITIGATING TECHNIQUES

Survey Question: What are the techniques that your organisation uses to assess supply chain security risks? Please select all that apply.

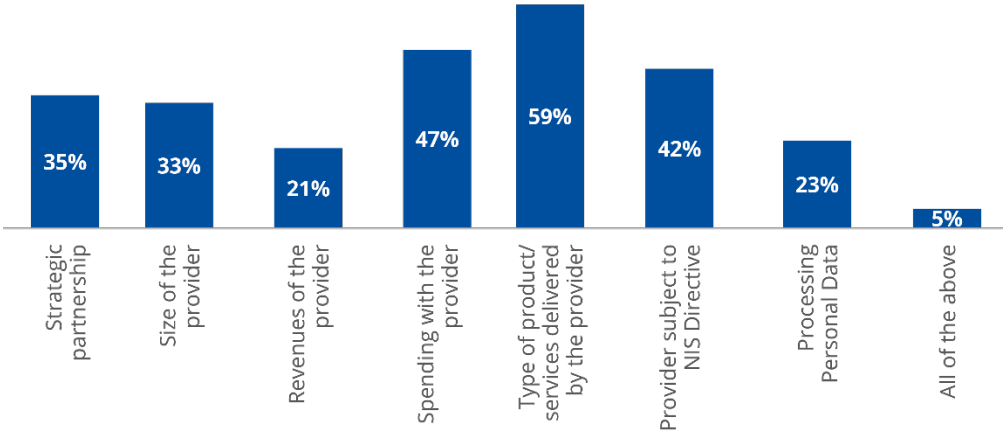
Figure 60: Supply chain security risk mitigation techniques – all sectors



When asked which TRM risk mitigation techniques were adopted, 61% of the organisations surveyed indicated a preference for Security Certificates, followed closely by Security Risk Rating Services (43%) and Due Diligence or Risk Assessments (37%). Only 9% of the OESs and DSPs in the EU indicate that they do not evaluate their supply chain security risks in any way.

Survey Question: What are the business criteria that your organisation considers when evaluating the security risks of its supply chain? Please select all that apply

Figure 61: Business criteria for supply chain risk analysis

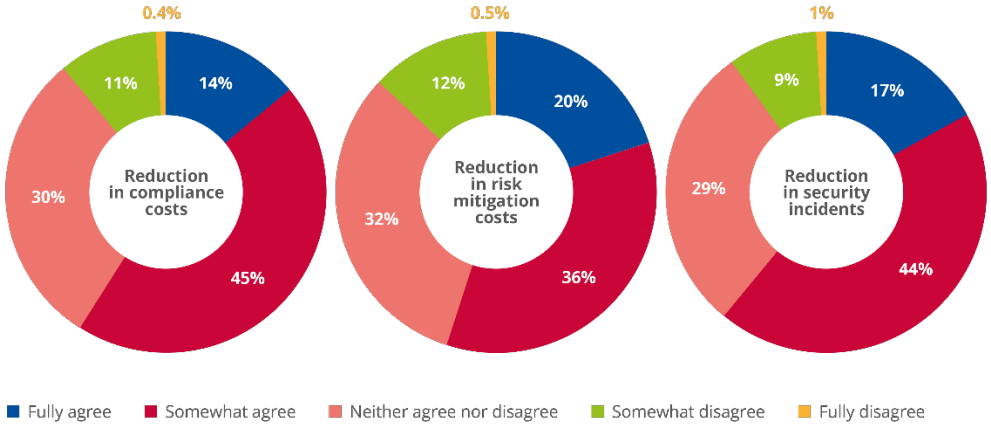


As illustrated in Figure 61, an OES or DSP in the EU focuses predominantly on the type of product or service (59%), the volume of spending with the provider (47%) and whether the provider is subject to the NIS Directive (42%), when assessing supply chain security concerns.

5.5 EUROPEAN CYBERSECURITY REQUIREMENTS

Survey Question: To which extent do you agree with the following statements regarding the impact of potential common European cybersecurity requirements for digital hardware and software products?

Figure 62: Perception of foreseen impact from the introduction of common European cybersecurity requirements for digital products



When asked what the impact of potential common EU cybersecurity requirements for digital hardware and software products would be, the OESs and DSPs in the EU replied as follows:

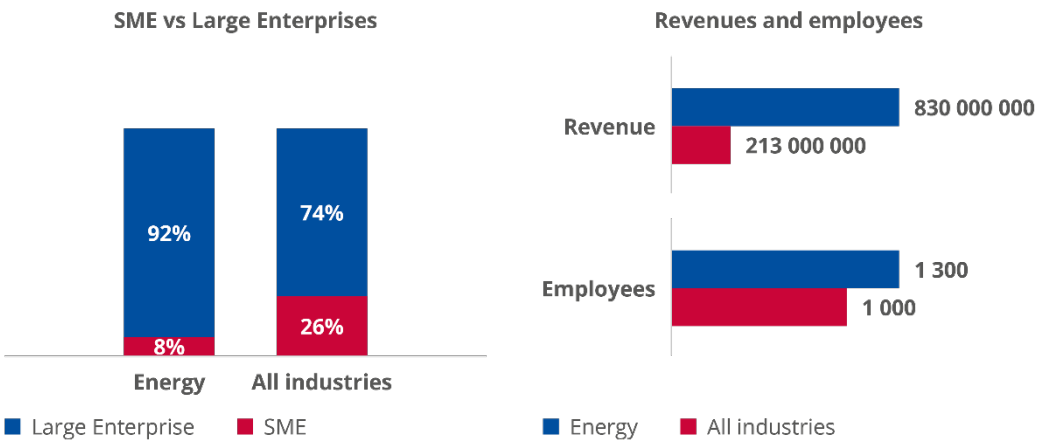
- The survey data indicates that 59% of the OESs and DSPs in the EU agree that common requirements would lead to a reduction in compliance costs for users as regards their supply chain. Furthermore, only 11.4% of the organisations surveyed would disagree with this statement.
- The survey data indicates that 56% of the OESs and DSPs in the EU agree that common requirements would lead to lower risk mitigation costs for users. Furthermore, only 12.5% of the surveyed organisations would disagree with this statement.
- The survey data indicates that 61% of the OESs and DSPs in the EU agree that common requirements would reduce the number of security incidents and as a result, the cost of managing and recovering from such incidents. Furthermore, only 10% of the organisations surveyed would disagree with this statement.

6. SECTORAL ANALYSIS: ENERGY

Key Figures
An OES operating within the Energy sector employs the same number of IT and IS FTEs as compared to the median value of all sectors. In terms of intensity in IS spending compared to IT spending, an OES within the Energy sector has a relative spending 1.7 points lower than the median across all sectors
81% of the OESs in the Energy sector comply with their national sector-specific certification and/or verification schemes.
Critical OT systems are monitored by a SOC in 68% of the OESs in the Energy sector which includes 52% that have a common IT and OT SOC.
A majority of the OESs in the Energy sector certify their systems and processes (79%) and procure products with information security certifications (73%).

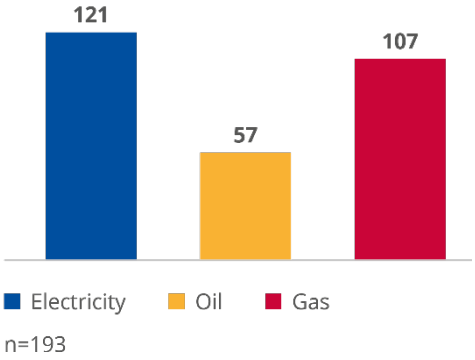
6.1 DEMOGRAPHICS OF A SECTORIAL DEEP DIVE

Figure 63: Size of OESs surveyed in the Energy sector



Unsurprisingly, the Energy sector is mostly composed of Large Enterprises with 92% of the organisations surveyed meeting the definition of Large Enterprise against 74% for all sectors.

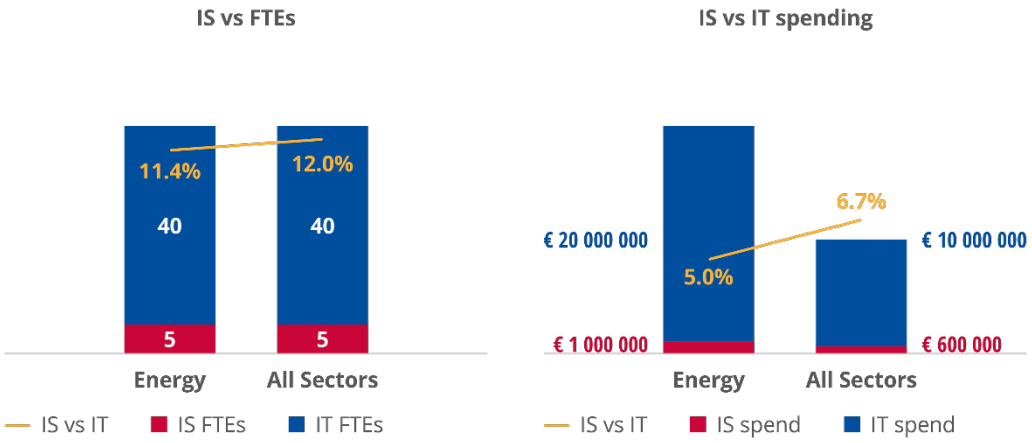
Figure 64: Sub-sectors



In terms of sub-sectors, out of the 193 organisations surveyed in the Energy sector, 121 have operations in Electricity (63%), 57 have operations in Oil (30%) and 107 have operations in Gas (55%). Those activities are not exclusive as 41% of the organisations surveyed in the Energy sector have operations in multiple sub-sectors.

6.2 INVESTMENT AND STAFFING INFORMATION

Figure 65: Energy vs all sectors (median values)

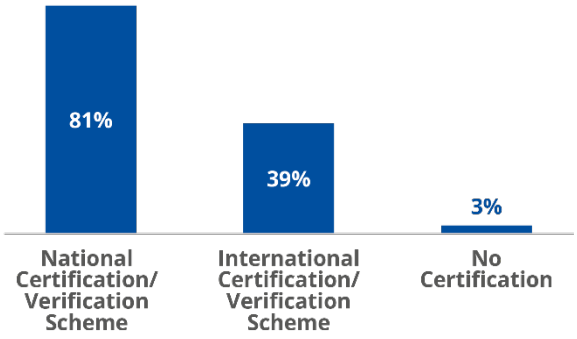


When comparing the Energy sector to the overall data set, it may be noted that an OES operating in the Energy sector employs the same number of IT and IS FTEs as compared to the median value of all sectors. In terms of intensity in IS spending against IT spending, an OES within the Energy sector has a relative spending 1.7 points lower than the median across all sectors, with 5% of IS spending as a share of IT spending, though the raw spending figures are higher with €1 million in IS spending.

6.3 CERTIFICATION SCHEMES

Survey Question: Is your organisation following specific Energy sector certifications for processes, systems or staff?

Figure 66: Certification schemes – Energy sector



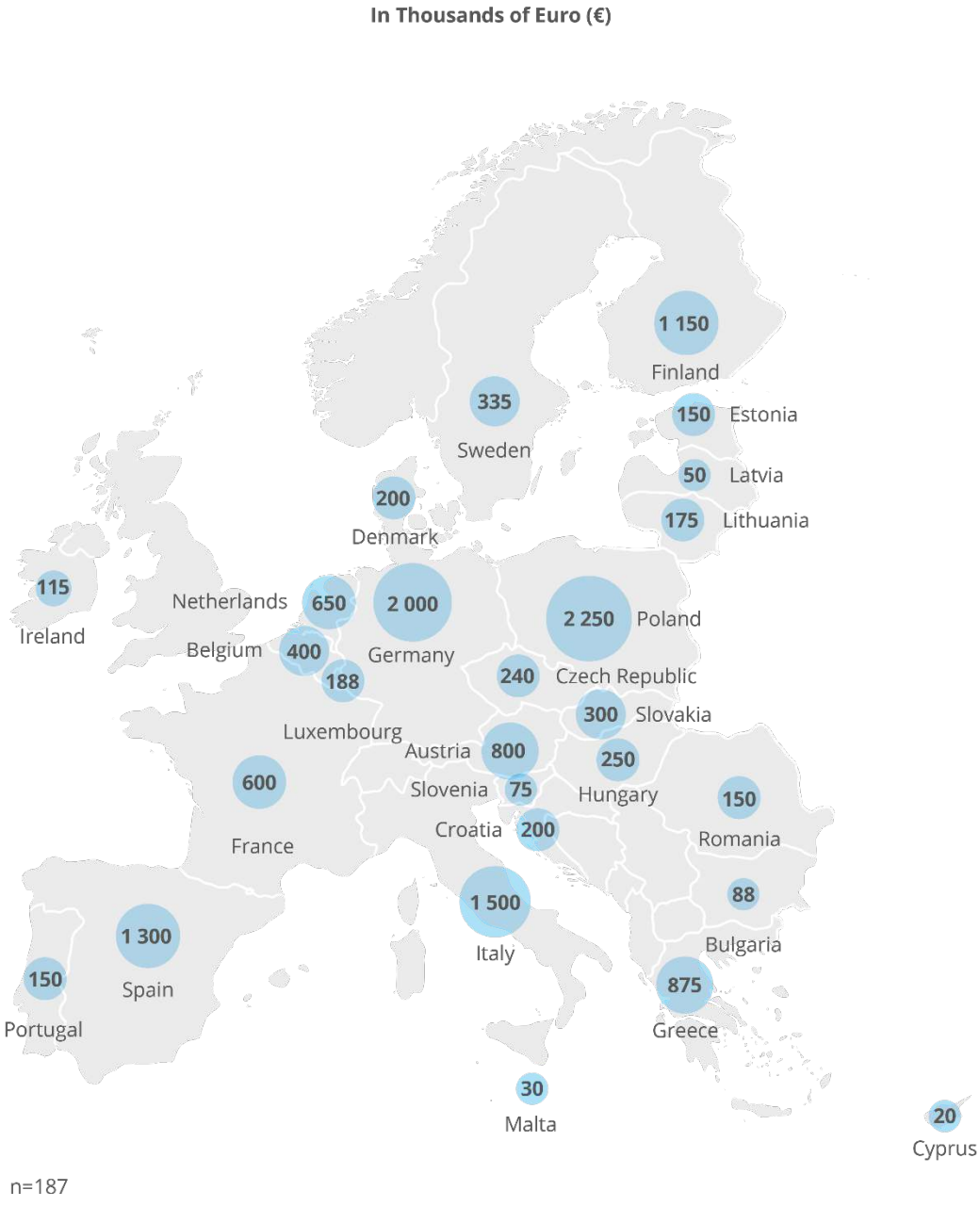
The survey data indicates that 81% of the OESs in the Energy sector comply with national sector-specific certification and/or verification schemes.

Moreover, 39% of the OESs in the Energy sector also possess international certification and/or verification schemes — such as GEC. Only 3% of the organisations surveyed indicated that they have no certification whatsoever.

6.4 OPERATIONAL TECHNOLOGY (OT) SECURITY

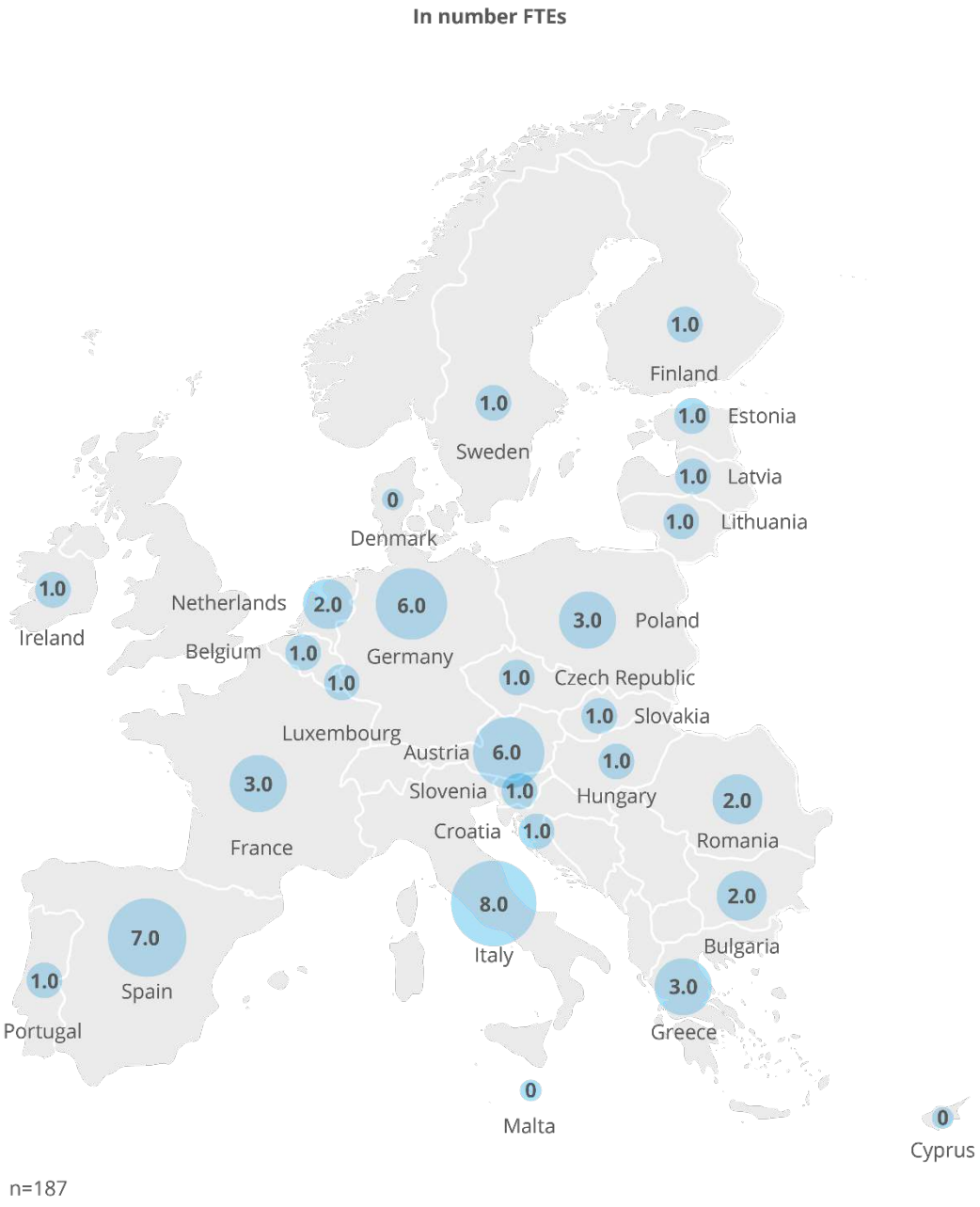
Survey Question: What was your organisation's estimated spending on Operational Technology (OT) Security in Euros for 2021?

Figure 67: OT security budget for OESs surveyed in the Energy sector in each Member State



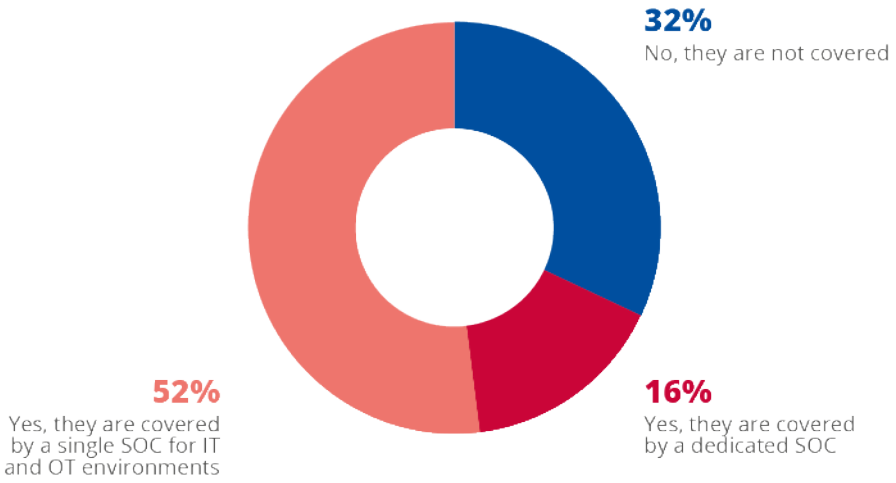
Survey Question: What was your organisation's estimated Operational Technology (OT) Security FTEs in 2021 for both internal staff and contractors?

Figure 68: OT security FTEs for OESs surveyed in the Energy sector in each Member State



Survey Question: Are the main critical OT systems of your organisation monitored by a Security Operations Centre (SOC)?

Figure 69: Monitoring of critical OT systems by SOC – Energy sector

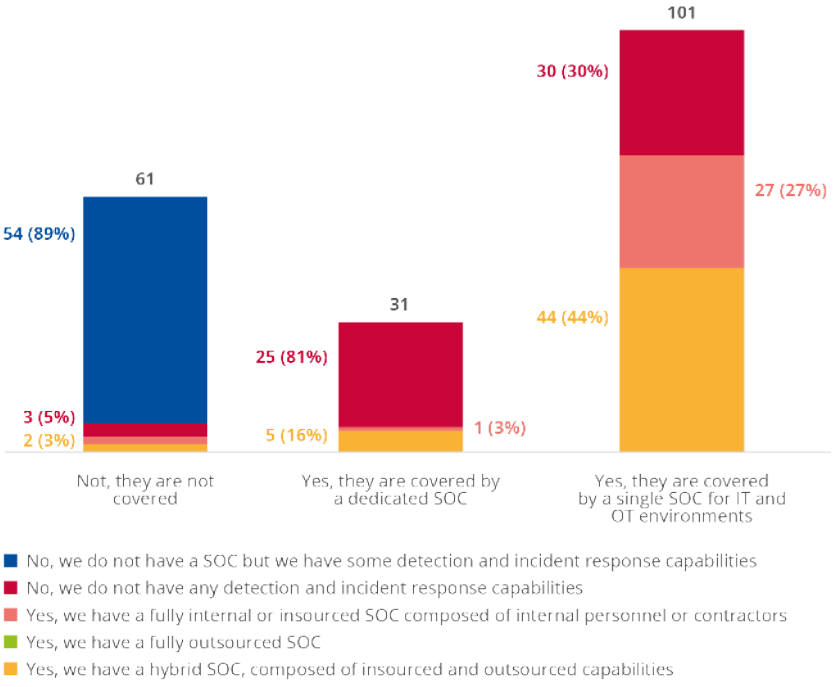


The survey data indicates that in 68% of the OESs in the Energy sector, critical OT systems are monitored by a SOC, of which 16% possesses a dedicated SOC for such OT systems.

Notably, however, 32% of the OESs within the Energy sector indicate that none of their critical OT processes are monitored by a SOC.

Figure 70 details the answers to this question in accordance with respondents' answers to question 21 related to the organisation's SOC strategy. 89% of the organisations that do not monitor critical OT systems also do not have a formal SOC in place.

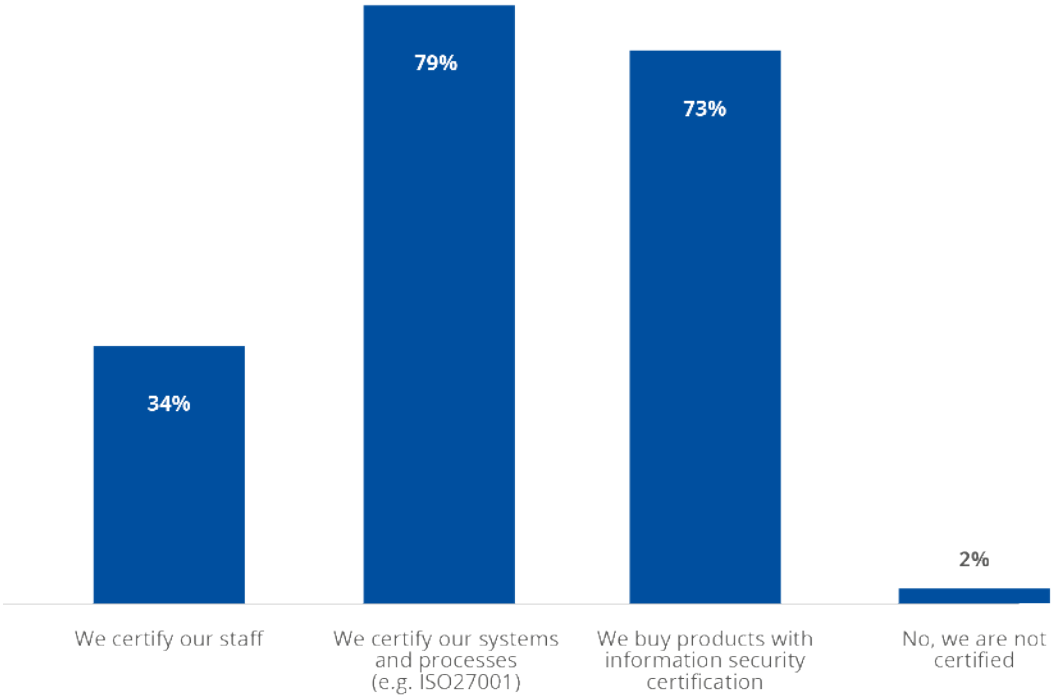
Figure 70: Organisational SOC strategy and monitoring of OT systems



6.5 CYBERSECURITY CERTIFICATION

Survey Question: Does your organisation have an information security related certification for processes, systems or staff?

Figure 71: Cybersecurity certification – Energy sector



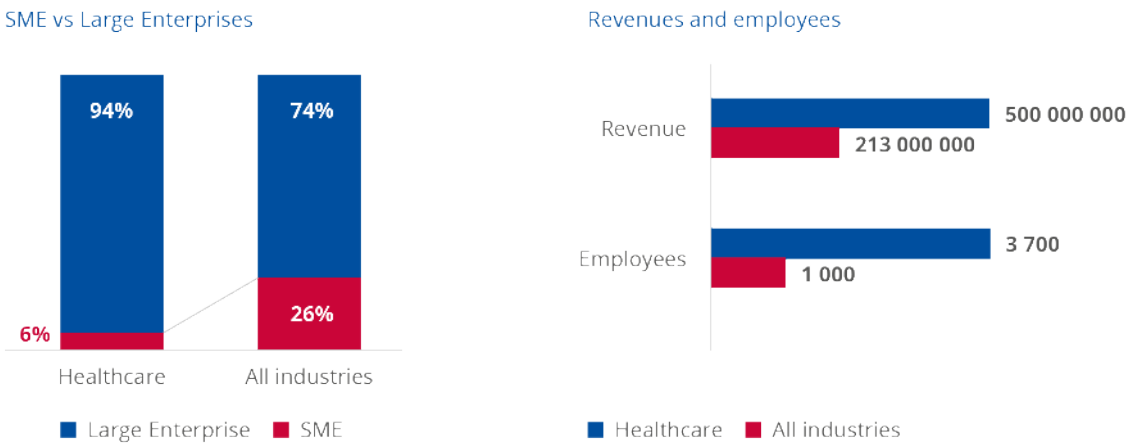
The survey data indicates that a majority of the OESs in the Energy sector certify their systems and processes (79%) and procure products with information security certifications (73%). However only 34% of the OESs within the Energy sector certify their staff.

7. SECTORAL ANALYSIS: HEALTH

Key Figures
An OES operating within the Health sector employs 50% more IS FTEs as compared to the median values of other sectors. When comparing IT staff, the Health sector rises far above the median value for the other sectors.
64% of the OESs in the Health sector are already using connected medical devices in their operations.
58% of the OESs in the Health sector are already using a digital health platform running on a specific healthcare cloud platform.
62% of the organisations surveyed have deployed specific security solutions for connected medical devices.
Only 27% of the OESs in the Health sector have a dedicated ransomware defence program.
60% of the OESs in the Health sector have provided awareness training to non-IT staff, and 22% of these have a dedicated training curricula for such staff.
A majority of the OESs in the Health sector certify their systems and processes (80%) and procure products with information security certifications (59%).

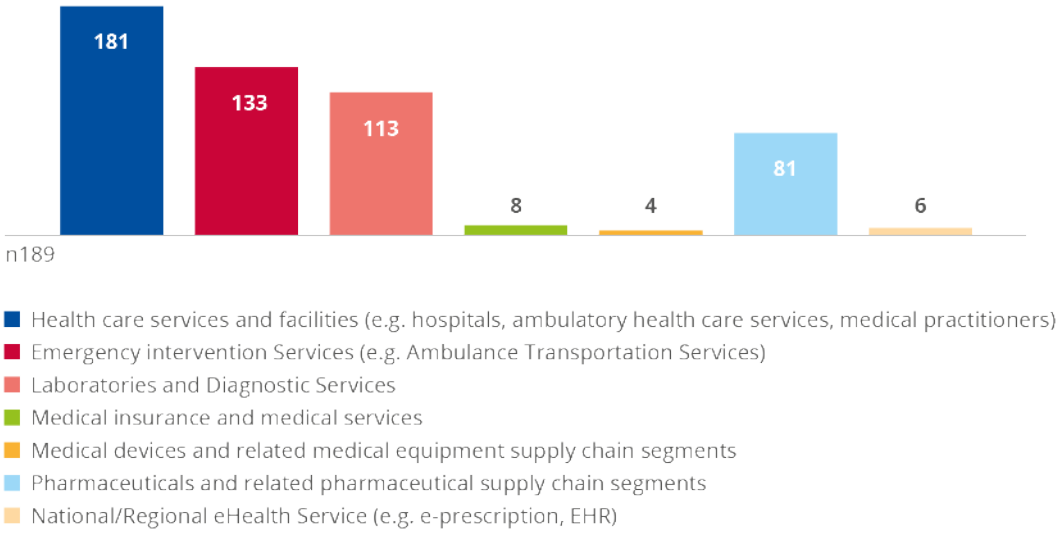
7.1 DEMOGRAPHICS OF A SECTORIAL DEEP DIVE

Figure 72: Size of OESs surveyed in the Health sector



The Health sector is mostly composed of Large Enterprises with 94% of the organisations surveyed meeting the definition of Large Enterprise compared to 74% for all sectors.

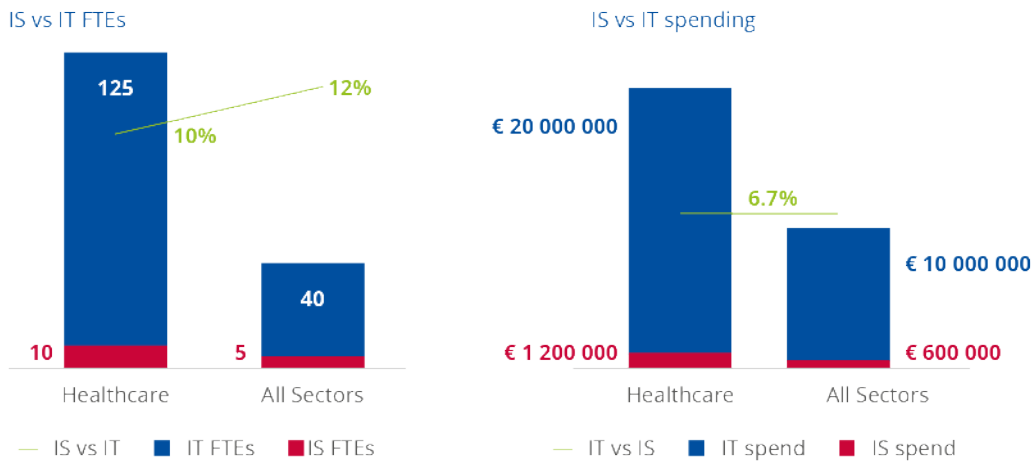
Figure 73: Sub-sectors



In terms of sub-sectors, most of the Health organisations operate in multiple sectors and less than 20 organisations operate in a single sub-sector. Out of the 189 organisations surveyed in the Health sector, 181 (96%) have operations in Healthcare Services and Facilities, 133 (70%) have operations in Emergency Intervention Services, 113 (60%) have operations in Laboratories and Diagnostic Services and 81 (43%) have operations in the Pharmaceutical and related Pharmaceutical Supply Chain Segments. The other sub-sectors had a very limited number of representative organisations in this survey.

7.2 INVESTMENT AND STAFFING INFORMATION

Figure 74: Health sector vs all sectors (median values)



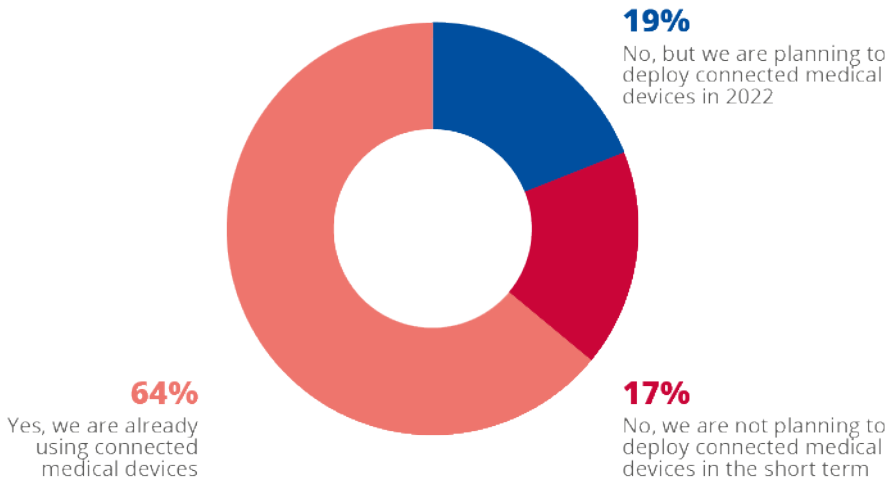
When comparing the Health sector to the overall data set, it may be noted that the IS FTEs as a share of IT FTEs is two points lower for an OES operating in the Health sector than the median across all sectors.

On the other hand, when comparing the intensity of spending in Information Security against IT spending, the Health sector spending ratio is equivalent to the median ratio across all sectors at 6,7%.

7.3 CONNECTED MEDICAL DEVICES AND CLOUD PLATFORMS IN HEALTH

Survey Question: Does your organisation use connected medical devices or Internet of Medical Things devices?

Figure 75: Connected medical devices in the Health sector

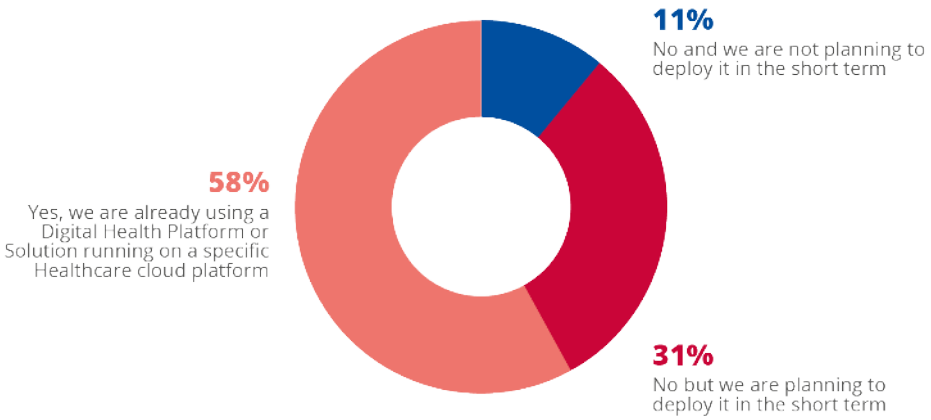


The survey data indicates that 64% of the OESs in the Health sector are already using connected medical devices in their operations.

Furthermore, 19% of the OESs in the Health sector are planning to deploy such devices in 2022.

Survey Question: Do you use a Digital Health Platform or Solution running on a Healthcare-specific cloud platform?

Figure 76: Adoption of Digital Health Cloud platforms in the Health sector



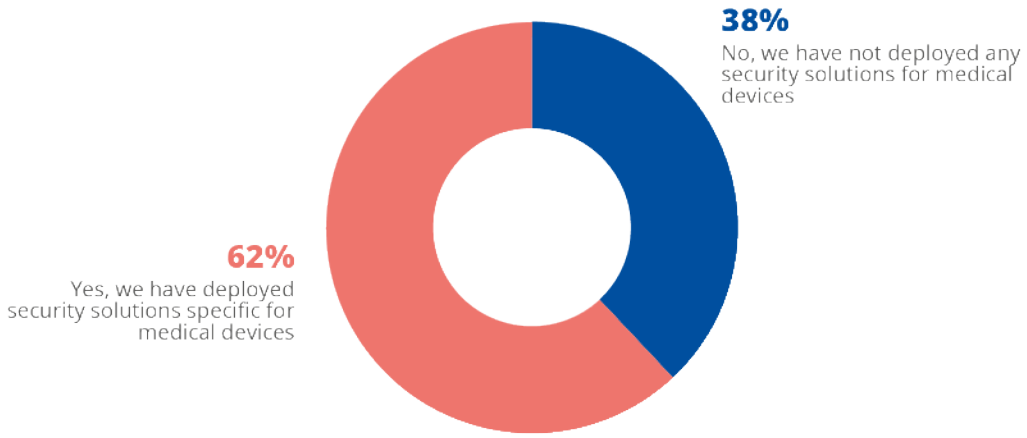
The survey data indicates that 58% of the OESs in the Health sector are already using a digital health platform running on a specific healthcare cloud platform.

Furthermore, 31% of the OESs in the Health sector are planning to deploy such a platform in the short term.

7.4 MEDICAL DEVICES SECURITY

Survey Question: Have you deployed specific security solution(s) for medical devices?

Figure 77: Security solutions for medical devices in the Health sector

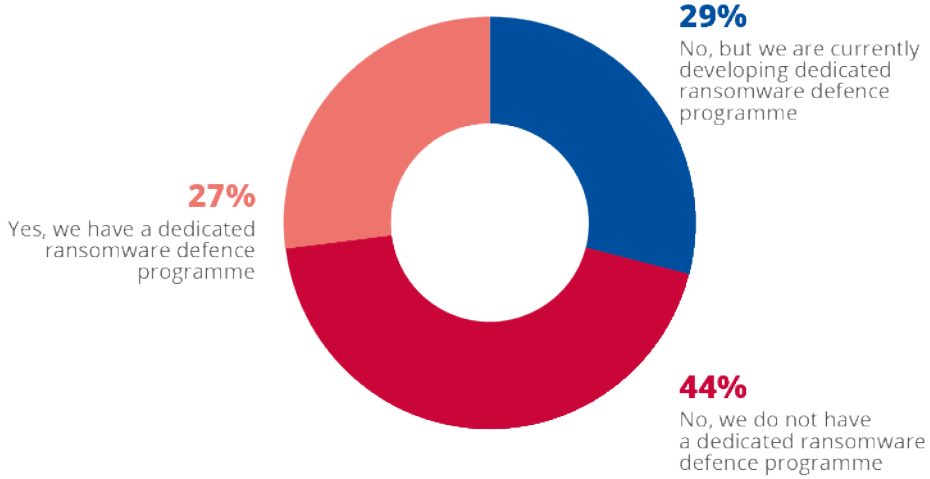


While 64% of the OESs in the Health sector are already using connected medical devices, 62% of the organisations surveyed have also deployed specific security solutions for such connected devices. It may be noted, however, that 38% of the OESs in the Health sector do not possess any specific security solution for connected medical devices.

7.5 RANSOMWARE DEFENCE AND AWARENESS TRAINING

Survey Question: Does your organisation have a dedicated ransomware defence programme? This means dedicated resources and budget allocation.

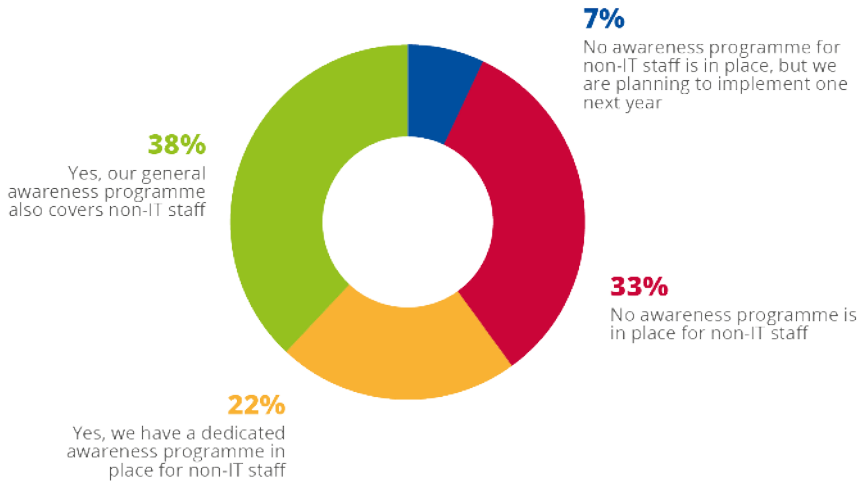
Figure 78: Ransomware defence programmes among Health sector OESs



The survey data indicates that only 27% of the OESs and DSPs in the Health sector have a dedicated ransomware defence programme. While 29% of the OESs and DSPs in the Health sector are currently developing such a programme, around 44% of the organisations surveyed has indicated that they are not doing so.

Survey Question: Does your organisation have an awareness raising or training programme in place for non-IT staff?

Figure 79: Awareness raising or training programmes for non-IT staff among Health sector OESs

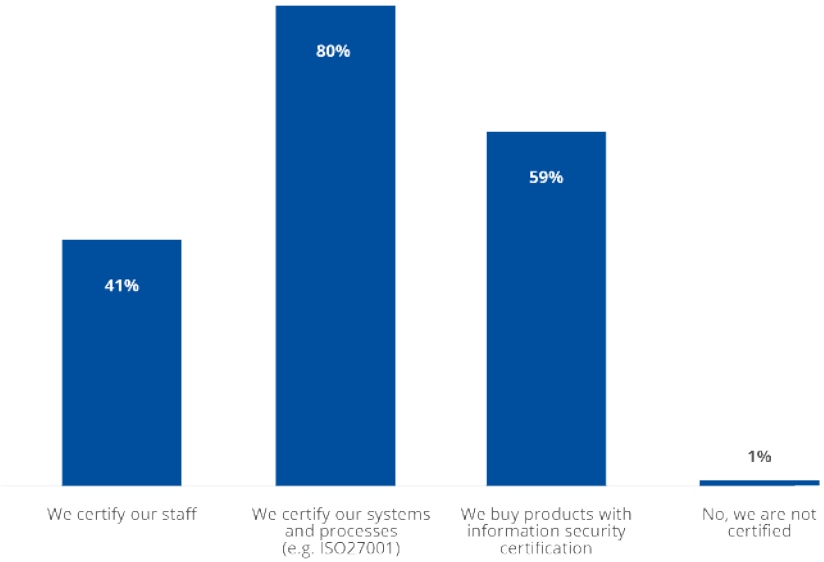


The survey data indicates that 60% of the OESs and DSPs in the Health sector have provided awareness training to non-IT staff, 22% of which have dedicated training curricula for such staff. It may however be noted that 33% of the organisations surveyed have no awareness programme at all in place for non-IT staff.

7.6 CYBERSECURITY CERTIFICATION

Survey Question: Does your organisation have information security-related certification for processes, systems or staff?

Figure 80: Cybersecurity certification in the Health sector

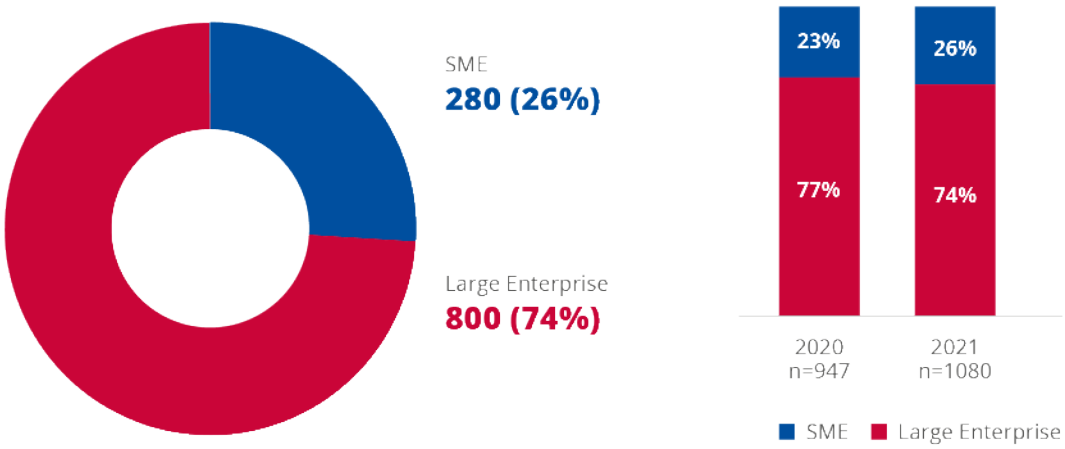


The survey data indicates that a majority of the OESs and DSPs in the Health sector certify their systems and processes (80%) and procure products with information security certifications (59%). However, only 41% of the OESs and DSPs in the Health sector certify their staff.

8. SME VS LARGE ENTERPRISES

8.1 SME AND LE DISTRIBUTION BY MEMBER STATE AND SECTOR

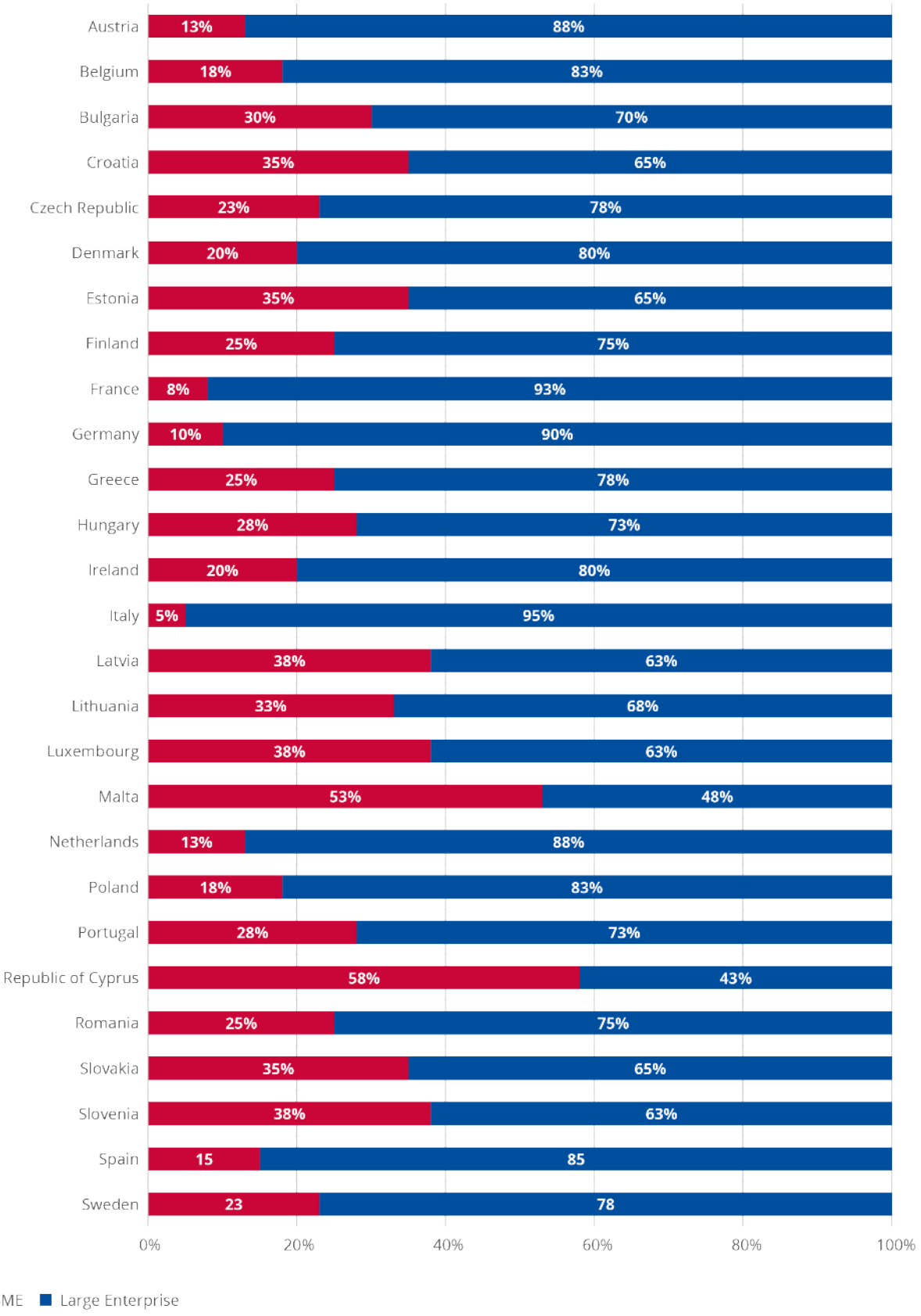
Figure 81: Distribution of SMEs and large enterprises



In this year's study, 280 SME organisations were surveyed as well as 800 Large Enterprises across all NIS sectors. When comparing the distribution of SMEs and LEs to last year, we can see a relative increase in the number of SME moving from 23% of the total samples to 26%. This relative increase must be kept in mind when analysing the results of this study as it will tend to lower the median and average values year over year as the SME have by nature lower raw figures.

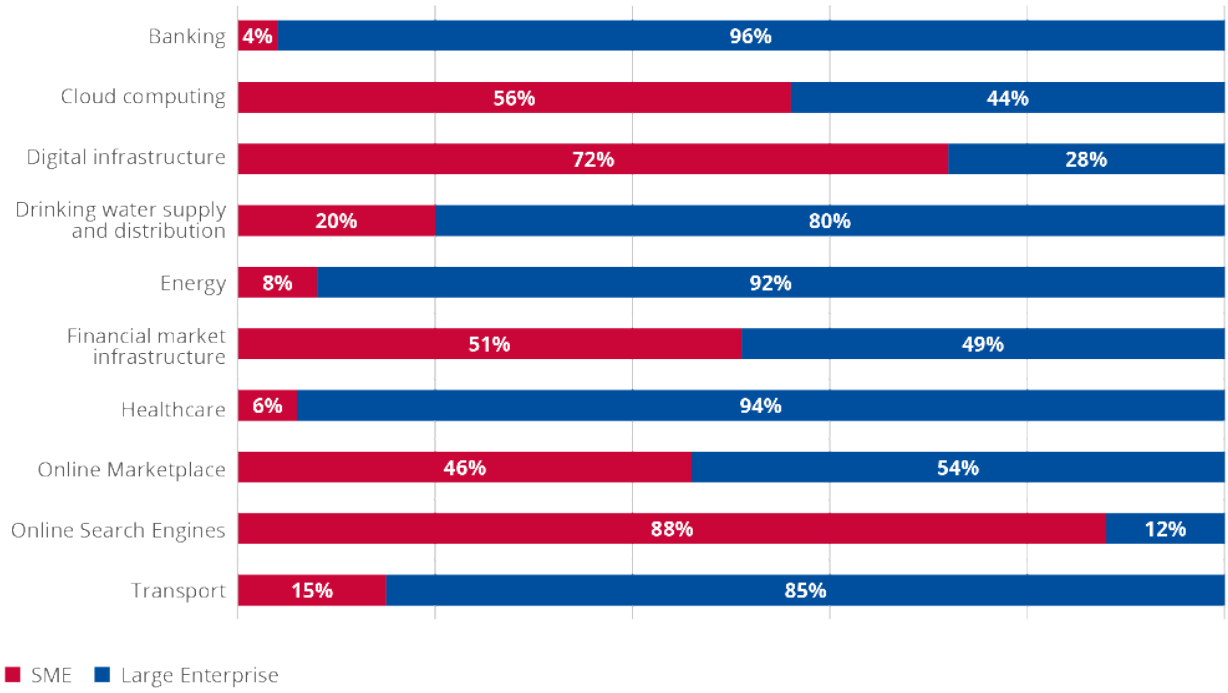
The details on the distribution of SMEs and LEs are provided in Figure 82. Italy (95%), France (93%) and Germany (90%) are the Member States with the highest share of Large Enterprises while the share of SMEs in the survey sample exceeds 50% for Cyprus (58%) and Malta (53%).

Figure 82: Distribution of SMEs and large enterprises surveyed in OESs and DSPs for each Member State



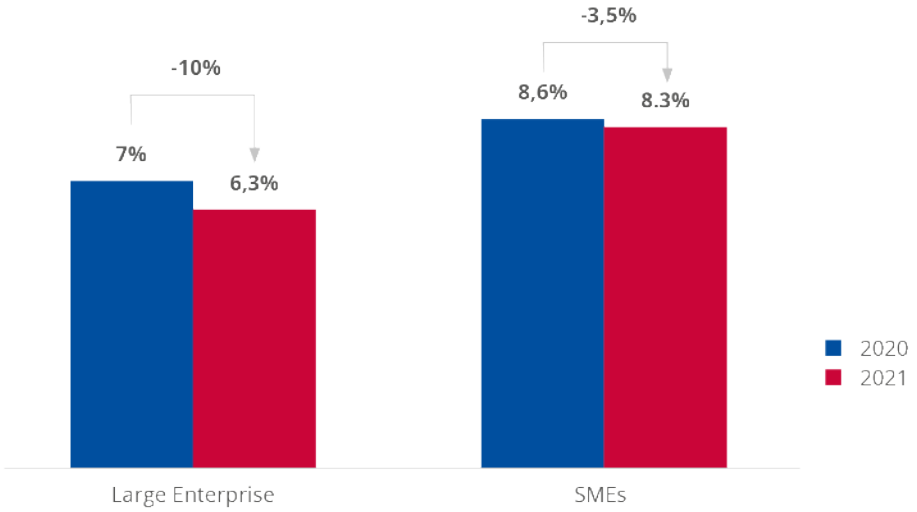
As depicted in Figure 83, the NIS sectors with the highest share of Large Enterprises are Banking (96%), Healthcare (94%) and Energy (92%). On the other end of the spectrum, the sectors with the highest share of SMEs are Online Search Engines (88%) and Digital Infrastructures (72%).

Figure 83: Distribution of SMEs and large enterprises by sector



8.2 IS SPEND AS A SHARE OF IT SPEND FOR SMEs AND LEs

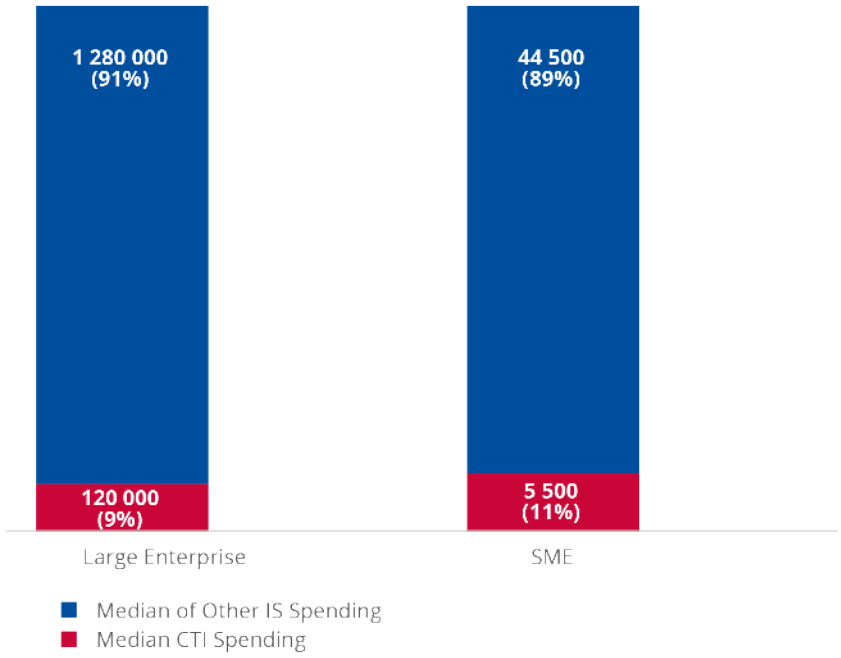
Figure 84: IS spend as a share of IT spend for SMEs and LEs



In this year's sample, the median IS spend as a share of IT spend is 8.3% for SMEs which is 3.5% lower than the 8.6% obtained in last year's study. On the other hand, we can observe an important decrease of 10% for Large Enterprises, where the share of IS spend against IT spend was 6.3% in this year's study and 7.0% last year.

8.3 CTI SPENDING FOR SMEs AND LEs

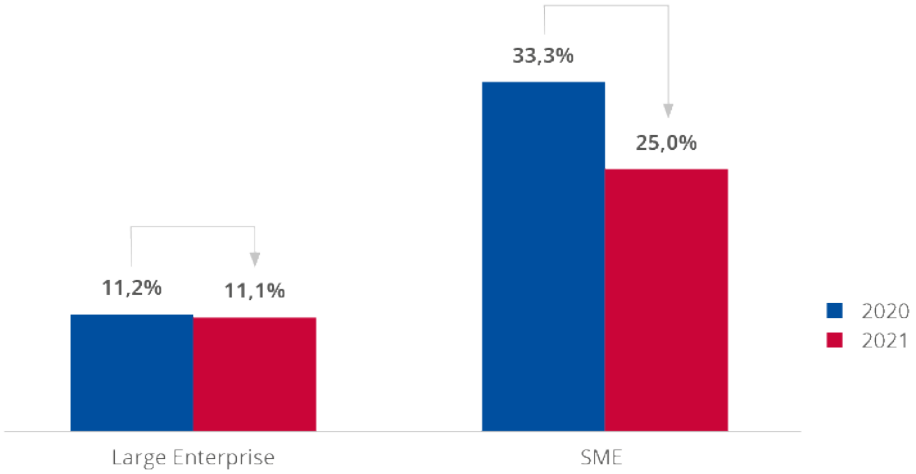
Figure 85: CTI spending for SMEs and LEs



The median cyber threat intelligence spending for SMEs is EUR 5 500 which represents 11% of their total IS spend; but it amounts to EUR 120 000 for large enterprises, which is 9% of their total IS spending.

8.4 IS FTEs AS A SHARE OF IT FTEs FOR SMEs AND LEs

Figure 86: IS FTEs as a share of IT FTEs for SMEs and LEs



The IS FTEs as a share of IT FTEs is rather stable for large enterprise but has decreased in this year's sample for SMEs. Although the difference is important, the percentage is highly sensitive because the total number of IT FTEs in SMEs is low (6 in last year's study and 4 this year).

8.5 SOC CAPABILITIES FOR SMEs AND LEs

Figure 87: SOC capabilities for SMEs and LEs

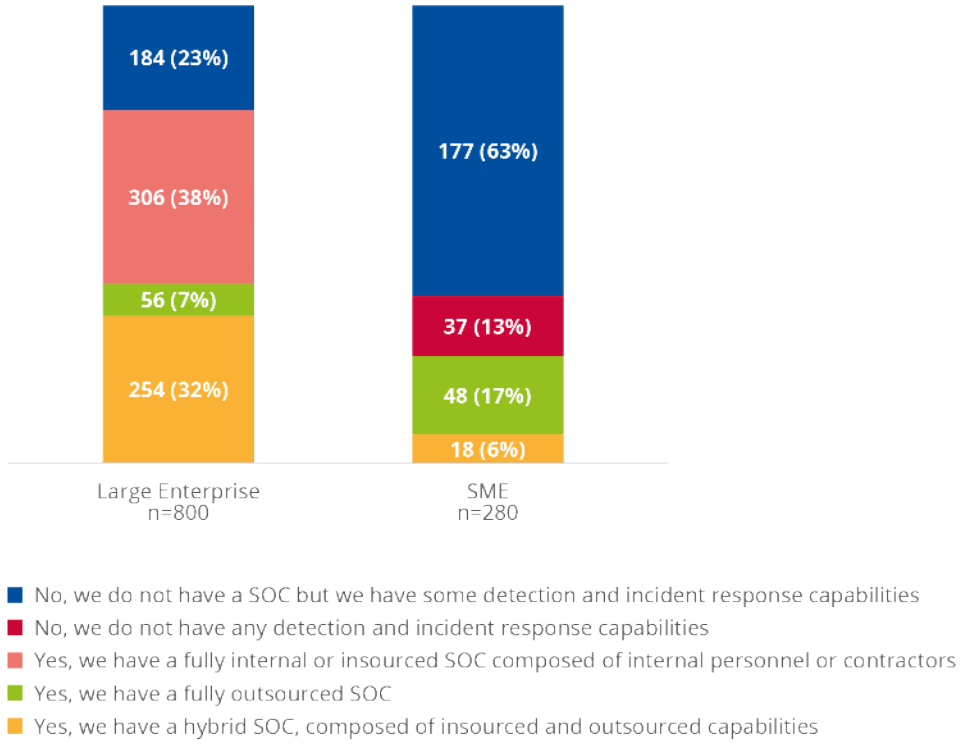
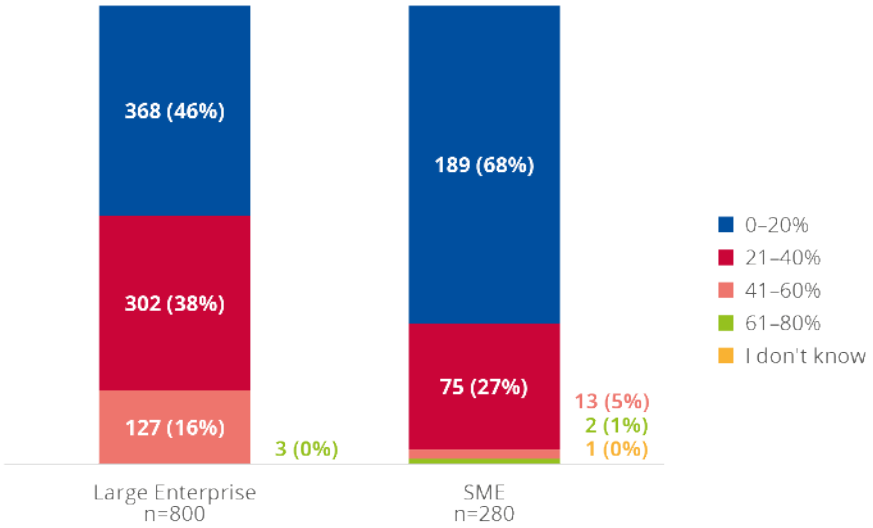


Figure 87 details the results of the organisations SOC capabilities for both SMEs and Large Enterprises across all NIS sectors. We can see that a large majority (76%) of SMEs do not have a formal SOC in place while only 23% of Large Enterprises are in the same situation. 13% of the SME organisations surveyed do not have basic detection and incident response capabilities in place.

8.6 SHARE OF ASSETS VISIBILITY FOR PATCHING FOR SMEs AND LEs

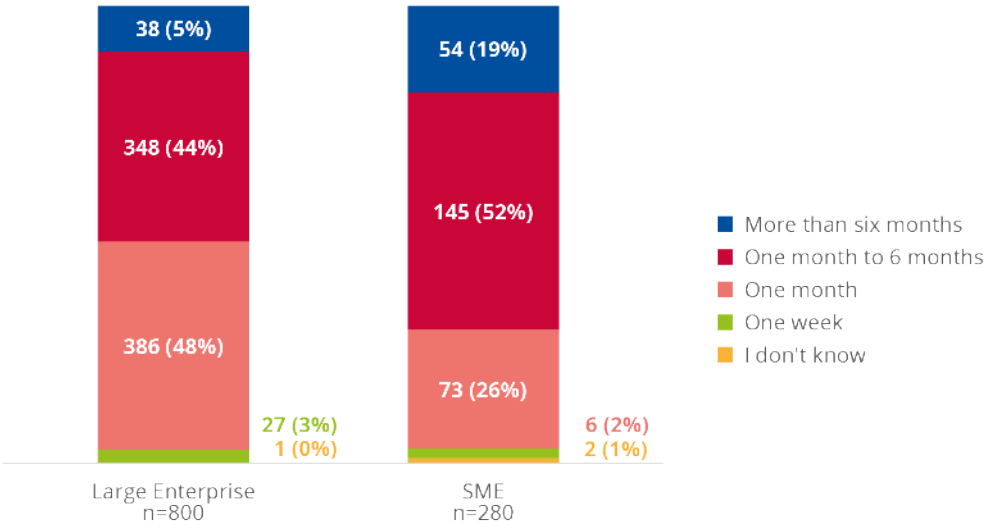
Figure 88: Visibility over the patching of assets for SMEs and LEs



68% of the SME organisations surveyed declared visibility for patching at less than 20% of their assets. This represents less than the majority of the Large Enterprise (46%).

8.7 AVERAGE TIME TO PATCH CRITICAL VULNERABILITIES IN IT ASSETS FOR SMEs AND LEs

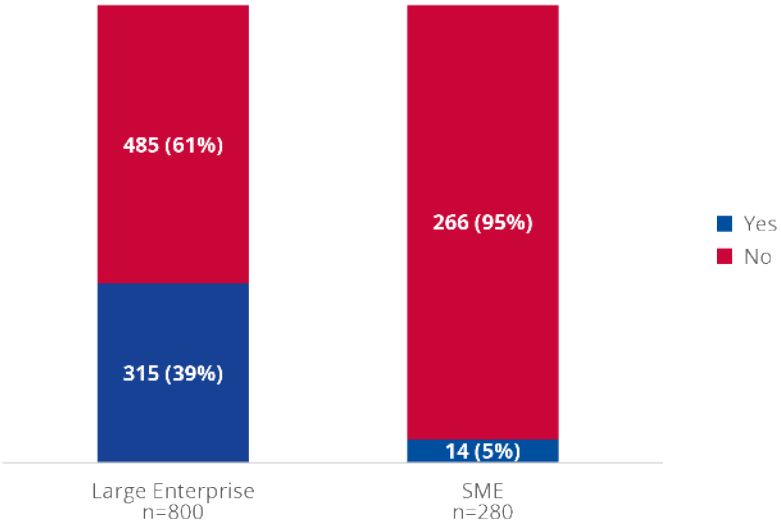
Figure 89: Average time to patch critical vulnerabilities in IT assets for SMEs and LEs



72% of the SME organisations surveyed patch critical vulnerabilities in their IT assets in more than one month on average against 49% for Large Enterprises.

8.8 CYBER INSURANCE FOR SMEs AND LEs

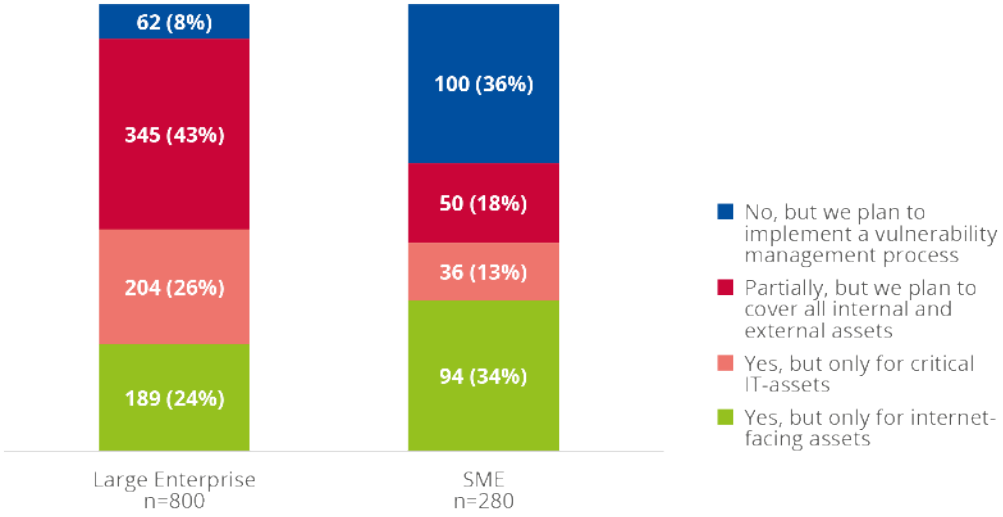
Figure 90: Cyber insurance for SMEs and LEs



39% of Large Enterprises have subscribed to a cyber insurance product while only 5% of the SME organisations surveyed have done the same.

8.9 VULNERABILITY MANAGEMENT FOR SMEs AND LEs

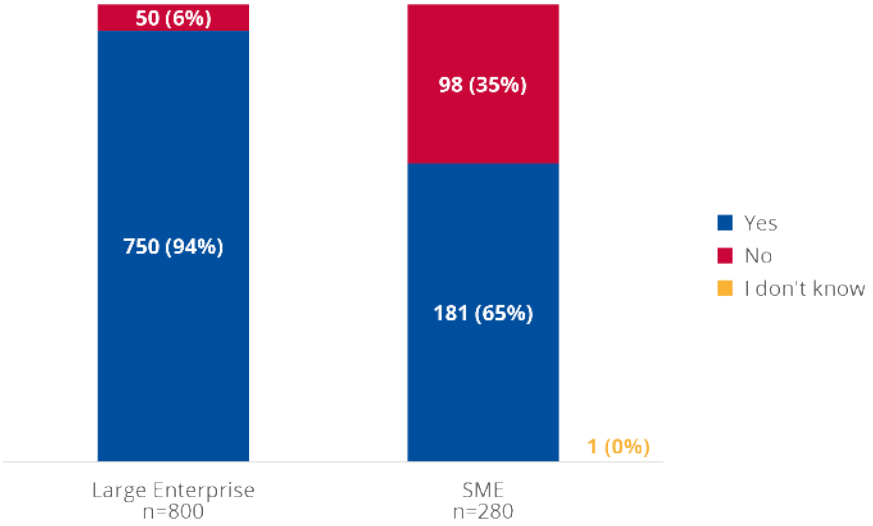
Figure 91: Vulnerability management for SMEs and LEs



With regards to the implementation of a risk-based vulnerability management process, 36% of the SME organisations surveyed do not have any but this figure is 8% for Large Enterprises.

8.10 THIRD PARTY RISK MANAGEMENT (TRM) POLICIES FOR SMEs AND LEs

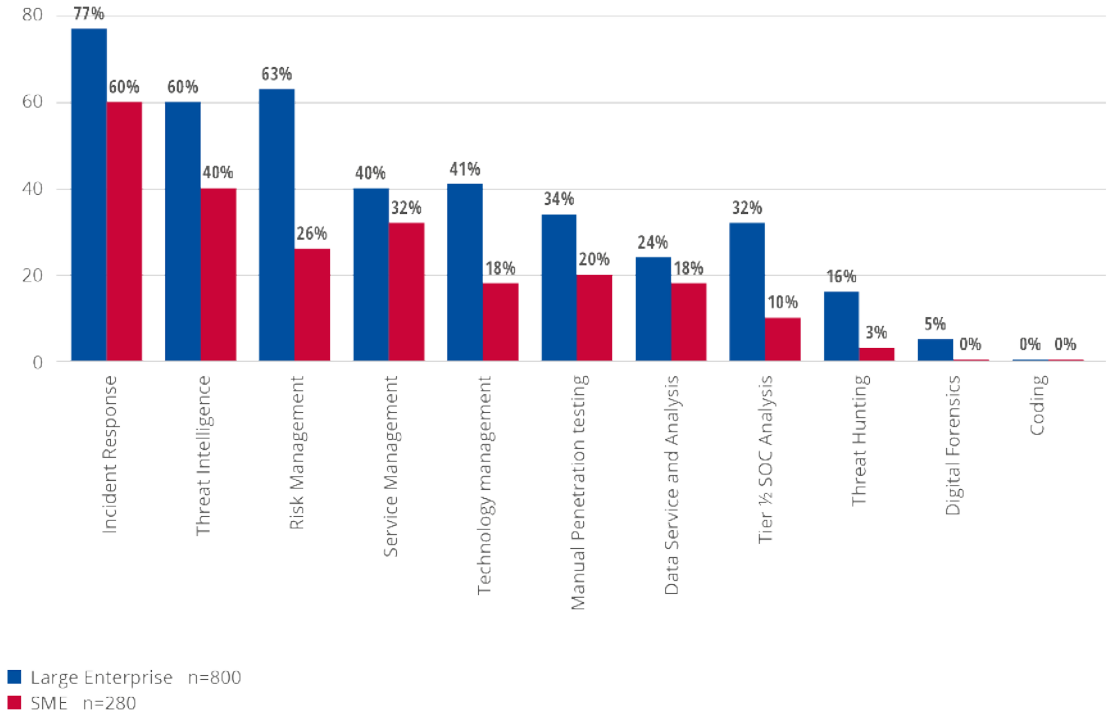
Figure 92: TRM policies for SMEs and LEs



35% of the SME organisations operating in the NIS sectors do not have Third-Party Risk Management policies in place but this is only 6% for Large Enterprises in the NIS sectors.

8.11 CYBERSECURITY SKILLS FOR SMEs AND LEs

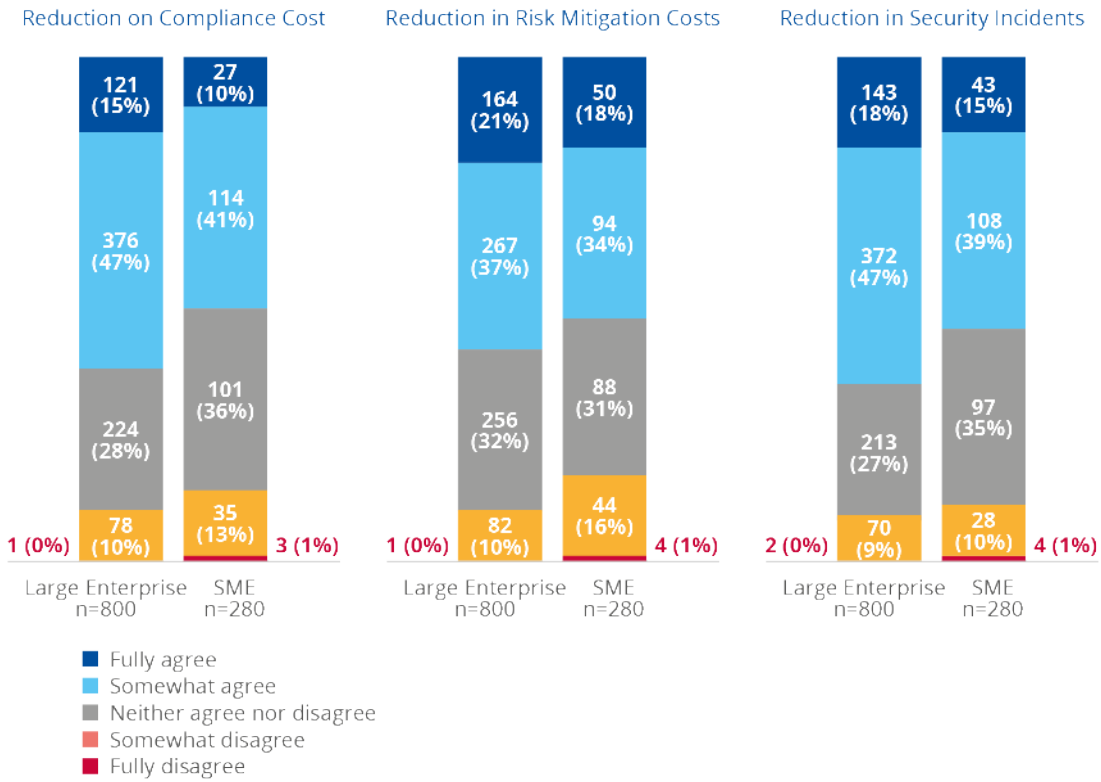
Figure 93: Cybersecurity skills prioritised for internal development among SMEs and LEs



The top three security skills that Large Enterprises aim to develop internally or hire are Incident Response (77%), Risk Management (63%) and Threat Intelligence (60%) while the top three for SMEs are Incident Response (60%), Threat Intelligence (40%) and Service Management (32%).

8.12 EUROPEAN CYBERSECURITY REQUIREMENTS FOR SMEs AND LEs

Figure 94: Perceptions of foreseen impacts from the introduction of common European cybersecurity requirements for digital products – comparisons between SMEs and LEs



62% of Large Enterprises agree that common European cybersecurity requirements for digital, hardware and software products would lead to a reduction in compliance costs but only 51% of SMEs agree.

58% of Large Enterprises agree that common European cybersecurity requirements for digital, hardware and software products would lead to a reduction in risk mitigation costs but only 52% of SMEs agree with this statement.

Lastly, 65% of Large Enterprises agree that common European cybersecurity requirements for digital, hardware and software products would lead to a reduction in security incidents while only 54% of SMEs agree with the same statement.

9. CONCLUSIONS

This report marks the third iteration of ENISA's work on NIS Investments, which examines the impact of the NIS Directive implementation on the cybersecurity budgets of OES/DSPs and looks into various aspects of how these budgets have been allocated to develop various cybersecurity capabilities. This year's study collects data from an even larger sample of OES/DSPs as it presents information collected from 1080 operators from all 27 EU MS. More importantly, as of this year the historical dataset 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 cybersecurity investments to develop specific cybersecurity capabilities, such as SOCs, and into how supply chain cyber risk management is organised among OES/DSPs, and it also provides sectorial deep dives for the Energy and Health sectors; for these two sectors additional operators were interviewed and the survey questionnaires were expanded to include additional, sector-specific questions.

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

On a global level, the cybersecurity market is expected to grow substantially over the next years, a growth driven also by the re-initiating of projects that were put on hold at the start of the pandemic. **Application Security** and **Cloud Security** are expected to drive this trend with projected **annual growth rates over 20% for the EU market** until 2025. **CTI especially is expected to grow at over 15% per year** as operators ranging from SMEs to Large Enterprises focus more and more on CTI, albeit with different priorities; more mature organisations require more technical, actionable CTI, whereas lower maturity organisations opt for tactically oriented information with SMEs opting for more contextualised information.

From a global point of view, investments in ICT for the health sector seem to be greatly impacted by COVID-19 with many hospitals looking for technologies to expand healthcare delivery outside the hospitals' four walls. Still, cybersecurity controls remain a top priority for spending with 55% of health operators targeting cybersecurity tools for increased funding. In the Energy sector, Oil and Gas operators at a global level seem to prioritise cybersecurity for increased investments at a rate of 74%. This sector also shows a trend in investments shifting from legacy infrastructure and data centres to cloud services.

The median IT budget for OES/DSP in 2021 was EUR 10 million, of which EUR 0.6 million was earmarked for information security. Both absolute values are lower compared to the 2021 NIS Investments report, a finding that is partly attributed to differences in the surveyed sample, but to some extent is also likely a result of reduced investments due to the macroeconomic landscape and, especially, the impact of COVID-19 on IT and cybersecurity budgets. OES/DSP in the EU earmarked on median **6.7 % of their IT investments for information security, 1 percentage point lower compared to last year's findings**. In addition to the influence of macroeconomic conditions, it is likely that this figure is influenced by the higher representation in the sample of OES from the Energy and Health sectors, which generally tend to allocate a lower percentage of their IT budgets to information security.

An OES or DSP in the EU spends on median EUR 50 000 on CTI, though data indicates that **most organisations do not earmark vast budgets for CTI, while larger operators — especially within the Banking and Energy sectors — do invest significantly in CTI**. Considering that CTI is a valuable source of information in the context of incident prevention and risk assessment, this finding seems to indicate a need to provide easier access to CTI to smaller OES/DSPs in the EU.

Most OES/DSPs in the EU indicate the **NIS Directive and other regulatory obligations, as well as the threat landscape as the main factors influencing their NIS budgets**.

OES/DSP employ on median 40 IT FTEs, five of whom are dedicated information security FTEs. The percentage of FTEs dedicated to information security is 1 percentage point lower compared to last year (12% compared to 13%), though the survey sample composition is likely the key factor resulting in this discrepancy.

The estimated direct cost of a major security incident is EUR 200 000 on median, **twice as large as last year, indicating an increase in the cost of incidents**. Same as last year, the highest median costs of major security incidents are found within the **Banking and Healthcare sectors** (EUR 300 000). **69% of OES/DSPs indicated that the majority of their information security incidents are caused by the exploitation of vulnerabilities** in software or hardware products with the Health sector declaring the most such incidents. 46% of OES/DSPs patch critical vulnerabilities in less than a month, while that 92% of OES/DSPs patch critical vulnerabilities within at least six months after their discovery. However, the **average time to patch tends to be significantly longer for SMEs** compared to Large Enterprises.

37% of the OESs and DSPs in the EU do not operate a dedicated SOC. Of these 4% do not possess any detection and/or incident response capabilities. Internal SOC capabilities seem to be very closely correlated with CTI spending, even though CTI is useful outside the context of SOC operations, e.g. in risk assessment. **76% of SMEs have no SOC capabilities**, either in-house or outsourced.

30% of OES/DSPs possessed cyber insurance in 2021, a decrease of 13% compared to 2020. The discrepancy is very stark when comparing cyber insurance adoption among Large Enterprises (39%) and SMEs (5%) indicating the need to improve both awareness among SMEs as well as cyber insurance product suitability for smaller organisations.

73% of OES/DSPs aim to further enhance incident response skills and talents, closely followed by cyberthreat intelligence (54%) and risk management (53%).

86% of OES/DSPs have implemented third-party risks management (TRM) policies, though the percentage seems to be lower for DSPs compared to OES. However, only 47% of surveyed organisations have a dedicated TRM budget and only 24% have a dedicated role for TRM. 61% of the organisations surveyed indicated a preference for Security Certificates for supply chain security risk mitigation, followed closely by Security Risk Rating Services (43%) and Due Diligence or Risk Assessments (37%).

The sectorial deep dive in the Energy sector revealed that **32% of the OESs within the Energy sector indicate that none of their critical OT processes are monitored by a SOC**. For 52% of Energy sector OES, OT and IT are covered by a single SOC.

The sectorial deep dive in the Health sector revealed that 64% of Health OES are already using connected medical devices with 62% having deployed a security solution specifically for medical devices. Although ransomware and human error remain key factors behind cybersecurity incidents in the Health sector, only **27% of surveyed OES in the sector have a dedicated ransomware defence programme** and **40% of surveyed OES have no security awareness programme for non-IT staff**.

A ANNEX: NIS DIRECTIVE SURVEY DEMOGRAPHICS

Figure 95: Organisations surveyed in each Member State and sector

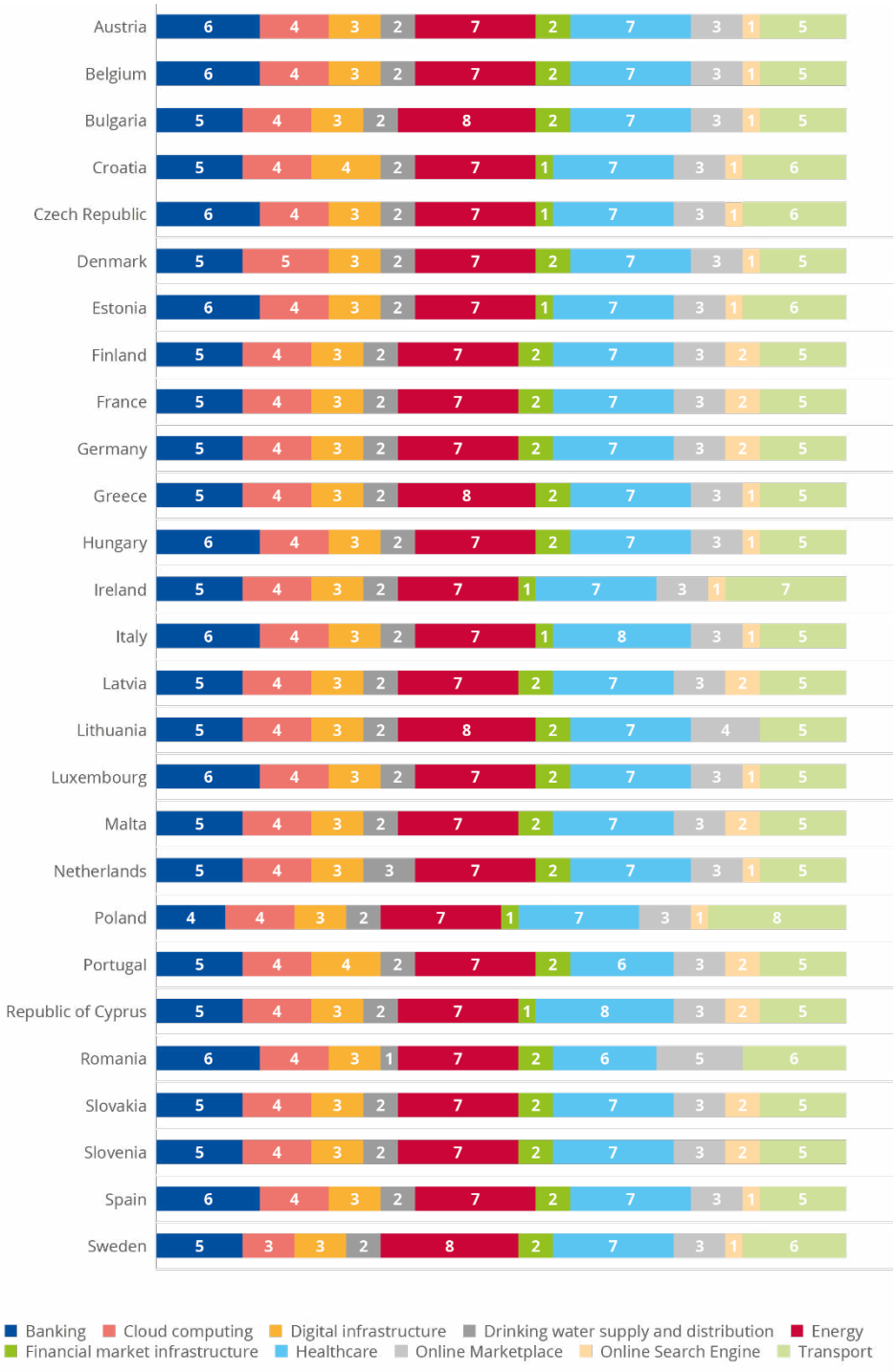


Figure 96: Organisations by sector

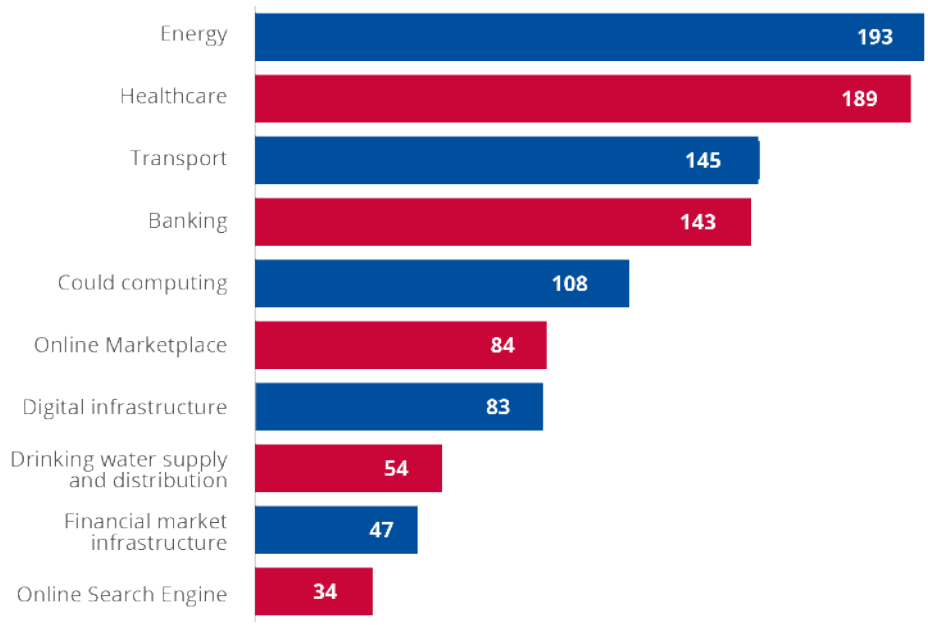


Figure 97: Estimated revenues by sector

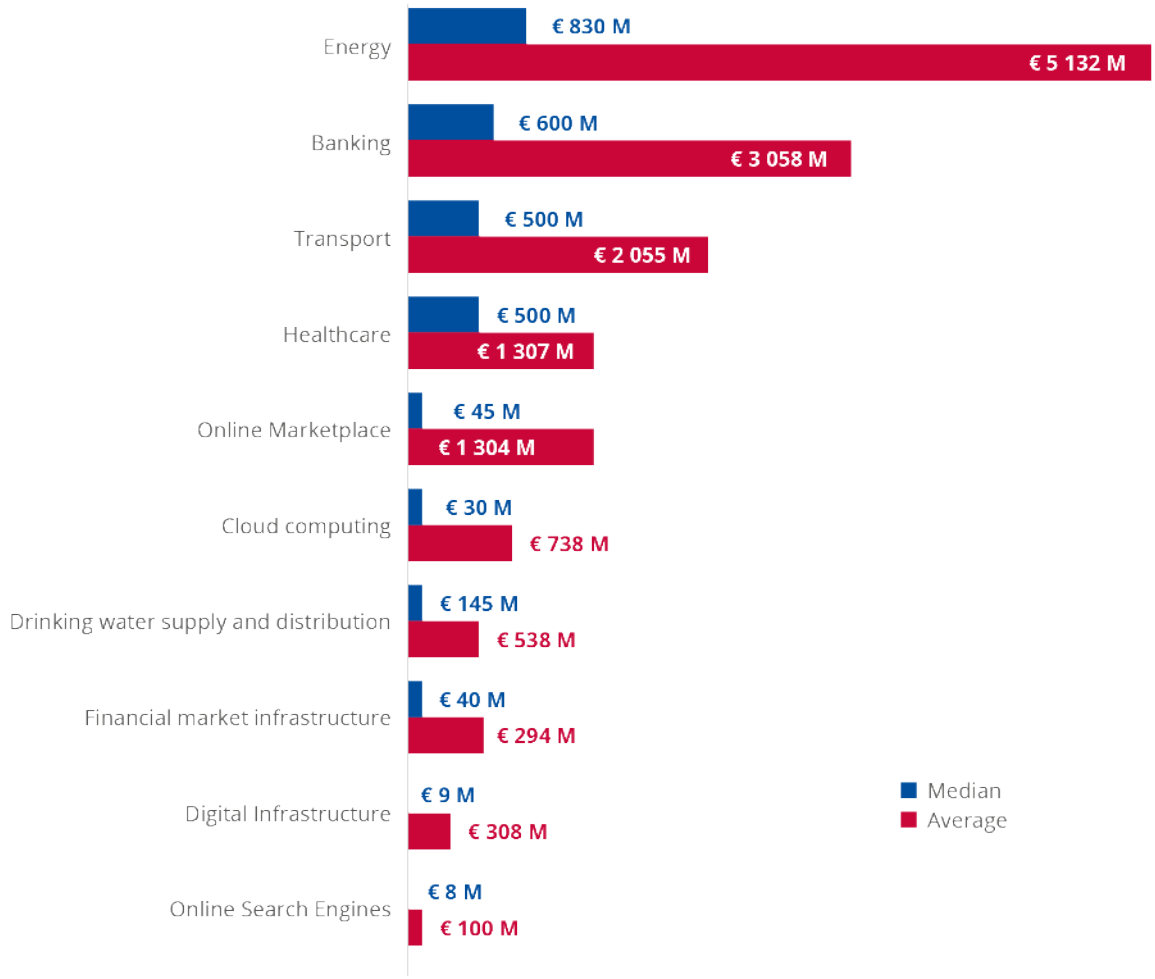


Figure 98: FTEs count by sector

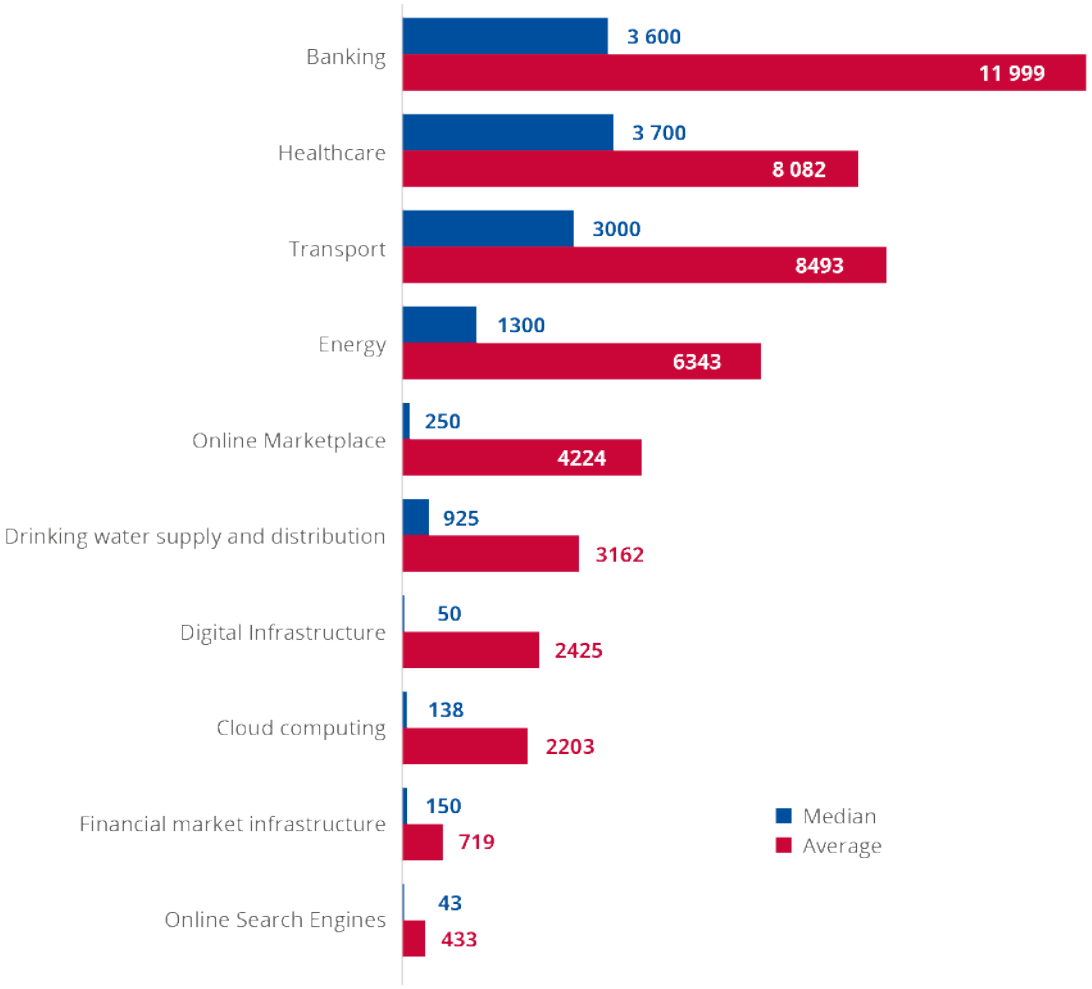


Figure 99: Distribution of OESs vs DSPs

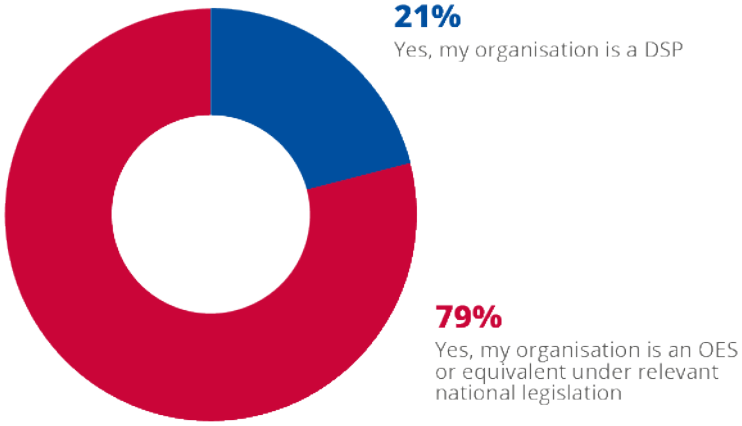
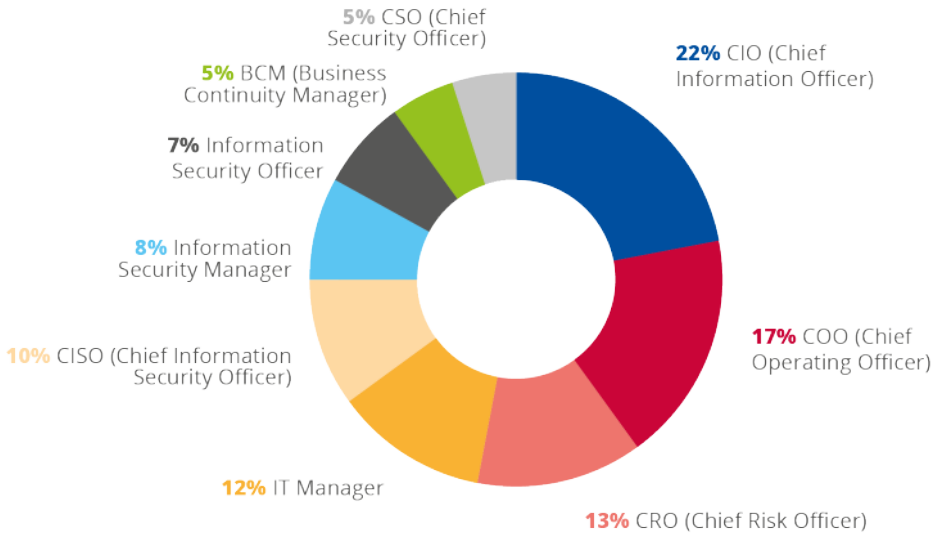


Figure 100: Function of respondent



B ANNEX: DEFINITIONS

B.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 data set, 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 data set.

Table 3: Median and average definitions

Type	Description	Example	Result
Arithmetic mean	Sum of values of a data set 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 data set	1, 2, 2, 3, 4, 7, 9	3

B.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]

B.3 SME DEFINITION

The main factors determining whether an enterprise is an SME are:

- staff headcount.
- either turnover or balance sheet total.

Table 4: SME definition

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

C ANNEX: ACRONYMS

BCM: Business Continuity Manager
CAASM: Cyber Asset Attack Surface Management
CAPEX: Capital Expenditure
CASB: Cloud Access Security Broker
CCO: Chief Operating Officer
CIO: Chief Information Officer
CIO: Chief Information Officer
CRM: Customer Relationship Management
CRO: Chief Risk Officer
CSO: Chief Security Officer
CTI: Cyber Threat Intelligence
DRM; Digital Risk Management
DRPS: Digital Risk Protection Service
DSP: Digital Service Providers
EASM: External Attack Surface Management
FTE: Full Time Equivalent
IAM: Identity and Access Management
ICT: Information and Communication Technology
IR: Incident Response
IRM: Integrated Risk Management
IS: Information Security
ISMR: Information Security and Risk Management
ISS: Information Security Manager
IT: Information Technology
ITDR: Identity Threat Detection and Response
LE: Large Enterprises
ML: Machine Learning
NIS: Network and Information Systems
OES: Operators of Essential Services
OPEX: Operating Expense
OT: Operational Technology
OT: Operational Technology
SASE: Secure Access Services Edge
SOC: Security Operations Centre
SWG: Secure Web Gateway
TRM: Third Party Risk Management
XTR: Extended Detection and Response

TP-AM-22-001-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

enisa.europa.eu

ISBN 978-92-9204-585-2
Doi: 10.2824/433214