EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NIS INVESTMENTS

NOVEMBER 2021

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 raising awareness, 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. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting 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 978-92-9204-537-1, ISSN 2600-4712, DOI: 10.2824/77127, Catalogue nr.TP-AM-21-001-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2020, ENISA published its first report on network and information systems (NIS) investments[1] in an attempt to collect 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**)[2] invest their cybersecurity budgets and how this investment has been influenced by the NIS Directive. **This report is a follow-up covering all 27 EU Member States and offering additional insights into the allocation of NIS budgets of OES/DSP**, the economic impact of cybersecurity incidents and the organisation of cybersecurity in these operators. 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.

Data was collected through a survey of **947 organisations identified as OES/DSP** across the **27 Member States**. In this second edition of the report, besides covering all Member States, additional and complementary questions were asked to the surveyed organisations.

Overall, **48.9 % of surveyed organisations acknowledge a very significant or significant impact of the NIS Directive on their information security (IS).** Other key findings of this report are as follows.

- Almost 50 % of the established OES/DSP within the EU believe that implementing the NIS Directive has strengthened their detection capabilities, while 26 % believe that it has strengthened their ability to recover from incidents.
- 67 % of OES/DSP required a dedicated budget for the NIS Directive implementation, with a median value of EUR 40 000 or 5.1 % of their overall information security budgets. Around 50 % of organisations required on median four additional full-time employees (FTEs) for the implementation, either via recruitment or outsourcing.
- The estimated direct cost of a major security incident is EUR 100 000 on median, with the banking and healthcare sectors experiencing the highest such costs of EUR 300 000 and EUR 213 000 respectively. The primary cost factors for this figure include costs related to revenue losses and data recovery or business continuity management. 9 % of organisations have suffered a major security incident that impacted external stakeholders.
- In 28 % of the surveyed OES/DSP, the Chief Information Officer (CIO) or Chief Technology Officer (CTO) is responsible for information security while in over 50 % of cases, the Head of Information Security reports directly to the Chief Executive Officer (CEO), the Board of Directors (BOD) or the President.
- More than 50 % of the surveyed OES/DSP do not possess any form of cyber insurance, but around 25 % are planning to obtain coverage.
- More than 50 % of the surveyed OES/DSP certify their systems and processes.
- The majority of the surveyed OES/DSP report that their information security controls meet or exceed industry standards, with only 5 % reporting that they do not meet those standards.
- The results indicate a strong correlation between a very positive self-perception of cybersecurity maturity and the existence of cybersecurity certifications for processes, people and products within an organisation.

[1] https://www.enisa.europa.eu/publications/nis-investment
[2] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148

1. INTRODUCTION

The **Directive on Security of Network and Information Systems** (**NIS Directive**)[3] represents the first EU-wide legislation on cybersecurity, with the objective of achieving a high common level of cybersecurity for all Member States. One of the three pillars of the NIS Directive is the implementation of risk management and reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP). Annex II and Annex III of the NIS Directive identify the following categories of operators/sectors as OES and DSPs respectively:

Table 1: Categories of OES/DSP as defined in the NIS Directive

Categories of OES 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 marketplace • Online search engine • Cloud computing service

The objective of this report is to document **how operators within these sectors invest in cybersecurity and comply with the objectives set forth in the NIS Directive, and to shed some light on other aspects such as certification, cyber insurance and organisation of information security in OES/DSP.** In this context, this report could provide additional inputs for 'NIS 2', a proposal for a directive on measures for a high common level of cybersecurity across the EU that is under discussion in the European Parliament and the Council of the European Union.

NIS investment data for this report was collected from two sources.

- **Chapter 2** (Information security dynamics and outlook), consisting of high-level insights into the EU cybersecurity market, is based on data drawn from **Gartner's research databases**, combined with additional analysis of the current market dynamics and the latest forecasts.
- **Chapter 3** (Information security investments for implementing the directive) is based on data from a **dedicated market survey** that focused on the directive and was conducted on 947 organisations identified as OES/DSP in the EU.

In order to ensure a representative account of all 27 Member States, a minimum of 35 organisations were surveyed per Member State.

Additional information on the survey demographics is available in Annex A.

The target audience of this report is **EU and national policymakers**. The report may also provide useful information to OES/DSP as a secondary audience.

[3] 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 information security trends and outlooks. In order to provide actionable insights, it leverages data and metrics that were collected and assessed by Gartner, independently from the dedicated survey at hand. The specific sources of data for the following analysis include:

- **Gartner IT Key Metrics Data 2021**: IT Security Measures[4], Worldwide
- **Gartner Forecast**: IT Security and Risk Management, Worldwide, 2020-2025, 2Q21 Update.[5]

It should be noted that **the source of the data for Chapter 2** (Gartner databases) is **different to the source of the data for Chapter 3** (survey). Specifically:

- the definitions of the industries referenced in Chapter 2 are not aligned with the definitions of the OES/DSP sectors in Chapter 3 and set out by the NIS Directive;
- the figures provided by Gartner in the IT Key Metrics data 2021 are financial figures collected for the entire year 2020.

A detailed description of the relevant definitions is available in Annex B.

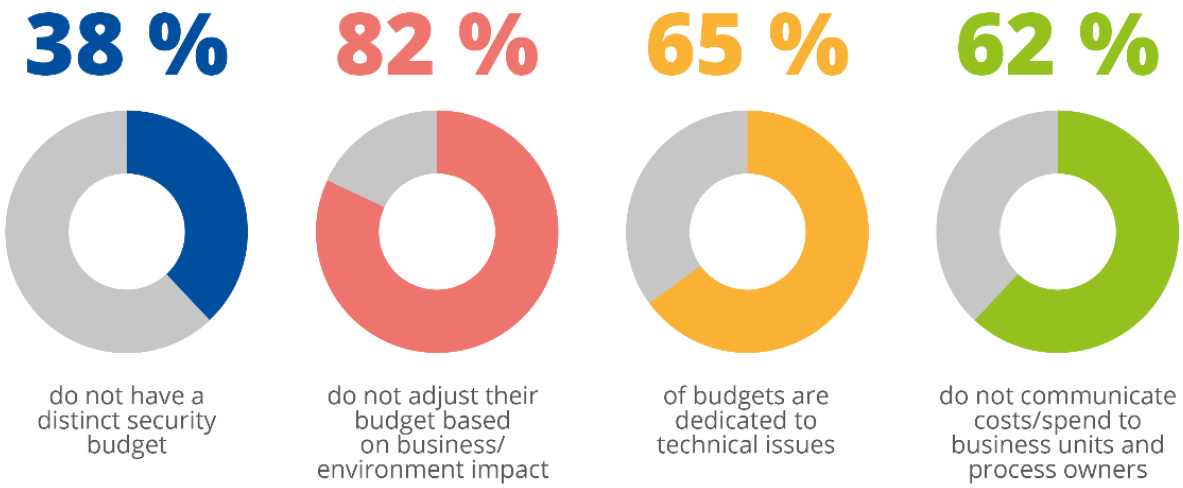
This data set is presented before the detailed data related to implementing the directive in order to provide a high-level overview of the global market (including Member States) in terms of information security investments and to highlight a few key statistics and trends. **This broader view serves as an introduction to the focused analysis presented in Chapter 3 for OES/DSP in the Member States**.

2.1 INFORMATION SECURITY BUDGETS

The data shows that tracking and the corresponding allocation of information security budgets is still increasing within most organisations and earmarked predominantly for IT security. Regardless of this positive trend, 38% of the surveyed organisations still did not possess a distinct information security budget and 62% of these organisations did not effectively communicate the costs associated with information security to the relevant business units and process owners.

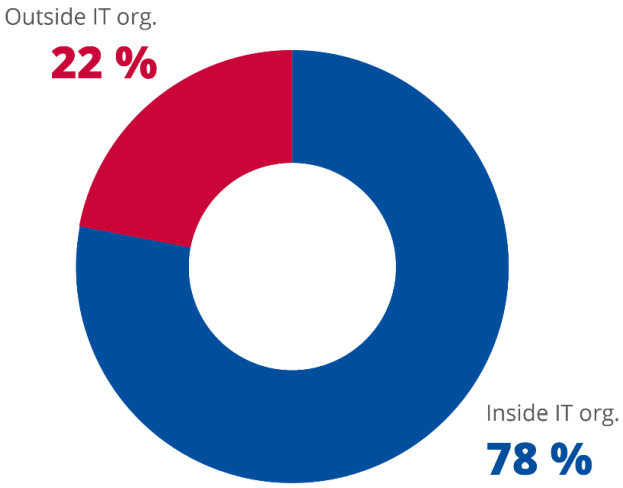
[4] https://www.gartner.com/document/3993567?ref=solrAll&refval=291617539
[5] https://www.gartner.com/document/code/752504?ref=authbody&refval=4004647

Figure 1: Overview of information security budgets (2020)



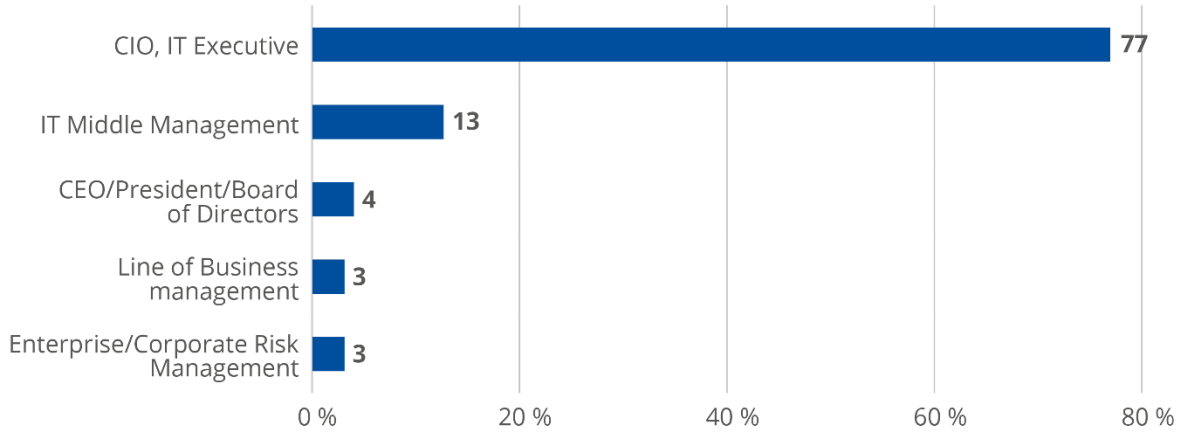
When evaluating the ownership of information security budgets (Figure 2) and the lines of hierarchical reporting (Figure 3), it must be observed that **information security is still widely recognised as an exclusive IT discipline**, without due consideration for the wider business impact thereof.

Figure 2: Location of information security budgets (2020)



Source: Gartner IT Key Metrics Data 2021: IT Security Measures, Worldwide

Figure 3: - Most senior level of reporting by IT security (2020)



Source: Gartner IT Key Metrics Data 2021: IT Security Measures, Worldwide

2.2 INFORMATION SECURITY SPENDING DISTRIBUTION

Further insights into the specific types of investments can be derived from a breakdown of the distribution of information security spending across functional security domains[6]. Following this approach, Gartner identifies the following categories.

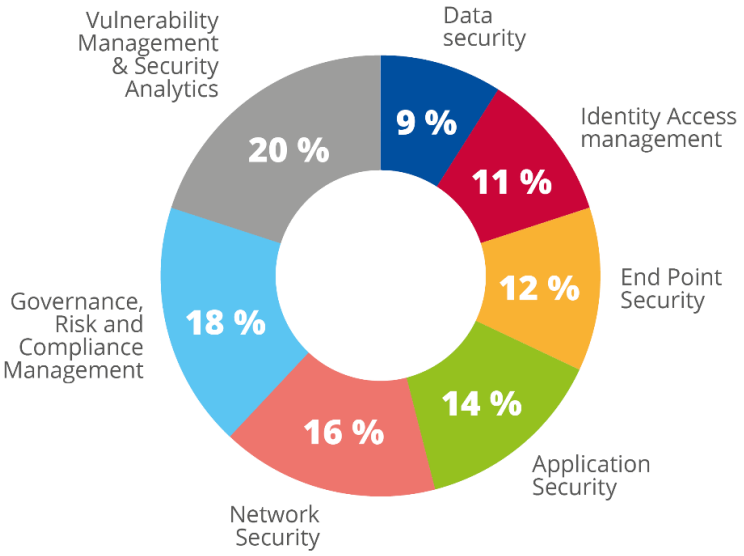
- **Vulnerability management** and **security analytics** investments focus on establishing proactive capabilities to minimise the impact of possible breaches once they occur.
- **Application security** encompasses the design, development and operation of a specific application. Furthermore, application security focuses on the configuration and deployment of both the application and its supporting components – such as network, operating system or database – with the objective of ensuring security.
- **Governance risk and compliance** focuses on how organisations mitigate a specific set of risks through developing strategies, policies, standards and awareness. It strives to manage risks in an effective and transparent manner while ensuring that legal and regulatory compliance requirements are met, and information security is embedded throughout the organisation.
- **Operational infrastructure security** – including network security, identity and access management, endpoint security and data security – focuses on protecting the network, the hosts and the data. Furthermore, it aims to guarantee secure and authorised access to systems.

Relevant data clearly indicates that organisations worldwide dedicate most of their security spending on the following three functional security domains:

- vulnerability management and security analytics, with a share of 20 %;
- governance, risk and compliance, with a share of 18 %;
- network security, with a share of 16 %.

[6] Annex B provides detailed definitions for the security domains referenced in Chapter 2.

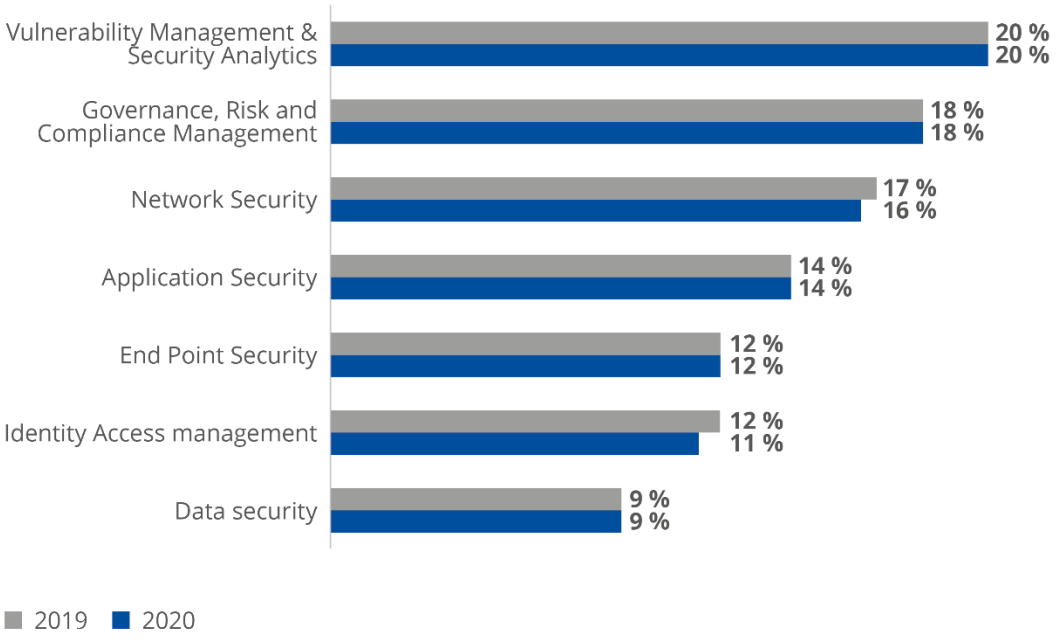
Figure 4: IT security spending distribution by functional area (2020)



Source: Gartner IT Key Metrics Data 2021: IT Security Measures, Worldwide

As illustrated in Figure 5, the year-on-year evolution between 2019 and 2020 shows only marginal changes in the overall distribution of IT security spending.

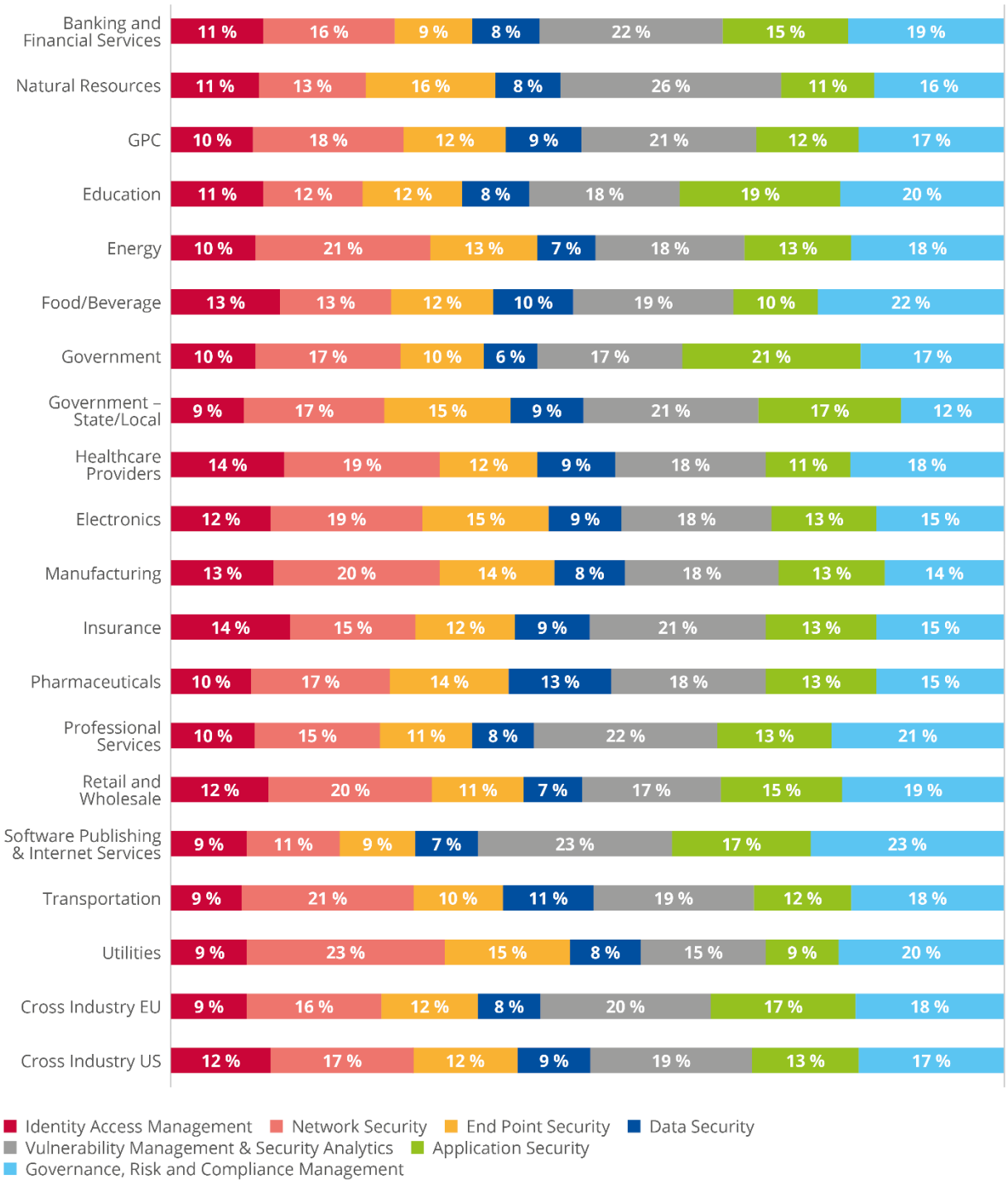
Figure 5: IT security spending distribution – year-on-year evolution by functional security domain



Sources: Gartner IT Key Metrics Data 2020: IT Security Measures, Gartner IT Key Metrics Data 2021: IT Security Measures, Worldwide

The distribution of IT spending between the different functional security domains has been relatively stable over the last 5 years. However, spending varies significantly between different industries, as illustrated in Figure 6.

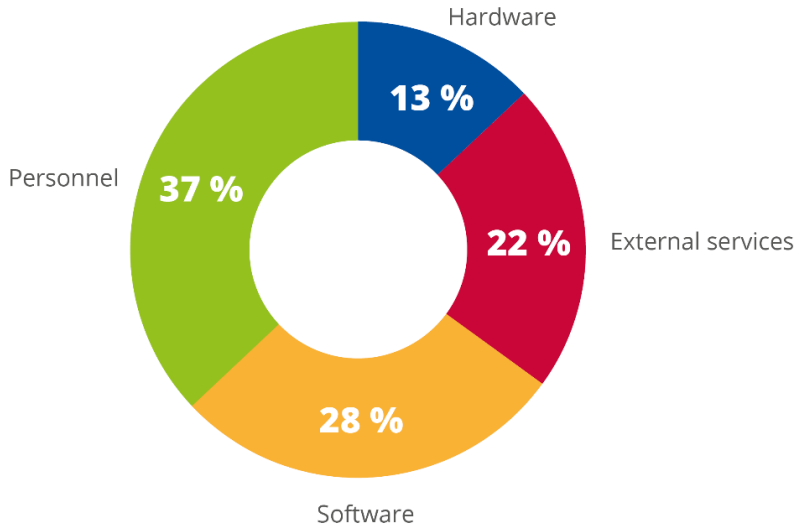
Figure 6: IT security spending distribution by functional area by industry (2020)



Source: Gartner IT Key Metrics Data 2021: IT Security Measures, EU countries

In terms of IT assets, the main area of spending for information security is personnel (37 %), followed by software (28 %) and hardware (13 %). The share of external services such as advisory, outsourcing or cloud-based services is 22 %.

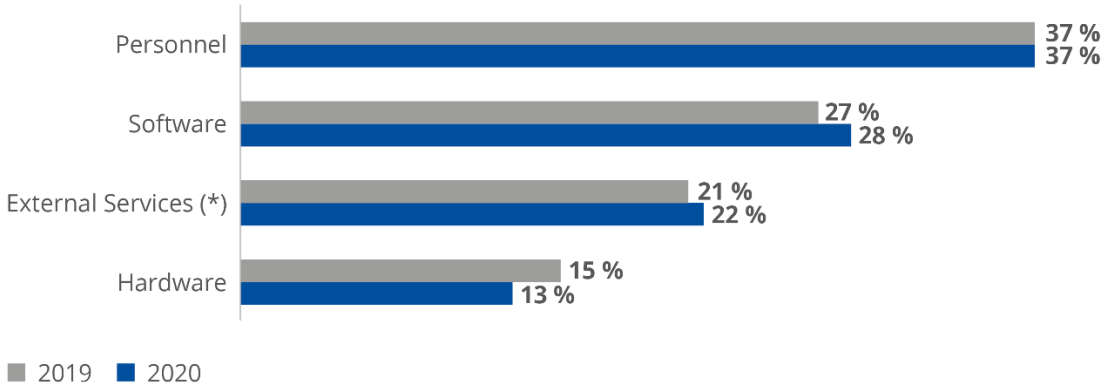
Figure 7: IT security spending distribution by asset class (2020)



Source: Gartner IT Key Metrics Data 2021: IT Security Measures, Worldwide

Similarly to the distribution by functional security domains, the distribution of spending by asset class remains relatively stable, despite a slight decrease (– 2 %) in hardware spending in 2020 compared to 2019.

Figure 8: IT security spending distribution – year-on-year evolution by asset class



(*) Note: External includes Outsourcing, Consulting, Management Services and Cloud providers

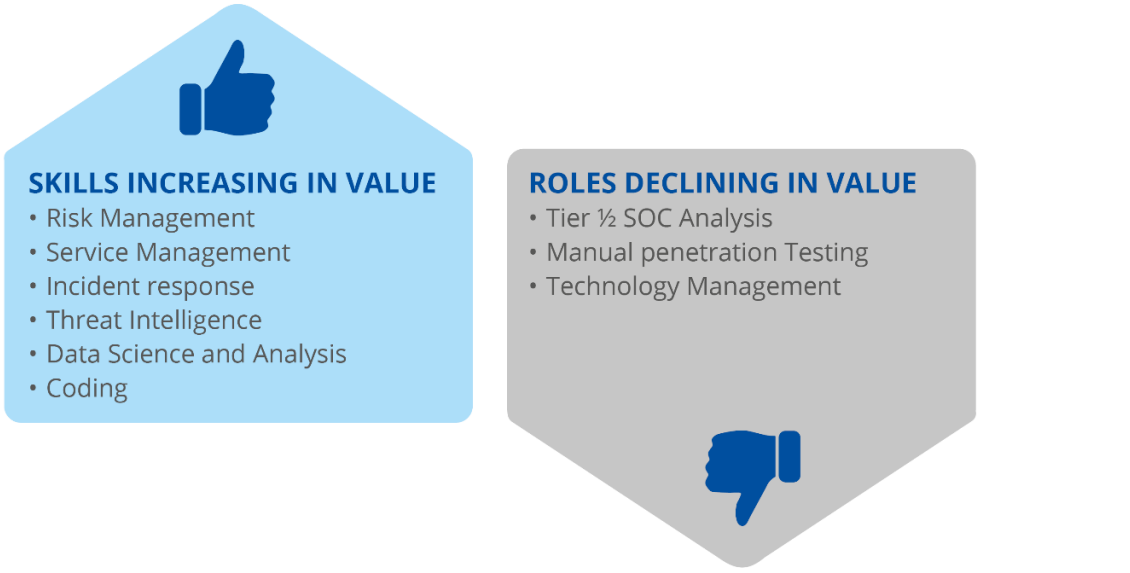
2.3 INFORMATION SECURITY STAFFING

As IT continues to develop exponentially, the demand for available and qualified information security professionals continues to grow. With competition steadily increasing, many organisations are facing real issues in finding talented people with the necessary skill sets and experience.

Figure 9: Global trends in information security staffing

In addition to the overall shortage of IT professionals, the increased focus on automation clearly affects the security skills and qualifications that are in market demand. As such, various skills that were in high demand during the previous years – such as manual penetration testing, tier 1/2 SOC[7] analysis or technology management – are expected to decrease in importance. They will be gradually replaced by skills in risk management, service management, incident response, threat intelligence, data science and analysis or coding.

Figure 10: The information security skills landscape dynamics

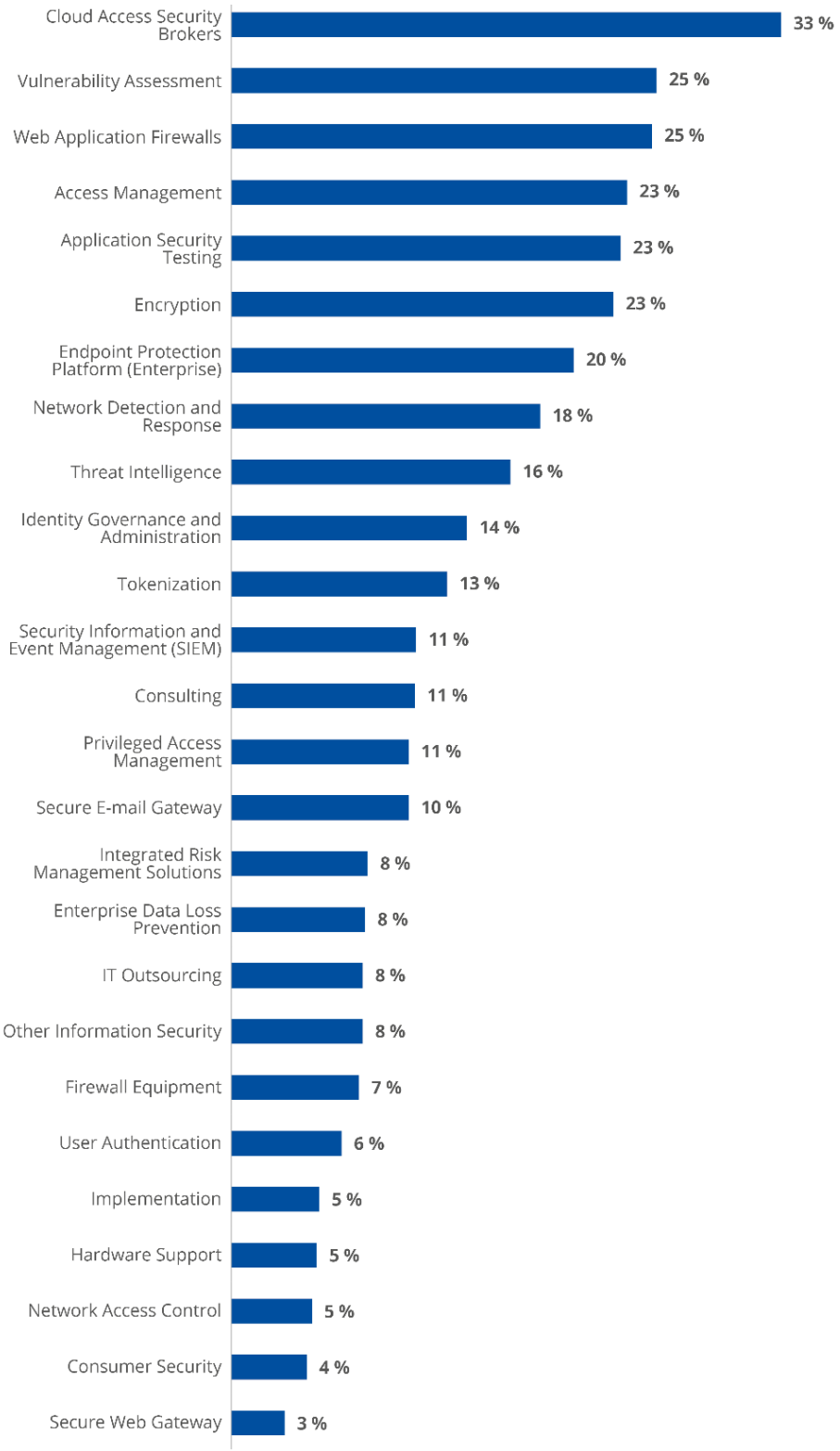


[7] Security Operations Centre

2.4 INFORMATION SECURITY MARKET OUTLOOK

In terms of market outlook, Gartner's IT security forecast indicates which solution types are expected to grow in the coming years. The main area of interest is cloud access security brokers (33 %), closely followed by vulnerability assessments and web application firewalls at 25 %. Furthermore, access management, application security testing and encryption are expected to benefit from a 23 % increase in market interest.

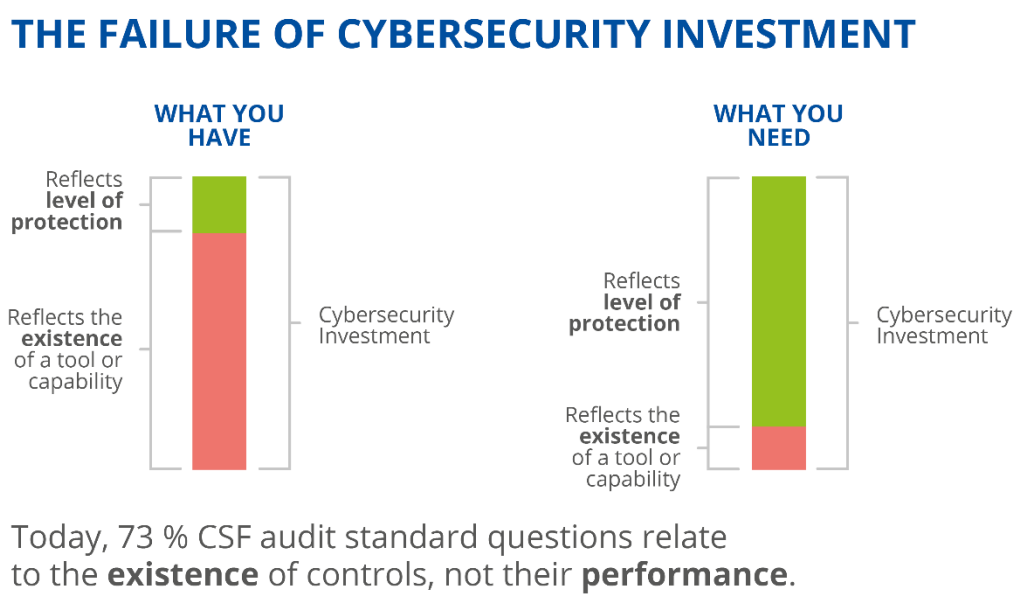
Figure 11: IT Security forecast — compound annual growth rate, 2020 – 2025 (%) by solution type



2.5 SECURITY PERFORMANCE

Despite multiple risks resulting from the COVID-19 pandemic – such as the new work environment and environmental, social and governance concerns – information security controls failure was listed as the top emerging risk within Gartner's latest Emerging Risks Monitor Report. To assess the maturity of an organisation, the mere existence of cybersecurity framework (CSF) controls or tooling does not necessarily imply a high level of cybersecurity maturity, their performance and effectiveness are more appropriate measures.

Figure 12: Cybersecurity controls – existence vs performance



2.6 FUTURE OF INFORMATION SECURITY

According to Gartner, it is estimated that[8]:

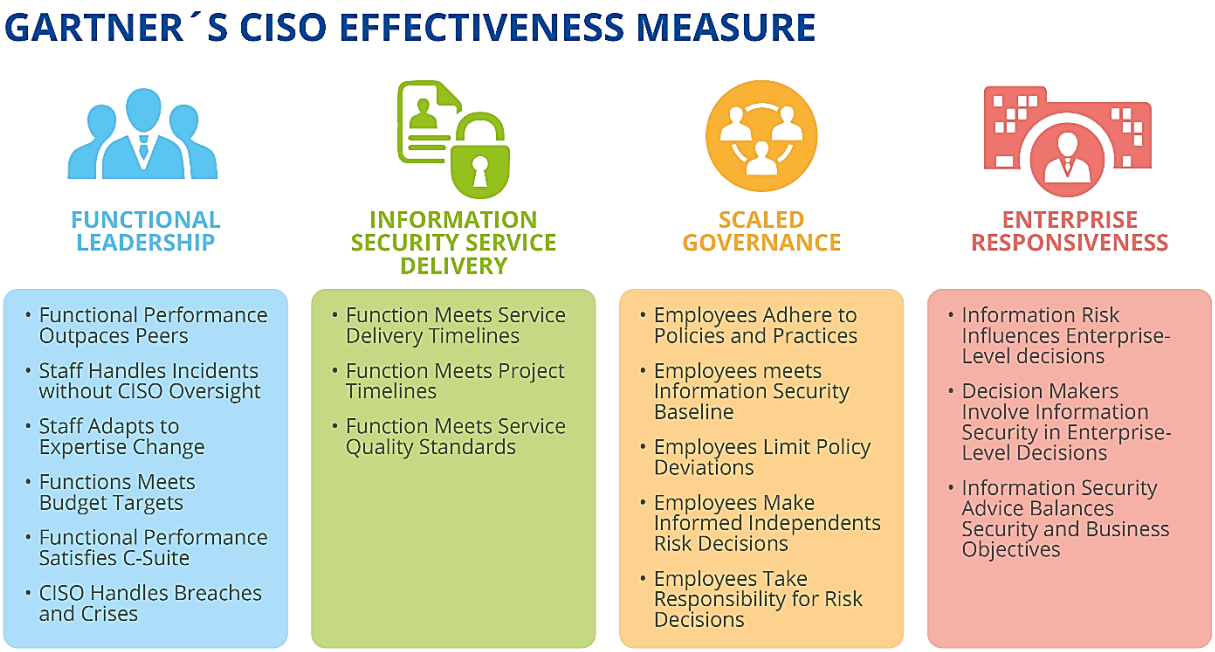
- by 2022, 30 % of all security teams will have increased the number of employees working remotely on a permanent basis.
- by 2025, 40 % of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% today.
- by 2024, 60 % of Chief Information Security Officers (CISO) will establish critical partnerships with key market-facing executives in sales, finance and marketing, up from less than 20 % today.
- by 2025, 50 % of asset-intensive organisations will converge their cyber, physical and supply chain security teams under a single Chief Security Officer (CSO) role that reports directly to the CEO.

[8] Gartner Predicts 2021: Cybersecurity Program Management and IT Risk Management ID G00735901 January 2021

2.7 CISO EFFECTIVENESS

The operating environment of CISOs is becoming more complex. Distributed decision-making has expanded the volume and variety of information risk decisions to support, while regulators are approaching data privacy with greater scrutiny and executive teams and boards of directors are starting to turn their sights toward information risk and its implications for strategic planning. All of these changes emphasise the need for CISOs to be effective in their roles.

Figure 13: Effectiveness of the CISO role



Based on Gartner Research, only 12 % of CISOs excel in all categories as defined in the CISO Effectiveness Index.

3. INFORMATION SECURITY INVESTMENTS FOR THE NIS DIRECTIVE IMPLEMENTATION

3.1 METHODOLOGY

This study is based on a dedicated market survey conducted among 947 organisations – with a minimum of 35 per Member State – that were identified as OES/DSP under the NIS Directive. The quantitative metrics in the survey have been analysed on the basis of **median** and **average** approaches in order for the reader to appreciate both viewpoints.

Although the median value should be regarded as the typical value for an OES/DSP within a specific sector or country, the average value will often be higher as it is affected by large organisations (statistical outliers) that do not necessarily reflect the populated and fragmented market of most of the sectors and countries that were analysed.

The specific market composition of each sector in terms of company size has also been analysed by categorising the organisations in terms of small and medium-sized enterprises (SMEs) or large enterprises, based on the EU definition[9] (see Chapter 4).

By way of example:

- the median value for information security spending amounts to EUR 2 million in 2020 (Section 3.2.2), which implies that a typical OES/DSP within the EU spends around EUR 2 million in information security yearly;
- contrasting this median value, the average information security spending for OES/DSP in the EU amounts to EUR 10.4 million, but this number is skewed by large organisations that possess significant budgets dedicated to information security.

With regard to the qualitative metrics in the study, the distribution of the organisations' answers has been calculated as a percentage, so as to balance the weight of each answer against the others.

Finally, additional information and insights on security performance have been derived from the initial data set by cross-analysing answers from multiple questions (Chapter 5).

[9] https://ec.europa.eu/growth/smes/sme-definition_en

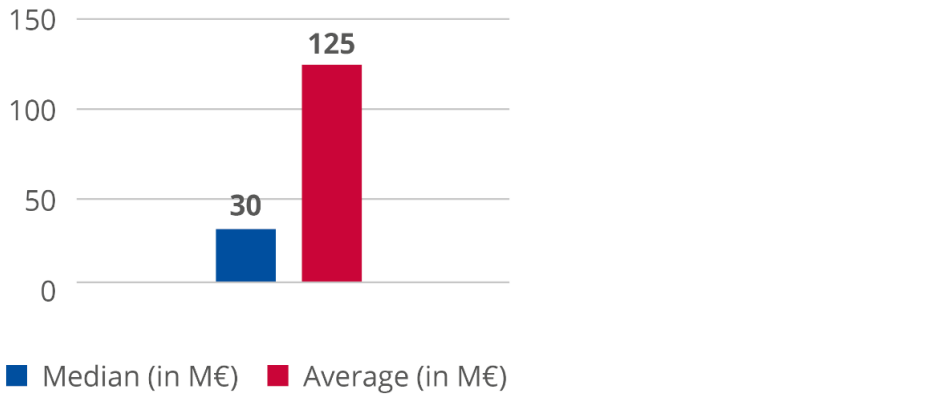
3.2 INFORMATION SECURITY AND NIS SPENDING

Key findings
A typical OES/DSP spent on median EUR 30 million on IT in 2020, of which EUR 2 million was earmarked for information security.
A typical OES/DSP in the EU earmarks on median 7.7 % of its IT investment for information security.
While the banking and energy sectors have the highest IT and information security spending in the EU, digital infrastructure and cloud computing have the highest information security vs IT spending.
A typical OES/DSP in the EU spends around EUR 40 000 on implementing the requirements of the NIS directive.
Governance, risk and compliance, network security and vulnerability management are the predominant areas of investment for the implementation of the directive.
The most procured tools and services are network intrusion detection and prevention, security awareness and training, vulnerability assessment tooling, security incident and event management, and risk assessment and business impact analysis.

3.2.1 IT spending

Survey question: **What was your organisation's estimated IT budget/spending in euro for 2020 (including capital expenditures (CAPEX) and operating expenses (OPEX) for hardware, software, internal personnel, contractors and outsourcing spending)?**

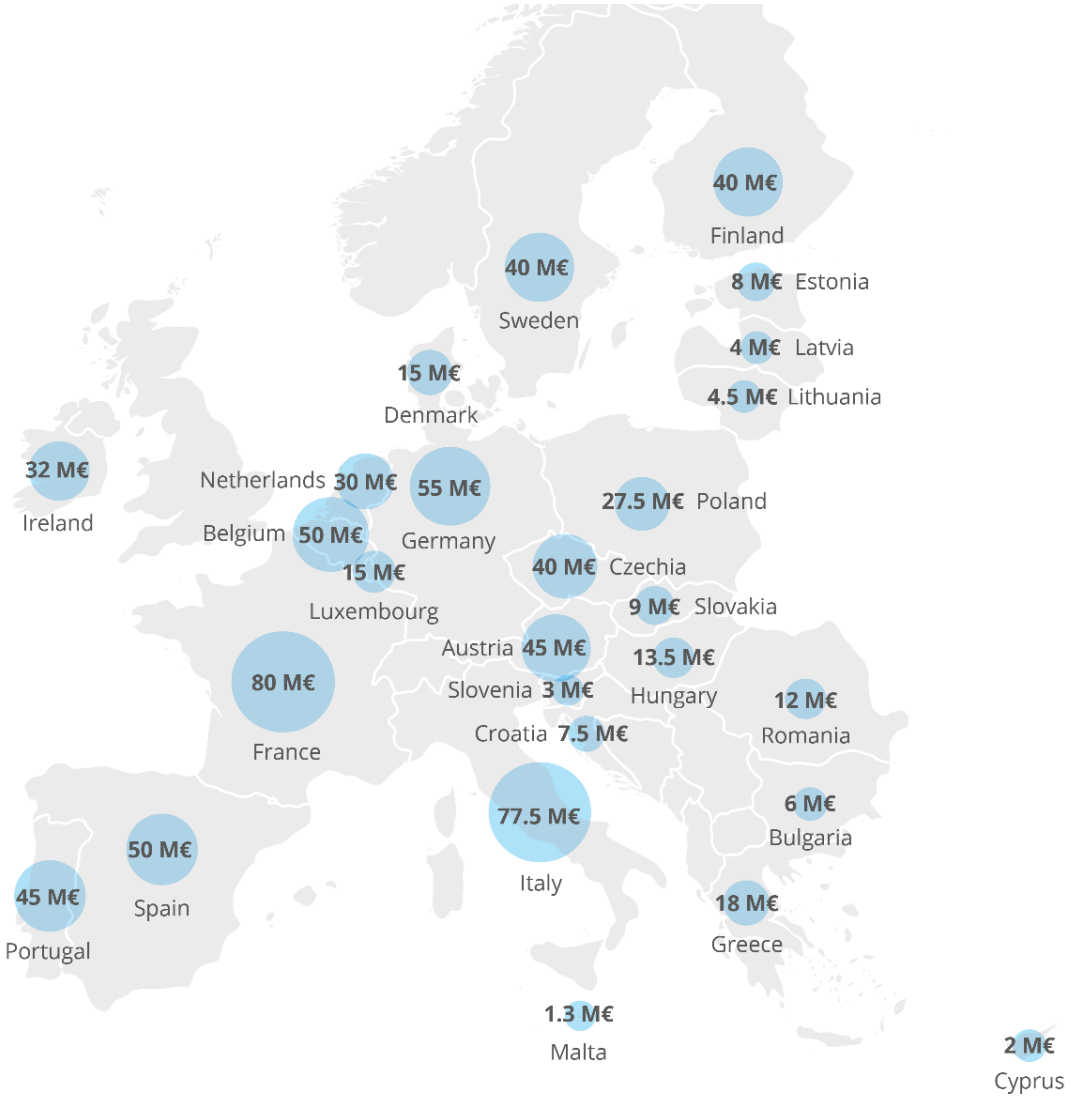
Figure 14: IT spending



n=930
[17 organisations responded with – "I have no visibility on the budget"]

The median IT spending of a typical OES/DSP in the EU was EUR 30 million in 2020, while the average value of IT spending was EUR 125 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.

Figure 15: IT spending of OES/DSP surveyed per Member State



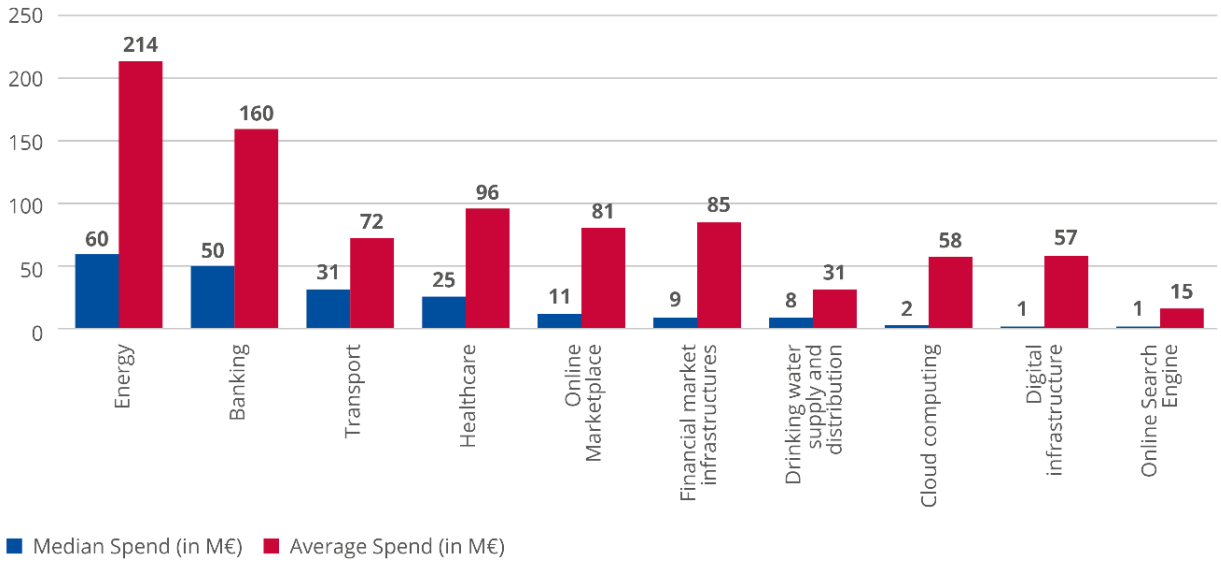
n=930
[17 organisations responded with – "I have no visibility on the budget"]

The map visualisations throughout the report depict data collected from the OES/DSP surveyed from each Member State.

NB: The map visualisations throughout the report depict data collected from the OES/DSP surveyed from each Member State. Hence, data on investments refers to average among surveyed OES/DPS and not Member State investments. In addition, when interpreting these figures, the market fragmentation / average operator size in each Member State, as well as the criteria for identifying OES/DSP in each Member State – including OES/DPS size – need to be factored in.

The survey data indicates that median IT spending is highest (EUR 60 million) within the energy and banking sectors (EUR 50 million), significantly exceeding IT spending in other sectors as illustrated in Figure 16. Furthermore, online search engines and digital infrastructure have the lowest IT spending across all sectors, with a median spending of EUR 1 million.

Figure 16: IT spending by sector

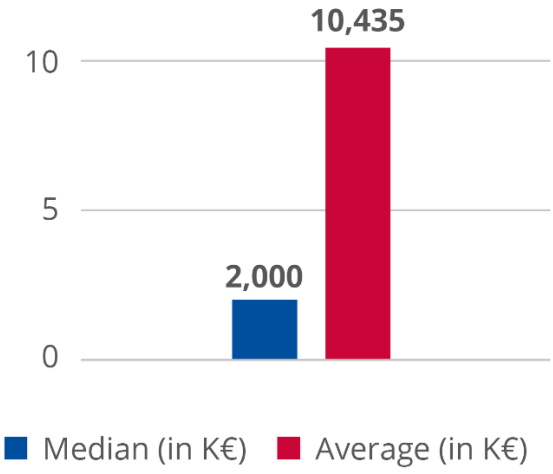


n=930
[17 organisations responded with – "I have no visibility on the budget"]

3.2.2 Information security spending

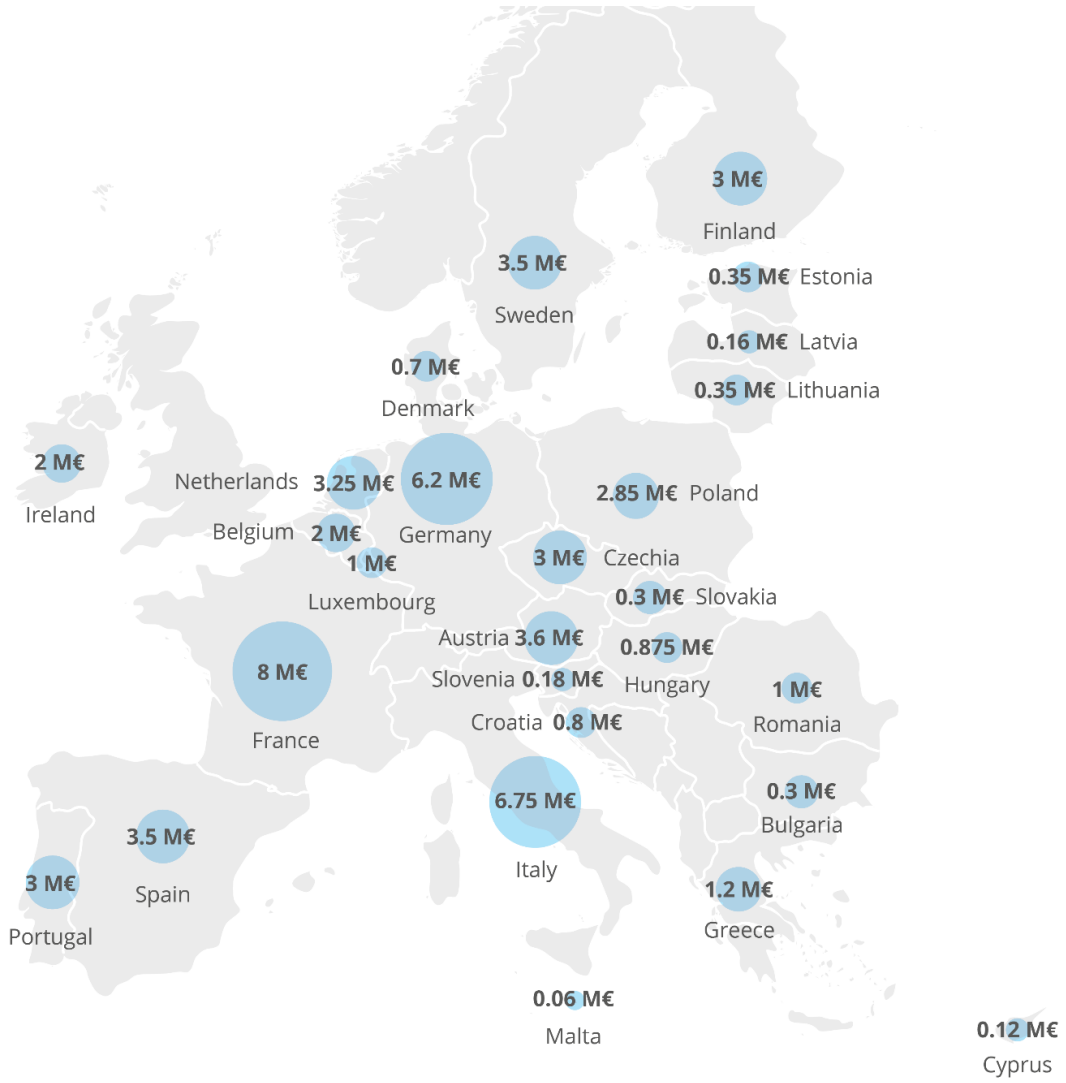
Survey question: **What was your organisation's estimated information security budget/spending in euro for 2020 (including CAPEX and OPEX for hardware, software, internal personnel, contractors and outsourcing spending)?**

Figure 17: Information security spending



The survey data indicates that the median spending for information security of a typical OES/DSP in the EU was EUR 2 million in 2020, while the average spending was EUR 10.4 million.

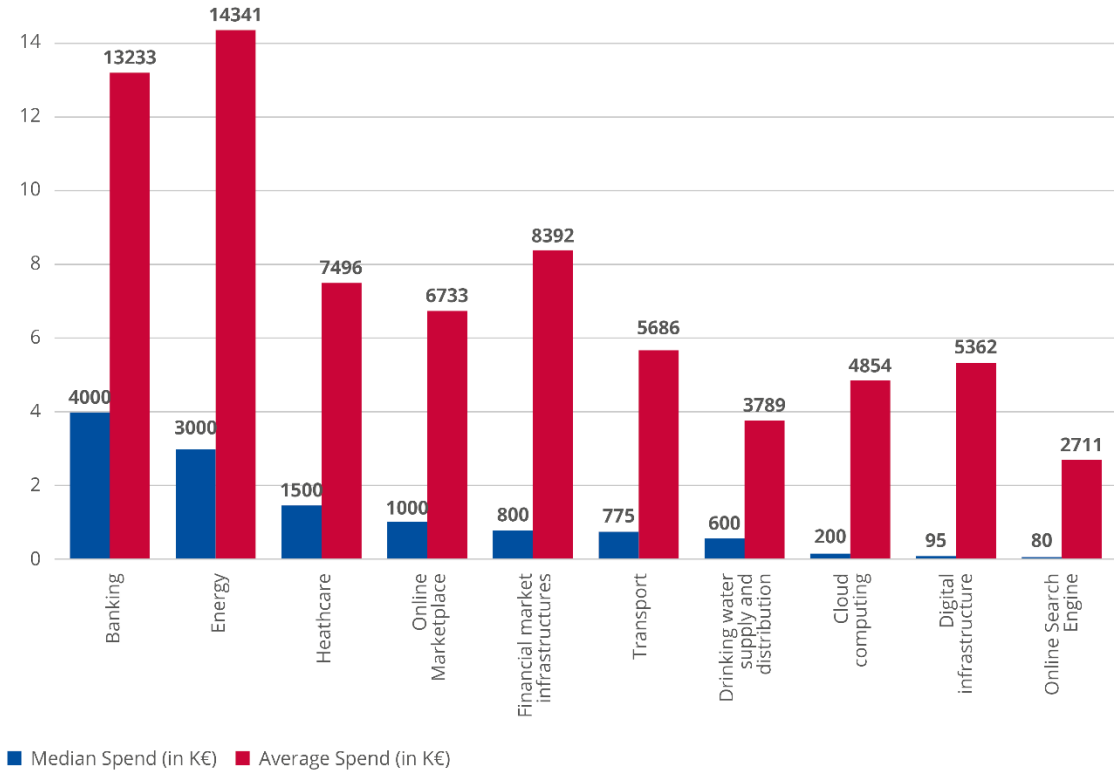
Figure 18: Information security spending of OES/DSP surveyed per Member State



n=941
[6 organisations responded with – "I have no visibility on the budget"]

In a manner similar to the total IT spending, the banking sector (EUR 4 million) and the energy sector (EUR 3 million) account for the highest median spending per sector. Moreover, the information security spend of digital infrastructure and online search engine companies is the lowest, amounting to a median spending below EUR 100 000.

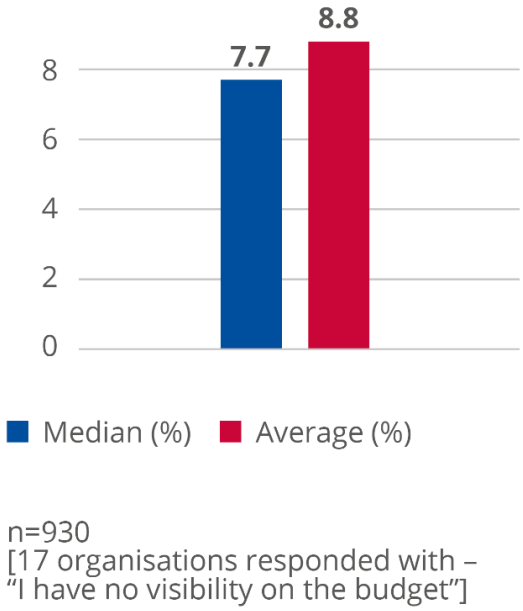
Figure 19: Information security spending by sector



3.2.3 Information security spending as a share of IT spending

In order to determine the importance of information security spending in a typical OES/DSP, the relative share of information security spending against overall IT spending was calculated and is depicted in Figure 20.

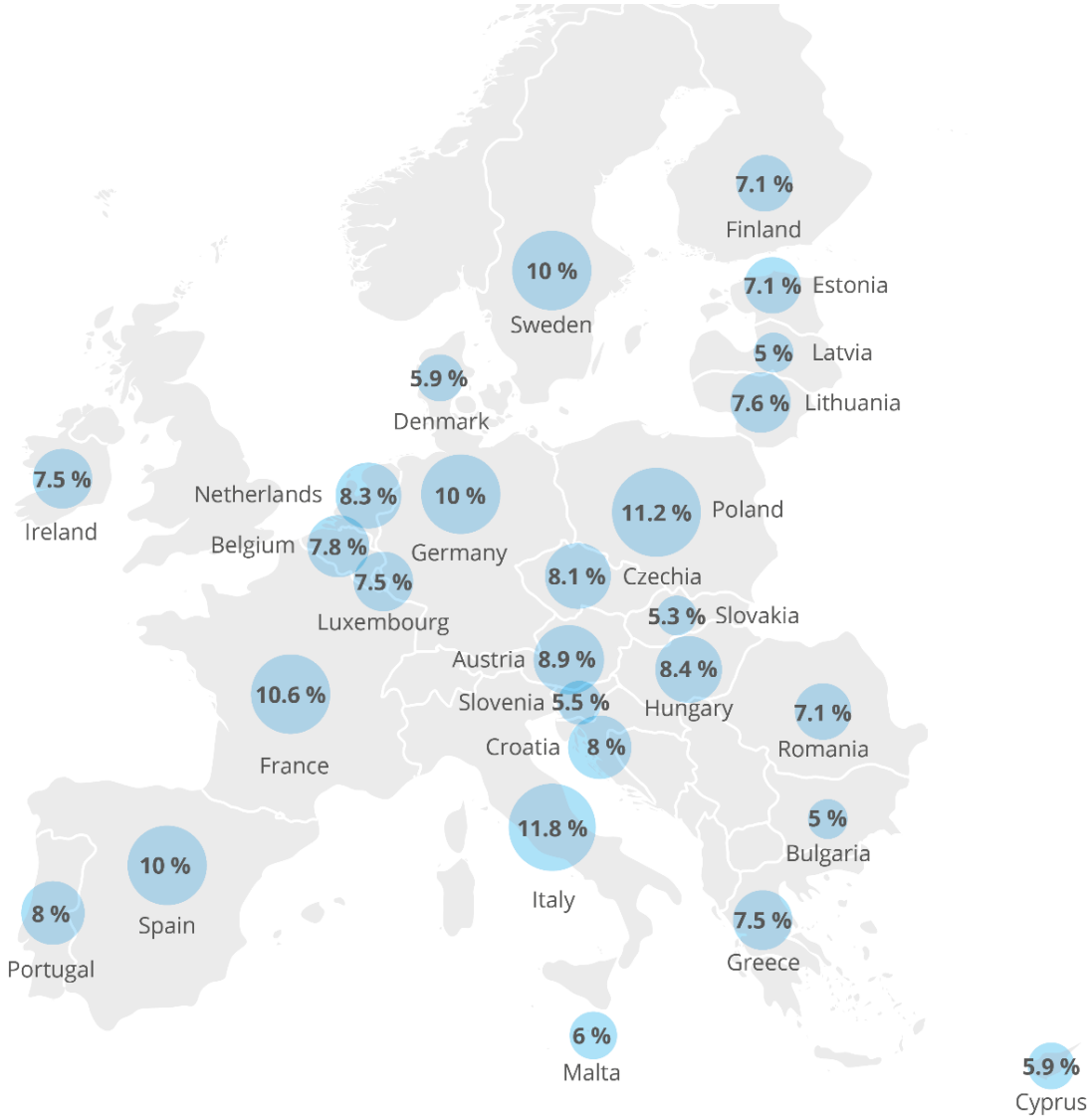
Figure 20: Information security spending as a share of IT spending



n=930
[17 organisations responded with –
"I have no visibility on the budget"]

As per the median value, a typical OES/DSP in the EU earmarks 7.7 % of its IT investments for information security, while the average value is 8.8 %.

Figure 21: Information security spending as a share of IT spending of OES/DSP surveyed per Member State

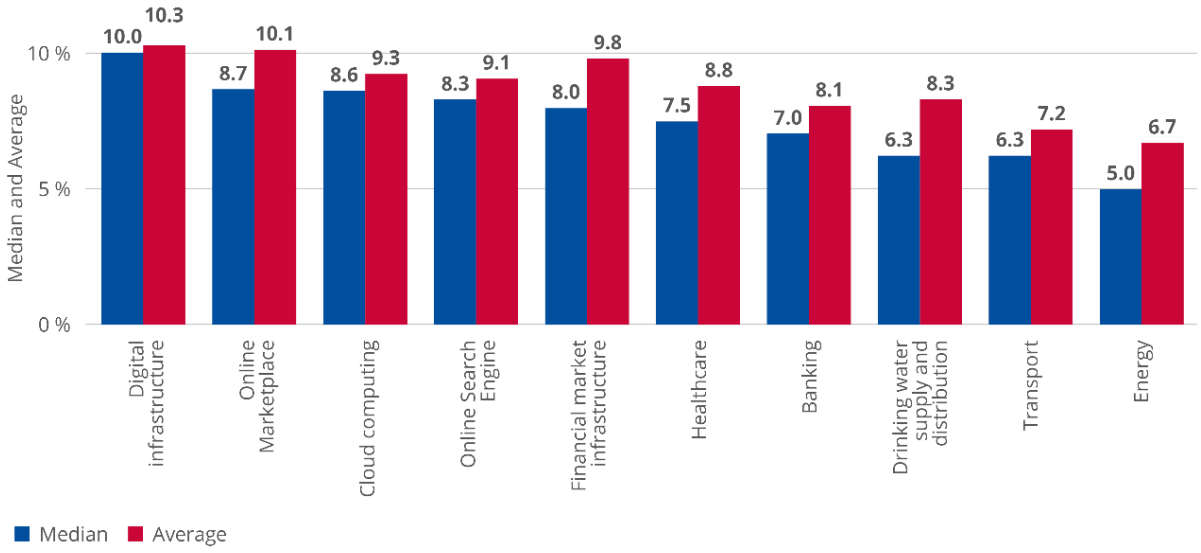


n=930
[17 organisations responded with – "I have no visibility on the budget"]

Digital infrastructure has the highest information security vs IT spending (10 %), followed closely by cloud computing (9 %) and online marketplaces (8.7 %). Drinking water supply and distribution, energy and transport bring up the rear, with values of information security vs IT spending lower than 7 %.

Even though the energy and banking sectors have a higher IT and Information security spending in absolute figures, their respective shares of information security vs IT spending are lower than most other sectors.

Figure 22: Information security spending as a share of IT spending by sector



n=930
[17 organisations responded with – "I have no visibility on the budget"]

3.2.4 NIS Directive spending

Survey question: **What was your organisation's estimated budget dedicated to the NIS Directive implementation (e.g. including CAPEX and OPEX for hardware, software, infrastructure, business continuity, internal personnel, contractors and outsourcing spending)?**

Out of 947 respondents, 775 (approx. 82 %) organisations have implemented the NIS Directive, while 635 (67 %) organisations require additional budget to implement all its requirements. Furthermore, 172 (approx. 18 %) organisations have not yet implemented the NIS Directive.

Figure 23: Implementation of the NIS Directive

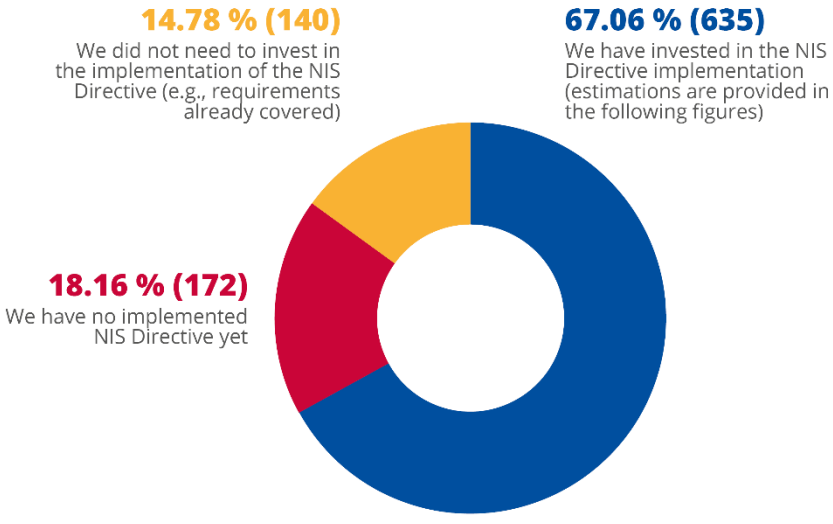
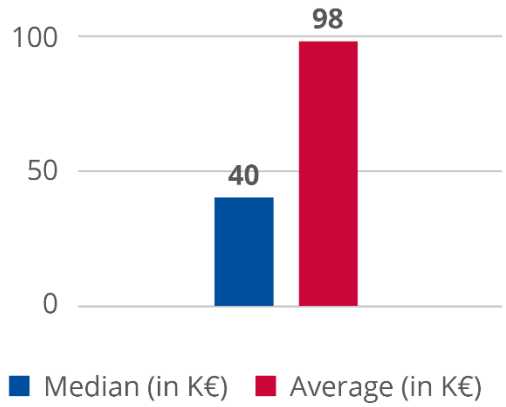
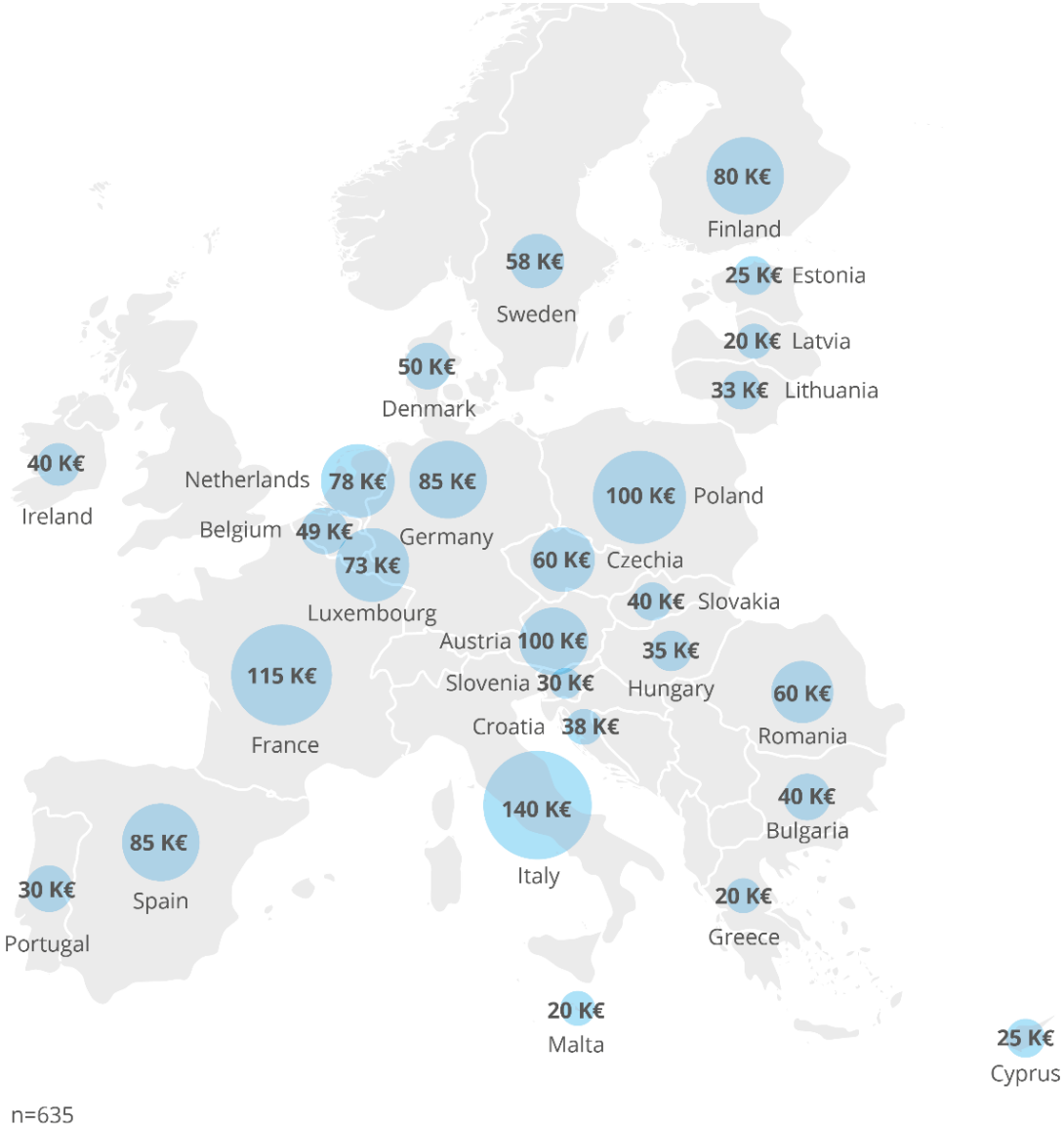


Figure 24: Budget allocated to implementing the NIS Directive



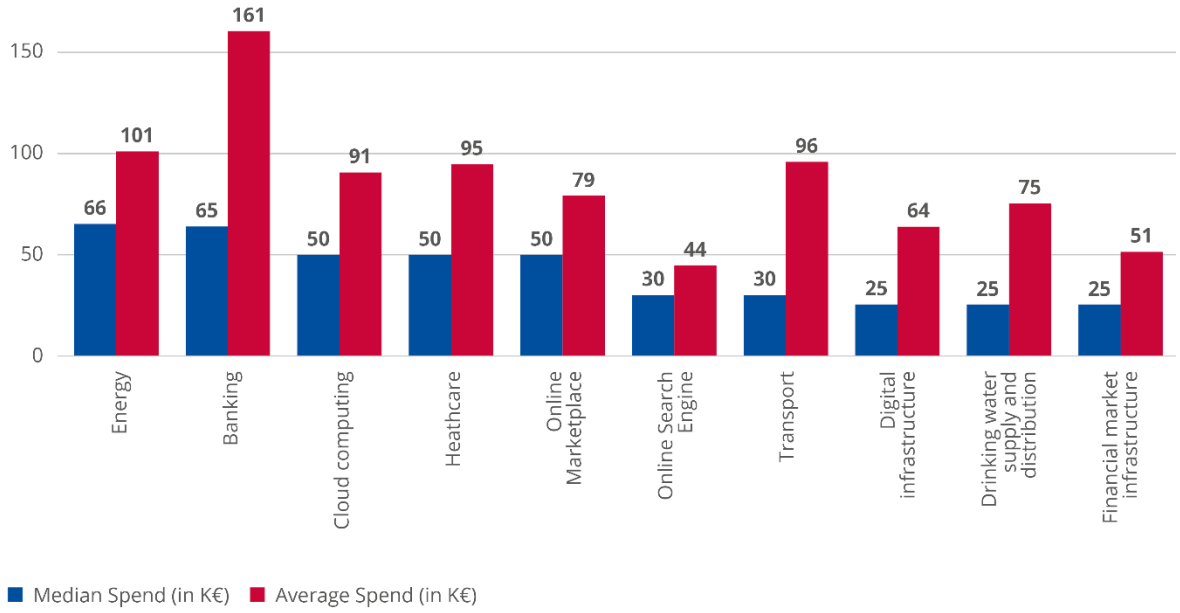
As per the median value, a typical OES/DSP in the EU spends EUR 40 000 on implementing the NIS Directive, while on average the spending amounts to EUR 98 000.

Figure 25: Budget allocated to implementing the NIS Directive for OES/DSP surveyed per Member State



The survey results indicate that a typical OES/DSP from the energy sector has allocated the highest budget to achieve implementation, with a median spending of EUR 66 000, closely followed by organisations in the banking sector with a median spending of EUR 65 000 for implementation. Drinking water supply and distribution, financial market infrastructures and digital infrastructure have allocated the lowest budgets to achieve compliance, with a median spending of just EUR 25 000.

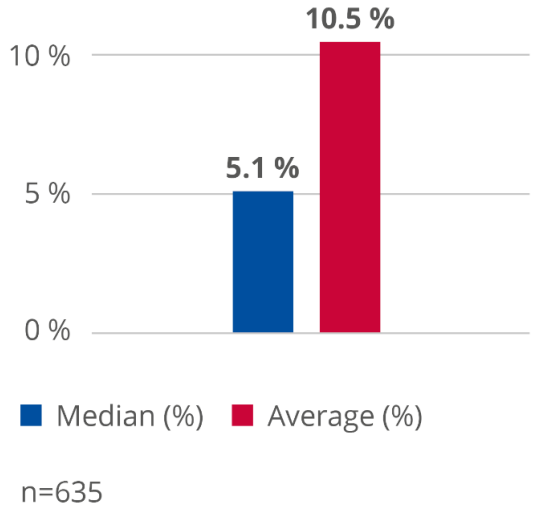
Figure 26: Budget allocated to implementing the NIS Directive by sector



3.2.5 NIS spending as a share of information security spending

In order to determine the impact of NIS spending in a typical OES/DSP, we calculated the relative share of NIS spending against overall information security spending, as illustrated in Figure 27.

Figure 27: NIS spending as a share of total information security spending



As per the median value, the typical spending on implementing the NIS directive within an OES/DSP amounts to 5.1 % of their overall information security spending, while the average value is 10.5 %.

Figure 28: NIS spending as a share of total information security spending for OES/DSP surveyed per Member State

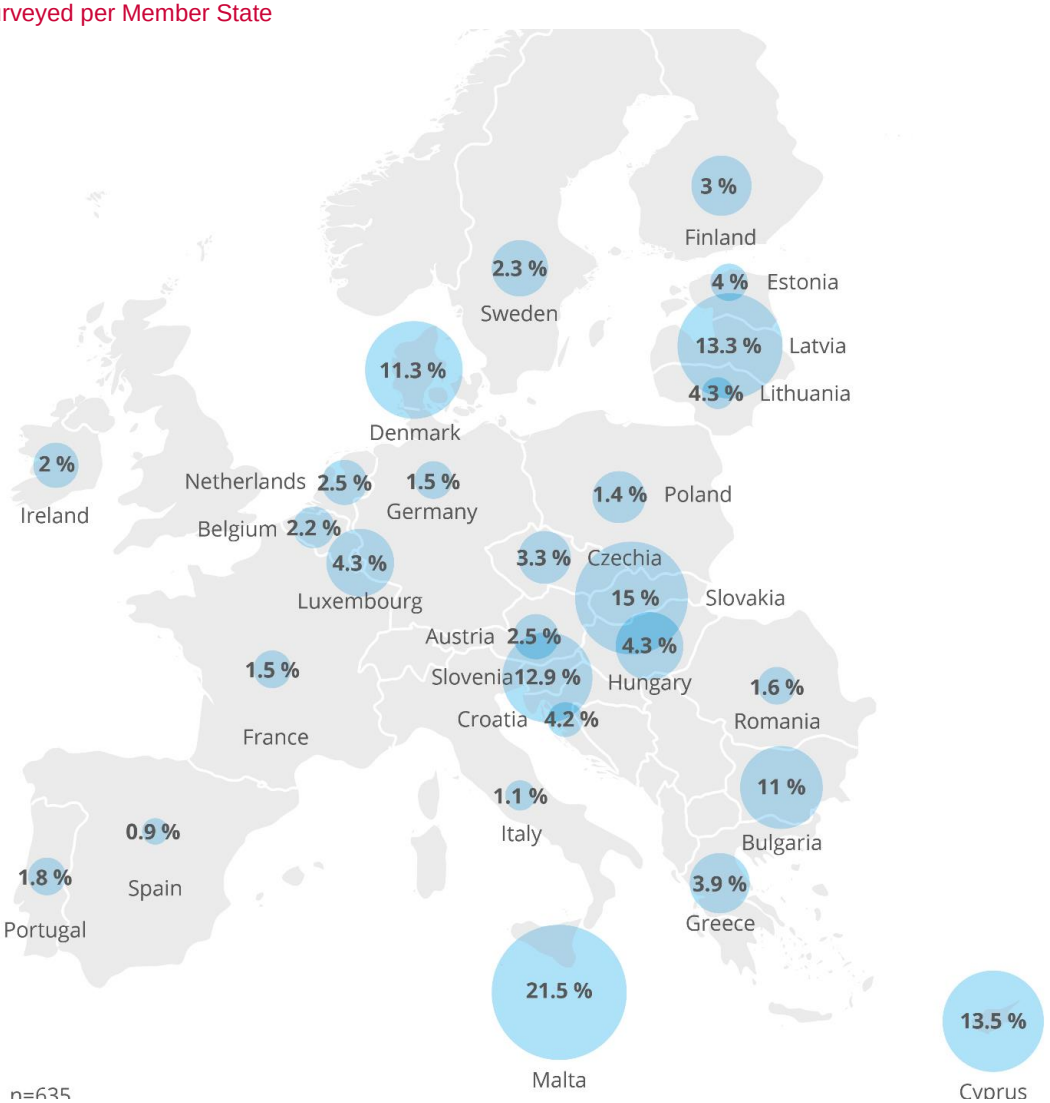
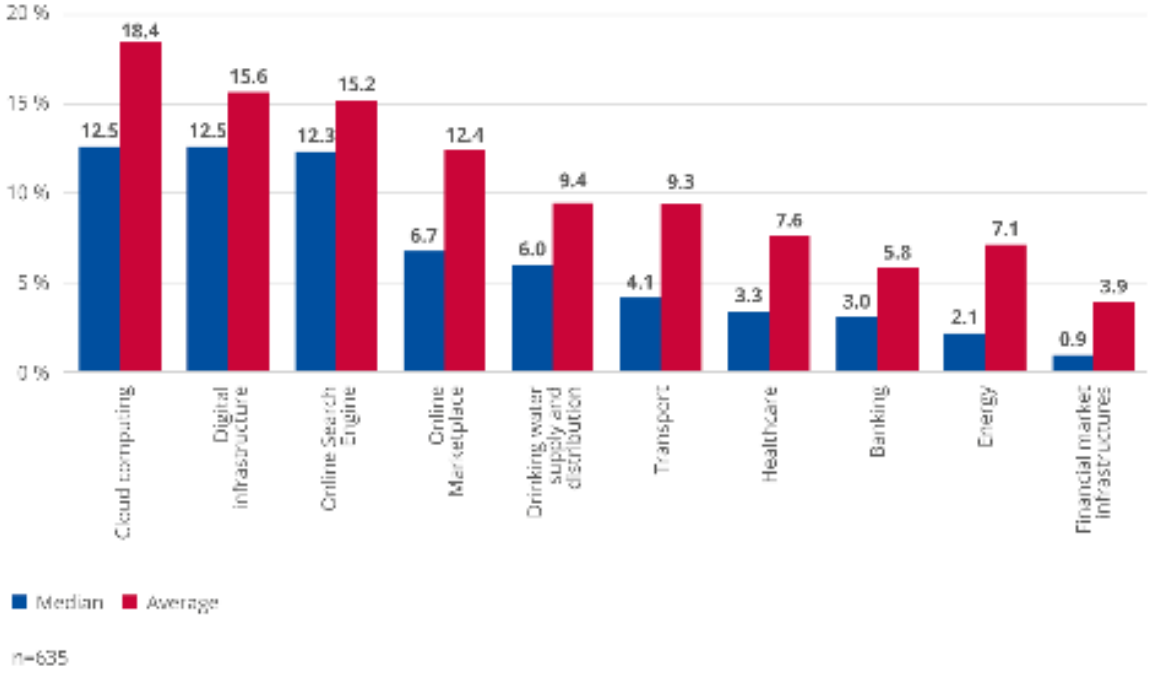


Figure 29: NIS spending as a share of total information security spending by sector



3.2.6 Top three security domains for implementing the NIS Directive

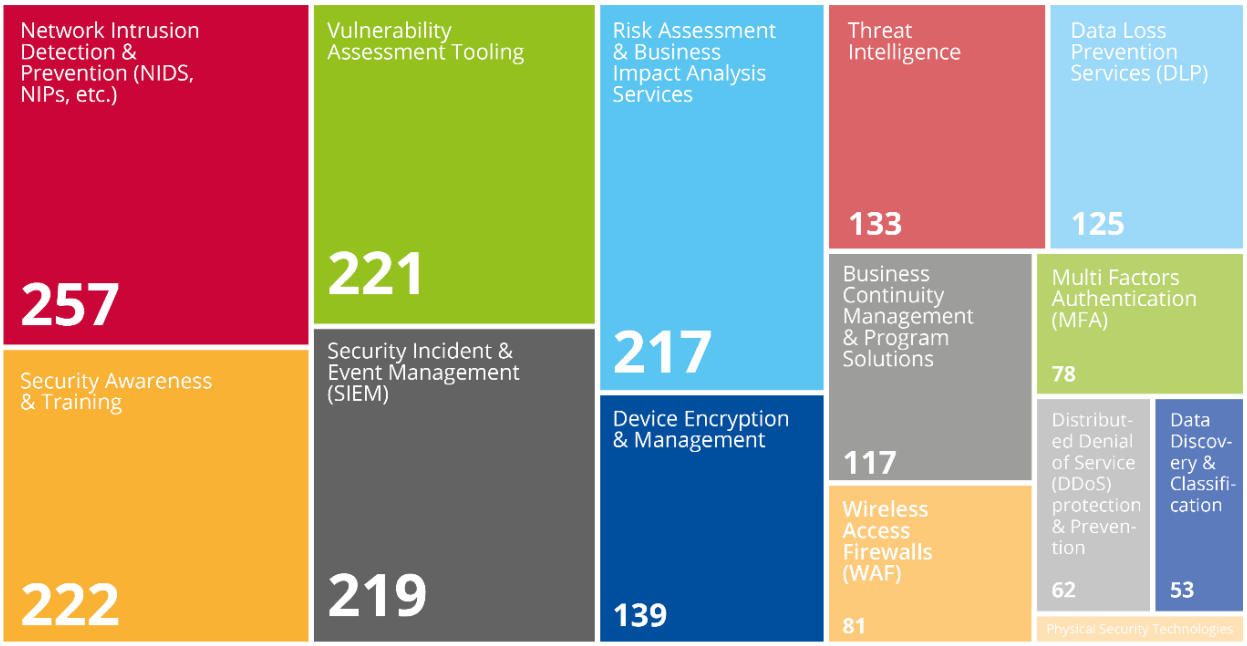
Governance risk and compliance has been reported as the main security domain where organisations have invested in the context of implementing NIS directive, with 383 organisations reporting investments in this domain.

Network security and vulnerability management has also seen investments from a large number of organisations, with 357 of them investing in network security and 316 investing in vulnerability management.

On the contrary, **business continuity management** has seen little investment in the context of NIS implementation, with only 69 organisations identifying this security domain in their top three domains.

Survey question: **What are the top three security domains where your organisation invested the most to implement the NIS Directive?**

Figure 30: Security domains for implementing the NIS Directive



n=631
[4 organisations did not procure any technologies]

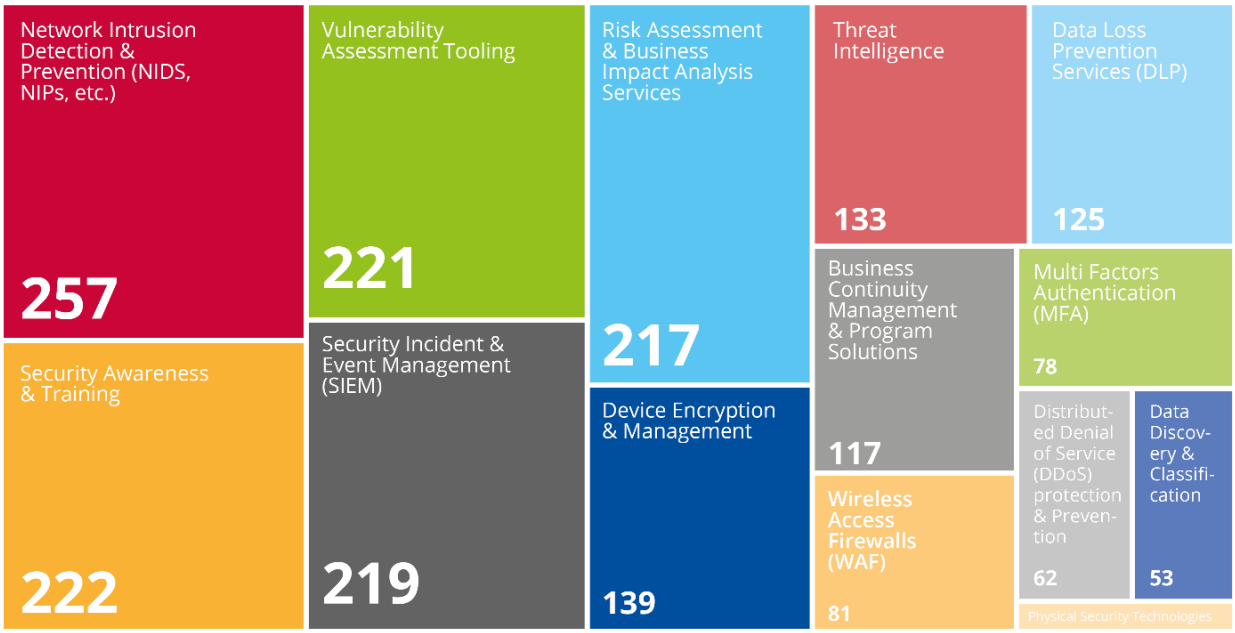
3.2.7 Technologies and services procured for the NIS Directive

The technology and services associated with **network intrusion detection and prevention** were the most procured in the context of NIS implementation, with 257 organisations reporting procurements in this domain.

This domain – along with **security awareness and training** (222 responses), **vulnerability assessment tooling** (221 responses), **security incident and event management** (219 responses) and **risk assessment and business impact analysis** (217 responses) – is one of the five main technologies and services that were procured in the context of NIS implementation.

Survey question: **Which of the following technologies or services did you procure because of the NIS directive implementation?**

Figure 31: Technologies and services procured for implementing the NIS Directive



n=631
[4 organisations did not procure any technologies]

3.3 INFORMATION SECURITY AND NIS STAFFING

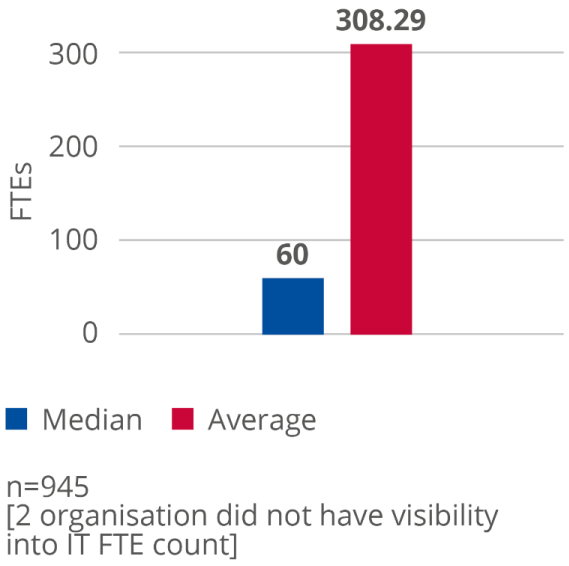
Key findings
A typical OES/DSP employs on median 60 IT FTEs, of which seven are dedicated information security FTEs.
Almost 50 % of the established OES/DSP within the EU hire contractors to support their information security workforce.
Almost 50 % of the established OES/DSP within the EU hired new staff members in the context of implementing the directive, with a median of four FTEs per sector.
A typical OES/DSP in the EU employs on median two dedicated FTEs for incident response.

3.3.1 IT FTEs

There are large discrepancies in the total number of IT FTEs in OES/DSP among the Member States. Median values range from over 400 IT employees in Italy to 20 employees in Latvia or Slovenia. Whereas these are total values – possibly reflecting the underlying sector structure and company size – a lower number of FTEs does not necessarily imply a lower level of security maturity. The data shows a disparity between the median and average values, which indicates that most organisations employ a low number of FTEs while larger organisations engage a substantial number of IT FTEs.

Survey question: What was your organisation's estimated number of IT FTEs for 2020 including internal staff and contractors?

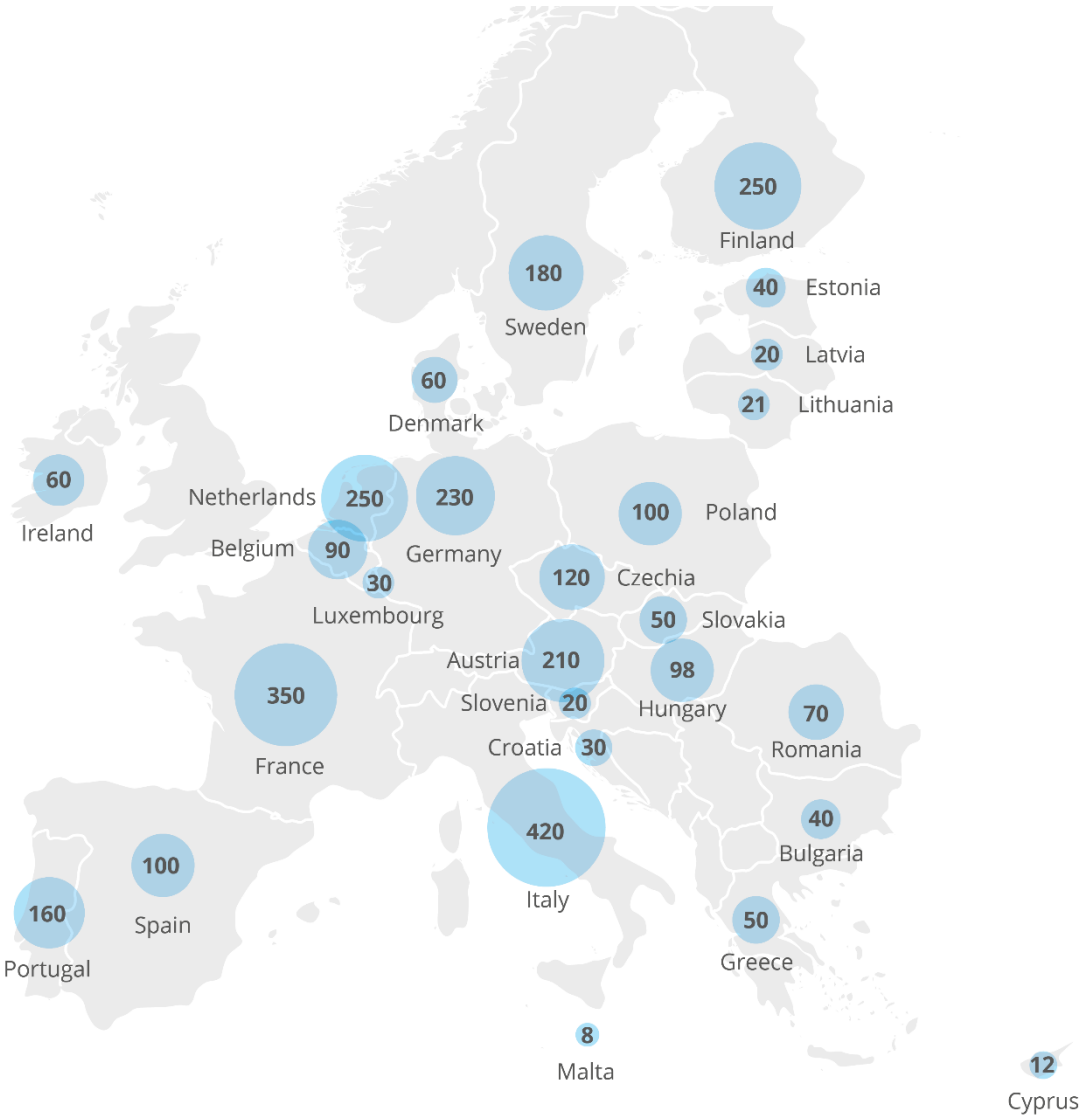
Figure 32: IT FTEs



The survey data indicates that a typical OES/DSP in Italy and France has the highest number of IT FTEs, with median values of 420 and 350 FTEs respectively.

However, these figures must be read with due regard for the structure of the sector and the size of the organisations surveyed for each Member State. For instance, French OES/DSP have the highest average number of employees.

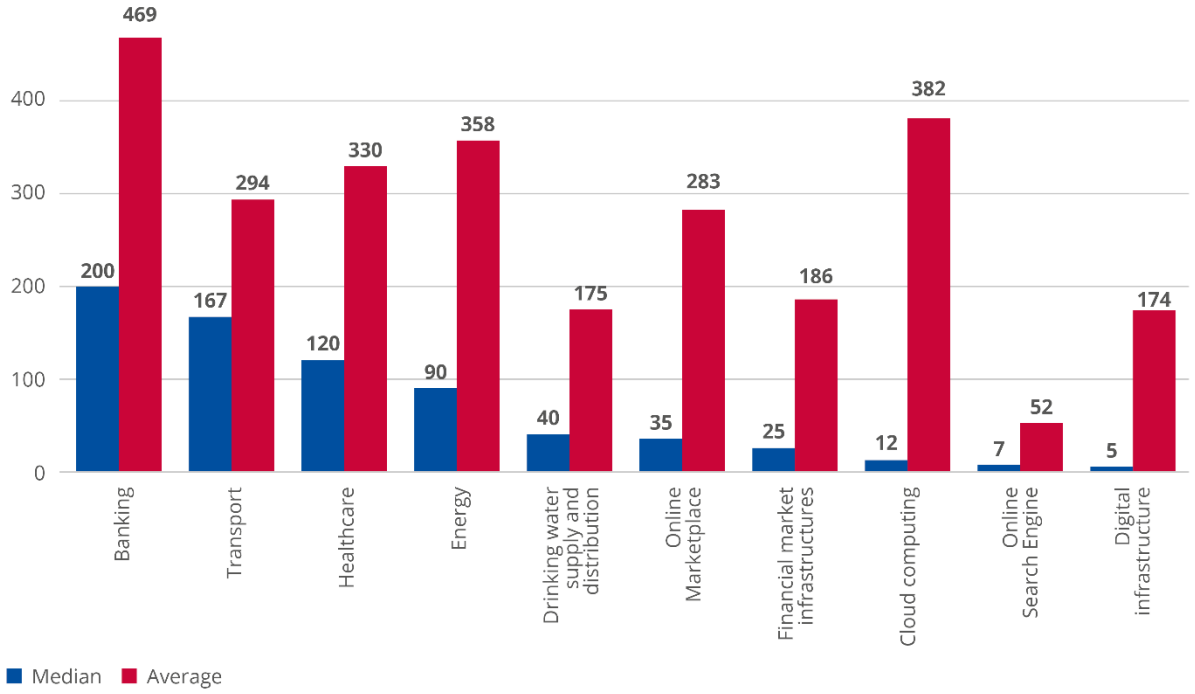
Figure 33: IT FTEs of OES/DSP surveyed per Member State



n=945
[2 organisation did not have visibility into IT FTE count]

As illustrated in Figure 34, there are large discrepancies in the number of IT FTEs across sectors. For example, the banking sector has the largest median value of 200 FTEs, which is 15 % higher than the median value of the transport sector, which employs 167 IT FTEs on median. However, online search engines and digital infrastructure have a significantly lower median value of seven IT FTEs.

Figure 34: IT FTEs by sector

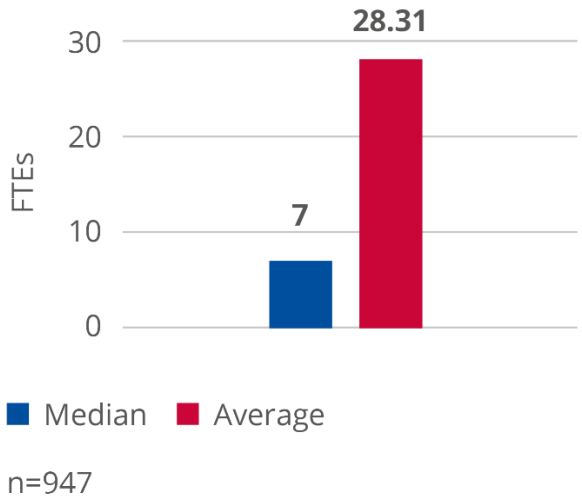


n=945
[2 organisation did not have visibility into IT FTE count]

3.3.2 Information security FTEs

Survey question: What was your organisation's estimated number of information security FTEs for 2020 including internal staff and contractors?

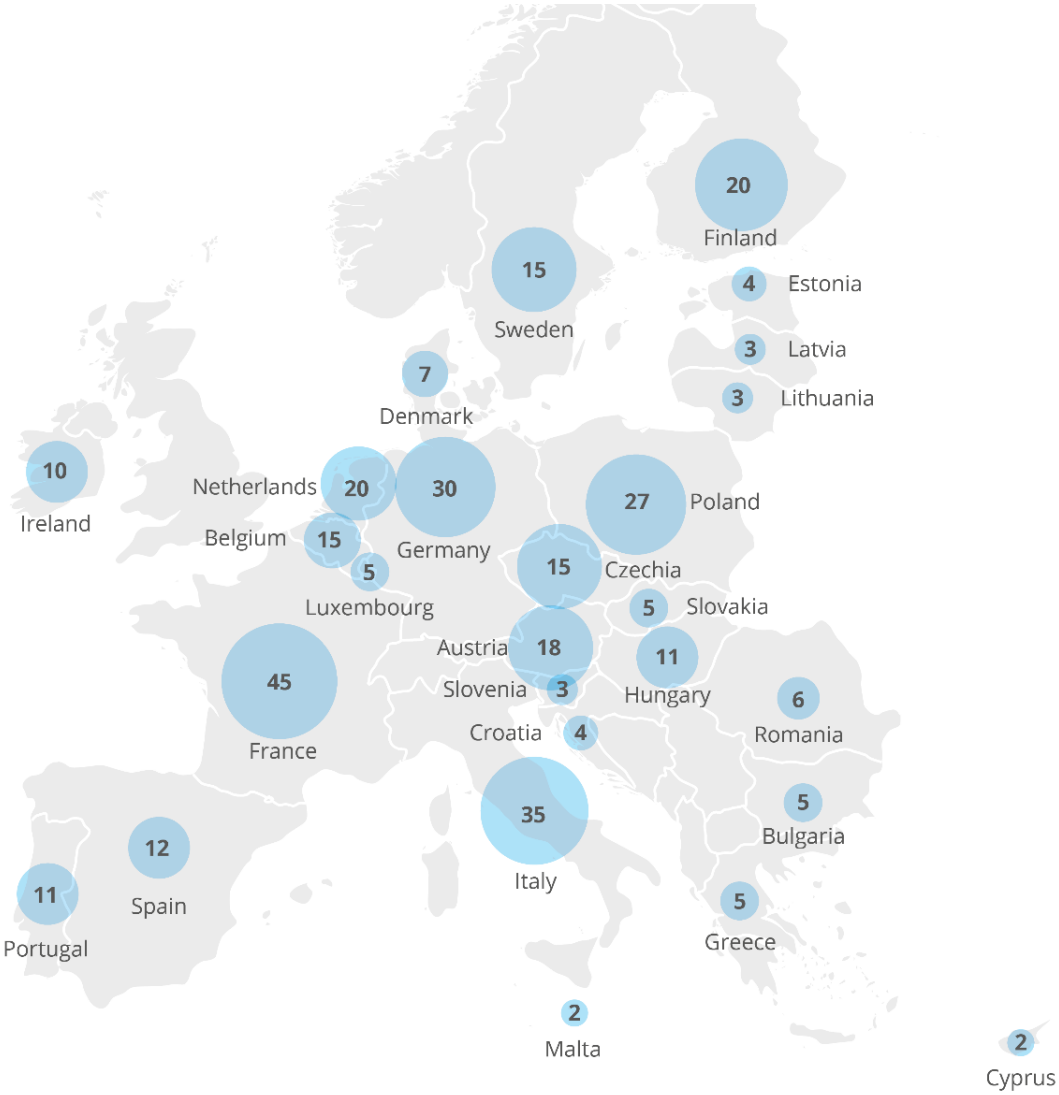
Figure 35: Information security FTEs



n=947

As with the overall discrepancy of IT FTEs, the distribution of information security FTEs follows a similar trend. With 45 FTEs, organisations from France have the highest median value in the EU, followed by organisations from Italy and Germany, with 35 and 30 FTEs respectively.

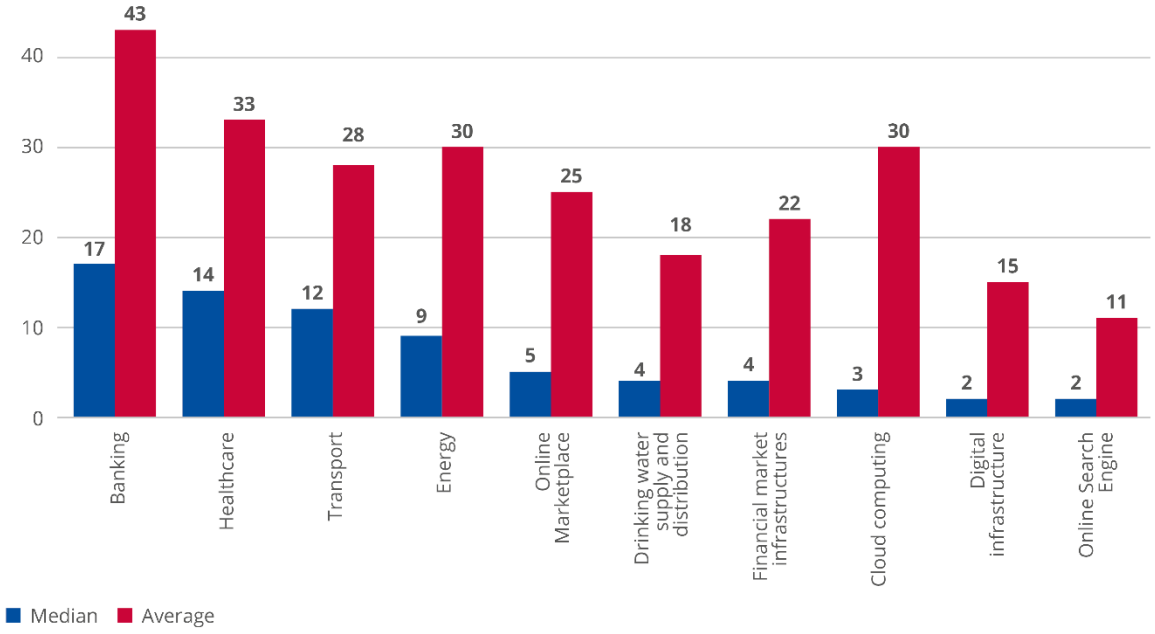
Figure 36: Information security FTEs for OES/DSP surveyed per Member State



n=945
[2 organisation did not have visibility into IT FTE count]

As illustrated in Figure 37, the banking sector has the highest number of information security FTEs, with a median value of 17 FTEs in 2020, followed by the healthcare and transport sectors, with 14 and 12 FTEs respectively. With two FTEs, the digital infrastructure and online search engine sectors have the lowest median number of information security FTEs.

Figure 37: Information security FTEs by sector



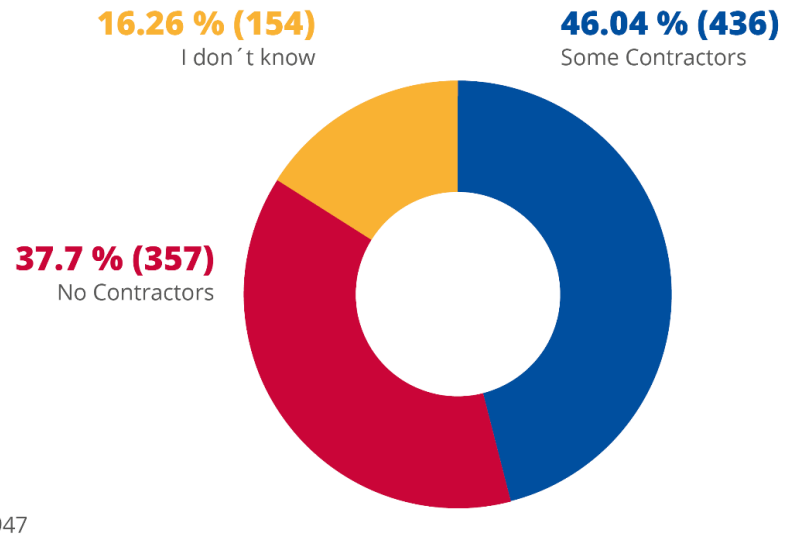
n=947

3.3.3 Share of contractors in information security FTEs

The survey data indicates that 357 (37.7 %) organisations have not hired any contractors in support of their information security workforce, while 436 (46.04 %) organisations report having contractors among their information security FTEs.

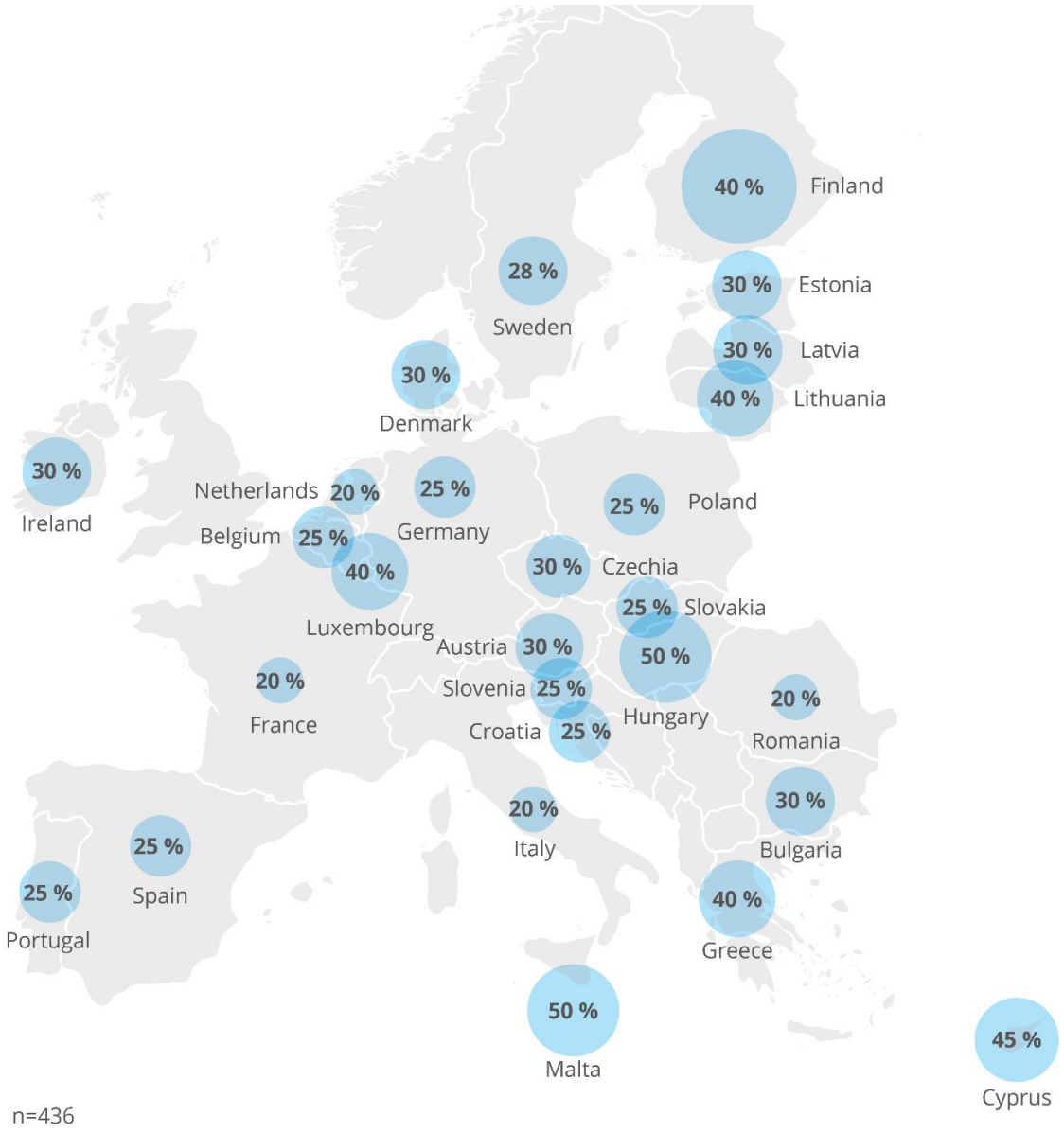
Survey question: Please indicate the percentage of information security FTEs that are contractors.

Figure 38: Contractors in information security FTEs



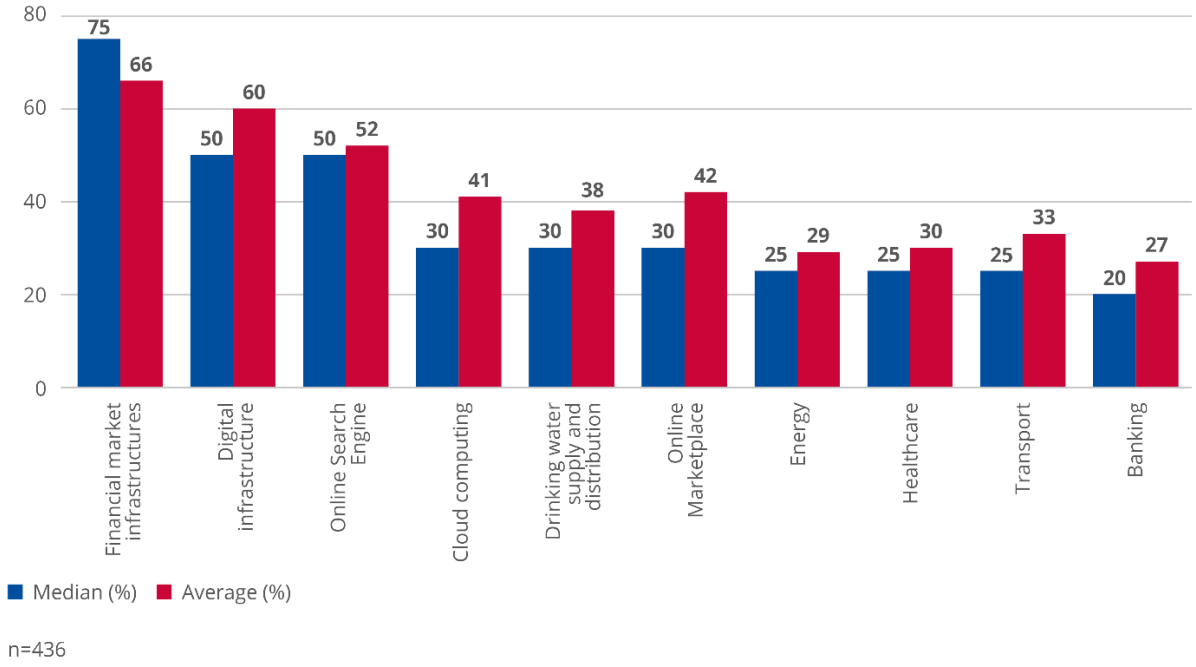
n=947

Figure 39: Contractors in information security FTEs for OES/DSP surveyed per Member State



The digital infrastructure and online search engine sectors use the most contractors, amounting to 50 % of the overall information security workforce. For the other sectors, the median value fluctuates between 20 % and 30 %.

Figure 40: Contractors in information security FTEs by sector

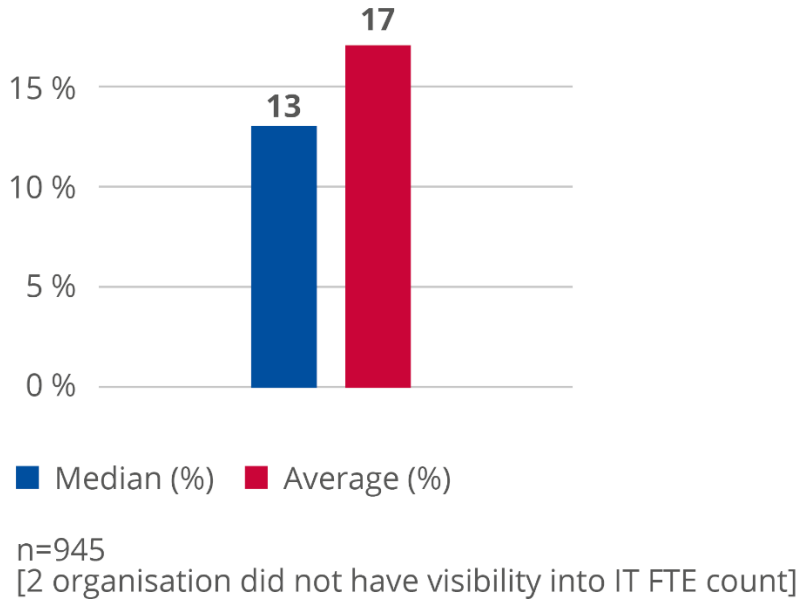


n=436

3.3.4 Information security FTEs as a share of IT FTEs

In order to determine the importance of information security FTEs in a typical OES/DSP, the relative share of these FTEs against the overall IT FTEs was calculated and is depicted in Figure 41.

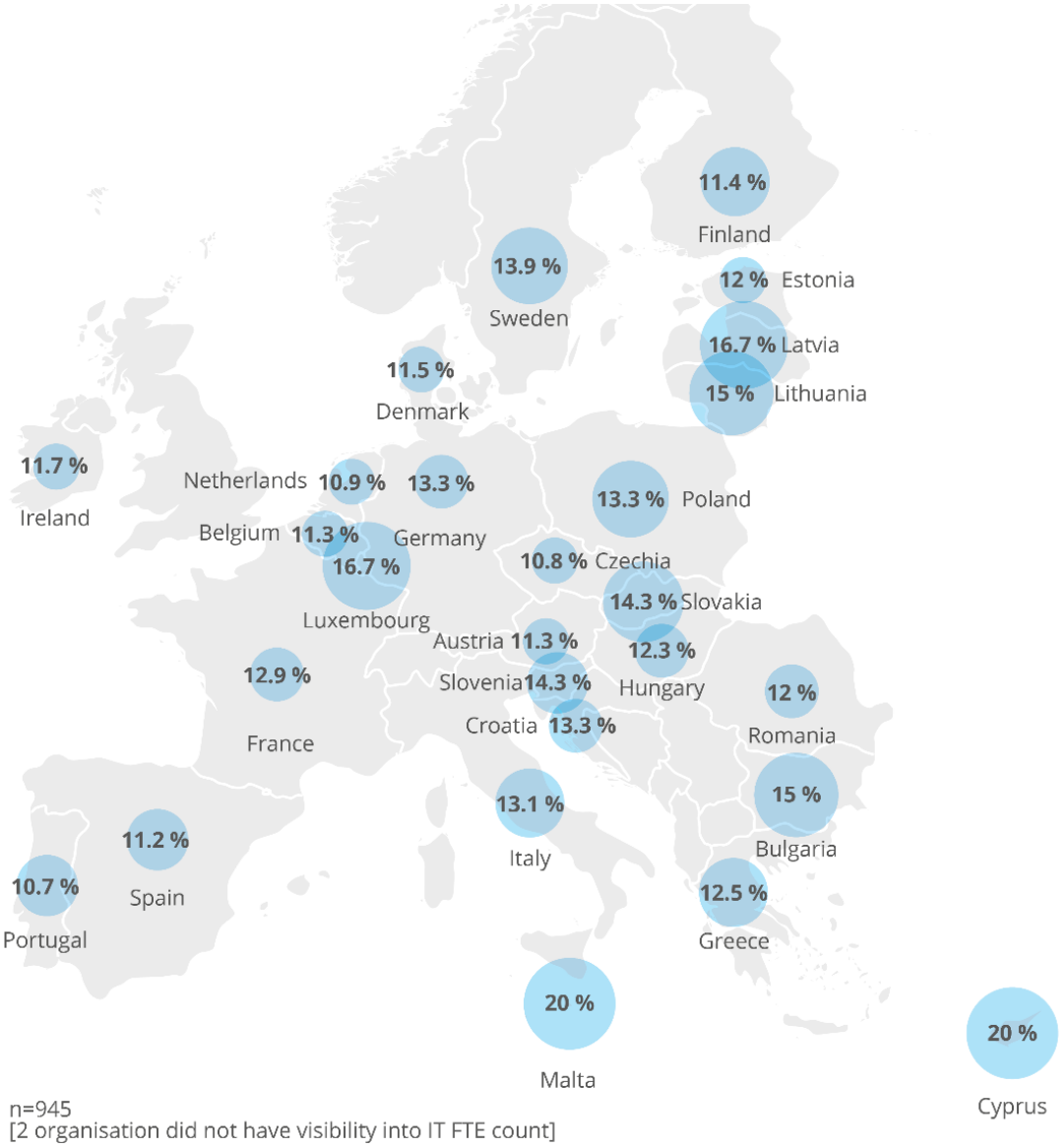
Figure 41: Information security FTEs as a share of IT FTEs



n=945
[2 organisation did not have visibility into IT FTE count]

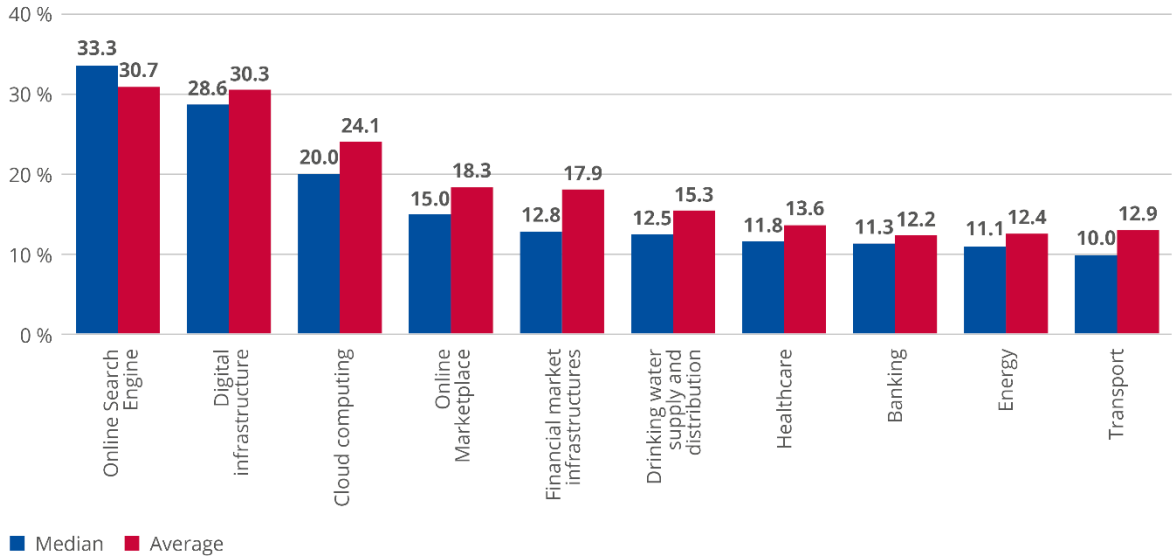
As per the median value, the typical percentage of information security FTEs against the overall IT FTEs amounts to 13 % for OES/DSP in the EU, with an average of 17 %.

Figure 42: Information security FTEs as a share of IT FTEs for OES/DSP surveyed per Member State



The online search engine sector has the highest information security to IT FTEs ratio, with a median value of 33.3 %, while digital infrastructures follows closely with a median value of 28.6 %. The information security to IT FTEs ratio is lowest for the transport sector, with a median value of 10 %.

Figure 43: Information security FTEs as a share of IT FTEs by sector



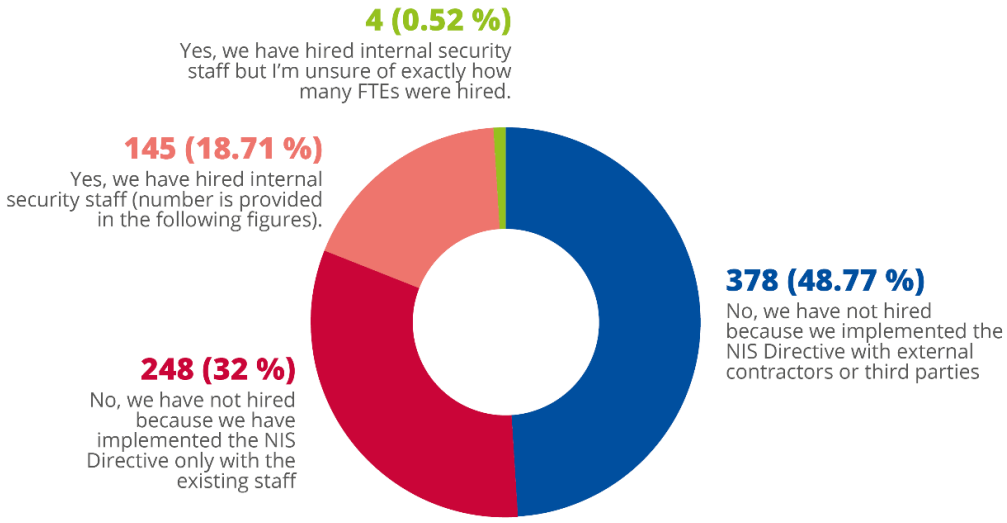
n=945
[2 organization did not have visibility into IT FTE count]

3.3.5 Specific hires for NIS implementation

While 49 % of the surveyed organisations did not hire any new staff in the context of their NIS implementation, 32 % of organisations said they had used external contractors or third parties for their implementation programmes.

Survey question: Did your organisation hire additional internal security staff (not contractors) specifically to implement the NIS Directive?

Figure 44: Information security hires related to implementing the NIS Directive



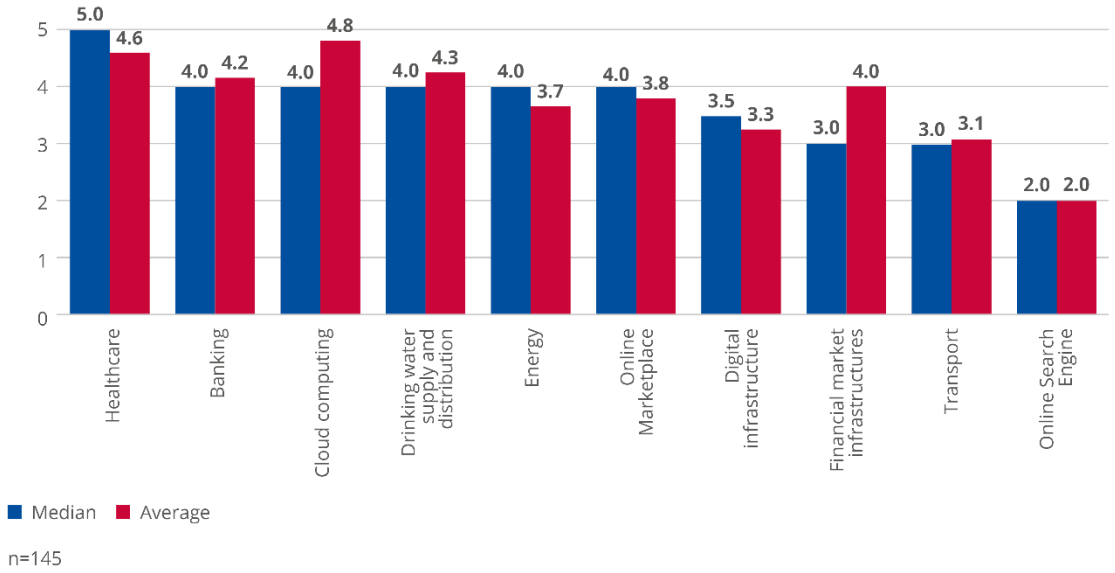
n=775
[172 organizations have not implemented the NIS directive]

None of the organisations answering for Malta and Latvia have hired information security FTEs for implementing the NIS Directive.

Figure 45: Information security hires related to implementing the NIS Directive for OES/DSP surveyed per Member State

When analysing the survey data from a sector perspective, the healthcare sector has the highest median value of five FTEs hired to ensure the implementation of the NIS Directive.

Figure 46: Information security hires related to the implementing the NIS Directive by sector

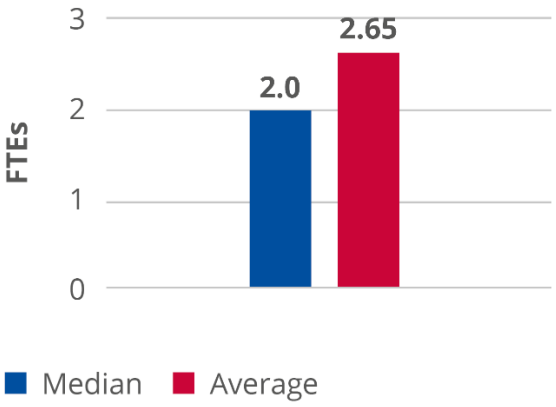


n=145

3.3.6 FTEs dedicated to security incident response

Survey question: In 2020, how many FTEs (internal staff and/or contractors) are fully dedicated to information security incident response activities in your organisation?

Figure 47: Information security FTEs for security incident response



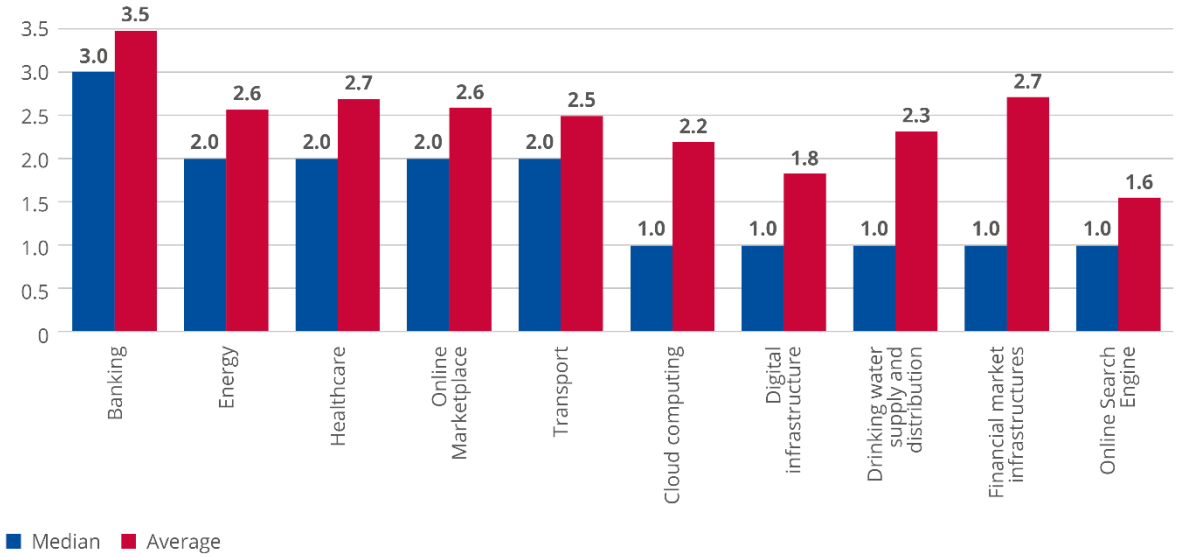
n=758
[186 organization have outsourced their incident response and 3 organizations didn't provide details for number of resources]

Figure 48: Information security FTEs for security incident response for OES/DSP surveyed per Member State

n=758
[186 organization have fully outsourced their incident response and 3 organizations didn't provide details for number of resources]

The banking sector has the highest median value of FTEs associated with incident management (three FTEs), while the other sectors employ one or two dedicated FTEs.

Figure 49: Information security FTEs for security incident response by sector



n=758
[186 organization have fully outsourced their incident response and 3 organizations didn't provide details for number of resources]

3.4 INFORMATION SECURITY INCIDENTS

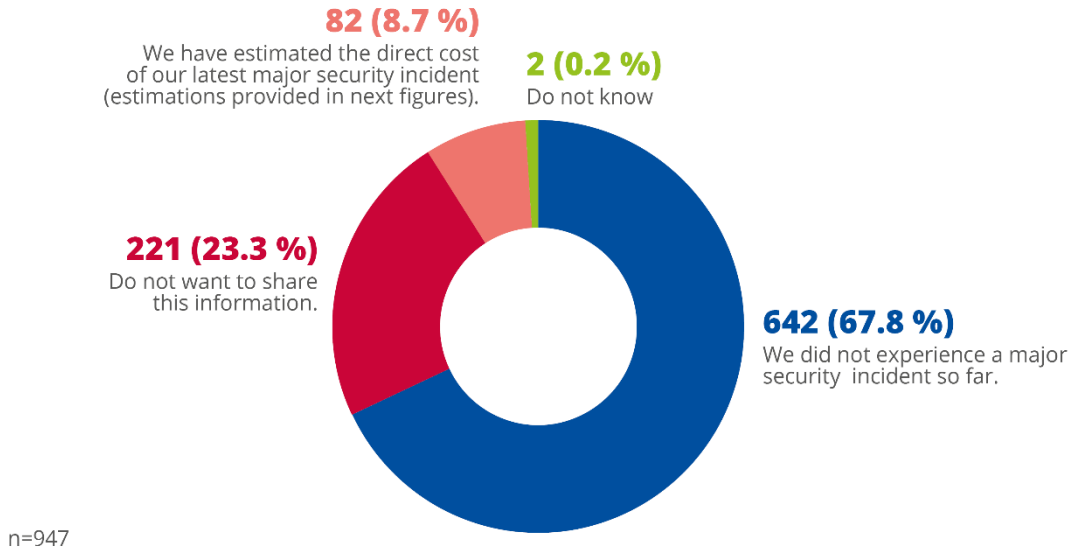
Key findings
The estimated direct cost of a major security incident for a typical OES/DSP is EUR 100 000 on median.
The costs related to revenue losses and data recovery or business continuity management are the predominant costs in the context of a major security incident.
Almost 50 % of surveyed OES/DSP indicate that the number of security incidents they are experiencing remains stable.
In 2020, only 8.8 % of surveyed OES/DSP experienced a major security incident.
Almost 50 % of surveyed OES/DSP believe that the NIS implementation has strengthened their detection capabilities, while 26 % believe that it has strengthened their ability to recover from incidents.

3.4.1 Cost of information security incidents

While 67.8 % of the 947 surveyed organisations declared that they had not experienced a major security incident so far, 8.7 % agreed to share the costs related to their last major security incident and 23.3 % refused to share this information.

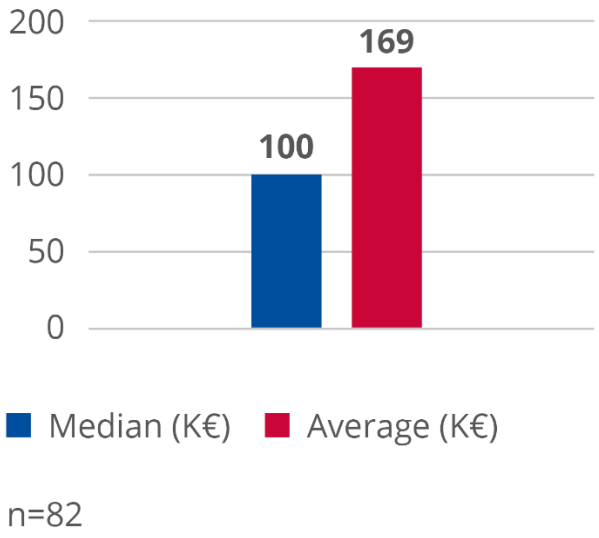
Survey question: What are the estimated direct costs incurred by the last major information security incident experienced by your organisation?

Figure 50: Has your organisation experienced a major security incident



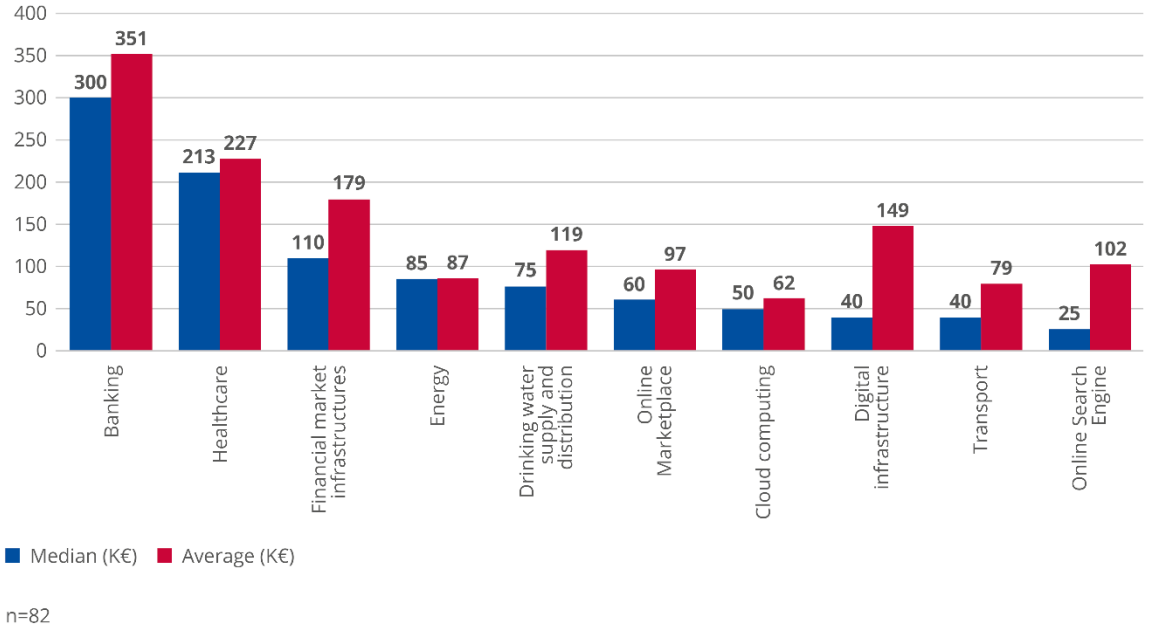
For the 82 organisations that declared the costs associated with their latest major information security incident, the direct cost of a security incident for an OES/DSP was EUR 100 000, while the average cost was EUR 169 000.

Figure 51: Estimated direct costs of a major cybersecurity incidents



The banking and healthcare sectors experience the highest costs associated with security incidents, with median values of EUR 300 000 and EUR 213 000 respectively.

Figure 52: Estimated direct costs of a major cybersecurity incident by sector

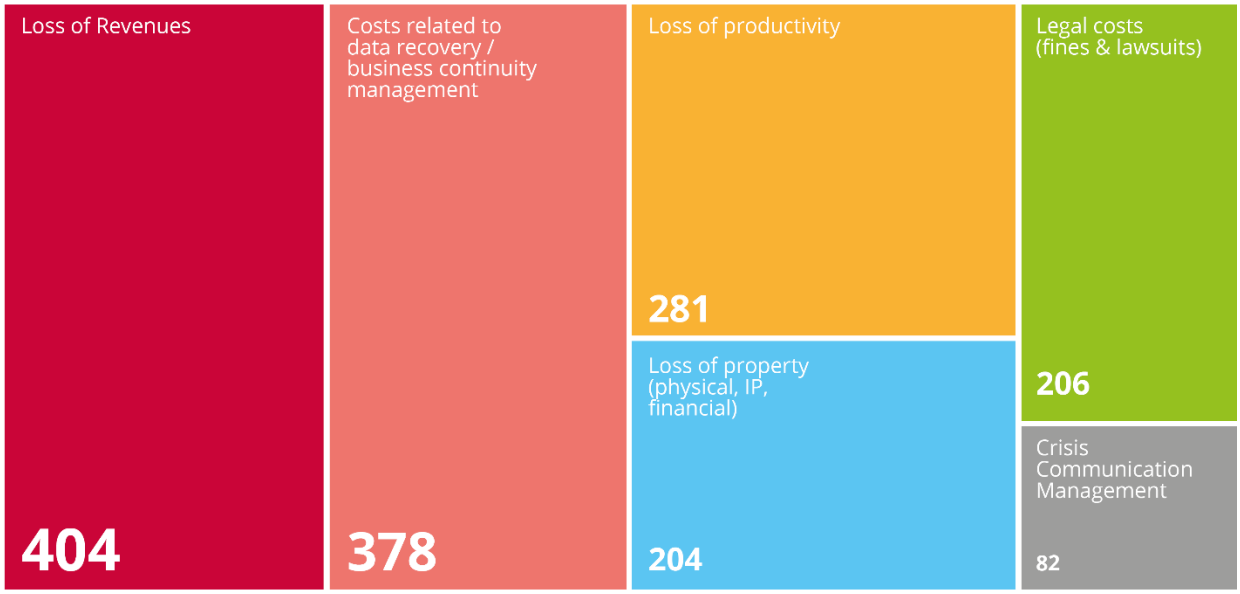


3.4.2 Top components of incident costs

With 404 organisations reporting losses of revenue and 378 organisations reporting costs related to data recovery / business continuity management, these components form the principal direct costs related to a security incident.

Survey question: What are the top two components of the direct costs associated with major information security incidents?

Figure 53: Top two components of direct cybersecurity incident costs



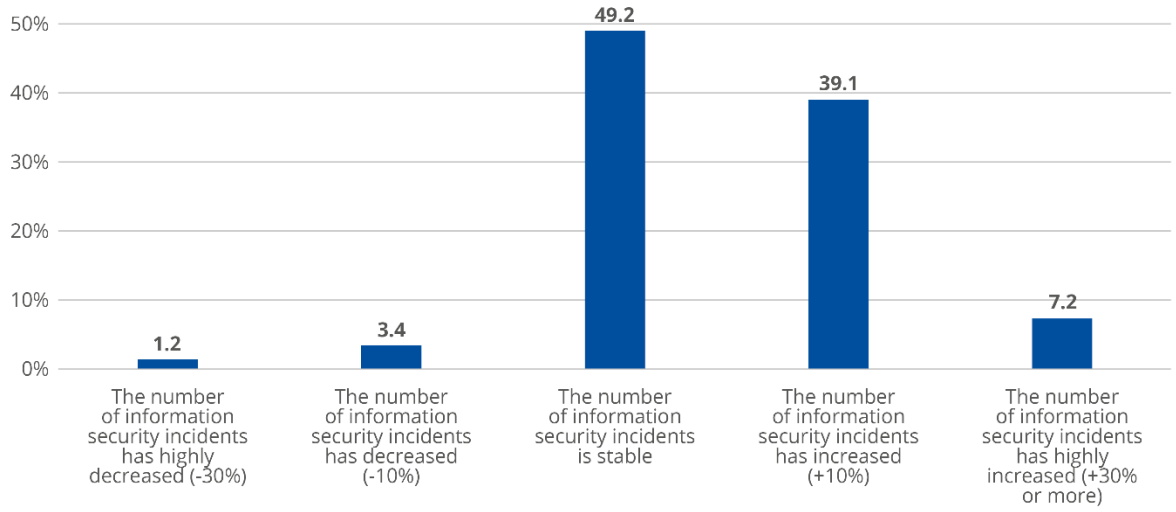
n=947

3.4.3 Trend in security incidents

The number of information security incidents has remained stable in almost half of the organisations (49.2 %). Be that as it may, 39 % of organisations report that the number of information security incidents has risen by over 10 %, while 7.18 % of organisations have experienced an increase of over 30 %. Only 43 (4.5 %) organisations report that the number of information security incidents has declined: 3.4 % of organisations reported a reduction of 10 % or more and 1.1 % of organisations reported a reduction of 30 % or more.

Survey question: How do you evaluate the year-on-year evolution of the number of information security incidents that your organisation is facing?

Figure 54: Trend in the number of information security incidents year-on-year



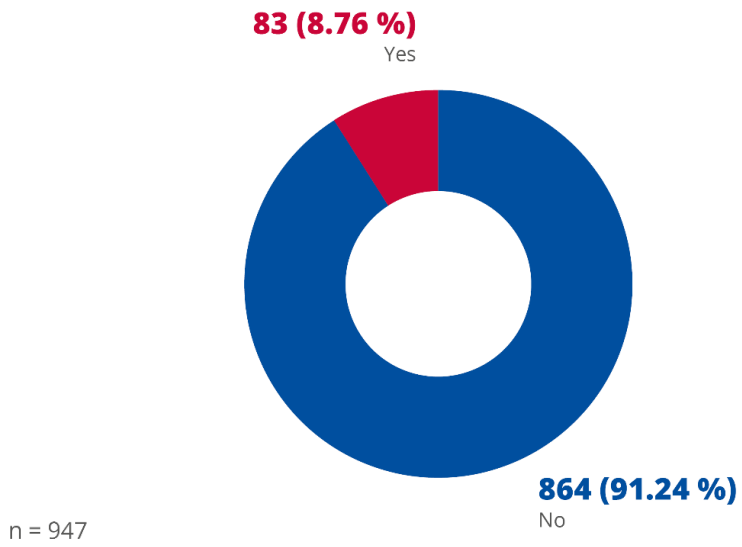
n=947

3.4.4 Spread of security incidents

Approximately 9 % of organisations have suffered a major security incident that impacted external stakeholders – such as customers or partners – within their business ecosystem.

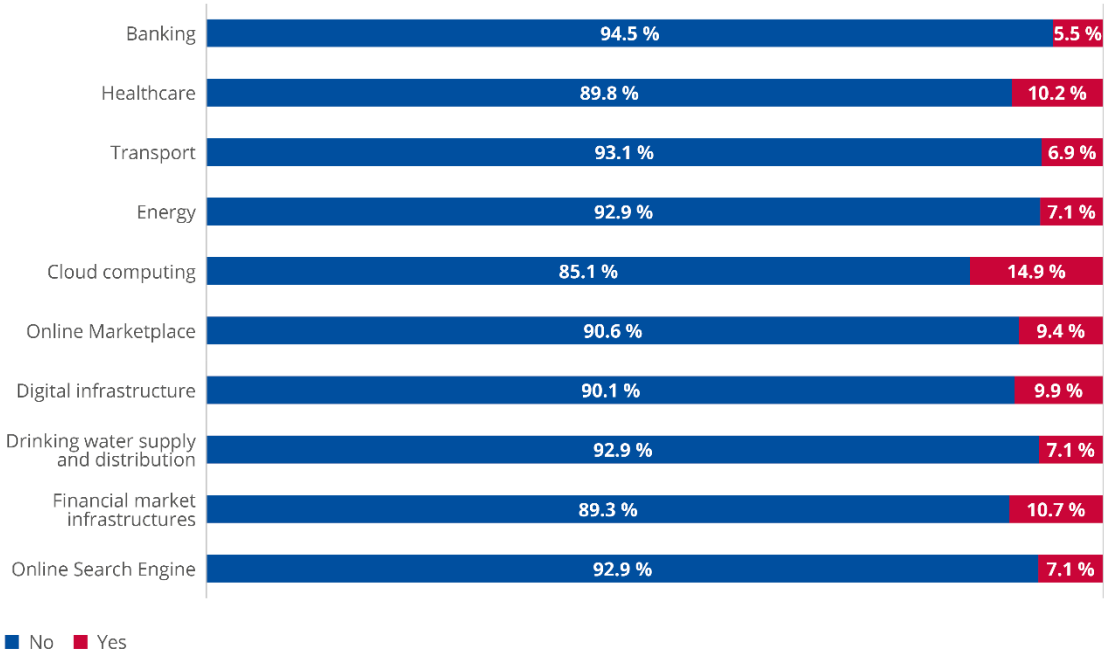
Survey question: In 2020, did your organisation suffer a major security incident impacting other organisations in your ecosystem (customers, partners)?

Figure 55: Spread of information security incidents



A detailed breakdown per sector indicates that the risk of a major security incident is comparable in the different verticals and varies between 5 and 15 %. Cloud computing is the sector with the highest probability of security incidents – approximately 15 % – whereas the banking sector experiences the lowest spread of security incidents.

Figure 56: Spread of information security incidents by sector

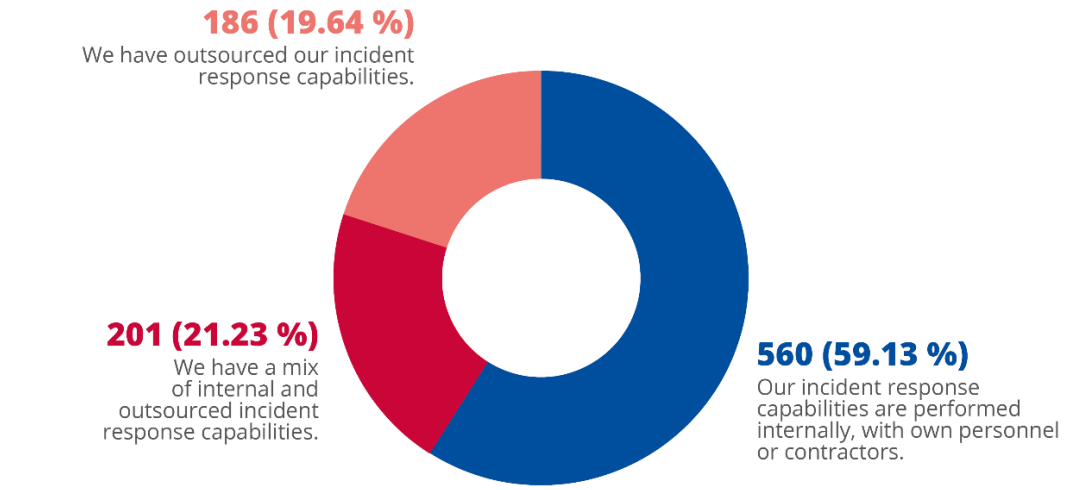


3.4.5 Security incident response sourcing

59 % of organisations have internal incident response capabilities at their disposal, while around 20 % combine both internal and outsourced capabilities. Furthermore, 21 % of organisations have completely outsourced these capabilities.

Survey question: What is your organisation's sourcing strategy for information security incident response capabilities?

Figure 57: Security incident response sourcing



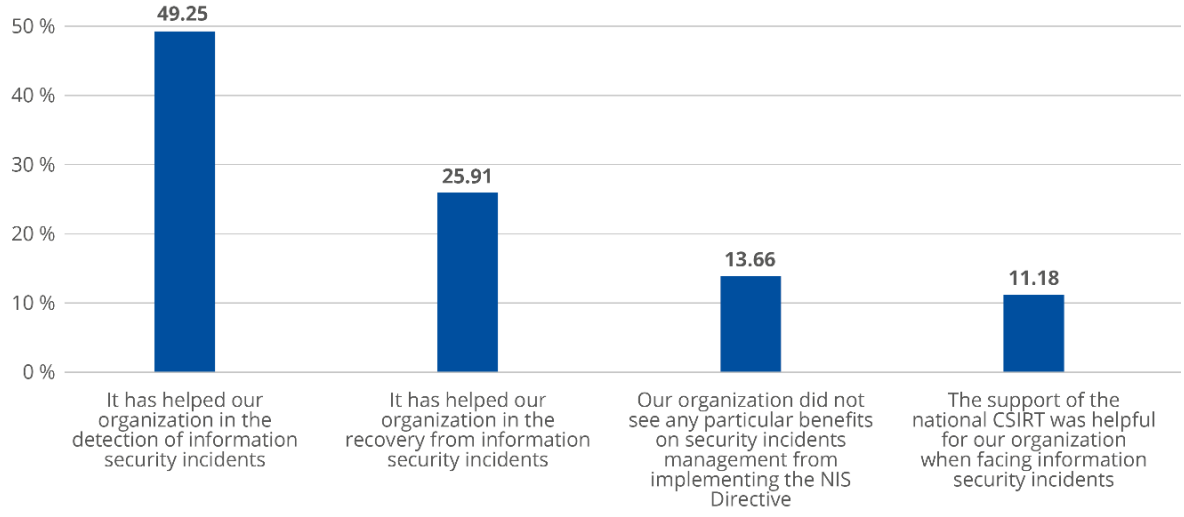
n = 947

3.4.6 NIS impact on incident response

49 % of organisations believe that the implementation of the NIS Directive has directly bolstered their detection capabilities and 26 % reported the strengthening of recovery capabilities due to the implementation of the NIS Directive. Nonetheless, 14 % of organisations did not observe any particular benefit after the implementation of the NIS Directive.

Survey question: How has the implementation of the NIS Directive helped your organisation mitigate the impact of the information security incidents?

Figure 58: Impact of implementing the NIS Directive



3.5 SECURITY ORGANISATION AND PERFORMANCE

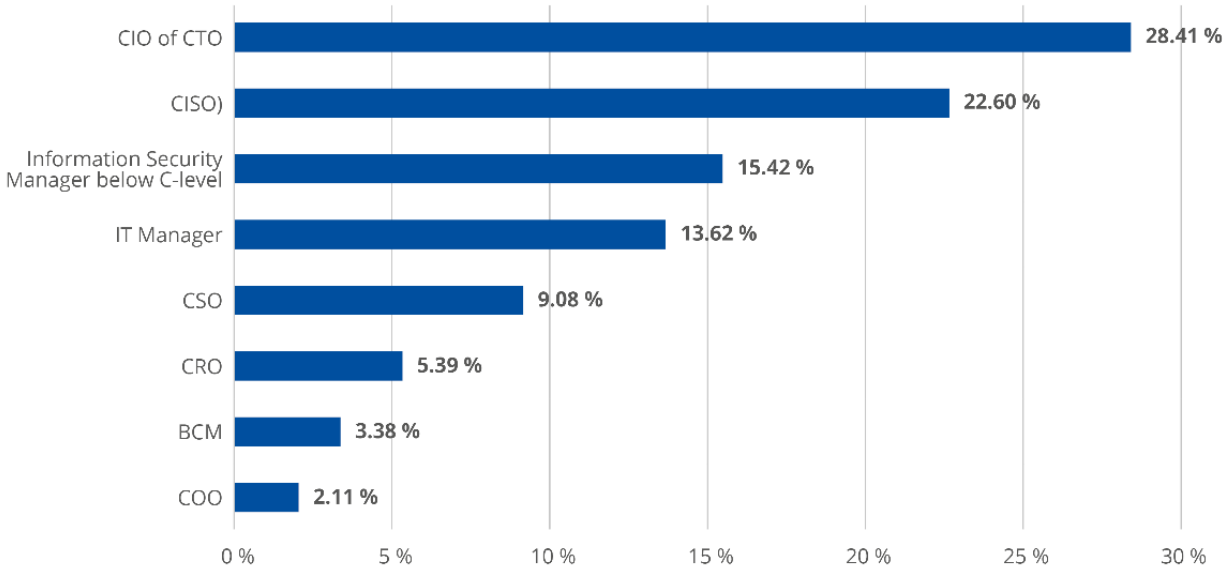
Key findings
In 28 % of the surveyed OES/DSP, the CIO or CTO is responsible for information security.
In over 50 % of the surveyed OES/DSP, the HIS reports directly to the CEO, the BOD or the President.
More than 50 % of the surveyed OES/DSP do not possess any form of cyber insurance, although around 25 % are planning to obtain coverage.
More than 50 % of the surveyed OES/DSP certify their systems and processes (e.g. on the basis of the International Organisation for Standardisation's ISO 27001 certification).
The majority of the surveyed OES/DSP report that their information security controls meet industry standards, with only 5 % reporting that they do not meet those standards.

3.5.1 Reporting line of information security

The Chief Information Officer (CIO) or Chief Technology Officer (CTO) are responsible for information security in over 28 % of the surveyed organisations. Moreover, the CISO is the most senior-level person responsible for information security in 22 % of the surveyed OES/DSP.

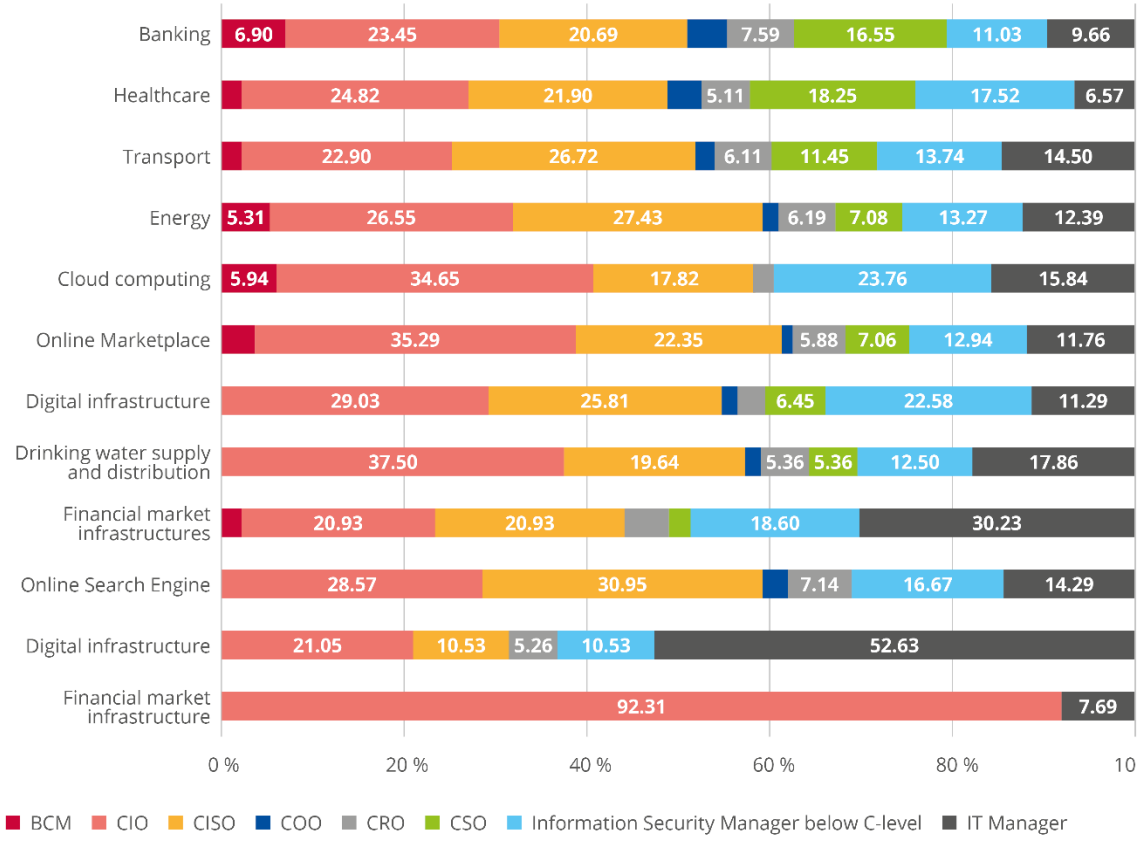
Survey question: What is the role in your organisation of the most senior-level person dedicated exclusively to information security?

Figure 59: Head of information security



n = 947

Figure 60: Head of information security by sector

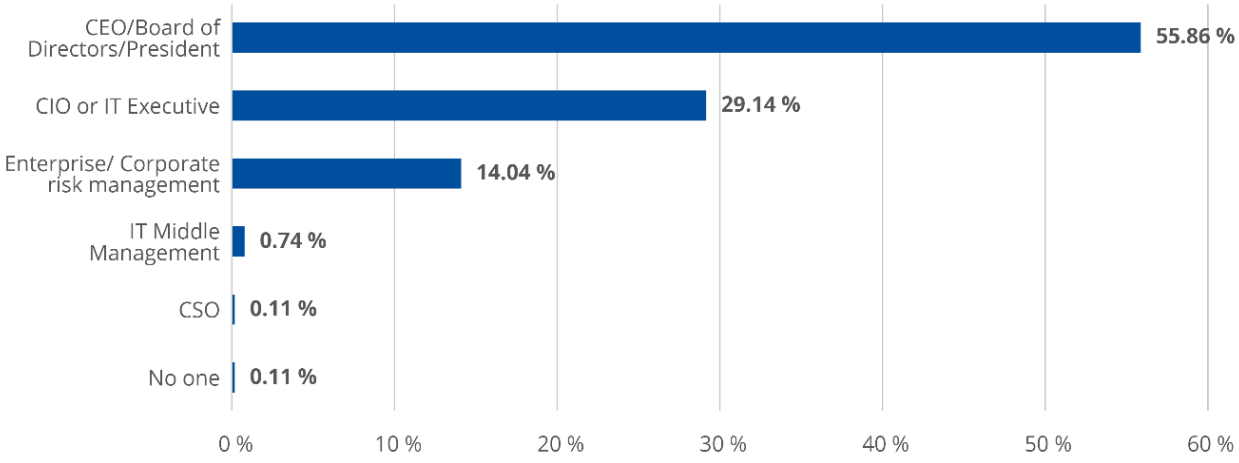


n = 947

As illustrated in Figure 61, the head of information security generally reports directly to the CEO or Board of directors (BOD), with 55.86 % of organisations having a direct line of reporting from the head of information security to the CEO.

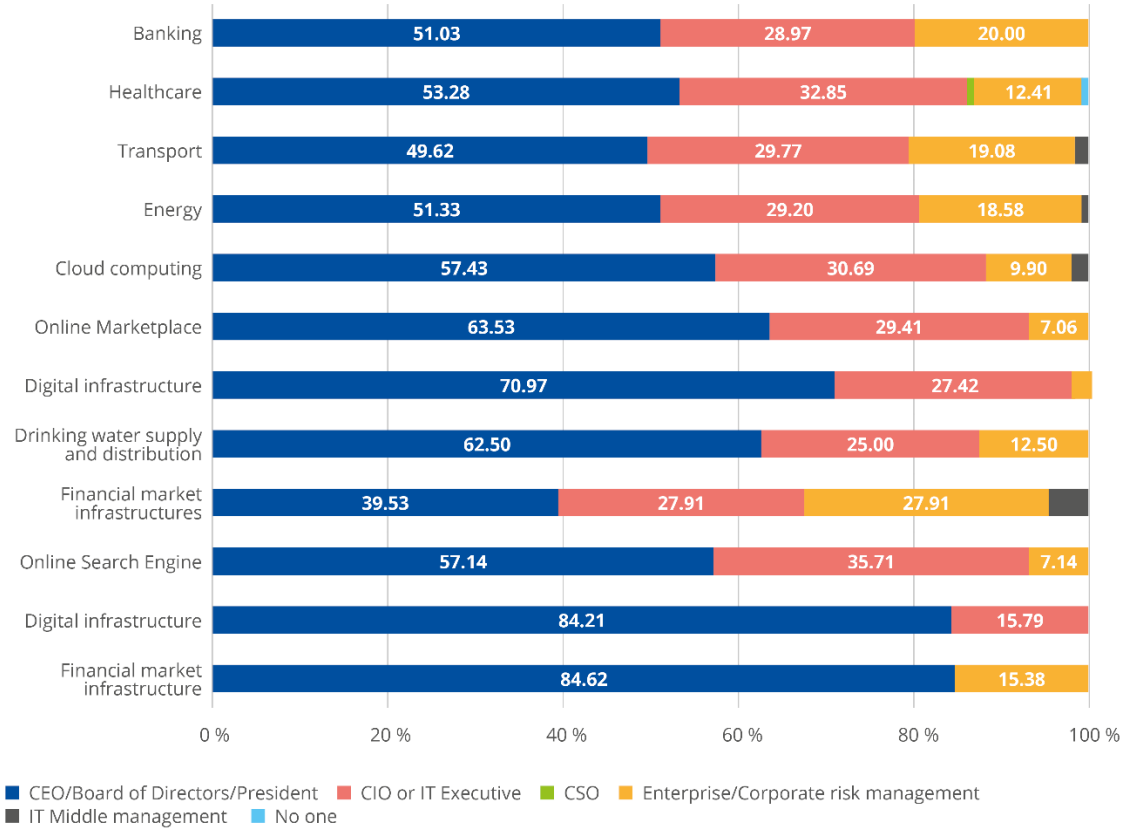
Survey question: Who does the head of information security directly report to?

Figure 61: Reporting line of information security



n = 947

Figure 62: Reporting line of information security by sector



n = 947

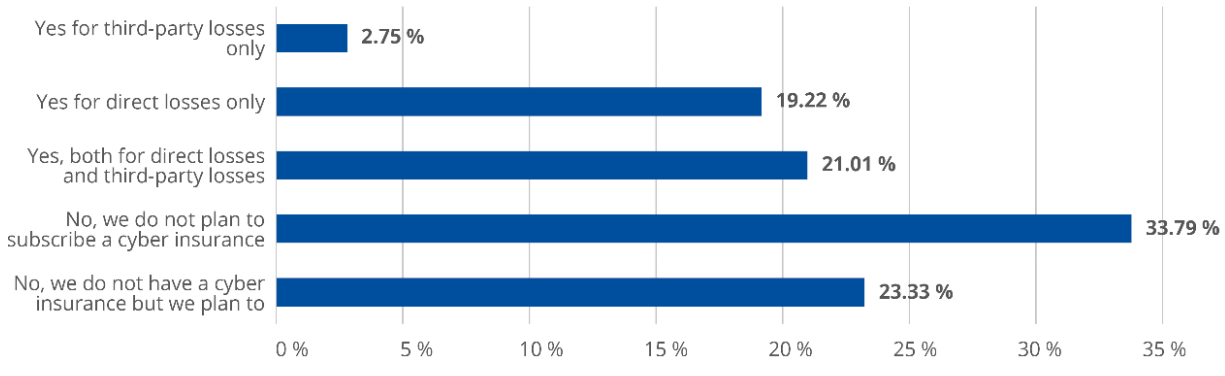
3.5.2 Cyber insurance

Over 57 % of organisations have not subscribed to a cyber insurance solution. While 21.01 % of organisations have subscribed to a solution that encompasses both direct incurred losses and third-party losses, 181 organisations only cover direct losses while 2.75 % of organisations only cover third-party losses.

Furthermore, 23.23 % of organisations reported that they currently do not subscribe to any cyber insurance solution, but are planning to implement one.

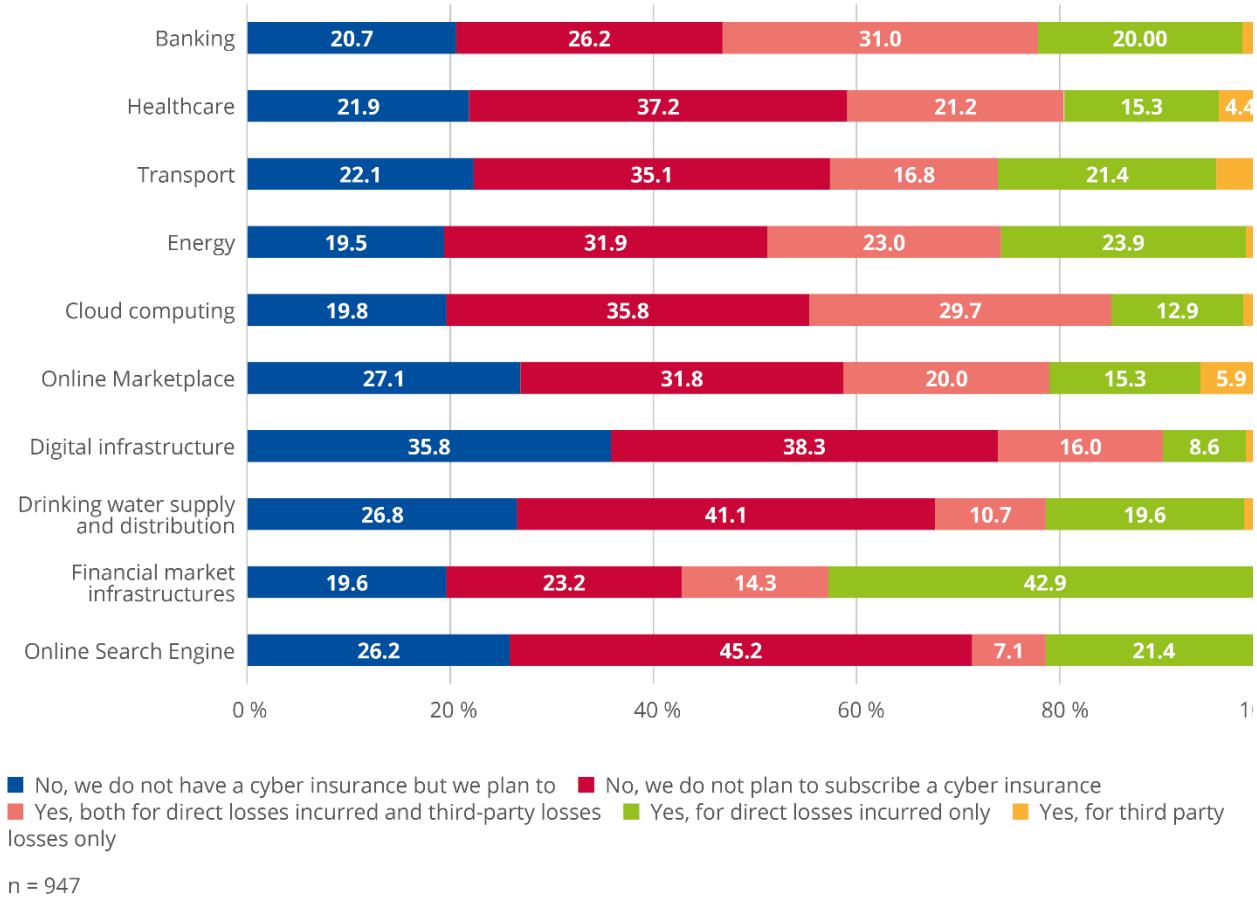
<u>Survey question:</u> Did your organisation subscribe to a dedicated cyber insurance solution?

Figure 63: Cyber insurance subscriptions



n = 947

Figure 64: Cyber insurance subscriptions by sector



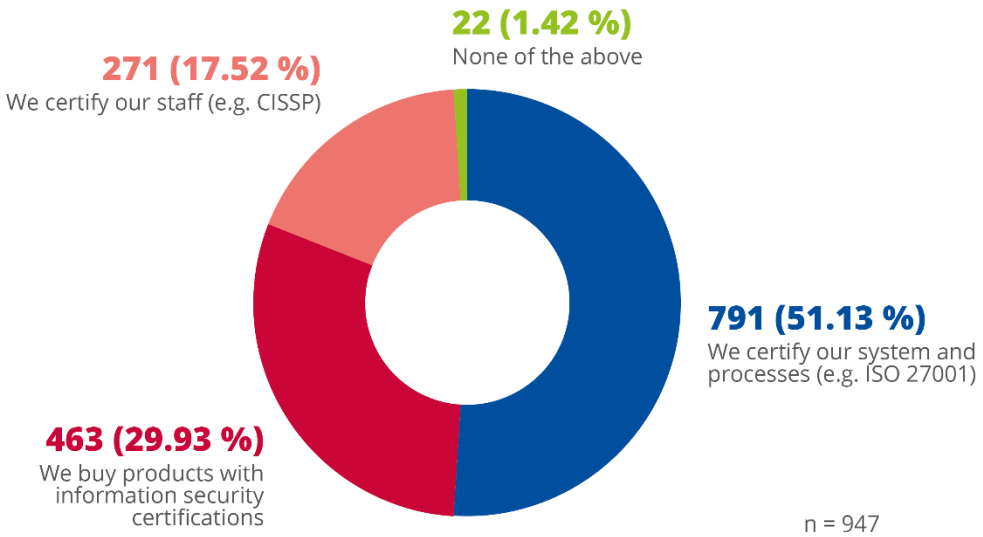
n = 947

3.5.3 Certification

A majority of organisations (51.1 %) certify their systems and processes, e.g. on the basis of ISO 27001 certification. Furthermore, 17.5 % of organisations reported that they certify their staff with certifications such as Certified Information Systems Security Professional (CISSP).

Survey question: Does the organisation have information security related certification for processes, systems or staff?

Figure 65: Certifications



n = 947

3.5.4 Performance of controls

68.2 % of organisations are convinced that their information security controls meet industry standards. Moreover, 27.8 % of organisations believe their information security controls are above (23.7 %) or far above (4.1 %) industry security standards. On the other hand, 38 organisations (almost 5 %) believe that their information security controls do not meet industry standards.

Survey question: How would you evaluate the overall performance (effectiveness) of your organisation's information security controls?

Figure 66: Overall performance (effectiveness) of your organisation's information security controls

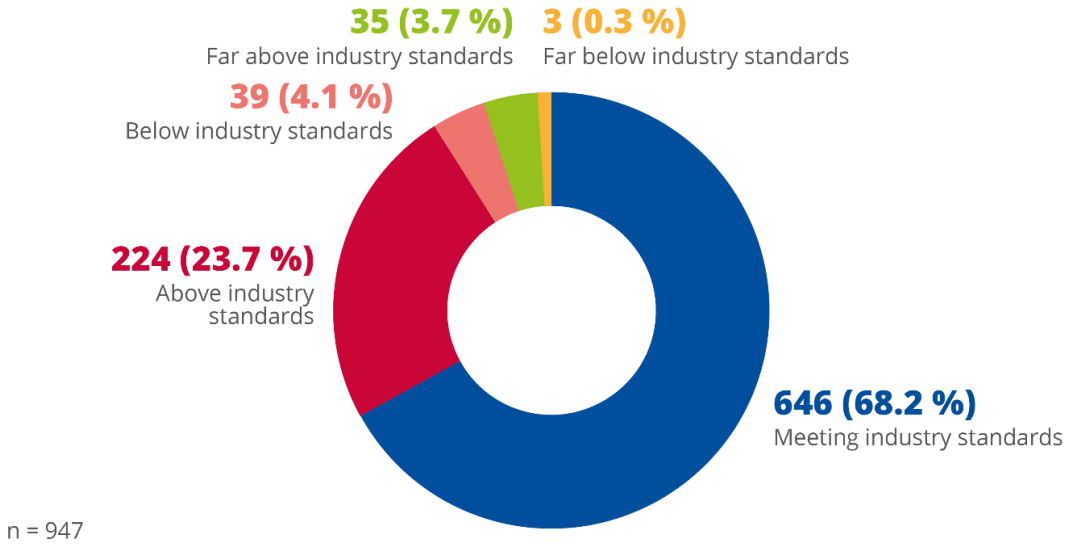
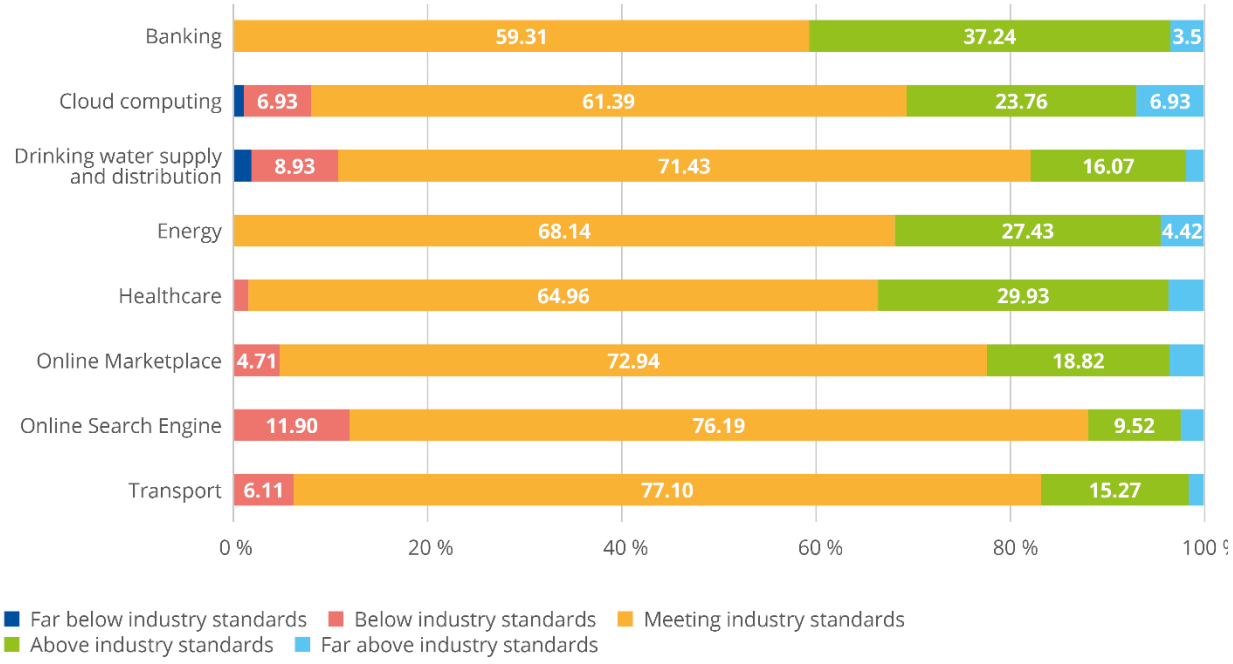


Figure 67: Overall performance (effectiveness) of your organisation's IS controls by sector



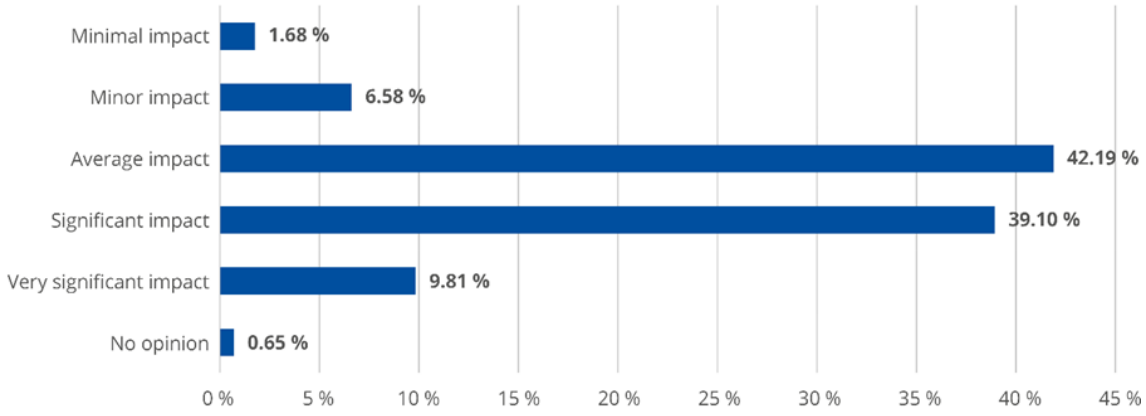
3.6 PERCEPTION OF THE IMPACT OF THE NIS DIRECTIVE

Key findings
Almost 50% of the surveyed OES/DSPs consider that the NIS Directive had a significant or very significant impact on their security posture.

A majority of the organisations that have implemented the NIS Directive report a corresponding positive impact on their security posture. Specifically, 9.8 % of organisations report that they have experienced a very significant impact, while 39.1 % report a significant impact.

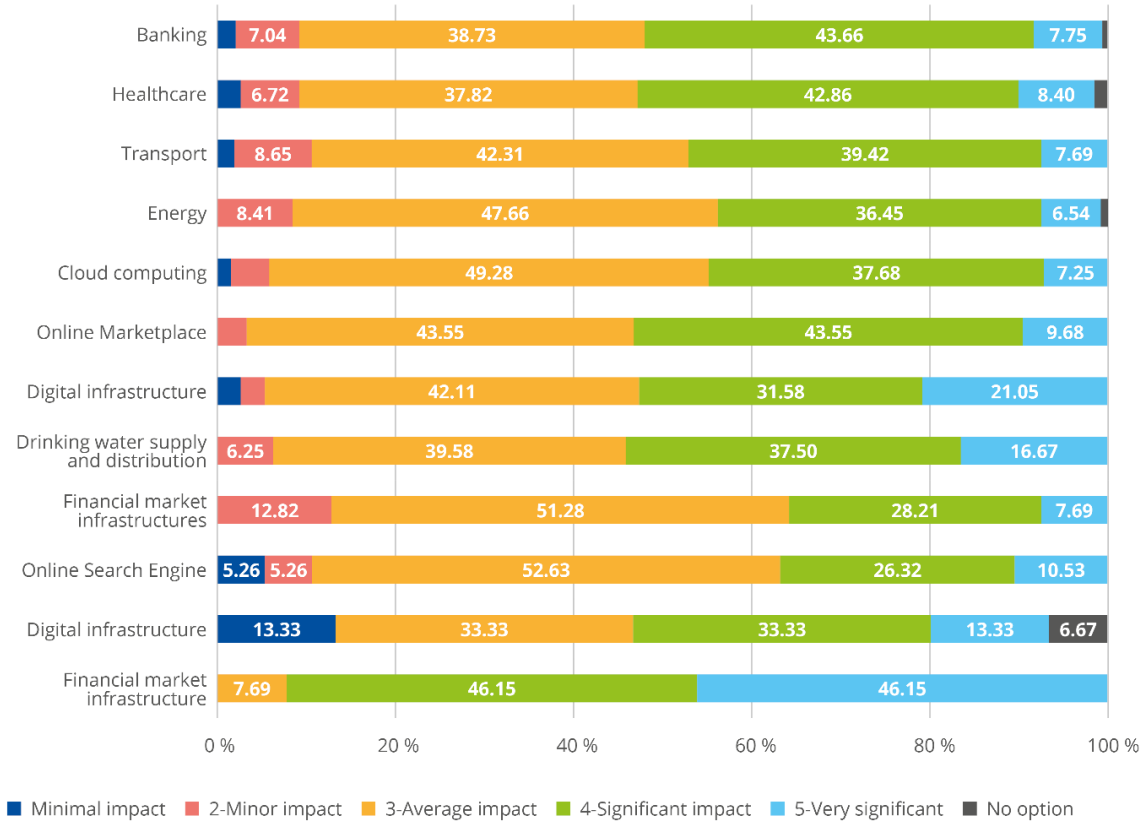
Survey question: Please evaluate the positive impact of the NIS directive on your organisation's security posture or maturity.

Figure 68: Impact of the NIS Directive



n=775
[172 organisations have not implemented the NIS directive]

Figure 69: Impact of the NIS Directive by sector



n=775
[172 organisations have not implemented the NIS directive]

4. INFORMATION SECURITY DATA FOR SMES AND LARGE ENTERPRISES

In line with the EU definition of SMEs[10] – based on revenues or employee count – the survey results have been further refined by classifying all organisations within these categories.

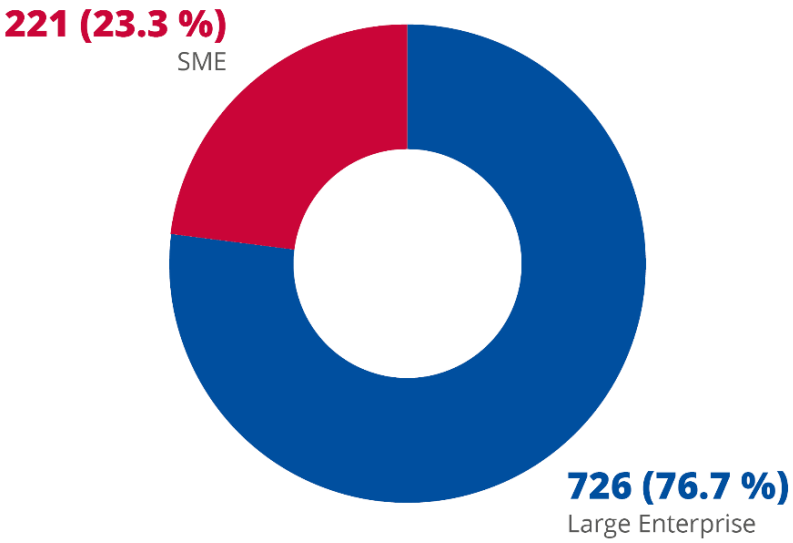
This chapter illustrates the results of the survey on the basis of organisation category.

4.1 DEMOGRAPHICS OF SMES AND LARGE ENTERPRISES

4.1.1 Distribution of SMEs and large enterprises

The share of SMEs in the survey data amounts to approximatively 23 %, whereas large enterprises compose 77 % of the data set.

Figure 70: Distribution of SMEs and Large Enterprises



[10] https://ec.europa.eu/growth/smes/sme-definition_en

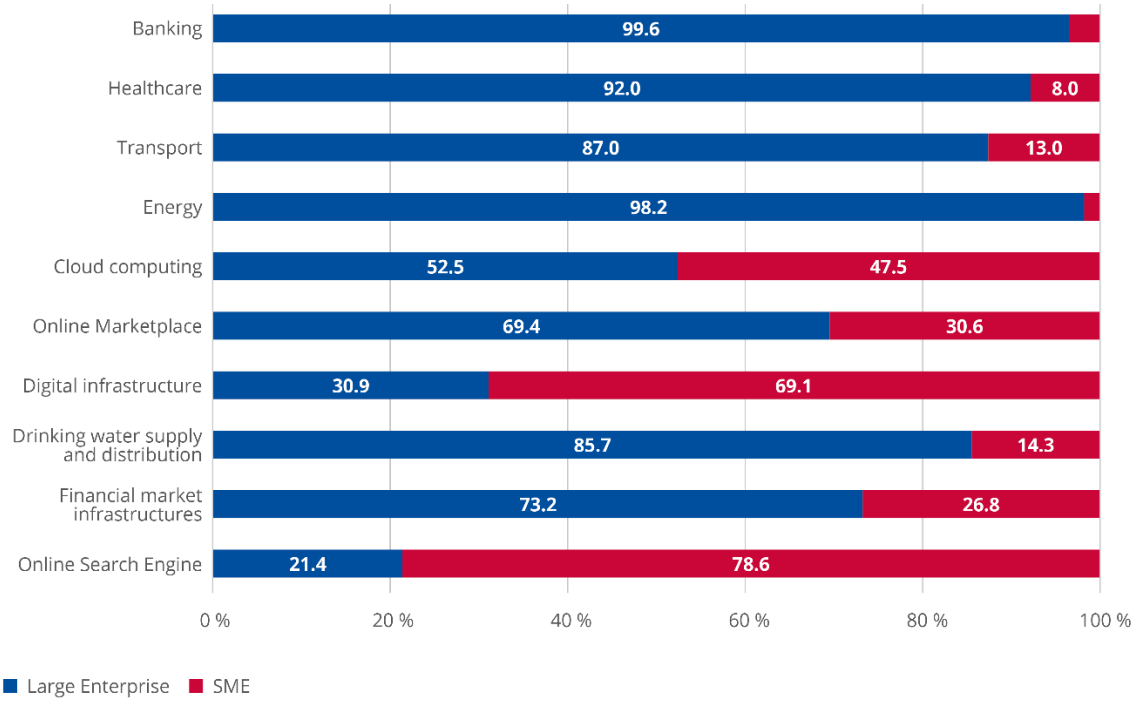
4.1.2 SMEs vs large enterprises by sector

The surveyed organisations have varying compositions depending on their operating sector. For instance, the online search engine and digital infrastructures sectors are composed mainly of SMEs, whereas these verticals are less mature and thus more fragmented than other traditional sectors.

Because of their mature and consolidated nature, the energy and banking sectors are mostly composed of large enterprises.

As stated earlier in the report, the size of the organisations within a certain sector has a direct influence on most of the collected data. For this reason, we have further normalised the collected data.

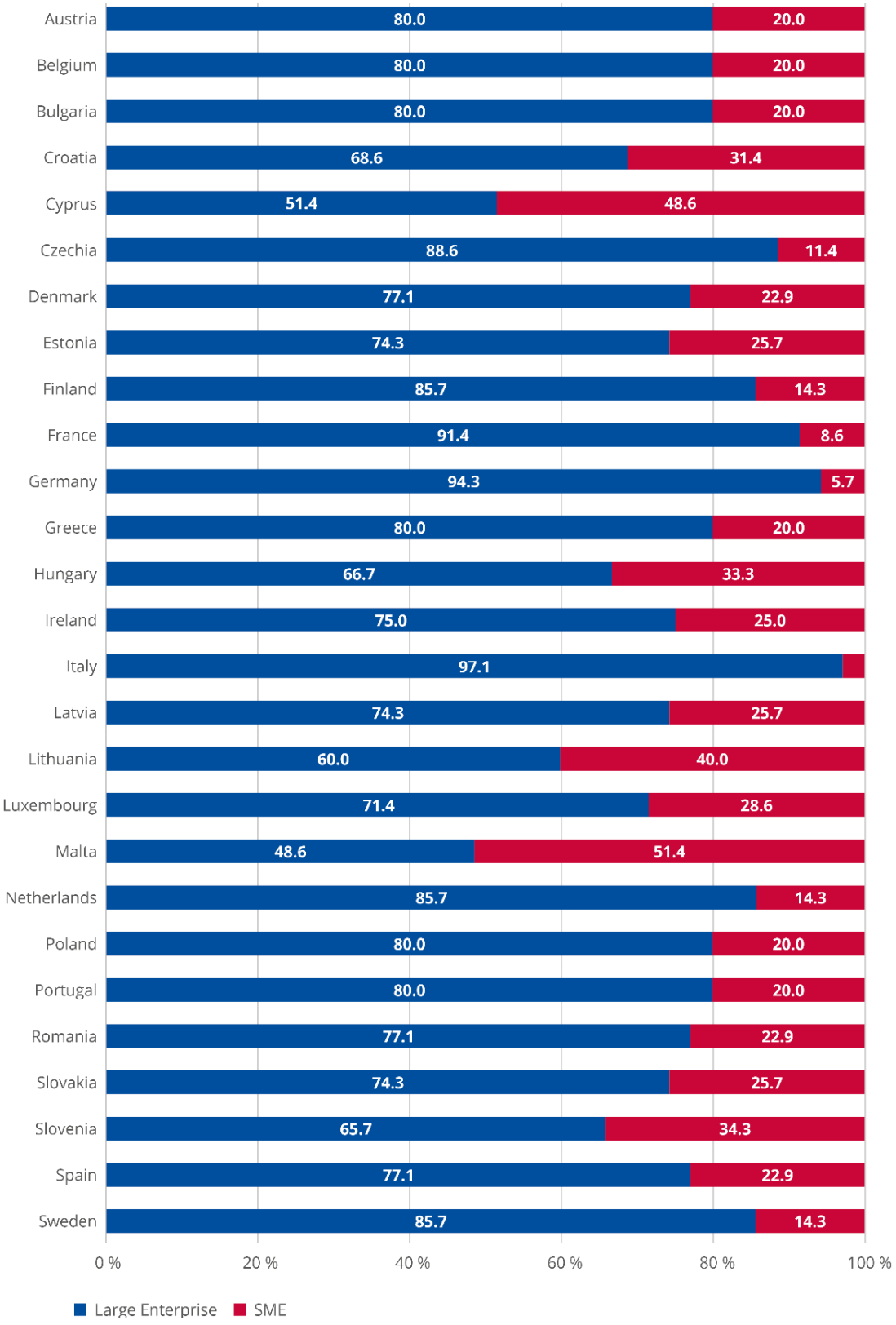
Figure 71: Large enterprises vs SME by sector



4.1.3 SMEs vs large enterprises by Member State

The OES/DSP sectors are highly consolidated in Italy (97.1 %), Germany (94.3 %) and France (91.4 %). On the other hand, OES/DSP organisations include a high number of SMEs in Malta (51.4 %), Cyprus (48.6 %) and Croatia (31.4 %).

Figure 72: Large Enterprises vs SME categorisation of OES/DSP surveyed per Member State

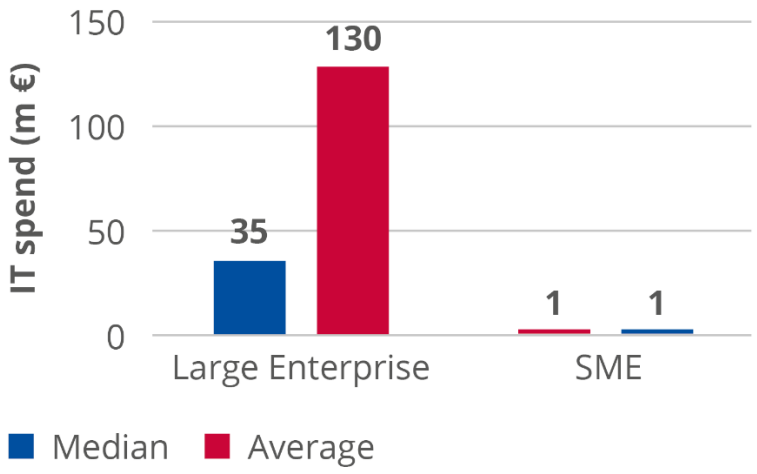


4.2 INFORMATION SECURITY SPENDING FOR SMES AND LARGE ENTERPRISES

4.2.1 IT spending

A typical SME spends approximately EUR 1 million on IT-related investments, whereas large enterprises spend around EUR 35 million.

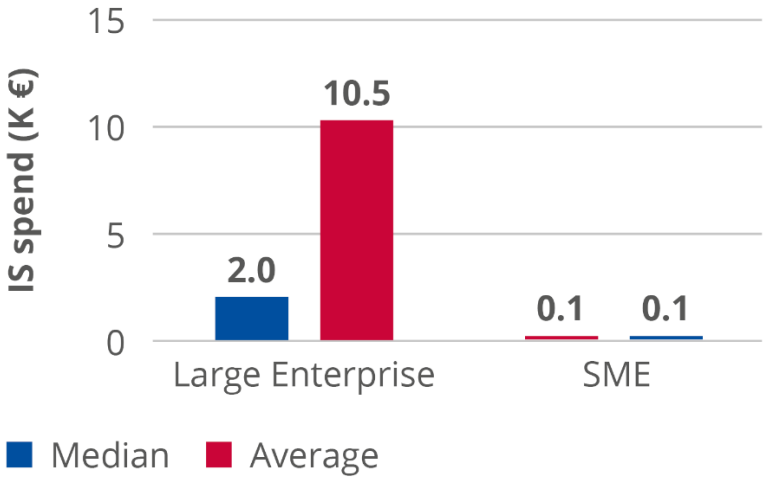
Figure 73: IT spending – SMEs vs large enterprises



4.2.2 Information security spending

A typical SME spends approximately EUR 100 000 on information security, whereas large enterprises spend around EUR 2 million.

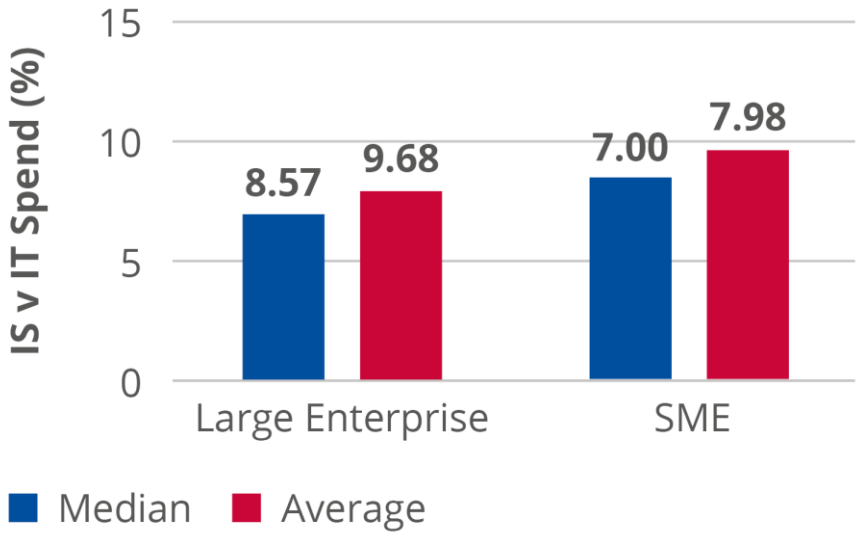
Figure 74: Information security spending – SMEs vs large enterprises



4.2.3 Information security spending as a share of IT spending

A typical SME allocated approximately 8.6 % of its IT spending to information security, whereas this figure stands at 7 % for large enterprises.

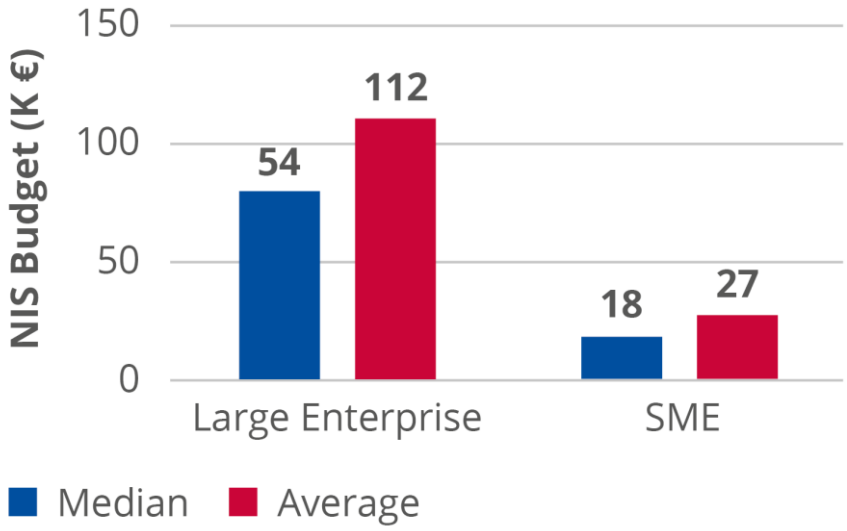
Figure 75: Information security spending as a share of IT spending – SMEs vs large enterprises



4.2.4 NIS budget

A typical SME earmarked approximately EUR 18 000 for implementing the NIS directive, whereas large enterprises allocated around EUR 54 000.

Figure 76: NIS budget – SMEs vs large enterprises

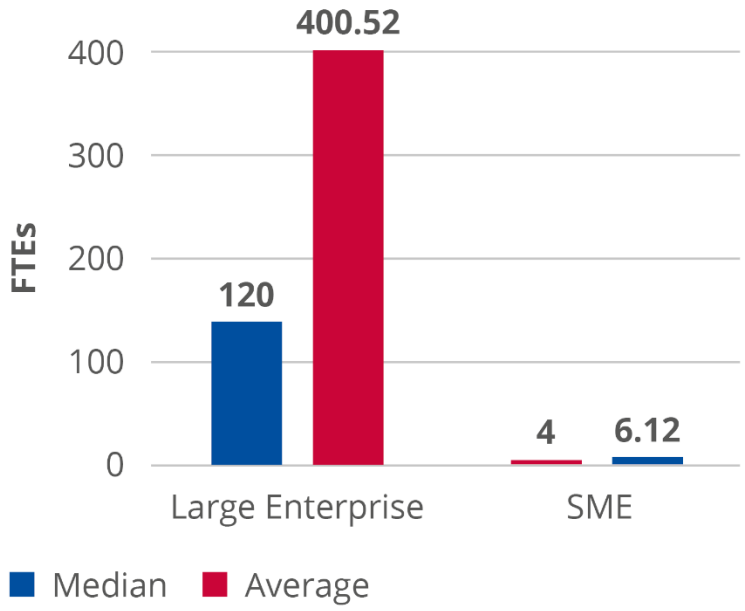


4.3 INFORMATION SECURITY STAFFING FOR SMES AND LARGE ENTERPRISES

4.3.1 IT FTEs for SMEs vs large enterprises

Within the sectors that were identified by the NIS Directive, a typical SME employed four FTEs whereas a large enterprise employed 120 dedicated IT FTEs.

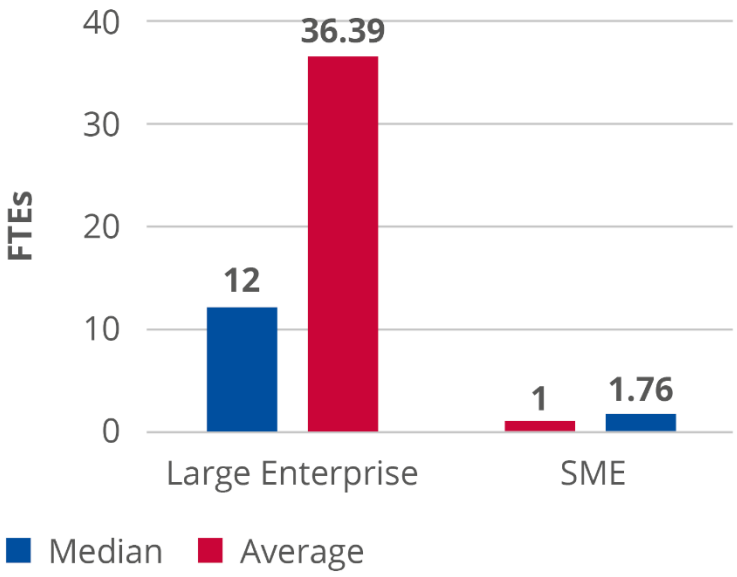
Figure 77: IT FTEs – SMEs vs large enterprises



4.3.2 Information security FTEs for SMEs vs large enterprises

Within the sectors that were identified by the NIS directive, a typical SME employed one FTE, whereas a large enterprise employed 12 dedicated information security FTEs.

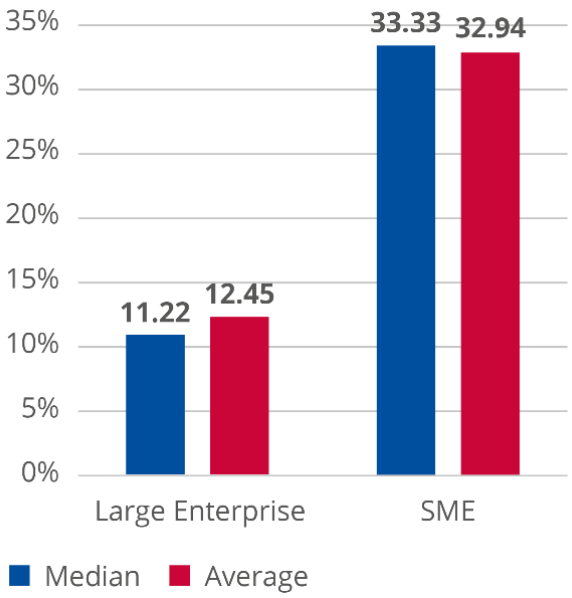
Figure 78: Information security FTEs – SMEs vs large enterprises



4.3.3 Information security FTEs as a share of IT FTEs for SMEs vs large enterprises

A typical SME allocated approximately 33 % of its IT FTEs to information security, whereas this figure stands at 11 % for large enterprises.

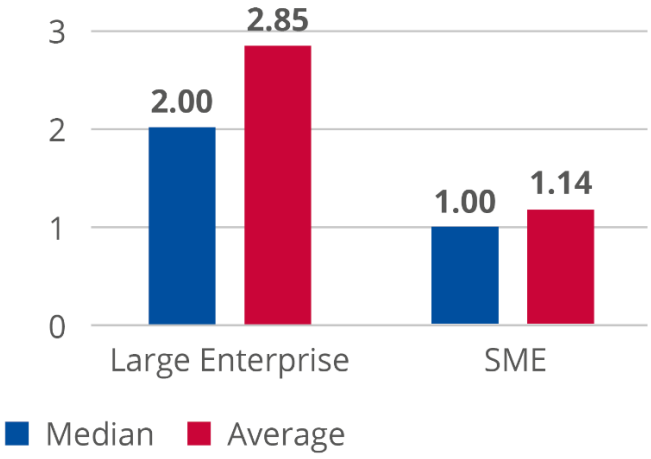
Figure 79: Information security FTEs as a share of IT FTEs – SMEs vs large enterprises



4.3.4 Incident response FTEs for SMEs vs large enterprises

Within the sectors that were identified by the NIS Directive, a typical SME employed one FTE whereas a large enterprise employed two dedicated FTEs for incident response.

Figure 80: Incident response FTEs – SMEs vs large enterprises



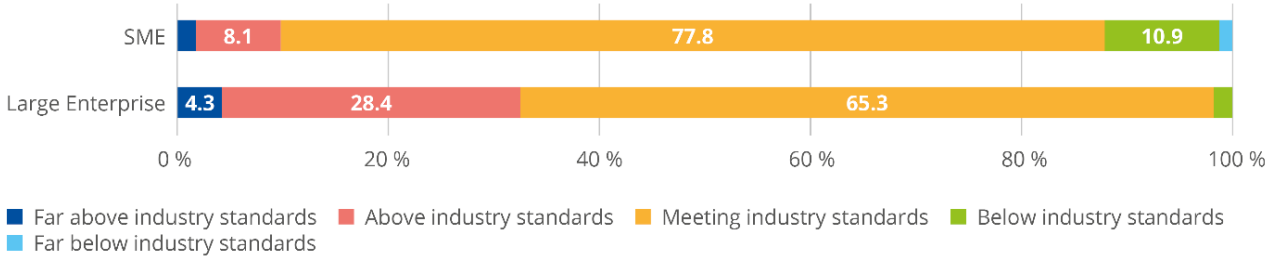
4.4 SECURITY PERFORMANCE FOR SMES VS LARGE ENTERPRISES

According to the data that was collected in the self-assessment, approximately 65 % of large enterprises and 78 % of SMEs consider themselves to meet industry requirements.

We can see a clear discrepancy between SMEs and large enterprises with regards to their self-perceived security performance: only around 10 % of SMEs perceive their information security performance as at least 'Above industry standards', compared to 32.7 % of large enterprises.

On the other hand, approximately 12.3 % of the SMEs answered that their information security performance is 'Below' or 'Far below industry standards', compared to only 2.1 % for the large enterprises.

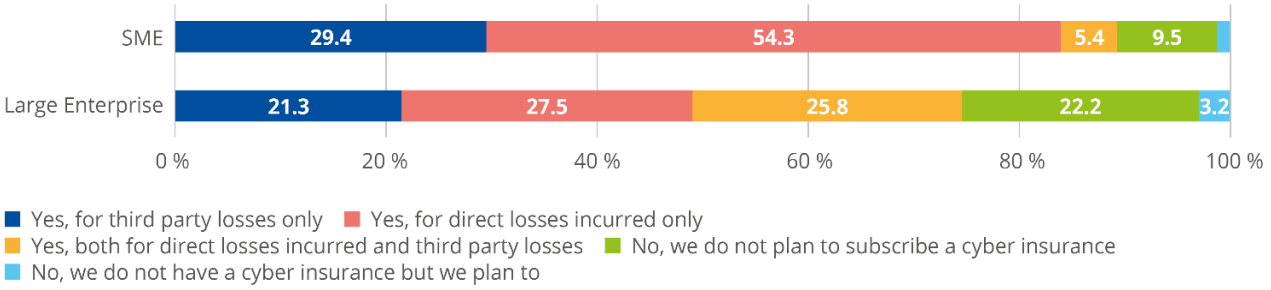
Figure 81: Security performance – SMEs vs large enterprises



4.5 CYBER INSURANCE FOR SMEs VS LARGE ENTERPRISES

The share of SMEs having subscribed to a cyber insurance policy (either for third-party losses or direct losses incurred or both) is around 16 %, compared to 51 % of the large enterprises.

Figure 82: Cyber insurance – SMEs vs large enterprises



5. ADDITIONAL INSIGHTS FROM SELF-ASSESSMENT

By leveraging the data that was collected in this survey, we identified specific practices that influence information security performance (based on a self-assessment of the interviewee).

Survey question: How would you evaluate the overall performance (effectiveness) of your organisation's information security controls?

5.1 INDICATORS ASSOCIATED WITH HIGH SELF-ASSESSED SECURITY MATURITY

In order to identify indicators of information security performance, we isolated and assessed the responses from the organisations that consider their information security performance as 'Far above industry standards' within the self-assessment.

Table 2: Correlation between best practices and security performance

BEST PRACTICES

When...	...the likelihood of a self-assessment score of "far above industry standards", increases by...
Organisations certify their staff, systems and processes as well as buy products with IS certifications	36.36 %
The IS/IT spending is more than 6.10 %	6.29 %
The most senior person dedicated to cybersecurity is the Business Continuity Manager	5.91%
An Organisation has cyber insurance	4.49 %
The most senior person dedicated to cybersecurity is the Information Security Manager, below the C-level	3.65 %
The reporting level of Information Security is the CIO or IT Executive	2.57%

5.2 INDICATORS ASSOCIATED WITH LOW SELF-ASSESSED SECURITY MATURITY

In a similar manner, we isolated and assessed the responses from the organisations that consider their security maturity as 'Below industry standard' within the self-assessment to define certain inadvisable practices.

Table 3: Correlation between inadvisable practices and cyber maturity

INADVISABLE PRACTICES	
When...	**...the likelihood of a self-assessment score of "below industry standards", increases by...**
Organisations only certify their staff	17.44 %
The reporting level for Information Security is either the CEO, Board of Directors or President	14. 58 %
Do not engage in certification	14.48 %
The organisation is classified as an SME	5.28 %
The most senior person dedicated to cybersecurity is the CIO or CTO	4.49 %
The organisation does not have cyber insurance	2.18 %

5.3 INFORMATION SECURITY SPENDING

A thorough analysis of the survey data showed that no distinctive manipulator of information security or share of information security / IT spending could be found in the data set.

6. CONCLUSIONS

This report offers interesting insights into how OES/DSP invest their cybersecurity budgets, both in the context of implementing the NIS Directive, but also from a broader perspective. Furthermore, it examines many additional aspects of cybersecurity for OES/DSP – including the cost of incidents and its key components – and how cybersecurity is organised in terms of reporting lines, cyber insurance products, certifications and more. Most importantly, this report builds on the work done in the previous year by ENISA on the topic and expands the data set to cover all 27 Member States.

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

On a global level, information security budgets seem to be increasing, although information security is still widely recognised as an **exclusive IT discipline**. Cloud access security brokers, vulnerability assessments and web application firewalls are the market segments that are expected to grow most over the next few years. **Skills shortages** persist as an issue for information security staffing: skills in risk management, service management, incident response, threat intelligence, data science / analysis and coding are all expected to be in growing demand in the near future.

Global trends also indicate a **shift of focus to the effectiveness of security controls and capabilities** – not just on the verification of their existence. CISO effectiveness across all required domains should also be emphasised: it is estimated that by 2025, **40 % of boards of directors will have a dedicated cybersecurity committee**, up from less than 10 % today.

The median IT budget for OES/DSP in 2020 was EUR 30 million, of which EUR 2 million was earmarked for information security. OES/DSP in the EU earmarked on median **7.7 % of their IT investments for information security**.

The NIS Directive has been **implemented by 82 % of surveyed organisations**, with **67 % requiring an additional budget for its implementation**. OES/DSP spent a median sum of **EUR 40 000 on implementing the NIS Directive**, while average spending was EUR 98 000. OES/DSP from the energy sector allocated the highest budget to achieve implementation, with a median spending of EUR 66 000.

OES/DSP employ on median 60 IT FTEs, seven of whom are dedicated information security FTEs. Almost **50 % of OES/DSP hired new staff in the context of the NIS Directive implementation**, with a median of four FTEs per sector.

The estimated direct **cost of a major security incident is EUR 100 000** on median. The primary cost factors are related to revenue losses and data recovery or business continuity management. 9 % of the organisations have suffered a major security incident that impacted external stakeholders. The **banking and healthcare sectors experienced the highest cost associated with security incidents**, with median values of EUR 300 000 and EUR 213 000 respectively.

Almost **50 % of surveyed OES/DSP believe that implementing NIS has strengthened their detection capabilities**, while **26 % believe that it has strengthened their ability to recover from incidents**.

In 28 % of the surveyed OES/DSP, the CIO or the CTO is responsible for information security, while in over 50 % of cases, the head of information security reports directly to the CEO, the BOD or the President.

More than **50 % of the surveyed OES/DSP do not possess any form of cyber insurance**, however around 25 % are planning to obtain coverage. At the same time, more than **50 % of OES/DSP certify their systems and processes**.

The majority of the surveyed OES/DSP report that their information security controls meet or exceed industry standards, with only 5 % reporting that they do not meet these standards.

Almost 50 % of the surveyed OES/DSP consider that the NIS Directive has had a significant or very significant impact on their security posture.

The report also examines the relationship between the self-perceived cybersecurity maturity of surveyed organisations and the different parameters covered in the document, such as NIS investments, reporting lines for information security, cyber insurance and certifications. This is an attempt to identify indications about which elements may be more closely associated with OES/DSP cybersecurity maturity. The results indicate **a strong correlation between a very positive self-perception of cybersecurity maturity and the existence of cybersecurity certifications** for processes, people and products. Organisations that certify their staff and systems and buy products with cybersecurity certifications **are 36.36 % more likely to self-assess their cybersecurity maturity as 'Far above industry standards'.** However, this is simply a correlation of data and does not necessarily imply causation.

The data and accompanying analysis presented in this report will hopefully provide useful evidence to support policy discussions around the NIS Directive and the 'NIS 2' proposal currently under discussion, as well as contribute to further policy reflections. Moreover, this report builds on the work done in the previous year and provides an expanded scope and additional streamlining of how the NIS investments data is presented, which can be used to establish a historical tracking of this data over the next years.

A ANNEX: SURVEY DEMOGRAPHICS

A.1 MEMBER STATE AND SECTOR OF SURVEYED ORGANISATIONS

Figure 83: Organisations by Member State and sector

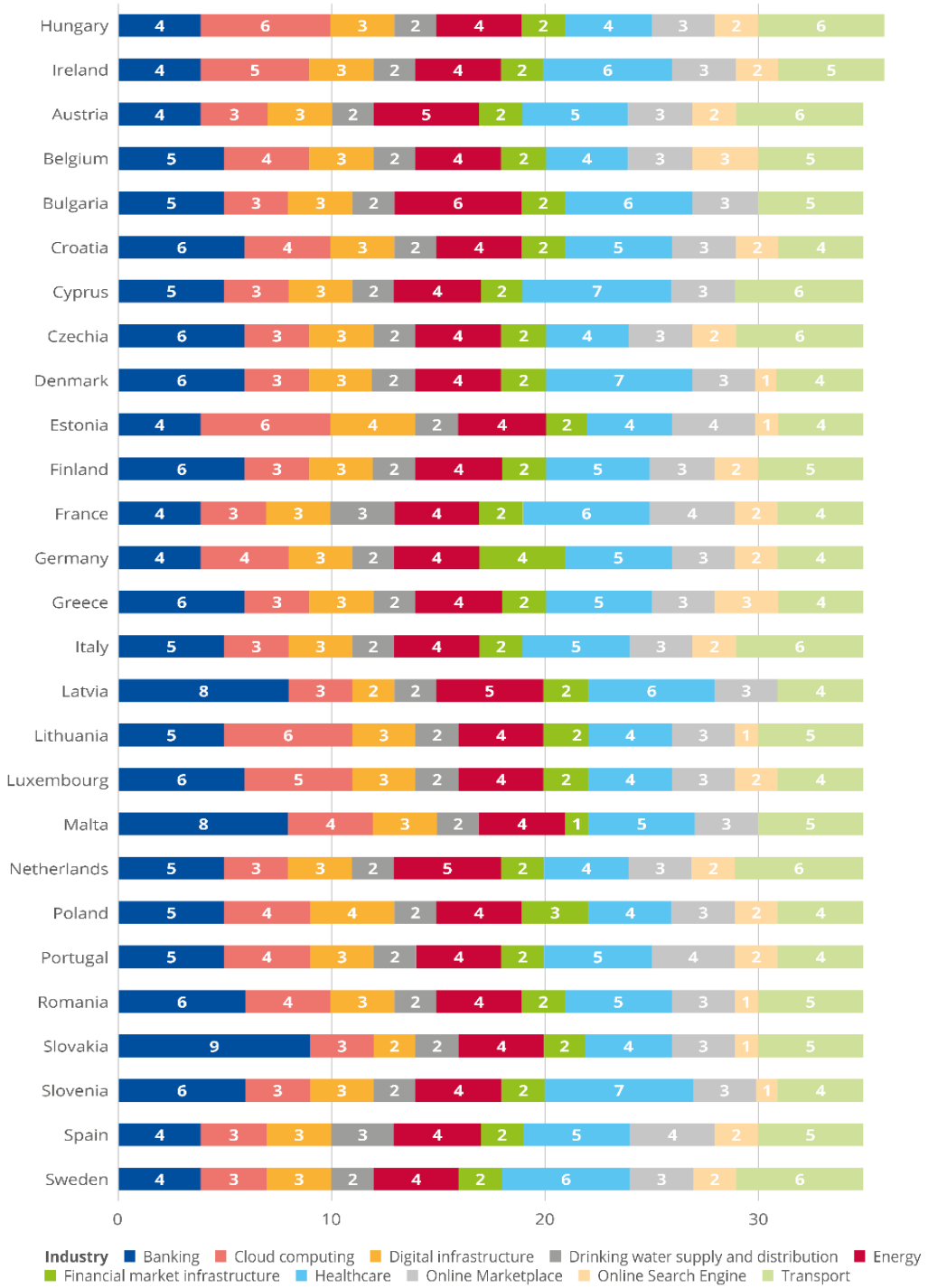
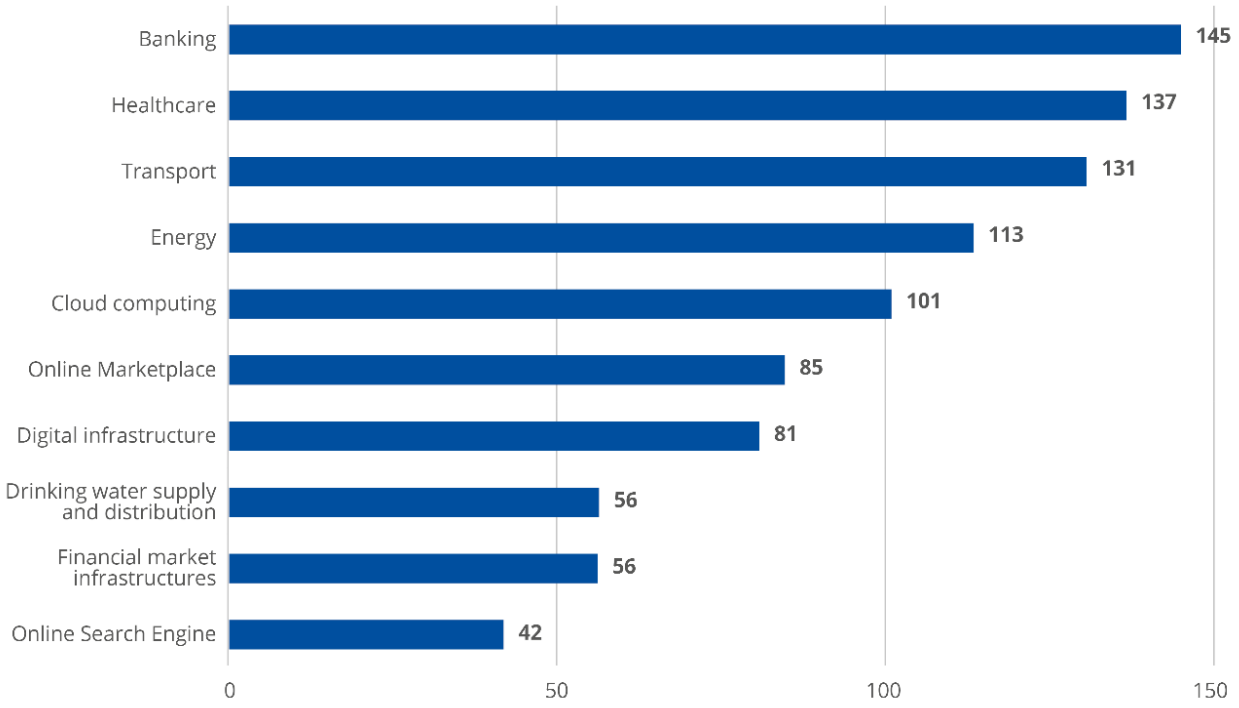


Figure 84: Organisations by sector



A.2 REVENUE BY SECTOR OF SURVEYED ORGANISATIONS

Figure 85: Estimated revenue by sector

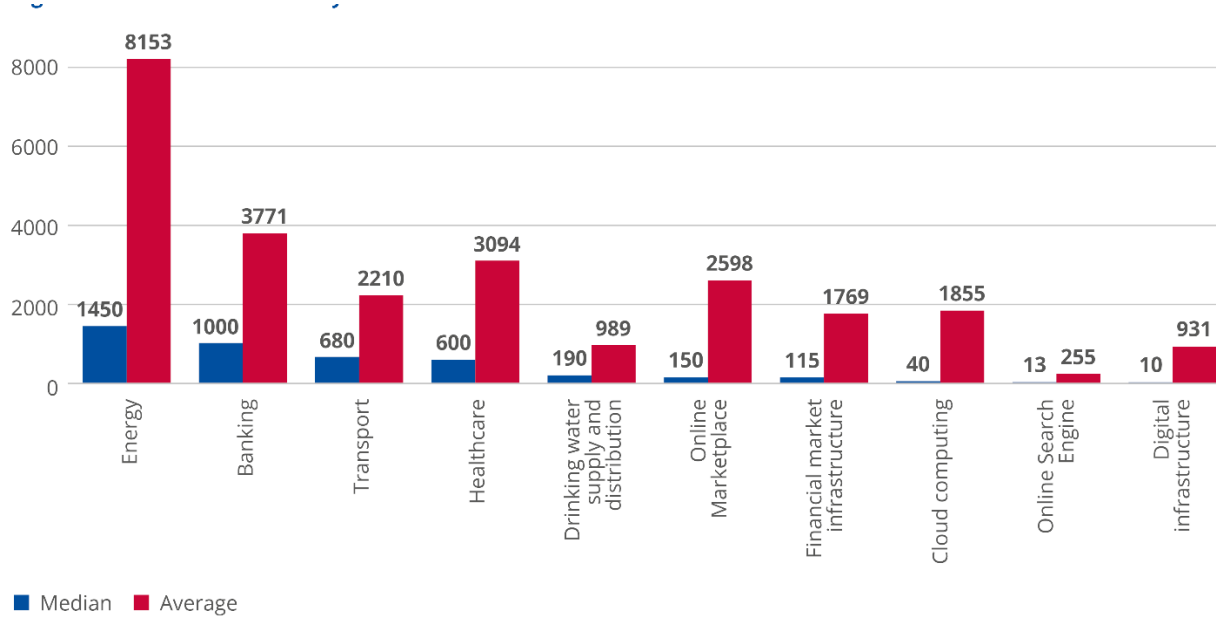
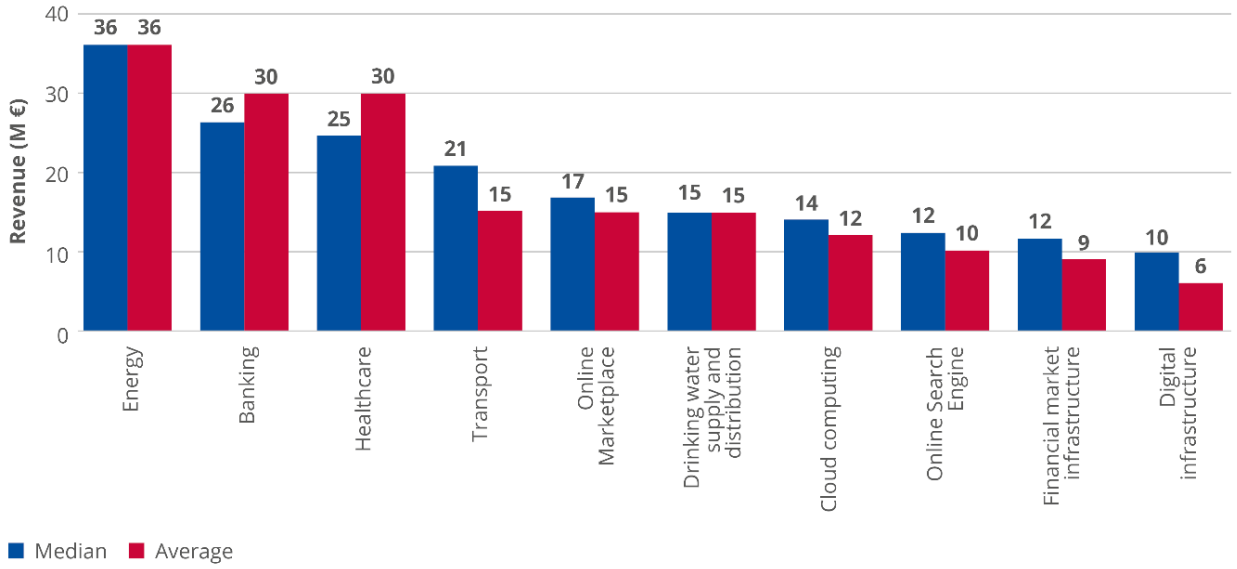


Figure 86: Revenue by sector for SMEs only



A.3 EMPLOYEE COUNT OF SURVEYED ORGANISATIONS

Figure 87: FTEs count by Member State

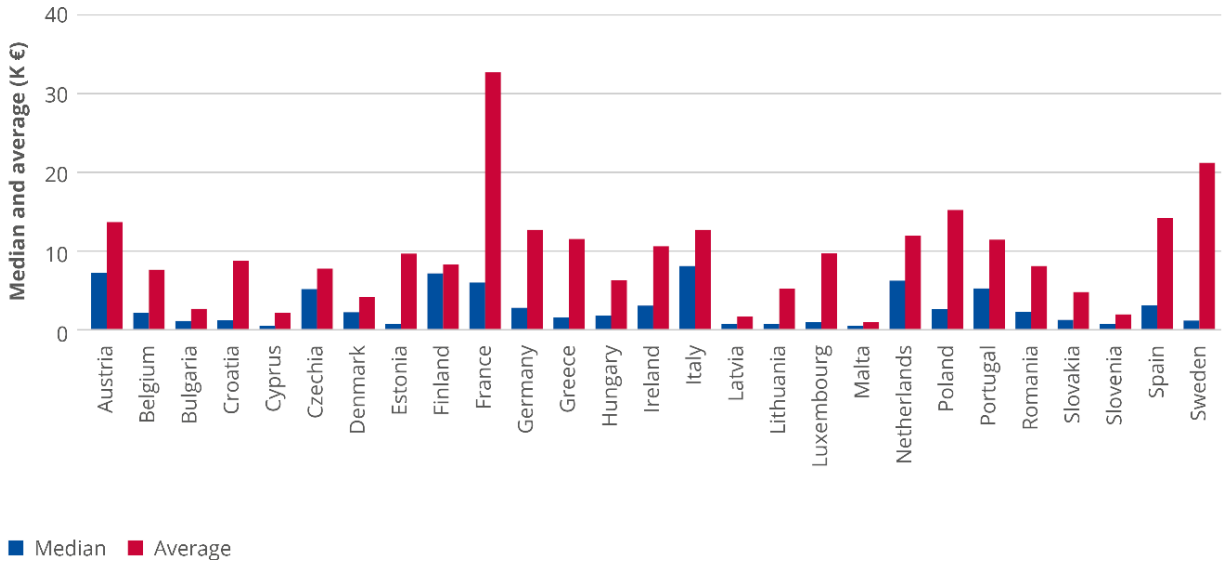


Figure 88: FTEs count by sector

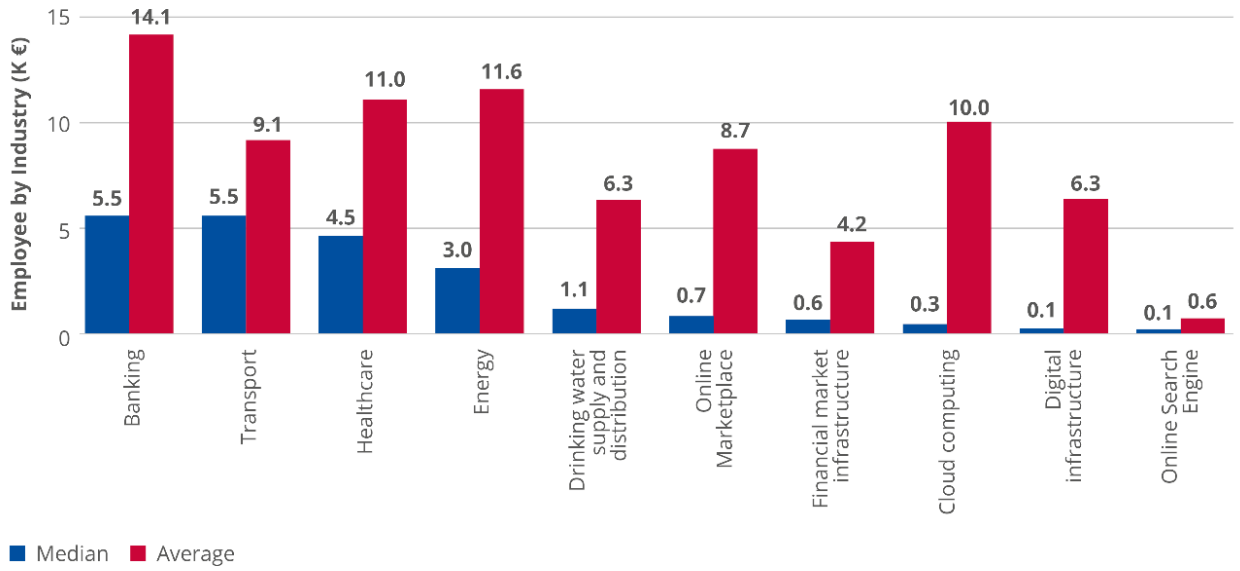
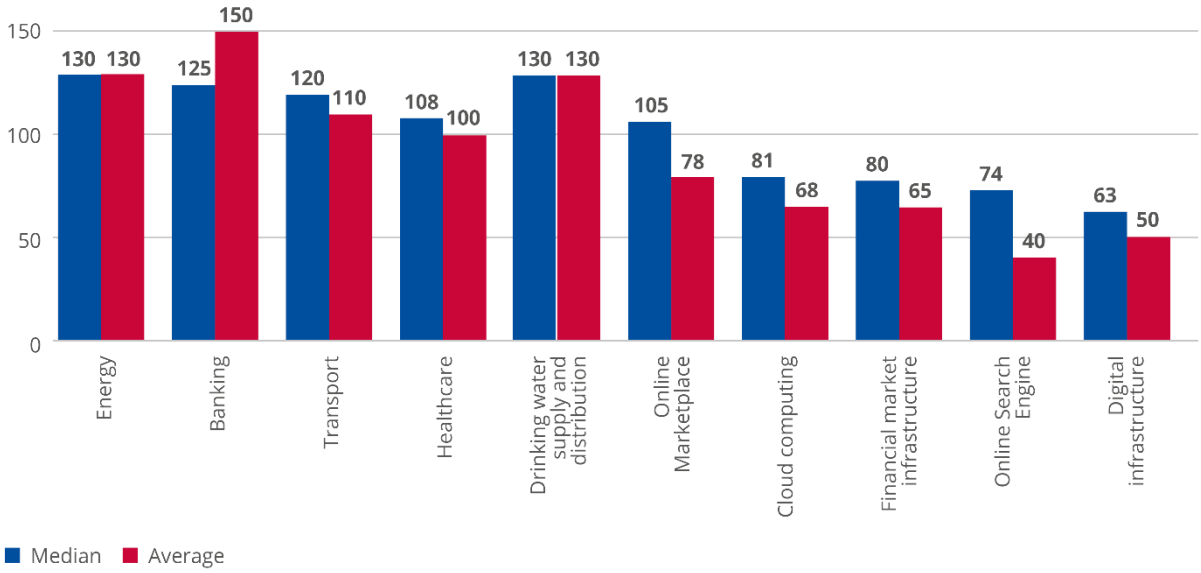
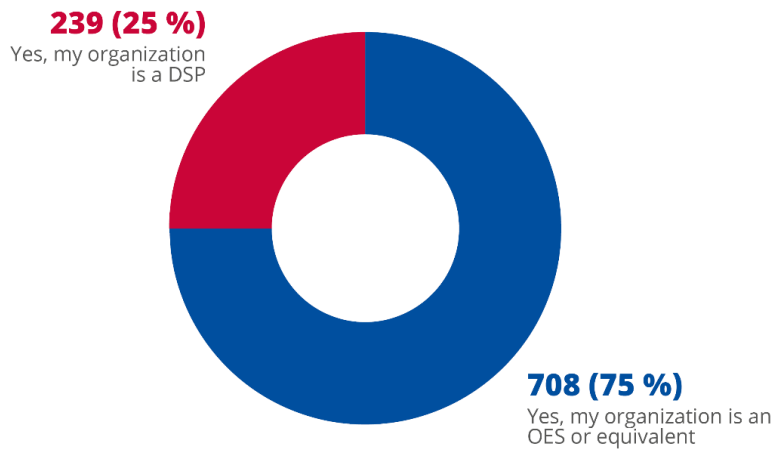


Figure 89: FTEs count by sector for SMEs only



A.4 TYPE OF ORGANISATION (OES VS DSP)

Figure 90: OES vs DSP count



A.5 ADDITIONAL DATA

Table 4: Median information security vs IT spending per sector and most senior role dedicated to information security

Industry	BCM (Business Continuity Manager)	CIO (Chief Information Officer) or CTO (Chief Technology Officer)	CISO (Chief Information Security Officer)	COO (Chief Operating Officer)	CRO (Chief Risk Officer)	CSO (Chief Security Officer)	Information Security Manager below C-level	IT Manager	Total
Banking	10,5 %	6,4 %	6,5 %	7,9 %	5,9 %	6,0 %	10,0 %	6,3 %	7,0 %
Cloud computing	11,6 %	7,3 %	7,1 %		6,4 %		11,0 %	10,8 %	8,6 %
Digital infrastructures		10,0 %	7,8 %	5,0 %	10,0 %	6,1 %	12,0 %	12,7 %	10,0 %
Drinking water supply and distribution		6,1 %	10,8 %	15,0 %	10,4 %	13,3 %	10,0 %	5,0 %	6,3 %
Energy	8,9 %	5,0 %	5,0 %	5,8 %	4,8 %	3,6 %	9,0 %	4,0 %	5,0 %
Financial market infrastructures	8,5 %	8,3 %	12,0 %		3,5 %	20,0 %	6,3 %	5,6 %	6,7 %
Healthcare	9,1 %	6,0 %	7,0 %	7,8 %	8,8 %	6,0 %	12,7 %	12,3 %	7,5 %
Online Marketplace	11,0 %	7,5 %	8,3 %	10,3 %	11,4 %	6,7 %	9,5 %	11,8 %	8,7 %
Online Search Engine		9,0 %	8,2 %	5,6 %	8,6 %		6,1 %	11,3 %	8,3 %
Transport	10,0 %	6,3 %	5,1 %	6,0 %	3,3 %	7,6 %	9,3 %	11,7 %	6,3 %
Total	**10,3 %**	**7,0 %**	**7,1 %**	**7,8 %**	**6,0 %**	**6,0 %**	**10,8 %**	**9,0 %**	**7,5 %**

Table 5: Performance of surveyed organisations vs median Information security / IT spending per sector

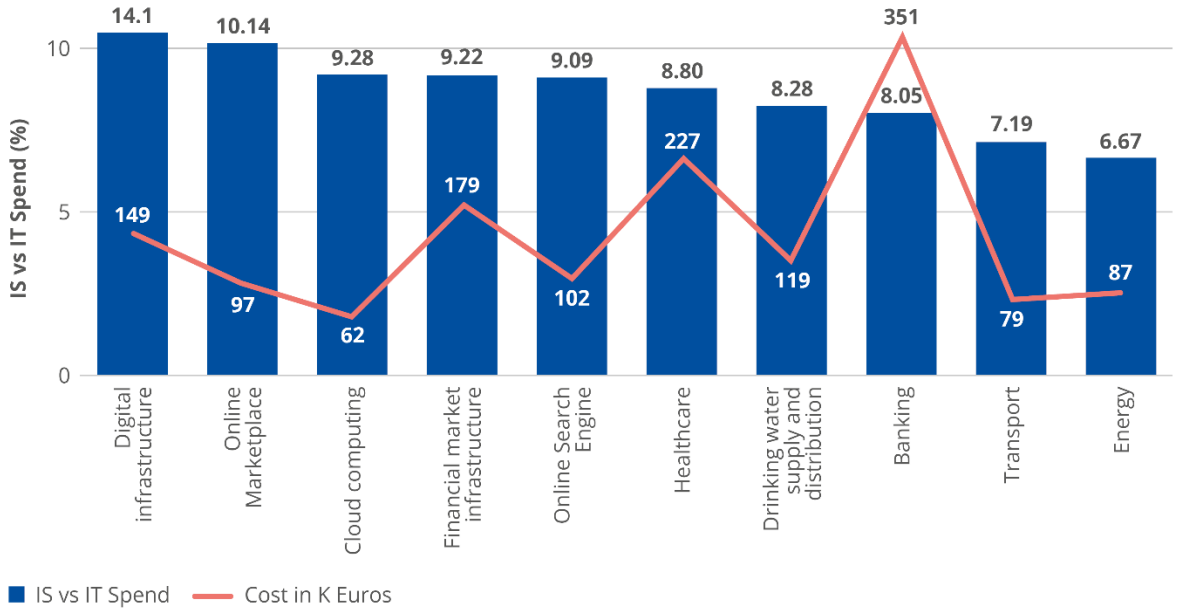
Security Performance	Banking	Cloud computing	Digital infrastructures	Drinking water supply and distribution	Energy	Financial market infrastructures	Healthcare	Online Marketplace	Online Search Engine	Transport	Total
5 - Far above industry standards	7,7 %	10,6 %	11,7 %	3,8 %	9,0 %	8,5 %	9,3 %	7,0 %	6,1 %	10,5 %	**9,2 %**
4 - Above industry standards	7,5 %	11,1 %	8,9 %	10,9 %	7,5 %	8,8 %	7,1 %	8,5 %	7,2 %	6,3 %	**7,9 %**
3 - Meeting industry standards	6,4 %	8,0 %	10,0 %	6,3 %	5,0 %	6,4 %	7,5 %	9,0 %	8,6 %	6,0 %	**7,5 %**
2 - Below industry standards		10,0 %	10,0 %	6,7 %		9,5 %	7,6 %	6,1 %	8,0 %	7,1 %	**7,5 %**
1 - Far below industry standards		7,5 %	12,5 %	7,5 %							**7,5 %**
Total	**7,0 %**	**8,6 %**	**10,0 %**	**6,3 %**	**5,0 %**	**6,7 %**	**7,5 %**	**8,7 %**	**8,3 %**	**6,3 %**	**7,5 %**

Table 6: Performance of surveyed organisations vs median Information security / IT spending per most senior role dedicated to information security

IS Spend per Industry and Security Performance

Security Performance	BCM (Business Continuity Manager)	CIO (Chief Information Officer) or CTO (Chief Technology Officer)	CISO (Chief Information Security Officer)	COO (Chief Operating Officer)	CRO (Chief Risk Officer)	CSO (Chief Security Officer)	Information Security Manager below C-level	IT Manager	Total
5 - Far above industry standards	9,7 %	6,7 %	6,8 %		4,8 %	7,4 %	10,9 %	9,2 %	**9,2 %**
4 - Above industry standards	10,0 %	5,5 %	7,1 %	8,5 %	8,2 %	5,5 %	11,1 %	11,8 %	**7,9 %**
3 - Meeting industry standards	11,2 %	7,3 %	7,0 %	6,9 %	5,6 %	7,5 %	10,0 %	7,0 %	**7,5 %**
2 - Below industry standards		7,1 %	9,4 %	7,5 %	9,1 %		10,8 %	10,4 %	**7,5 %**
1 - Far below industry standards		7,5 %							**7,5 %**
Total	**10,3 %**	**7,0 %**	**7,1 %**	**7,8 %**	**6,0 %**	**6,0 %**	**10,8 %**	**9,0 %**	**7,5 %**

Figure 91: Cost of security incidents vs. ratio of Information security / IT spending



The data shows that there is no correlation between the ratio of information security to IT spending for organisations with the cost of incidents, as the organisations with the highest ratio do not necessarily have a low average of incident costs.

Figure 92: Ratio of information security / IT spending vs ratio of information security / IT FTEs

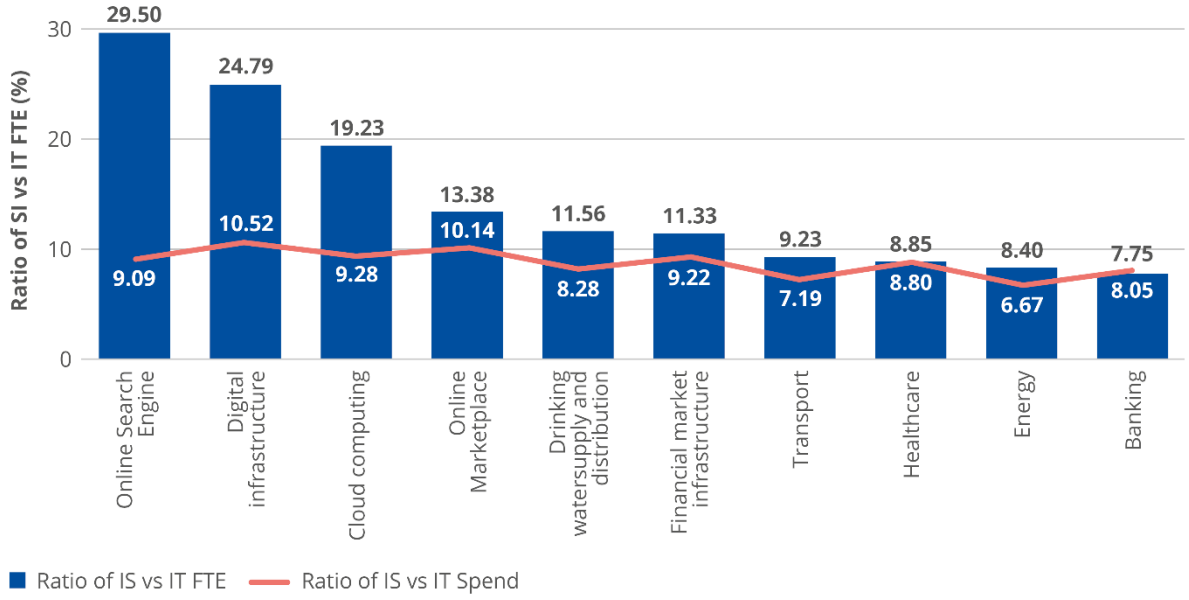


Table 7: Median information security vs IT spending per sector and types of certifications

Certifications	Banking	Cloud computing	Digital infrastructures	Drinking water supply and distribution	Energy	Financial market infrastructures	Healthcare	Online Marketplace	Online Search Engine	Transport	**Total**
1. No certifications		21.7 %	16.0 %	9.6 %			4.3 %	8.3 %	6.0 %	6.7 %	**8.3 %**
2. We certify our staff	11.0 %		6.0 %	9.1 %	9.3 %	9.5 %	10.0 %	10.0 %	5.6 %	6.9 %	**7.5 %**
3. We certify our systems and processes	5.5 %	7.3 %	10.0 %	5.3 %	4.5 %	5.9 %	6.0 %	9.0 %	9.7 %	5.3 %	**6.0 %**
4. We buy products with information security certifications	5.9 %	7.3 %	10.0 %	6.3 %	2.7 %	5.7 %	7.0 %	8.3 %	8.1 %	4.0 %	**5.9 %**
5. We certify our staff , We certify our systems and processes	8.0 %	10.0 %	10.0 %	5.4 %	5.9 %	12.9 %	7.3 %	7.5 %		7.0 %	**7.9 %**
6. We certify our staff , We buy products with information security certifications	7.8 %	7.1 %			9.6 %		5.0 %	11.4 %		2.5 %	**7.5 %**
7.We certify our systems and processes , We buy products with information security certifications	8.3 %	11.1 %	10.5 %	10.1 %	8.3 %	10.0 %	11.9 %	9.5 %	8.7 %	7.5 %	**9.3 %**
8. We certify our staff, We certify our system & processes, We buy products with sec certifications	8.3 %	8.6 %	7.7 %	15.0 %	9.0 %	12.0 %	8.8 %	7.5 %	6.8 %	10.8 %	**8.8 %**
Total	**7.0 %**	**8.6 %**	**10.0 %**	**6.3 %**	**5.0 %**	**6.7 %**	**7.5 %**	**8.7 %**	**8.3 %**	**6.3 %**	**7.5 %**

Table 8: Performance of surveyed organisations vs median information security / IT spending per type of certification

Security Performance	1. No certifications	2. We certify our staff	3. We certify our systems and processes	4. We buy products with information security certifications	5. We certify our staff , We certify our systems and processes	6. We certify our staff , We buy products with information security certifications	7.We certify our systems and processes , We buy products with information security certifications	8. We certify our staff, We certify our system & processes, We buy products with sec certifications	Total
1 - Far below industry standards				7.5 %					**7.5 %**
2 - Below industry standards	8.0 %	6.7 %	10.4 %	10.0 %	6.7 %		7.1 %		**7.5 %**
3 - Meeting industry standards	9.2 %	9.7 %	6.5 %	5.7 %	8.0 %	7.5 %	10.0 %	8.5 %	**7.5 %**
4 - Above industry standards		14.3 %	4.9 %		7.5 %	13.3 %	10.0 %	8.3 %	**7.9 %**
5 - Far above industry standards					9.0 %		6.3 %	9.7 %	**9.2 %**
Total	**8.3 %**	**7.5 %**	**6.0 %**	**5.9 %**	**7.9 %**	**7.5 %**	**9.3 %**	**8.8 %**	**7.5 %**

Table 9: Median information security vs IT spending per sector and cyber insurance solution

Cyberinsurance solution	Banking	Cloud computing	Digital infrastructures	Drinking water supply and distribution	Energy	Financial market infrastructures	Healthcare	Online Marketplace	Online Search Engine	Transport	Total
No, we do not have a cyber insurance but we plan to	5.8 %	6.8 %	10.0 %	6.7 %	5.4 %	6.5 %	6.5 %	9.3 %	8.1 %	7.0 %	**7.1 %**
No, we do not plan to subscribe a cyber insurance	5.5 %	7.8 %	8.3 %	5.6 %	4.3 %	7.6 %	6.0 %	7.0 %	8.7 %	4.3 %	**6.0 %**
Yes, both for direct losses incurred and third-party losses	10.0 %	11.1 %	12.0 %	14.6 %	9.2 %	11.9 %	10.8 %	8.8 %	8.1 %	10.7 %	**10.5 %**
Yes, for direct losses incurred only (network interruption, cyber extorsion, cyber theft)	6.0 %	7.1 %	12.6 %	10.9 %	4.0 %	5.9 %	11.1 %	10.0 %	7.2 %	6.1 %	**7.0 %**
Yes, for third party losses only (data protection and cyber liability, wrongful collection of information)	14.3 %	12.0 %	13.0 %	4.0 %	6.9 %		8.1 %	16.0 %		8.9 %	**9.4 %**
Total	**7.0 %**	**8.6 %**	**10.0 %**	**6.3 %**	**5.0 %**	**6.7 %**	**7.5 %**	**8.7 %**	**8.3 %**	**6.3 %**	**7.5 %**

Table 10: Performance of surveyed organisations vs median information security / IT spending per cyber insurance solution

Security Performance	No, we do not have a cyber insurance but we plan to	No, we do not plan to subscribe a cyber insurance	Yes, both for direct losses incurred and third-party losses	Yes, for direct losses incurred only (network interruption, cyber extorsion, cyber theft)	Yes, for third party losses only (data protection and cyber liability, wrongful collection of information)	Total
1 - Far below industry standards		7.5 %				**7.5 %**
2 - Below industry standards	10.4 %	7.5 %	6.0 %	9.0 %	9.4 %	**7.5 %**
3 - Meeting industry standards	8.0 %	6.0 %	11.0 %	6.7 %	8.9 %	**7.5 %**
4 - Above industry standards	6.0 %	5.8 %	10.7 %	7.7 %	12.0 %	**7.9 %**
5 - Far above industry standards	7.1 %	6.3 %	10.0 %	8.8 %		**9.2 %**
Total	**7.1 %**	**6.0 %**	**10.5 %**	**7.0 %**	**9.4 %**	**7.5 %**

B ANNEX: DEFINITIONS

This annex provides definitions for the industries, security domains and other terms used in Chapter 2, in accordance with the relevant Gartner 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 11: Median and average definitions

Type	Description	Example	Result
Arithmetic mean	Sum of the values of a data set divided by the 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 annualised average rate of revenue growth between 2 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 2 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 12: SME definitions

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

B.4 FINANCIALS

- **Operational expense** is defined as the total expense associated with the business units supported by the IT organisation. This includes items such as selling, general and administrative expenses, cost of goods sold (or cost of revenue), research and development, depreciation and depletion and amortisation expenses. For insurance, this includes underwriting expenses, loss and loss-adjustment expenses. For banking organisations, it includes interest expenses and noninterest expenses. For government and non-profit organisations, it is represented by the enterprise operating budget.
- **Total IT spending** is defined as total spending at the end of the 12-month budget period for IT to support the enterprise. IT spending/budget can come from anywhere in the enterprise that incurs IT costs and is not limited to the IT organisation. It includes estimates by enterprises of decentralised IT spending and or 'shadow IT'. It is calculated on an annualised 'cash flow view' basis and therefore contains capital spending and operational expenses, but not depreciation or amortisation.

B.5 INDUSTRIES

- **Banking and financial services:** organisations whose primary revenue stream is derived from one or more of:
  - banking: commercial banks, diversified banks, central depository reserve institutions, federal reserve banks, international trade financing, private and industrial banking, regional banks, national and state commercial banks, thrifts and mortgage finance;
  - other financial services;
  - diversified financials, capital markets, asset management and custody banks, investment funds, investment banking, loan syndication services, merger and acquisition advisory services, private placement advisory services, debt and equity underwriting services, investment brokerage services, investment advice, institutional investment advice, personal investment advice, securities and commodities markets services, commodity contract services, commodity brokers, commodity contract pool operators, commodity contract trading organisations, etc.
- **Education:** organisations whose primary revenue stream is derived from one or more of:
  - higher education;
  - colleges, universities and junior colleges;
  - other (professional schools, elementary and secondary schools, vocational schools, specialty educational services. automobile driving instruction, child daycare services, educational curriculum development, exam preparation and tutoring, online education courses and online training services).
- **Energy**: organisations whose primary revenue stream is derived from one or more of:
  - energy services, oil and gas drilling, oil rig services, oil and gas field services, oil and gas exploration and production, oil and gas exploration services, mixed, manufactured and liquefied petroleum gas production, oil and gas extraction;

- oil and gas refining and marketing, petroleum and petroleum products, crude petroleum and natural gas, gasoline, lubricating oils and greases, natural gas liquids and petroleum refining;
- oil and gas storage and transportation, natural gas pipelines and oil and gas pipelines.

- **Natural resources**: organisations whose primary revenue stream is derived from one or more of:
  - gold, gold ores, silver ores, precious metals and minerals, non-metallic mineral mining, precious gemstone mining and production precious metal ores, etc.;
  - rolling, drawing, and extruding of diversified metals, diversified metal foundries and castings, copper foundries, diversified metal die-castings, injection moulding and die casting, drawing and insulating of diversified metal wire, copper wire drawing, fibre optic cable, rolling, drawing, and extruding of copper, copper powder, paste and flakes and smelting and refining of diversified metals;
  - agricultural services, animal services, horses and equine services and breeding, livestock services and crop services.
- **Government:** organisations from national governments, international organisations performing government services and government-affiliated organisations.
- **Government – state/local:** organisations from state/province and local governments and government-affiliated organisations.
- **Healthcare providers:**
  - healthcare facilities, assisted living facilities and services, nursing homes, retirement communities, hospitals and healthcare centres, veterinary services and animal hospitals, healthcare services, dental services, home healthcare services, midwifery and child birth preparation services, nursing services, specialist services, chiropractic services, optometry services and healthcare referral services;
  - medical laboratory services, mental care facilities, rehabilitation services, occupational therapy services, physical therapy services, speech and language therapy services, medical practice organisations, physician practice management organisations, primary care practitioner services and ambulance services.
- **Electronics and electrical equipment providers:**
  - computers and peripherals, computer hardware, computer components, industry specific electronics, automated teller machines, personal computers and accessories, computer audio equipment, desktop computers, game controllers, keyboards and pointing devices, laptop computers, monitors, multimedia devices, printers, scanners, servers, computer storage and peripherals and networking equipment;
  - electronic equipment, instruments and components, amplifiers, antennas, electronic component, resistors and diodes, receivers, switches, transceivers, transformers, electronic connectors, liquid crystal display screens, microelectronics, nanotechnology, optoelectronics, photodetectors, power assembly, solid state switches and relays, measuring, analysing, and controlling instruments, electronic laboratory apparatus, security, control, surveillance and detection equipment, law enforcement equipment, alcohol and narcotic testing devices, electronic manufacturing services and electronics manufacturing equipment;
  - defence electronics, command, control and communication equipment, electronic warfare systems and infrared sensors;
  - semiconductors and semiconductor equipment, semiconductor manufacturing machinery, automatic testing equipment, semiconductor fabrication facility support equipment, semiconductor handling, assembly and packaging equipment, deposition equipment, etching and cleaning tools, photolithography equipment, analogue and mixed signal semiconductors, digital semiconductors, logic devices, memory chips, microcontrollers and microprocessors;

- electrical equipment, electrical components and equipment, batteries, electric lighting and wiring equipment, electrical apparatus, relays and industrial controls, electromagnetic devices and magnetic and optical recording media devices;
- heavy electrical equipment, power generation equipment, industrial lasers, motors and generators, outboard electric motors, portable generators, transmission and distribution equipment, alternative-energy-producing equipment, photovoltaic cells and fuel cells.

- **Food and beverage (processing):**
  - food products, agricultural products, fruits, vegetables, and nuts, grain and field beans, packaged foods and meats, animal feed, bread and bakery products, confectionery products, candy, chewing gum, chocolate and cocoa products, mints, dairy products and eggs, edible oils, ethnic foods, frozen foods, grain mill products, cereal breakfast foods, health and breakfast bars, flour, prepared flour mixes and dough, meats, meat processing and meat-related products, meat processing, organic foods, prepared and preserved foods, desserts and dessert toppings, dietary foods, infant food, packaged food mixes, pasta, prepared soups and stews, preserves, jams, jellies and nut spreads, sandwiches and filled rolls, snack food, seafood, seafood processing and seafood products, animal and plant aquaculture, commercial fishing, fish hatcheries and preserves and seafood products;
  - seasonings and preservatives, herbs, spices and extracts, sauces and salad dressings, vinegar and cooking wines, sweeteners, artificial sweeteners, sugar and syrup;
  - beverages, brewers, distillers and vintners, soft drinks, bottled water, chocolate, malt and drink mixes, flavouring extracts, flavouring syrup and concentrate, powdered drink mixes, juices, manufactured ice, non-carbonated drinks, soda and other carbonated drinks.
- **Manufacturing:** organisations whose primary revenue stream is derived from one or more of:
  - railroad equipment, locomotives and electronic trolleys, railroad support equipment and systems, railway and tramway cars, automobile manufacturers, passenger motor vehicles, recreational vehicles, safety and rescue motor vehicles, motorcycle manufacturers, auto parts and equipment and motor vehicle tires;
  - passenger and cargo aircraft and airplanes, aircraft de-icing equipment, aircraft refuelling equipment, aircraft composite structures, aircraft engines and engine parts, aircraft fuel tanks and systems, aircraft fuselage and components, aircraft landing and braking systems, aircraft propulsion systems, fluid power aircraft subassemblies, construction and farm machinery and heavy trucks, ship and boat building, ship and boat repairing and ship and boat scaling;
  - military satellites, navigation satellites, scientific and research satellites, weather satellites, spacecraft, space structures and components, rockets and subsystems, weapons, military aircraft, military armoured vehicles and military watercraft;
  - industrial machinery, chemical processing machinery and equipment, rubber and plastics processing machinery, food and beverage machinery, industrial filtration systems, air and gas compressors and air purification equipment;
  - machinery components, ball and roller bearings, pumps and pumping equipment, automatic vending machines, machinery and equipment for material handling, metal and mineral mining, metalworking, printing, recycling and reclamation, service industries, textiles, commercial laundries and dry cleaning and pressing;
  - oil and gas machinery and equipment, oil and gas field exploration machinery, oil and gas production equipment and well drilling machinery and equipment;
  - office furnishings and equipment, classroom and institutional furniture, bookcases, chairs, desks, file cabinets, wood office furniture, workstations and office storage units.

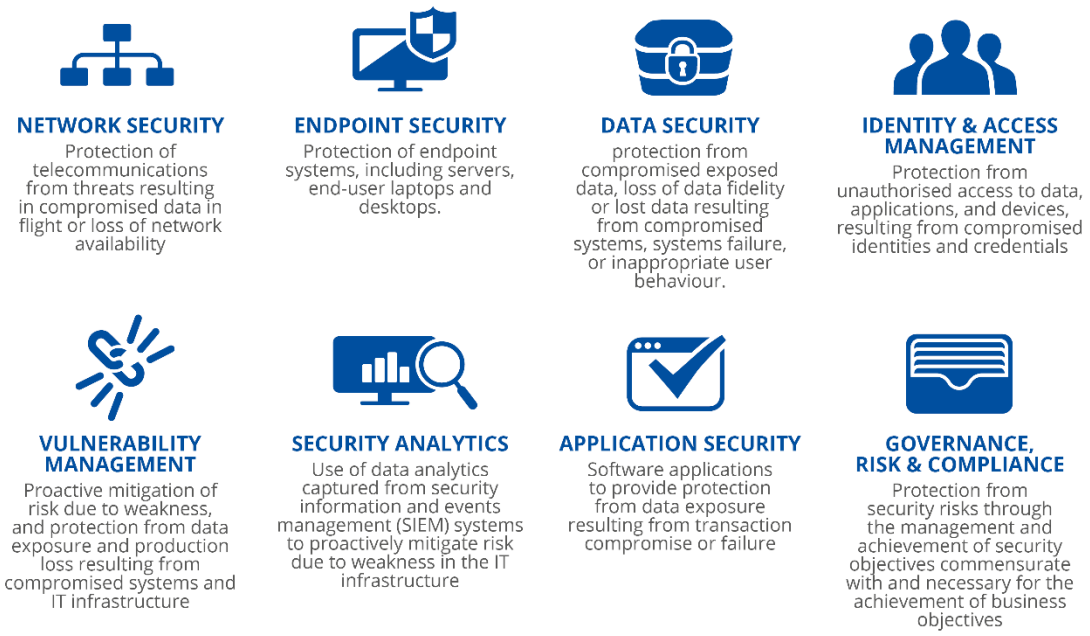
- **Pharmaceuticals (and life science):**
  - pharmaceuticals, generic pharmaceuticals, hormones and hormone antagonists, vaccines, medicinal chemicals and botanical products, non-prescription drugs, veterinary drugs, vitamins and nutritional supplements;
  - pharmaceutical contract laboratories, pharmaceutical contract manufacturing services, pharmaceutical contract research organisations and pharmaceutical research and development;
  - biotechnology, agricultural biotechnology, biological products, biotechnology research equipment manufacturers, combinatorial chemistry and other lead-generating technologies, drug delivery technologies, gene research and development, in vivo (in the body) diagnostic substances, microbiology, orthobiologic products, protein and genome sequence products, RDNA pharmaceuticals and life sciences tools and services.
- **Professional services:**
  - commercial services: commercial rental and leasing services for office equipment, computers, passenger and cargo aircraft, construction, oil and gas, and other machinery, commercial design services, commercial interior design, fashion and other design services, commercial photography, advertising services for broadcast, internet, radio, television, direct mail, point of sale and print marketing services, marketing consulting, market research, public relations services, investor relations services, telemarketing and services. general management services, facilities support management services, risk management services, outsourced business services, security and safety services, human resource and employment services, human resources and personnel management, professional and management development training, secretarial services, temporary help supply, online recruiting and job listing services, real estate investment trusts and real estate management and development;
  - research and consulting services, legal services, social sciences and humanities research, non-healthcare-related testing laboratories, IT services, data processing and outsourced services, infrastructure services, application management, computer facilities management services, data management, data recovery, data storage services, infrastructure consulting, remote data backup, data processing and entry services, data warehousing, enterprise resource planning and hardware services;
  - residential design services, residential interior services, residential security and personal safety services, ticket sales, sanitary services, cesspool and septic tank cleaning, hazardous waste collection, diet and weight reducing services, consumer electronics repair services, camera repair, radio and television repair, telephone and communications equipment repair, electrical repair, refrigeration and air conditioning repair, re-upholstery and furniture repair;
  - environment, conservation and wildlife organisations, humane societies, membership organisations, business associations, civic, social and fraternal associations, farm business organisations, labour unions and labour organisations, professional membership organisations and political organisations.
- **Retail and wholesale:**
  - internet and catalogue retail, department stores, general merchandise stores, apparel retail, motor vehicle retail, motor vehicle renting and leasing, motor vehicle repair and services. oil and gas retail, fuel and bottled gas dealers, gas stations, computers, software, electronics and camera retail, home furnishing and home improvement retail, automatic vending machines, florists, gift and novelty, healthcare and medical supplies, household products, housewares, leisure equipment, music, newspaper and magazines, office furnishings, food and drug retail including pharmacies, grocery stores and supermarkets, seafood stores and markets, tobacco retail, hypermarkets and super centres;

- distributors including food, healthcare equipment, pharmaceuticals, technology, machinery, building products, chemicals, apparel and textiles, household durables, jewellery, leisure equipment, office furnishings and equipment, electrical equipment, media, paper and forest products and transportation equipment and supplies.

- **Software publishing and internet services:**
  - internet software and services, agents and spider software, browser software, content management software, tracking software, plug-in software, search engine software, website management software, website infrastructure software, application hosting services, application service providers, custom website design and business solutions, online research services, online small business portals, online supply customer relationship management software, document management software, EDI, enterprise data management, enterprise information portals, enterprise middleware, multimedia software, office and home productivity software, home entertainment software, educational and training software, entertainment software, computer games, computer game console platforms, systems software, automation products and services, backup and recovery software, computer telephone integration software, design automation software, maintenance encryption software, network administration and operating system software.
- **Telecommunications:**
  - communications equipment, communications processing equipment, communications towers, telephone and telecommunications equipment, telecommunications equipment, integrated services digital network equipment, private branch exchange network equipment, switchboard equipment, telephone switching equipment, telephone equipment, paging systems, teleconferencing equipment, wireless telephone equipment, wireline telephone equipment, answering machines and cordless telephones;
  - telecommunications services, diversified telecommunications services, alternative carriers, broadband telecommunications services, asynchronous transfer mode network services, digital telecommunications services, digital subscriber line services, integrated services digital network services, point to point digital telecommunications services, fibre telecommunications services and virtual private network services.
- **Transportation:**
  - air freight and logistics, air courier services, national postal delivery services, airlines, commercial airlines, helicopter transportation services, private or business aircraft services, tankers, marine transportation of passengers, ferries, dock and pier operations, floating dry docks, marinas, marine cargo services, marine salvage, cruise ships. railroad transportation of freight, railroad transportation of passengers, commuter rail systems, trucking, road transportation of freight, road transportation of passengers, carpool and vanpool operations, livery services, limousines and taxicabs.
- **Utilities:**
  - electric utilities, electric power generation by solar, wind, fossil fuels, nuclear and hydro, electric power distribution, electric power transmission and control, gas utilities, natural gas transmission, retail energy marketing, independent/merchant power, water utilities, wastewater treatment and water distribution.

B.6 IT SECURITY ANALYSIS FRAMEWORK

Figure 93: IT security analysis framework



- **Identity and access management** is the discipline that enables the right individuals to access the right resources at the right times and for the right reasons. It comprises a set of practices, processes and technology responsible for the management of digital identities and their associated access to resources. Specific related activities are: user account provisioning, password management, user access administration (e.g. changes in roles, position or status), directory integration, single sign-on, active directory, remote access services, strong or multi factor authentication / two-factor / three-factor, hard and soft token-based authentication services, public key infrastructure and federation-type services, privileged user management, identity and access governance (including the processes for user access certification/re-certification, attestation, application access audits, etc.) and cloud-based identity services (e.g. IDaaS).
- **Network security** comprises measures taken to protect a communication pathway from unauthorised access to, and accidental or wilful interference with, regular operations, and hence involves protecting computers and computer networks from attack and infiltration. Network security provides network protection through the restricting of network traffic, based on a set of policy-defined rules. Network security provides protection at key ingress and egress points in the form of perimeters, segments and zones, typically defined and enforced by firewalls/NGFWs/firewall administration, wireless access firewalls/RASP, network intrusion detection and prevention, virtual private networking concentrators, hardware security modules, proxy servers, secure email and/or web gateways, unified threat management appliances, network access control services and distributed denial of service protection and prevention services.
- **Endpoint security** is a set of capabilities and services provisioned across devices and platforms to provide the required and expected level of protection against potential compromise resulting from inappropriate configuration, use or attack(s). It covers the security services, capabilities and associated management and support thereof used in the protection of all endpoint devices such as desktops, servers, laptops and mobile devices which users leverage to access corporate data and information. Specific

examples would typically include antivirus/anti-spyware/anti-malware software on PCs and servers, mobile device management, device encryption and management, host intrusion detection and prevention, hardware-based protection (e.g. personal firewalls), advanced anti-malware and threat detection software and also any physical security control in place for these assets (e.g. locks).

- **Data security** ensures confidence in the ability of users, systems and business processes to provide the required and expected level of protection from data compromise or loss of data fidelity resulting from system compromise or failure, or inappropriate user behaviour with regard to data in whatever stage of its lifecycle. It focuses on confidentiality (to protect against unauthorised or inappropriate access), integrity (to ensure data is not improperly changed or deleted), availability (to ensure appropriate access to data for the right parties) and privacy (to assure personal information is only used for the specific business purpose for which it was collected). Typical data security protection capabilities include data discovery and classification, encryption/decryption of data 'at rest', 'in motion' or 'in use' (including endpoint and bulk storage data encryption/decryption), digital certificate lifecycle management for digital signature-based services, privacy enforcement techniques (data masking), database audit and protection techniques, data loss prevention services and data destruction and removal and erasure-type services.
- **Vulnerability management** is the process cycle for finding, assessing, remediating and mitigating security weaknesses. It comprises the policy and scope definition, proactive identification, remediation, mitigation and ongoing monitoring of security vulnerabilities via dedicated vulnerability assessment and management products and services. These services typically scan enterprise networks (IP ranges) and establish a baseline and trending of vulnerability status of devices, applications and databases; identify and report on the security configuration of IT assets; discover unmanaged assets; support specific compliance reporting and control frameworks; support risk assessment and remediation prioritisation; and support remediation by IT operations groups which involves scanning (through resident agents on network-attached devices) of all internal and external facing target applications or devices for vulnerabilities, to determine if they are at latest available historic patch level. Service typically also includes periodic penetration testing, vulnerability assessments, asset auto discovery, generation of patch and vulnerability status compliance reports, vulnerability monitoring and ticket raising.
- **Security analytics** comprises the ability of the security program via technologies, processes and people to identify, define, react and remediate against potential or current or active attacks and the associated threat actors, that may result in system or service compromise, breaches or data loss events. It is essentially a set of services delivered by a security operations centre (SOC) or equivalent capability consisting of a centralised focal point of security specialists where enterprise information systems (websites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended, and action plans devised to counter any undesirable events detected. Typical security analytics services include security incident and event log collection, monitoring and management (SIEM), managed log retention and analysis, user behaviour analytics (UBA), threat intelligence services, fraud detection and response services, digital forensics and cyber incident response services.
- **Application security** describes the use of software, hardware, staff and process methods to provide through life application protection from threats. It therefore comprises a set of measures built into the application development process to prevent the unauthorised access, theft, modification or erasure of sensitive data through the exploitation of applications. Specific examples include: the identification of security flaws in application design, development, deployment, upgrade, or maintenance through code assurance techniques such as black box analysis and testing, health checks, the use of static and dynamic application testing techniques and application

security frameworks, and/or via data obfuscation, filtering and masking, secure coding practices and software composition analysis (SCA), etc.

- **Governance, risk and compliance management** generally comprises the set of practices and processes, supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organisation manages its unique set of risks.
  - Security governance is thus defined as a number of 'cross-functional' security activities which include the development and maintenance of security policies, standards and procedures, the communication of business values, culture and principles, security strategy and organisation, training and awareness, documentation and guidance, communication plans, security service metrics, audit and compliance oversight, financial management of security services, security vendor management, security PMO etc. obligations. Governance costs and staffing include the strategic leadership of security standards, policies and practices, as typically represented by the CISO (or equivalent) and their immediate office.
  - Risk management is defined as the function dedicated to ensuring that adequate controls are designed and implemented to mitigate the various risks associated with IT assets (including data), infrastructure and processes. It includes activities such as periodic and annual IT audits (non-regulatory), risk assessment / monitoring, issue management and action tracking, and the development and execution of remediation plans.
- Compliance management is the process of identifying, managing and reporting compliance activities related to organisational, commercial and regulatory compliance obligations. Compliance requirements can be derived from internal directives, procedures and requirements, or from external laws, regulations, standards and contractual agreements.

B.7 SECURITY ASSET TYPES

- **Hardware** is defined as follows:
  - All dedicated hardware assets utilised in support of the security operations, for each category indicated (i.e. network security, endpoint security, etc.).
  - Examples include firewalls, security gateways, security appliances, security toolset platforms and ID tokens.
  - Only annual asset costs that are directly or recognisably related to the defined in-scope security functions are included. Costs of hardware assets whose prime purpose is not security are not included. For example, there may be routers deployed that have firewall, encryption or NIPS capabilities, but any apportionment of their annual costs cannot be included unless a cost to specifically enable a security function – such as a firewall 'add-on' enabler cost of extra router hardware or software – can be identified.
  - Hosting/facilities/occupancy costs for space dedicated to in-scope security hardware, such as the apportioned annual costs of hosting security-related devices, storage arrays and appliances in the data centre, including power / heat management and raised floor. It also includes the annual cost of any consumables related to the security activities.
- **Software** is defined as follows:
  - Annual licence and maintenance, along with costs associated with new purchases and upgrades for all software dedicated to operating or managing the security systems applications for each category of security expenditure.
  - Examples include endpoint security suites, identity and access management, security information and event management and content filtering.

  - Only software licence costs that are directly or recognisably related to the defined in-scope security functions are included. Costs of software whose prime purpose is not security are excluded.
  - For example, there may be enterprise licences for operating systems, productivity suite software or enterprise packages that have security capabilities (e.g. BitLocker encryption in WinOS). No apportionment of their annual costs is included unless a cost to specifically enable a security function can be identified. An example would be an 'add-on' software charge for a security capability or a specific module licence charge for security functionality (e.g. Oracle Identity Manager).
- **Outsourcing** is defined as follows:
  - Outsourcing is the use of external service providers to effectively deliver IT-enabled business process, application service and infrastructure solutions for business outcomes. Outsourcing, which also includes utility services and cloud-enabled outsourcing, helps clients to develop the right sourcing strategies and vision, select the right IT service providers, structure the best possible contracts and govern deals for sustainable win-win relationships with external providers. Outsourcing can enable enterprises to reduce costs, accelerate time to market and take advantage of external expertise, assets and/or intellectual property. This includes:
    - fees for third-party or outsourcing contracts primarily comprising services for managing or monitoring security devices, systems or processes where the services are provided on-site.
    - managed service provider / cloud is defined as: remote subscription-based monitoring and/or management of security devices such as firewalls, intrusion detection and prevention functions via customer-premises-based or network-based devices. It also includes remotely delivered specialist managed security services such as threat intelligence, SIEM/SOC, distributed denial of service, etc., and cloud-based security services such as IDaaS.
    - consulting, defined as: security advisory services that help organisations analyse and improve the efficacy of business operations and technologies strategies.
- **Personnel** is defined as follows:
  - Costs/FTEs include in-house and contract personnel supporting IT operational infrastructure security, vulnerability management and security analytics, application security and governance and risk and compliance management.

TP-AM-21-001-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 raising awareness, 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. For more information, visit 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 978-92-9204-537-1
doi:10.2824/77127