EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NIS INVESTMENTS

DECEMBER 2020

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, Georgia Bafoutsou, Viktor Paggio EU Agency for Cybersecurity

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-442-8 - DOI 10.2824/50973

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Directive on Security of Network and Information Systems (NIS Directive) represents the first EU-wide legislation on cybersecurity, with the objective to achieve a high common level of cybersecurity across all European Union (EU) 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).

82% of surveyed organisations acknowledge a positive impact of the NIS Directive on their information security

Four years after the NIS Directive entered into force and two years after the transposition by Member States into their national laws, this report presents the findings of a **survey of 251 organisations** across **five EU Member States** (France, Germany, Italy, Spain and Poland) with regards to NIS investments. The report depicts and analyses **how OES and DSPs spend their information security budget** and provides indications as to **how this spending has been influenced by the introduction of the NIS Directive**. The results of this NIS survey were correlated with Gartner security data and insights observed globally and in the EU in order to better understand the current NIS Directive adoption dynamics and impact on related investments.

This report provides comprehensive data and insights regarding the NIS Directive adoption and the effects on the information security budget, staffing, solutions adoption and security posture of organisations within its scope.

Overall, **82% of surveyed organisations acknowledge a positive impact of the NIS Directive on their information security.**

Regarding the NIS Directive implementation, the collected data revealed the following:

- More than 80% of surveyed organisations declared that their NIS Directive implementation program is either completed or in progress. The average NIS implementation program is between 14 and 18 months
- The average budget for NIS Directive implementation projects is approximately 175 K€, with 42.7% of affected organisations allocating between 100 and 250 K€. A little under 50% of surveyed organisations had to hire additional security matter experts (both internally and through staff augmentation), in the majority of cases hiring up to 4 FTEs
- Surveyed organisations prioritised the following security domains: Governance, Risk and Compliance (GRC), Network Security, Business Continuity Management (BCM) and Vulnerability Management (VM).
- When implementing the NIS Directive, 64% of surveyed organisations procured security incident & event log collection solutions, as well as security awareness & training services.
- “Unclear expectations” and “Limited support from the national authority” are among the top challenges faced by surveyed organisations when implementing the NIS Directive.
- 81% of the surveyed organisations have established a mechanism to report information security incidents to their national authority, with the majority of surveyed organisations allocating up to 4 people for incident reporting.
- Nearly 60% of surveyed organisations reported major information security incidents.
- 43% of surveyed organisations experienced information security incidents with a direct financial impact up to 500 k€.

1. INTRODUCTION

The **Directive on Security of Network and Information Systems** (**NIS Directive**)[1] represents the first EU-wide legislation on cybersecurity, with the objective to achieve a high common level of cybersecurity for all EU 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 and DSPs 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 in these sectors invest in cybersecurity** and how the implementation of the NIS Directive has influenced this investment.

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

- High-level insights on the EU cybersecurity market were drawn from **Gartner's Research databases**, combined with additional analysis of the current market dynamics and latest forecasts.
- To collect specific data on the NIS Directive, an **ad hoc survey** was conducted on 250+ European organisations identified as OES or DSPs

Surveyed organisations originated from five Member States chosen due to the size of their information security market as well as the number of OES and DSPs declared: Germany, France, Italy, Spain and Poland. Additional information on the methodology, rationale for selecting these 5 MS and additional survey demographics is available in Annex A.

The target audience of this report are **EU and National policy makers**. As a secondary audience, this report may provide useful information to OES and DSPs as well.

[1] 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 view of the global information security trends and outlook. It leverages data provided by Gartner, uncorrelated to the dedicated survey specifically for NIS investments related to the implementation of the NIS Directive. The specific sources of data for the following analysis include:

- Gartner's IT Score for Security Management 2020 survey
- Gartner IT Key Metrics Data 2020
- Gartner forecast: IT security and Risk Management, Worldwide

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

- The definitions of the industries in chapter 2 is not the same as the definitions of the OES used in chapter 3. Moreover, data in chapter 2 also covers sectors that are not in the NIS Directive.
- The source of data in chapter 2 cover a broad EU Member State (MS) and international scope, whereas data in chapter 3 was collected from OES in 5 MS

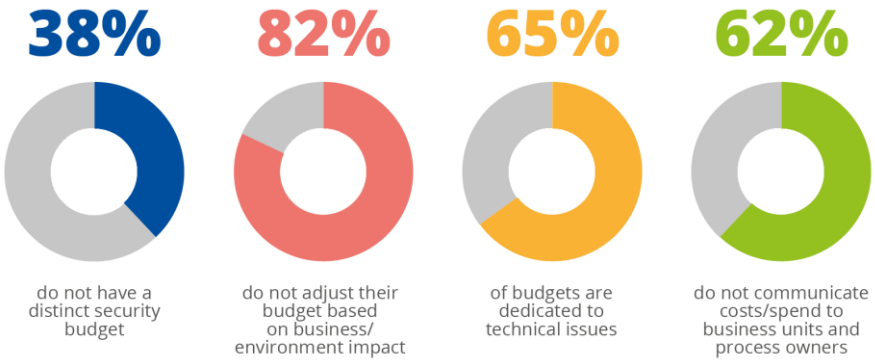
A detailed description of the relevant definitions is available in Annex B.

The reason this dataset is presented before the detailed data related to the NIS Directive implementation is to provide a high level overview of the global market, including EU MS, in terms of information security investments and highlight a few key statistics and trends. **This broader view serves as an introduction to the more focused analysis presented in chapter 3 for OES and DSPs in the aforementioned EU Member States**.

2.1 SECURITY BUDGETS

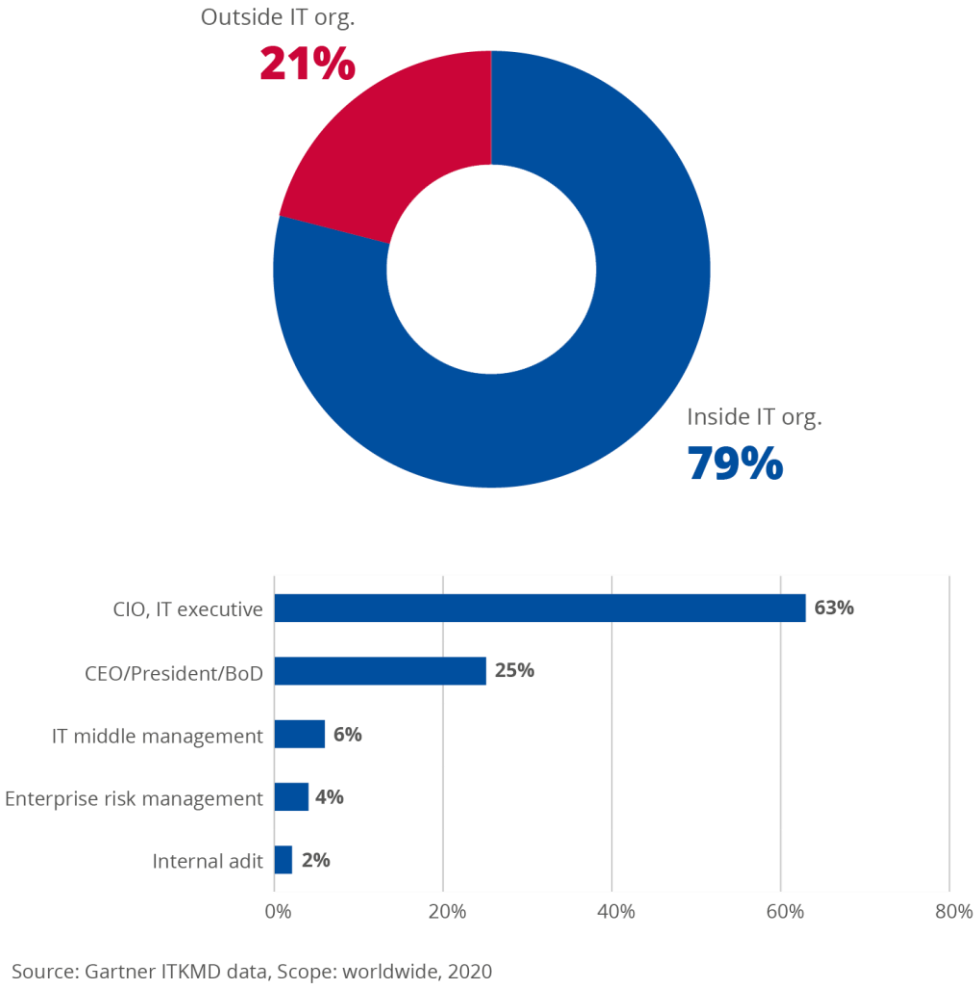
Data shows that the tracking and associated allocation of IT security budgets is still growing within most organisations. Indeed, it is observed that 38% of surveyed organisations still do not have a distinct security budget and 62% of organisations do not effectively communicate costs associated to information security to business units and process owners.

Figure 1: Overview of budget issues



When looking at the ownership of Information security budgets and the lines of reporting, it can be observed that information security is widely recognised as an IT discipline.

Figure 2: Ownership of Information security budgets and the lines of reporting



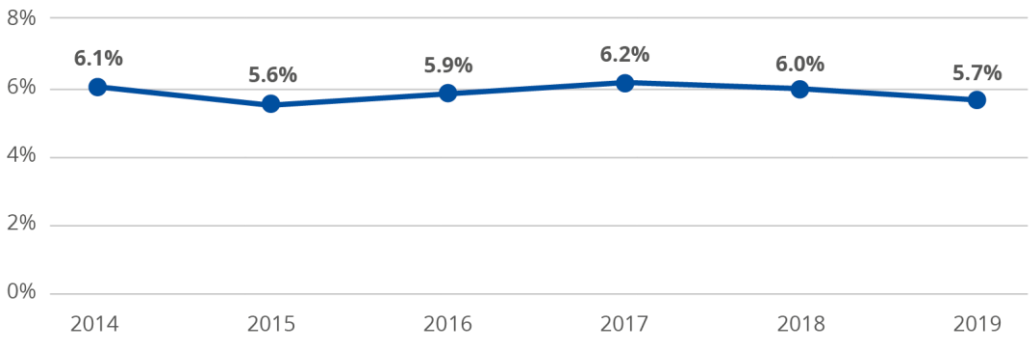
Source: Gartner ITKMD data, Scope: worldwide, 2020

Data shows that organisations allocate a rather stable share of their IT budget to information security, with a relevant portion of around 6% since 2016.

The decline in IT Security spend Vs Overall IT Budget actually reflects an accelerated growth of Overall IT Budget vs IT Security spend resulting in a 'negative' proportional trend.

Organisations allocate a rather stable share around 6% of their IT budget to information security

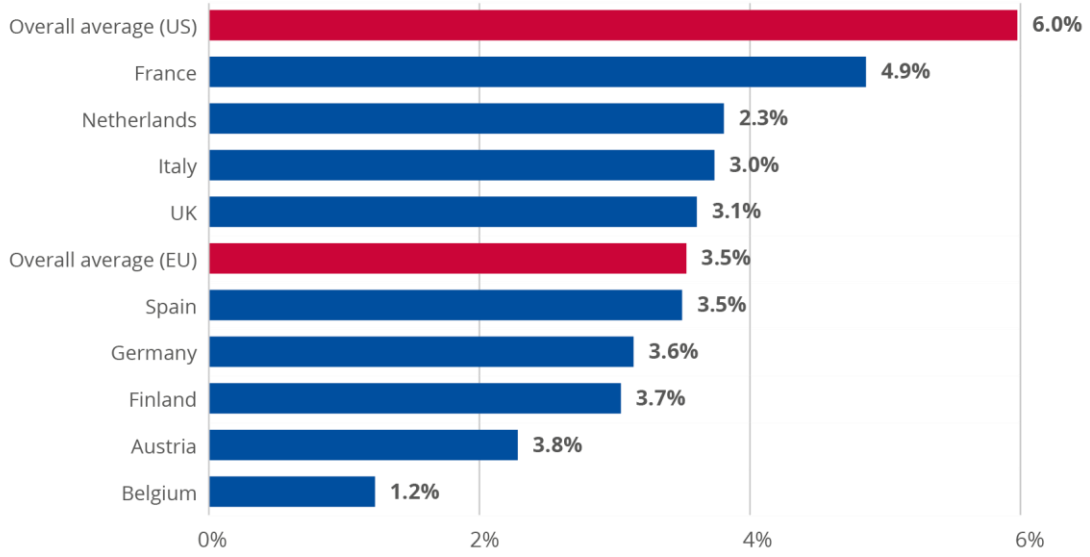
Figure 3: Global IT security spending as a share of total IT budget



Source: Gartner ITKMD data, Scope: worldwide

When comparing organisations from the EU to organisations from the United States of America, data shows that EU organisations allocate on average 41% less to information security than their American counterparts.

Figure 4: IT security spending as a share of total IT budget by geography

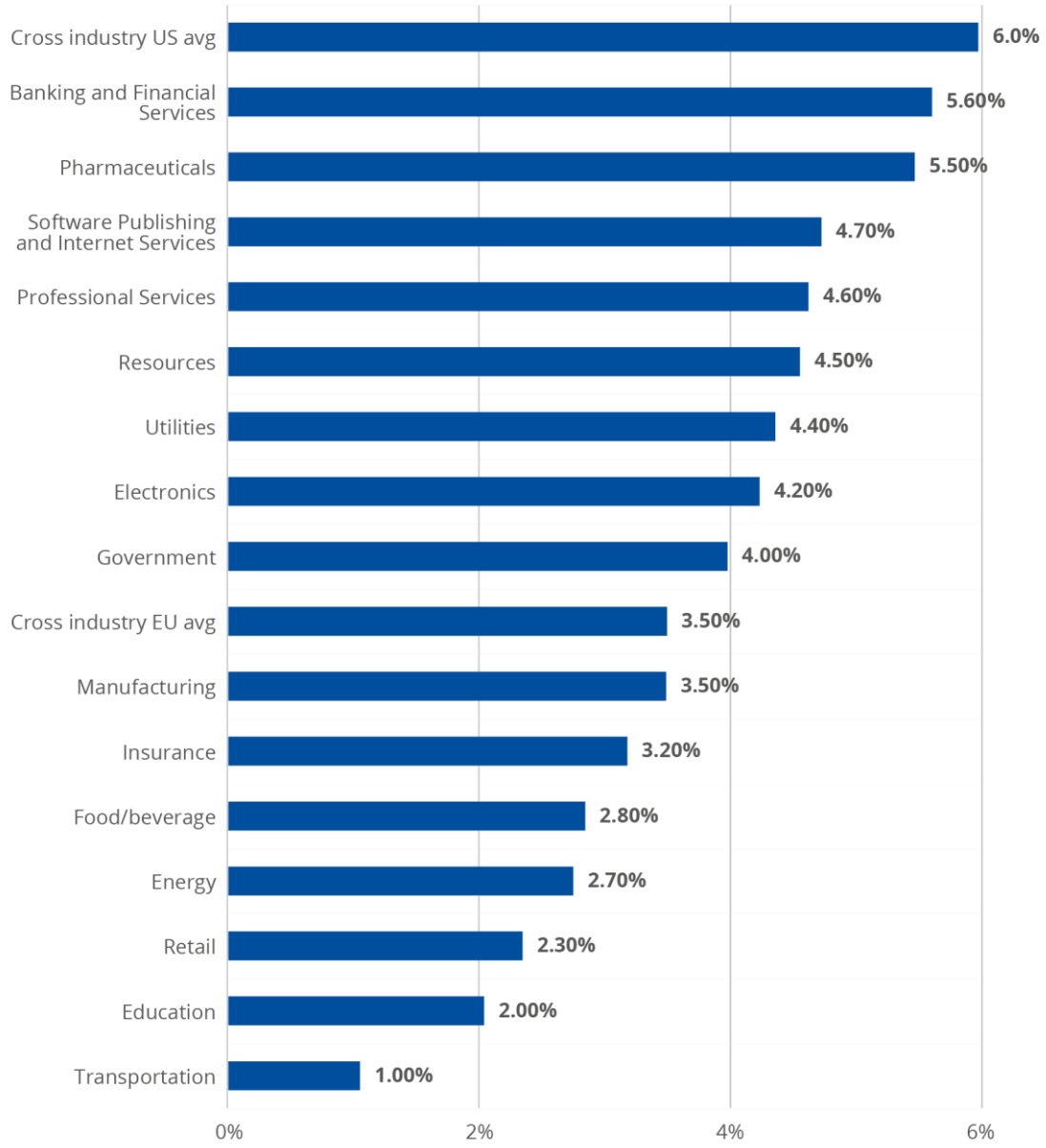


Source: Gartner ITKMD data, Scope: EU countries + UK and US for reference, 2020

The below breakdown analysis per industry highlights major discrepancies between different sectors. The three industries with the highest Information Security (IS) spend as a percentage of their overall IT budgets are Banking, Financial Services and Pharmaceuticals organisations, with a ratio higher than 5%. Transportation, Education and Retail are the sectors with the lowest such ratios, all below 2,5%.[2]

[2] As previously stated, the definition of the industries is not directly related to the definition of the sectors in the NIS Directive used in chapter 3 of this report. The relevant definitions are available in Annex B.

Figure 5: IT security spending as a share of total IT budget by industry



Source: Gartner ITKMD data, Scope: EU countries + UK and US for reference, 2020

2.2 INFORMATION SECURITY SPEND DISTRIBUTION

The analysis of the information security budget distribution across various information security domains (see appendix for the definition of the information security domains) gives further insights to the type of investment organisations are making[3].

In summary:

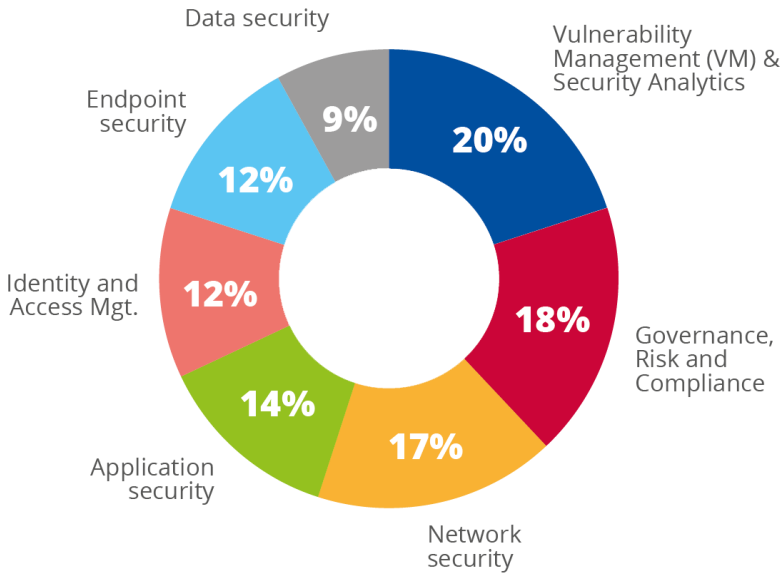
- Vulnerability management and security analytics investments focus on proactive capabilities for minimising the impact of any breaches once they have occurred.
- Application security is how the application was designed and developed, how it's operated, and how the application and its supporting elements (network, OS, database etc.) are configured and deployed to ensure security.
- Governance, risk, and compliance management (GRC) focuses on how organisations deal with their unique set of risks by developing strategies, policies, standards and awareness that underpin security services. GRC ensures that risk is managed openly and effectively, that legal and regulatory compliance requirements are met and that information security is embedded throughout the organisation
- Network security, Identity and Access Management (IAM), endpoint security and data security are part of the operational infrastructure security, which focuses on protecting the network, hosts and data and on ensuring secure access to systems for authorised users.

Data indicates that the top 3 domains in terms of spending are:

- Vulnerability Management and Security Analytics with a share of 20%
- Governance, Risks and Compliance (GRC) with a share of 18%
- Network Security with a share of 17%

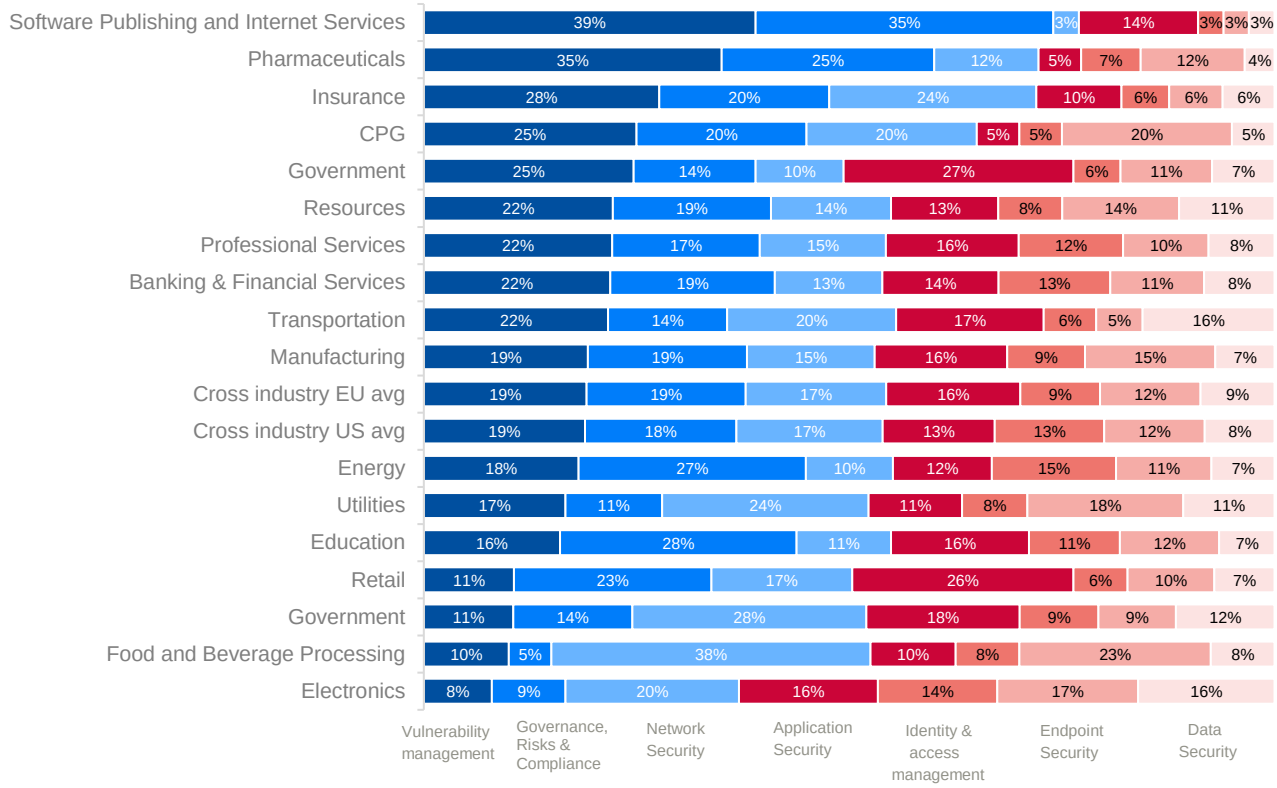
This distribution between the different functional areas has been quite stable over the last four years, but, although quite similar when comparing organisations in the EU and US, varies greatly between industries.

Figure 6: IT security spending distribution by functional area



Source: Gartner ITKMD data, Scope: worldwide, 2020

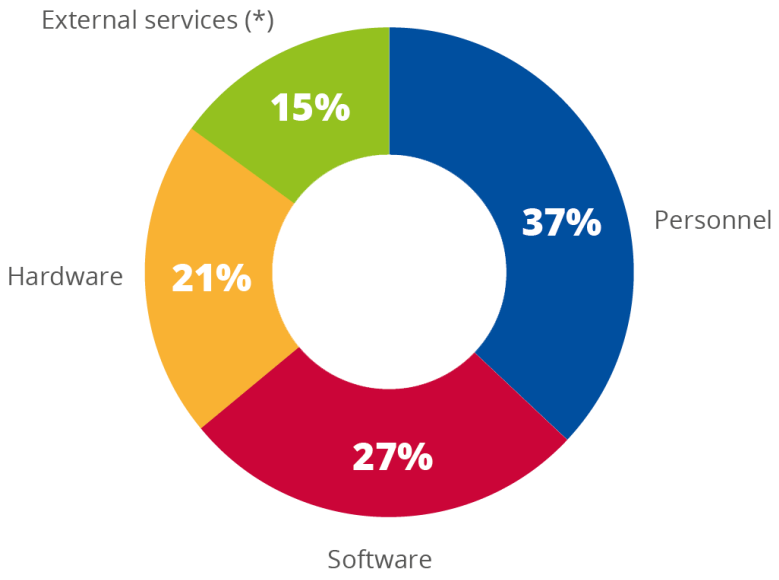
[3] Annex B provides detailed definitions for the security domains referenced in chapter 2.



Source: Gartner ITKMD 2020 data, Scope: EU countries + UK and US for reference

In terms of asset class, it is observed that the main area of spending for information security is Personnel (37%), followed by Software (27%) and Hardware (21%). The share of external services such as advisory, outsourcing or cloud services is only 15%.

Figure 7: IT security spending distribution by asset class



Source: Gartner ITKMD data, Scope: worldwide, 2020
(*) includes Outsourcing, Consulting, Managed Services and Cloud providers

2.3 INFORMATION SECURITY STAFFING

The demand for information security trained resources is very high and still growing. Many organisations are facing real issues in hiring resources with the required skillset & experience.

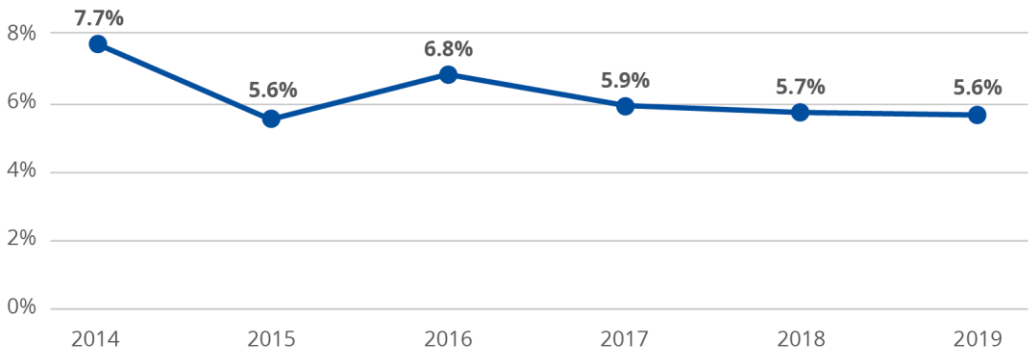
As such, it is foreseen that the number of unfilled information security positions will reach 3.5 million globally by 2022, going up from 1 million in 2016.

Figure 8: Information Security Staffing

Even though the demand for security resources is already high and growing, due to the ongoing scarcity of these resources in the market, the share of information security resources within the overall IT staff does not increase.

As of 2020, information security staff represents 5,6% of total IT staff, measured in terms of FTEs. (Information security personnel includes in-house and contract full-time equivalents supporting the IT security domains).

Figure 9: Information Security FTEs as a share of total IT staff

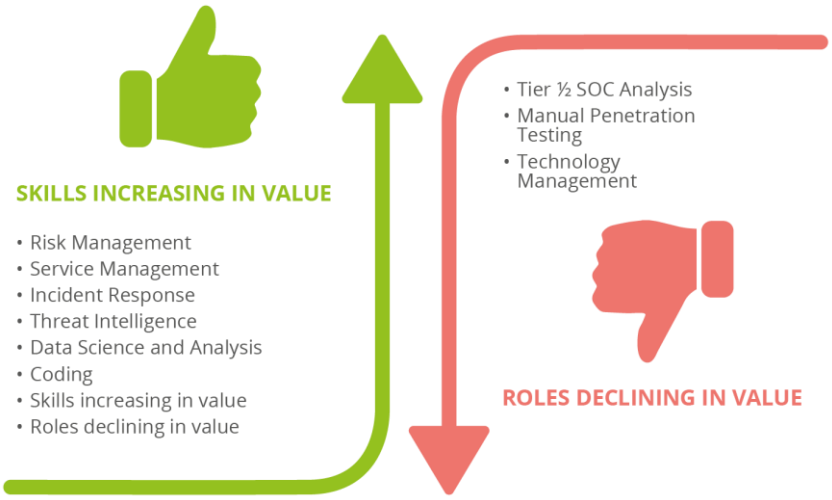


Source: Gartner ITKMD data, Scope: worldwide, 2020

On top of the overall lack of security resources, there is also a change in the security skills that are in demand. This change directly reflects the increasing use of automation in information security.

Skills that were in high demand in the previous years such as Manual Penetration Testing, Tier 1/2 SOC Analysis or Technology Management are now decreasing in value and are being replaced by skills in Risk Management, Service Management, Incident Response, Threat Intelligence, Data Science and Analysis or Coding.

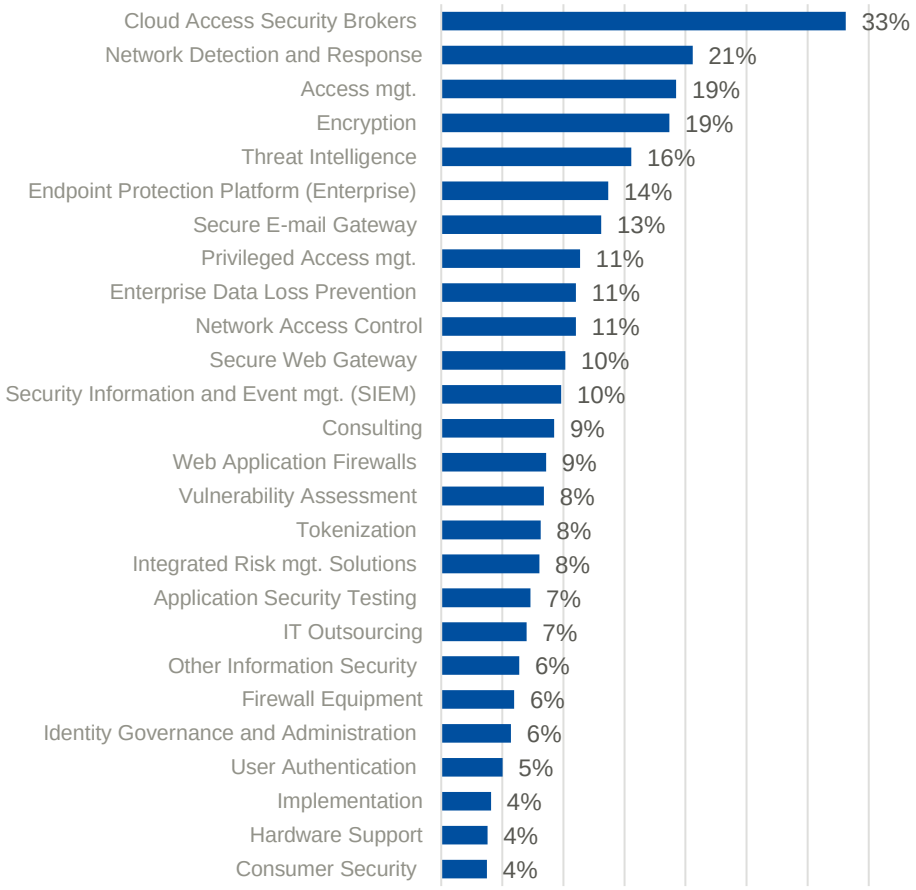
Figure 10: Change the security skills demand



2.4 INFORMATION SECURITY MARKET OUTLOOK

Forecasted growth rates for 2020 through 2024 have recently been substantially revised in alignment with the revised outlook driven by post-COVID-19 IT spending. Figure below shows the overall information security and risk management spending and the compound annual growth rate (CAGR) for 2019 through 2024.

Figure 11: IT security Forecast — Compound Annual Growth Rate (CAGR), 2019 - 2024 (%)



Source: Gartner Forecast: IT security and Risk Management, Worldwide, 2019 - 2024, 3Q20 Update

The fastest growing security segment is Cloud Access Security Brokers (CASB), albeit being one of the smallest security segments listed. The reason cloud security continues to grow, even in these difficult economic times, is largely because of its role in digital transformation, protecting data and user access to Software as a Service (SaaS) services. As organisations look to support remote workers and continue to move business services to the cloud, CASB is a key part of that security strategy.

Another security segment that is continuing to grow despite the current economic situation is the Identity and Access Management segment, including four sub-segments: Access Management (AM), Identity Governance and Administration (IGA), Privileged Access Management (PAM), and User Authentication. Indeed, organisations need to provide secure access to their remote workforce users, including IT users with privileged access. The use of cloud technologies has also shifted the need from a perimeter-based approach to an identity and context-based approach.

2.5 TRENDS ON SECURITY INCIDENTS LIABILITY

It is forecasted by Gartner that by 2024 liability for cyber physical systems (CPS) incidents (impacting human safety or the environment) will break through the corporate protective barrier to personal liability for 75% of CEOs.

Regulators and governments around the world are expected to strengthen laws and regulations for CPS as they are viewed as critical systems where incidents can result in physical harm to people, destruction of property or environmental disasters.

This trend may result CEOs no longer being able to hide behind complex corporate organisational hierarchies, a potential 'lack of knowledge', processes, or insurance policies. This will be the case particularly in asset-intensive, critical infrastructure and clinical healthcare environments that extensively use CPS, or for organizations that sell CPS to others.

An example of this trend is the Corporate Executive Accountability Act introduced in the U.S. Senate in 2019[4]. This development would render CEOs liable for their companies' failure to implement basic security measures that would have prevented a fatal CPS incident.

If not through a legal action, CEOs may find themselves responsible in front of the shareholders. There already exists several recent examples: The Yahoo breach settlement[5] opened the doors to company officers being directly sued by shareholders. The judge in the legal proceedings following the Equifax breach refused to dismiss a suit against the former company CEO[6]; a suit against the company Chegg and its CEO claiming they failed to disclose a lack of security measures has been filed[7]; and Marriott International shareholders filed a similar suit against that company's officers[8].

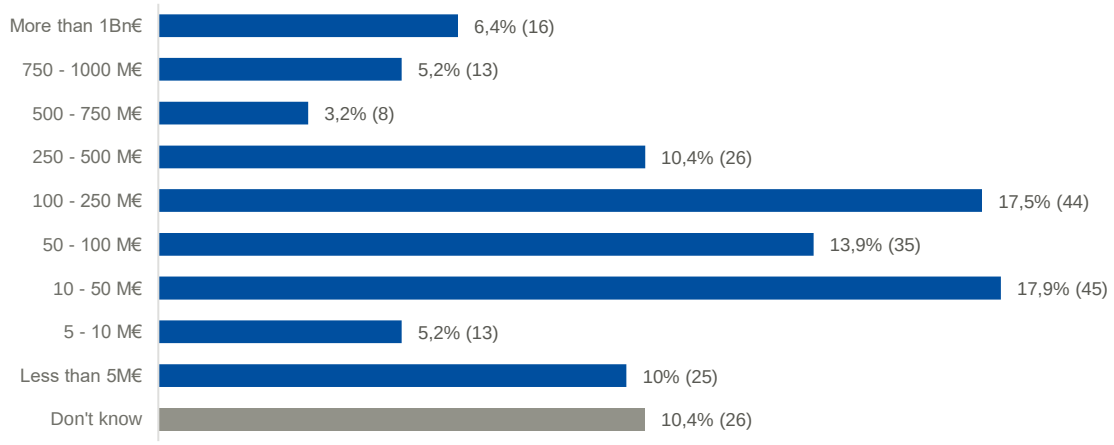
[4] https://www.congress.gov/bill/116th-congress/senate-bill/1010
[5] https://www.natlawreview.com/article/court-approves-class-action-settlement-re-yahoo-inc-customer-data-security-breach
[6] https://www.reuters.com/article/otc-equifax-frankel-idUSKCN1PN2TJ
[7] https://in.reuters.com/article/dataprivacy-chegg/chegg-data-breach-lawsuit-heads-to-arbitration-idUSL2N2CG2JU
[8] https://www.reuters.com/article/us-britain-marriott-dataprotection-idUSKCN25F0S2

3. INFORMATION SECURITY INVESTMENTS FOR THE NIS DIRECTIVE IMPLEMENTATION

3.1 INFORMATION SECURITY SPEND IN THE NIS DIRECTIVE SECTORS

The surveyed organisations represent a large range of information technology budgets, ranging from SMEs devoting less than 5 M€ to IT, to multinational corporations with more than one billion euros of IT spending, reflecting the diversity of actors identified as OES and DSPs by national authorities.

Figure 12: IT budget range of surveyed organisations



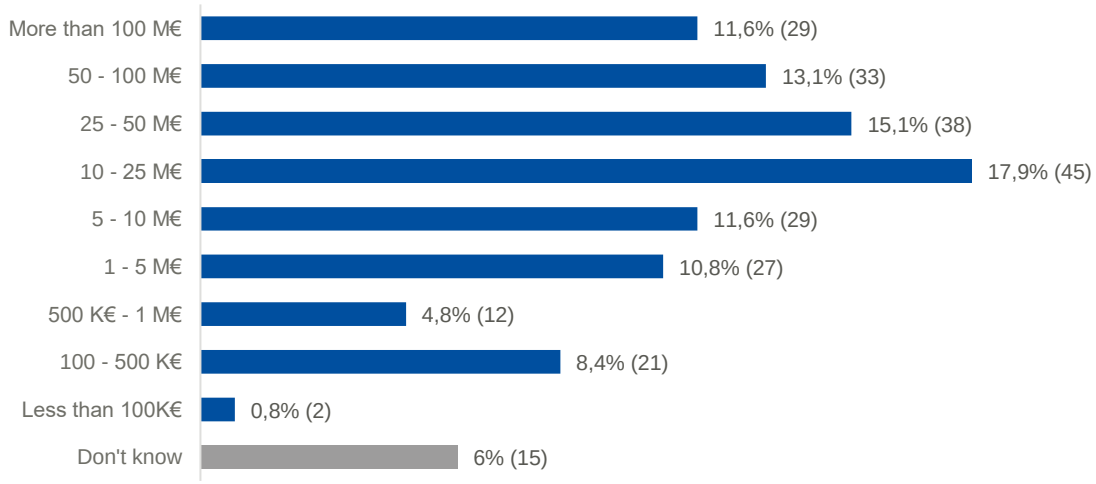
n = 251
Q: What is your organization estimated IT budget range for 2019 (including hardware, software, internal personnel, contractors and outsourcing spend)?

Figure 13: IT budget range of surveyed organisations by industry

	5M€or less	5 - 10 M€	11 - 50 M€	50 - 100 M€	100 - 250 M€	250 - 500 M€	500 - 750 M€	750 - 1,000 M€	1Bn€or more	Doesn't know
Banking	0,0%	0,0%	17,5%	5,0%	22,5%	10,0%	2,5%	15,0%	15,0%	12,5%
Cloud computing	8,0%	16,0%	12,0%	16,0%	0,0%	12,0%	0,0%	4,0%	16,0%	16,0%
Digital infra.	44,0%	8,0%	16,0%	4,0%	4,0%	8,0%	0,0%	4,0%	4,0%	8,0%
Drinking water	0,0%	6,7%	46,7%	40,0%	0,0%	6,7%	0,0%	0,0%	0,0%	0,0%
Energy	0,0%	0,0%	0,0%	23,3%	33,3%	16,7%	6,7%	10,0%	3,3%	6,7%
Financial market infra.	0,0%	26,7%	20,0%	20,0%	13,3%	6,7%	0,0%	6,7%	0,0%	6,7%
Healthcare	5,7%	0,0%	22,9%	25,7%	22,9%	11,4%	2,9%	0,0%	0,0%	8,6%
Online Marketplace	12,0%	4,0%	24,0%	0,0%	4,0%	4,0%	12,0%	4,0%	16,0%	20,0%
Transport	11,4%	2,9%	20,0%	8,6%	34,3%	14,3%	0,0%	0,0%	0,0%	8,6%
Overall	9,0%	5,3%	18,4%	14,3%	17,6%	10,6%	2,9%	5,3%	6,5%	10,2%

This diversity can also be observed in the ranges of Information Security budgets, ranging from less than 100 K€ to above 100 M€, with the highest percentage of Information Security budget range among the surveyed organisations being 10 – 25 M€.

Figure 14: Information security budget range of surveyed organisations



n = 251
Q: What is your organization estimated information security budget range for 2019 (including hardware, software, internal personnel, contractors and outsourcing spend)?

Figure 15: Information security budget range of surveyed organisations by sector

	More than 100 M€	50 - 100 M€	25-100 M€	10-25 M€	5-10 M€	2-5 M€	0.5-1M€	100-500 K€	Less than 100K€	Doesn't know
Banking	0,0%	2,5%	0,0%	10,0%	5,0%	15,0%	22,5%	20,0%	20,0%	5,0%
Cloud computing	0,0%	12,0%	12,0%	12,0%	4,0%	16,0%	0,0%	16,0%	20,0%	8,0%
Digital infra.	8,0%	32,0%	16,0%	20,0%	4,0%	0,0%	4,0%	4,0%	12,0%	0,0%
Drinking water	0,0%	0,0%	0,0%	33,3%	40,0%	20,0%	0,0%	6,7%	0,0%	0,0%
Energy	0,0%	0,0%	0,0%	0,0%	3,3%	30,0%	33,3%	20,0%	10,0%	3,3%
Financial market infra.	0,0%	0,0%	6,7%	20,0%	20,0%	33,3%	0,0%	6,7%	6,7%	6,7%
Healthcare	0,0%	5,7%	0,0%	11,4%	14,3%	22,9%	20,0%	17,1%	0,0%	8,6%
Online Marketplace	0,0%	8,0%	8,0%	0,0%	24,0%	0,0%	4,0%	12,0%	32,0%	12,0%
Transport	0,0%	11,4%	0,0%	8,6%	11,4%	28,6%	25,7%	8,6%	0,0%	5,7%
Overall	0,8%	8,2%	4,1%	11,0%	11,8%	18,4%	15,1%	13,5%	11,4%	5,7%

The analysis of the financial data shows that there is a strong correlation between overall IT budget and Information Security budget, as organisations with a higher IT budget will also spend more in information security.

Figure 16: Information Security budget vs. overall IT budget for surveyed organisations

	5M€ or less	5 - 10 M€	11 - 50 M€	50 - 100 M€	100 - 250 M€	250 - 500 M€	500 - 750 M€	750 - 1,000 M€	1Bn€ or more	Doesn't know
More than 100 M€	0,0%	0,0%	0,0%	0,0%	0,0%	7,7%	62,5%	30,8%	93,8%	11,5%
50 - 100 M€	0,0%	0,0%	0,0%	2,9%	2,3%	73,1%	25,0%	46,2%	6,3%	11,5%
25-100 M€	0,0%	0,0%	0,0%	0,0%	63,6%	19,2%	12,5%	15,4%	0,0%	7,7%
10-25 M€	0,0%	0,0%	8,9%	74,3%	34,1%	0,0%	0,0%	0,0%	0,0%	0,0%
5-10 M€	0,0%	0,0%	46,7%	22,9%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
2-5 M€	0,0%	53,8%	42,2%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	3,8%
0.5-1M€	24,0%	30,8%	2,2%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	3,8%
100-500 K€	68,0%	15,4%	0,0%	0,0%	0,0%	0,0%	0,0%	7,7%	0,0%	3,8%
Less than 100K€	8,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Doesn't know	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	57,7%

The Information Security budget ranges in these figures refer to investments directly related to NIS products and services. They do not include for instance additional budget forecasted for built-in security features in non-NIS products.

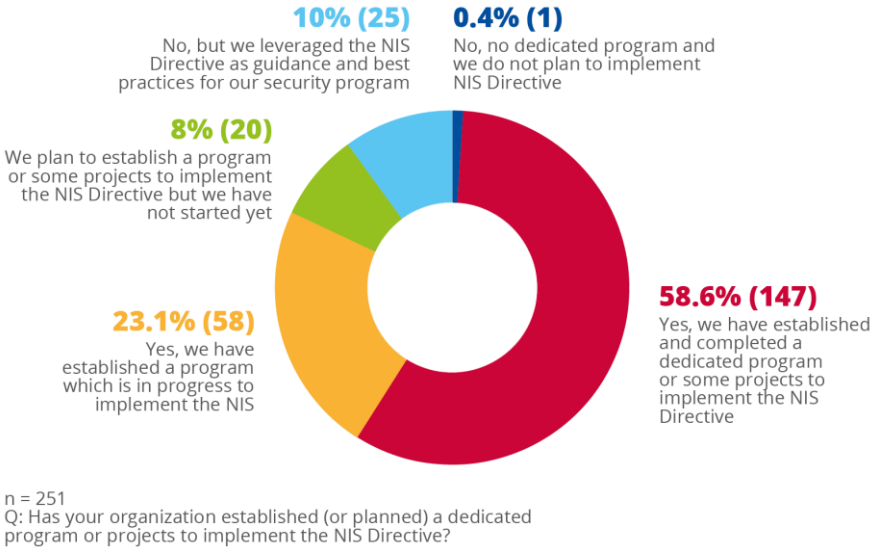
3.2 NIS DIRECTIVE IMPLEMENTATION

3.2.1 Current state

As of November 2020, more than 80% of surveyed organisations declared that their NIS Directive implementation program is either completed or in progress and 8% of surveyed organisations plan to implement the NIS Directive but have not started yet.

For the 10% remaining that do not intend to launch a dedicated program or projects, less than 1% actually do not plan to implement the NIS Directive at all, while the rest will leverage some of its key requirements to improve and guide their information security practices.

Figure 17: Current state of NIS Directive implementation among surveyed organisations



Minor differences can be observed when comparing the NIS Directive implementation status between operators in different MS. An interesting find is that 10% of all surveyed organisations are not following an NIS Directive implementation program but are using the NIS Directive as best practice.

Figure 18: Current state of NIS Directive implementation per country

	Not planned	Leveraged as best practices	Planned	Work in progress	Completed
France	2,0%	7,8%	5,9%	17,6%	66,7%
Germany	0,0%	3,9%	5,9%	19,6%	70,6%
Italy	0,0%	8,0%	8,0%	20,0%	64,0%
Poland	0,0%	16,3%	10,2%	30,6%	42,9%
Spain	0,0%	14,0%	10,0%	28,0%	48,0%
Overall	0,4%	10,0%	8,0%	23,1%	58,6%

The analysis also shows additional differentiation between sectors as regards the implementation of the NIS Directive. For instance, more than three quarters of surveyed organisations in the Banking and Energy sectors have fully implemented the Directive, well above the cross-sector average (58.8%).

Furthermore the percentage of surveyed organisations that declared they will not directly implement the NIS Directive, but will instead leverage its principles as best practices, varies substantially across the different sectors.

Over 75% of surveyed organisations in the Banking and Energy sectors have fully implemented the Directive, well above the cross-sector average (58.8%)

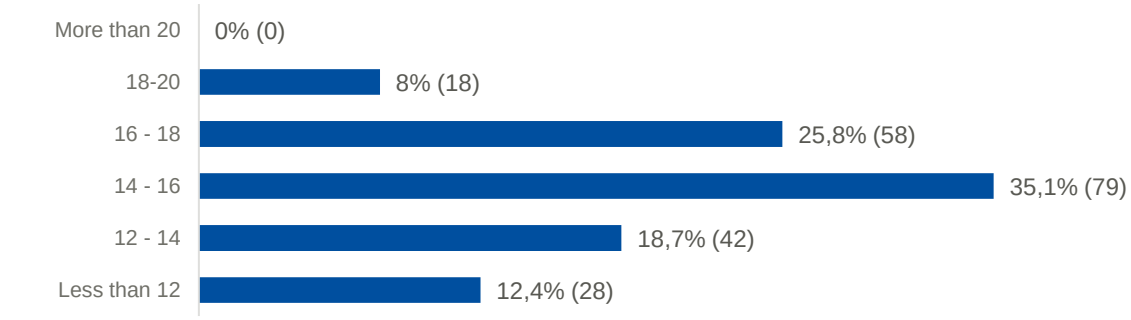
Figure 19: Current state of the NIS Directive implementation per sector

	Not planned	Leveraged as best practices	Planned	Work in progress	Completed
Banking	0,0%	2,5%	5,0%	15,0%	77,5%
Cloud computing	0,0%	16,0%	8,0%	20,0%	56,0%
Digital infra.	4,0%	24,0%	24,0%	16,0%	32,0%
Drinking water	0,0%	26,7%	0,0%	40,0%	33,3%
Energy	0,0%	0,0%	0,0%	23,3%	76,7%
Financial market infra.	0,0%	6,7%	20,0%	6,7%	66,7%
Healthcare	0,0%	5,7%	5,7%	37,1%	51,4%
Online Marketplace	0,0%	12,0%	0,0%	20,0%	68,0%
Transport	0,0%	11,4%	8,6%	28,6%	51,4%
Overall	0,4%	10,2%	7,3%	23,3%	58,8%

3.2.2 NIS Directive implementation program timeline

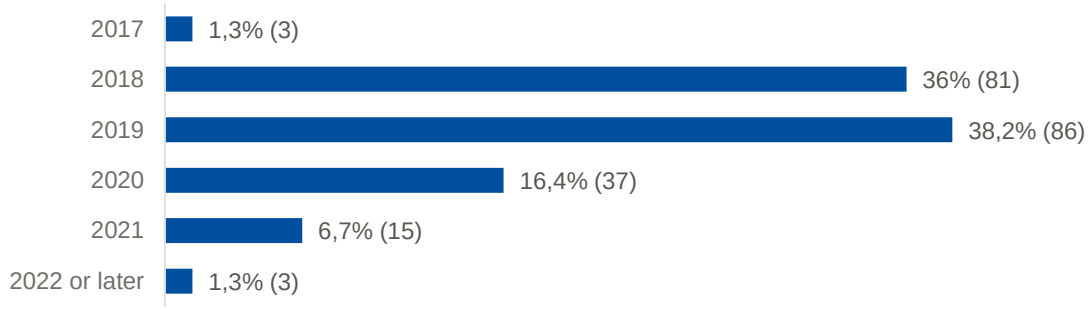
The majority of organisations falling under the provisions of the NIS directive report having launched implementation projects by the end of 2019 (64,2% of surveyed organisations), and nearly a third by the end of 2018, year of transposition into nation law and identification of OES and DSPs. With 16,4% of organisations having started the implementation in 2020, there remains an 8% of organisations that will implement the NIS Directive in the future, from 2021 onwards. Furthermore, the analysis shows that implementation projects of the NIS Directive typically last between 14 and 18 months, with little differentiation between countries or sectors.

Figure 20: Duration of NIS Directive implementation program among surveyed organisations (in months)



n = 225
Q: What are the start date and estimated duration of the NIS program or projects?
Scope: Organizations with existing or planned NIS program

Figure 21: Start year of NIS Directive implementation program among surveyed organisations



n = 225
Q: What are the start date and estimated duration of the NIS program or projects?
Scope: Organizations with existing or planned NIS program

Variance between countries in terms of project initiation start dates can be explained by timeline differences in the transposition of the NIS Directive into national laws, including the publication of detailed requirements[9].

[9] https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool

Figure 22: NIS Directive implementation program start year per country

	2017	2018	2019	2020	2021	2022 or later
France	2,2%	50,0%	28,3%	13,0%	4,3%	2,2%
Germany	4,1%	40,8%	36,7%	12,2%	6,1%	0,0%
Italy	0,0%	37,0%	43,5%	13,0%	4,3%	2,2%
Poland	0,0%	19,5%	43,9%	24,4%	12,2%	0,0%
Spain	0,0%	30,2%	39,5%	20,9%	7,0%	2,3%
Grand Total	1,3%	36,0%	38,2%	16,4%	6,7%	1,3%

The analysis of the start year per sector correlates with previous findings indicating that operators from the Banking and Energy sectors were ahead of the curve in terms of implementation: more than 50% of organisations started their NIS Directive programs in 2018, compared with an average baseline of approximately a third among all sectors.

Figure 23: NIS Directive implementation program start year per sector

	2017	2018	2019	2020	2021	2022 or later
Banking	0,0%	51,3%	33,3%	10,3%	5,1%	0,0%
Cloud computing	0,0%	28,6%	38,1%	23,8%	9,5%	0,0%
Digital infra.	0,0%	22,2%	38,9%	11,1%	22,2%	5,6%
Drinking water	0,0%	9,1%	54,5%	36,4%	0,0%	0,0%
Energy	0,0%	63,3%	23,3%	13,3%	0,0%	0,0%
Financial market infra.	0,0%	21,4%	50,0%	7,1%	21,4%	0,0%
Healthcare	0,0%	33,3%	39,4%	21,2%	3,0%	3,0%
Online Marketplace	4,5%	36,4%	40,9%	18,2%	0,0%	0,0%
Transport	3,2%	25,8%	45,2%	19,4%	6,5%	0,0%
Overall	0,9%	36,5%	38,4%	16,9%	6,4%	0,9%

3.3 NIS DIRECTIVE RESOURCES

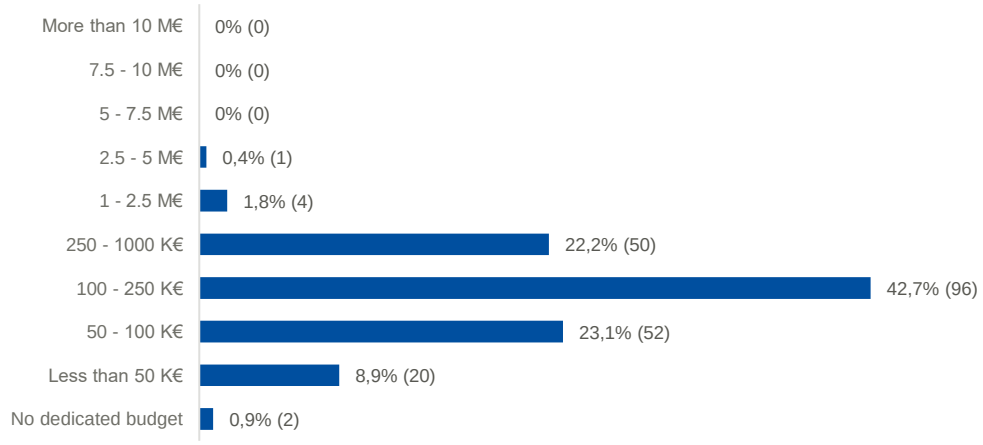
3.3.1 NIS dedicated budget

***Disclaimer**: for the following financial figures, it is important to bear in mind the following limitations.*

- *While low levels of investments cannot be sustained without adverse impact on the information security readiness**, higher spending does not necessarily correlate with an associated improved maturity***
- ***Certain cybersecurity expenditures are not accurately captured** such as secure-by-design ICT products and services, that elevate the overall security level of an organisation, but do not fall under specialised security-related budgets*

The average budget for NIS Directive implementation projects is approximately 175 K€, with 42.7% of affected organisations allocating between 100 and 250 K€. Such amounts typically represent a low share of the organisations' overall Information Security budgets.

Figure 24: Dedicated NIS Directive budget among surveyed organisations



n = 225
Q: What is the estimated budget of your organization dedicated to the NIS program or projects?
Scope: Organizations with existing or planned NIS program

The NIS Directive dedicated budgets are broadly similar and mostly fall in the 100 to 250 K€ range across all countries in scope of the survey.

Figure 25: Dedicated NIS Directive budget per country

	<50K€	50 - 100 K€	100 - 250 K€	250 K€ - 1M€	1 - 2.5 M€	2.5 - 5 M€	no dedicated budget
France	6,5%	17,4%	60,9%	15,2%	0,0%	0,0%	0,0%
Germany	6,1%	28,6%	42,9%	20,4%	2,0%	0,0%	0,0%
Italy	10,9%	19,6%	30,4%	32,6%	4,3%	0,0%	2,2%
Poland	14,6%	26,8%	31,7%	26,8%	0,0%	0,0%	0,0%
Spain	7,0%	23,3%	46,5%	16,3%	2,3%	2,3%	2,3%
Grand Total	8,9%	23,1%	42,7%	22,2%	1,8%	0,4%	0,9%

Outside of the 100-250 K€ central budget range, Energy OES seem to allocate larger sums to NIS Directive programs compared to other sectors: nearly half of these OES allocate more than 250 K€, vs. less than 25% on the overall average of affected organisations.

Figure 26: Dedicated NIS Directive budget per sector.

	<50K€	50 - 100 K€	100 - 250 K€	250 K€ - 1M€	1 - 2.5 M€	2.5 - 5 M€	no dedicated budget
Banking	2,6%	20,5%	46,2%	28,2%	2,6%	0,0%	0,0%
Cloud computing	9,5%	38,1%	28,6%	23,8%	0,0%	0,0%	0,0%
Digital infra.	38,9%	27,8%	11,1%	16,7%	0,0%	0,0%	5,6%
Drinking water	9,1%	36,4%	54,5%	0,0%	0,0%	0,0%	0,0%
Energy	0,0%	6,7%	46,7%	40,0%	3,3%	3,3%	0,0%
Financial market infra.	21,4%	35,7%	21,4%	14,3%	0,0%	0,0%	7,1%
Healthcare	3,0%	27,3%	54,5%	12,1%	3,0%	0,0%	0,0%
Online Marketplace	4,5%	22,7%	40,9%	27,3%	4,5%	0,0%	0,0%
Transport	3,2%	16,1%	61,3%	19,4%	0,0%	0,0%	0,0%
Overall	7,8%	23,3%	43,4%	22,4%	1,8%	0,5%	0,9%

The analysis of the NIS security program budget against the organisations' information security budget shows a correlation between the two figures, though more limited than the link existing between information security budget and IT budget as reflected in Figure . This is mostly due to the fact that more than 80% of surveyed organisations allocated less than 1 M€ of budget to their NIS-related security program.

Figure 27: NIS Directive implementation budget vs. overall information security budget for surveyed organisations

	100K€ or less	100-500 K€	0.5-1 M€	1-5 M€	5-10 M€	10-25 M€	25-100 M€	50 - 100 M€	100 M€ or more	Doesn't know
5M€ or more	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
2.5 - 5 M€	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	3,4%	0,0%
1 - 2.5 M€	0,0%	0,0%	0,0%	0,0%	0,0%	2,3%	0,0%	3,0%	6,9%	0,0%
0.25 - 1 M€	0,0%	0,0%	0,0%	0,0%	4,0%	4,5%	21,1%	45,5%	72,4%	23,1%
100 - 250 K€	0,0%	0,0%	10,0%	20,0%	56,0%	59,1%	68,4%	45,5%	17,2%	38,5%
50 - 100 K€	0,0%	54,5%	50,0%	45,0%	28,0%	31,8%	10,5%	6,1%	0,0%	38,5%
50 K€ or less	100,0%	45,5%	40,0%	30,0%	8,0%	2,3%	0,0%	0,0%	0,0%	0,0%
No NIS budget	0,0%	0,0%	0,0%	5,0%	4,0%	0,0%	0,0%	0,0%	0,0%	0,0%

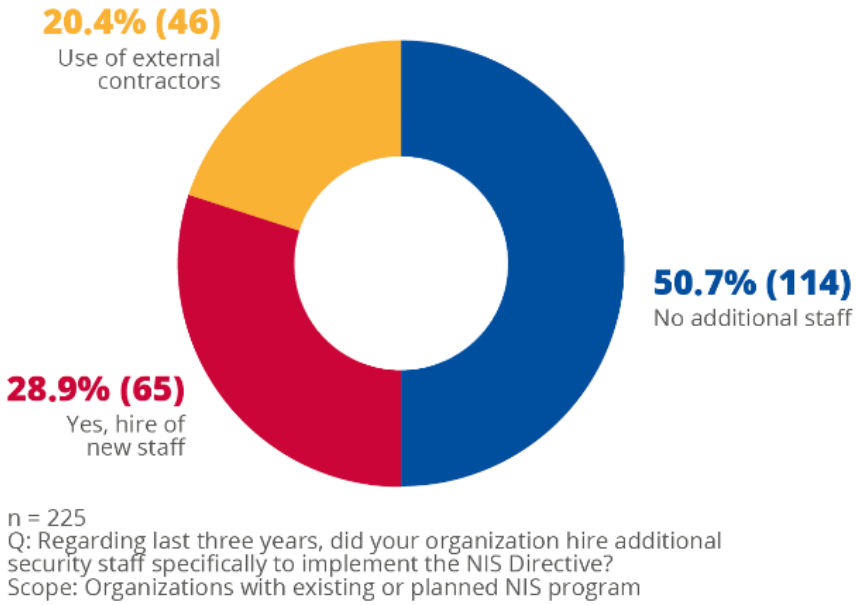
3.3.2 NIS dedicated hires

The majority of affected organisations did not require additional staff to implement the NIS Directive (50.7% of total respondents). Among those that did, ~29% filled that need by hiring new staff, while the remainder had recourse to external contractors (20.4% of total respondents).

Amongst organisations that employed additional staff to implement the NIS Directive, the large majority recruited up to 4 people.

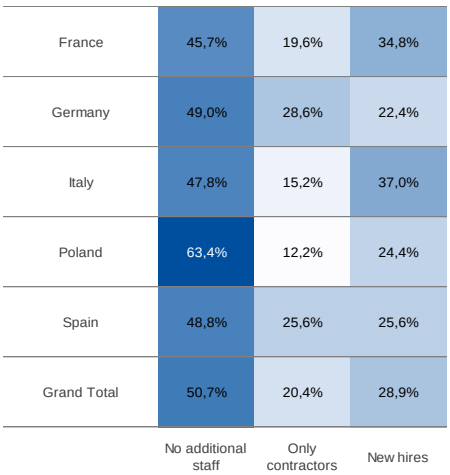
Amongst organisations that employed additional staff to implement the NIS Directive, the large majority recruited up to 4 people.

Figure 28: NIS Directive-related hires amongst surveyed organisations



This observation is valid across the EU MS in scope of the survey. Poland is the country where the NIS Directive was mostly implemented with internal resources. On the other side, organisations in Italy and France resorted more to new hires, while organisations in Germany and Spain made a more intensive use of external contractors.

Figure 29: Additional staff hired to implement the NIS Directive per country



Banking, Healthcare and Energy OES were more likely to have hired additional staff to implement the NIS Directive (respectively 43,6%, 42,4% and 40,0% vs. 29,7% on average).

Conversely, organisations in the Cloud computing, Transport and Online marketplace sectors appear to have relied the least on additional staff.

Figure 30: Additional staff hired to implement the NIS Directive per sector

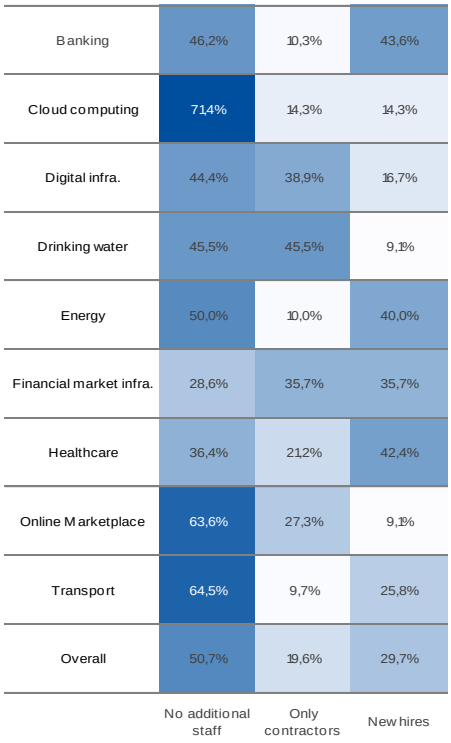
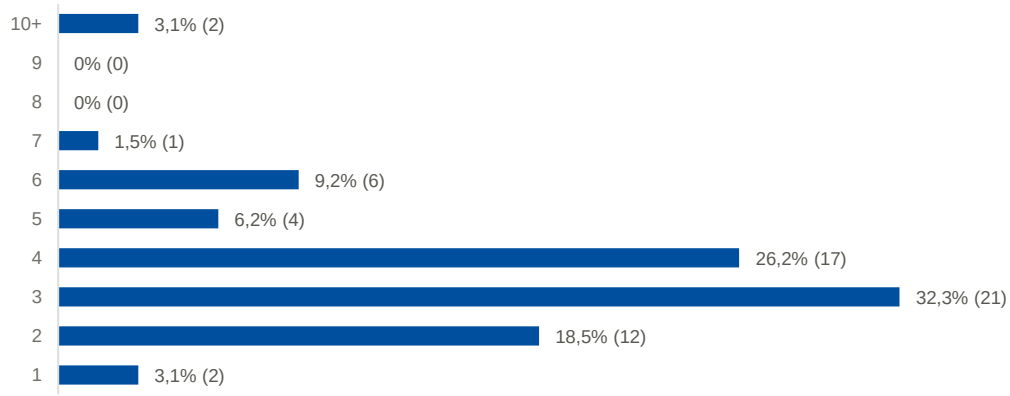


Figure 31: Number of additional staff hired to implement the NIS Directive among surveyed organisations



n = 65
Q: Regarding last three years, did your organization hire additional security staff specifically to implement the NIS Directive? If yes, how many?
Scope: Organizations with existing or planned NIS program that hired new staff to implement NIS Directive

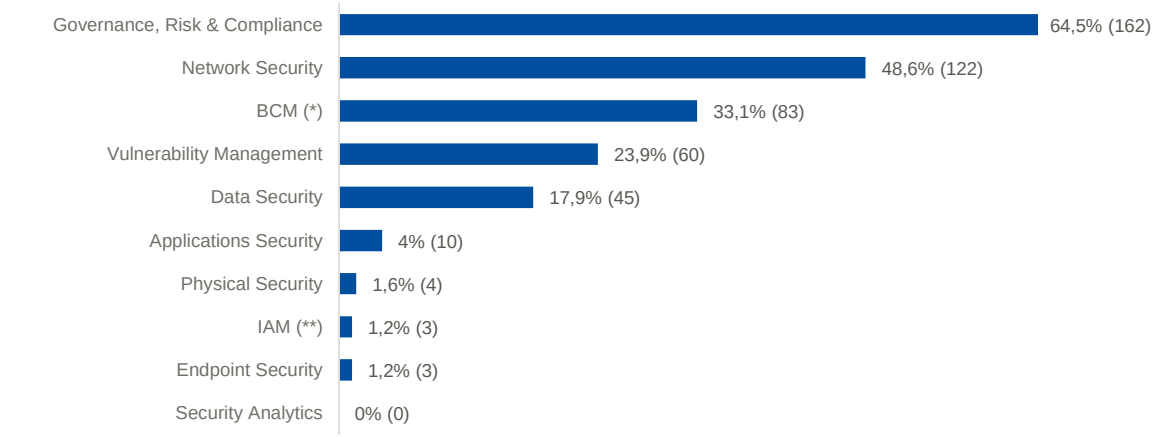
3.4 NIS DIRECTIVE SECURITY IMPACT

3.4.1 Impact on information security domains

According to surveyed organisations, the most frequently cited domains impacted by the NIS Directive implementation are:

- **Governance, Risks and Compliance** (64.5%), which was to be expected since the NIS Directive itself is a legislative document.
- **Network Securit**y (48.6%), which can be explained by the NIS provisions on security incidents detection and reporting requirements.
- **Business Continuity Management** (33.1%), also related to the management of security incidents.

Figure 32: Information security domains prioritised for NIS investments among surveyed organisations



n = 225
Q: What are the top 3 security domains where your organization invested the most to implement the NIS Directive?
Scope: Organizations with existing or planned NIS program, (*) = Business Continuity Management (**) = Identity Access Management

Figure 33: Information security domains prioritised for NIS investments per country

	Applications Security	Data Security	Vulnerability Management	Network Security	Endpoint Security	Security Analytics	Identity and Access Management	Governance, Risk and Compliance	Business Continuity Management	Physical Security
France	5,9%	17,6%	25,5%	43,1%	0,0%	49,0%	0,0%	72,5%	35,3%	2,0%
Germany	3,9%	9,8%	25,5%	58,8%	0,0%	51,0%	3,9%	62,7%	39,2%	2,0%
Italy	4,0%	14,0%	32,0%	46,0%	2,0%	52,0%	0,0%	66,0%	30,0%	4,0%
Poland	2,0%	18,4%	16,3%	44,9%	4,1%	55,1%	0,0%	59,2%	30,6%	0,0%
Spain	4,0%	30,0%	20,0%	50,0%	0,0%	40,0%	2,0%	62,0%	30,0%	0,0%
Overall	4,0%	17,9%	23,9%	48,6%	1,2%	49,4%	1,2%	64,5%	33,1%	1,6%

Figure 34: Information security domains prioritised for NIS investments per sector

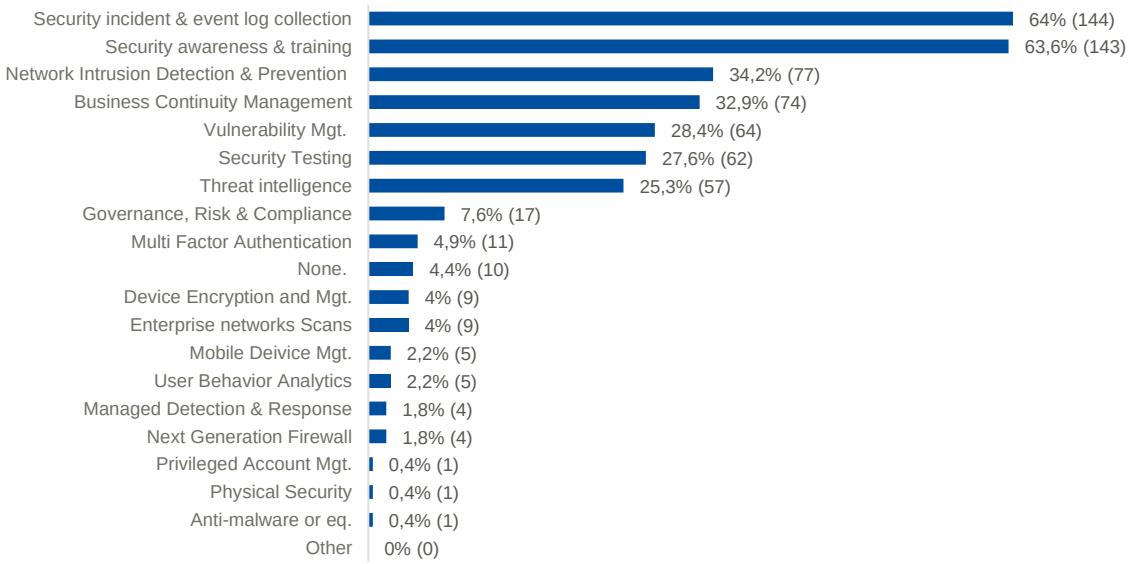
	Applications Security	Data Security	Vulnerability Management	Network Security	Endpoint Security	Security Analytics	Identity and Access Management	Governance, Risk and Compliance	Business Continuity Management	Physical Security
Banking	10,0%	22,5%	37,5%	47,5%	0,0%	47,5%	0,0%	65,0%	40,0%	2,5%
Cloud computing	0,0%	24,0%	16,0%	40,0%	4,0%	56,0%	0,0%	56,0%	28,0%	0,0%
Digital infra.	8,0%	28,0%	4,0%	44,0%	4,0%	40,0%	4,0%	40,0%	28,0%	0,0%
Drinking water	0,0%	0,0%	13,3%	40,0%	0,0%	13,3%	6,7%	66,7%	40,0%	0,0%
Energy	6,7%	10,0%	30,0%	53,3%	0,0%	60,0%	3,3%	80,0%	36,7%	3,3%
Financial market infra.	0,0%	20,0%	13,3%	66,7%	0,0%	60,0%	0,0%	66,7%	26,7%	0,0%
Healthcare	2,9%	8,6%	31,4%	45,7%	2,9%	60,0%	0,0%	68,6%	25,7%	2,9%
Online Marketplace	4,0%	24,0%	24,0%	56,0%	0,0%	48,0%	0,0%	52,0%	36,0%	4,0%
Transport	0,0%	20,0%	20,0%	45,7%	0,0%	45,7%	0,0%	74,3%	37,1%	0,0%
Overall	4,1%	18,0%	23,3%	48,2%	1,2%	49,4%	1,2%	64,1%	33,5%	1,6%

3.4.2 Impact on procurement of technology and services

It is worth noting that NIS Directive investments did not seem to focus on new technologies. The services most cited in the survey as NIS investment targets are:

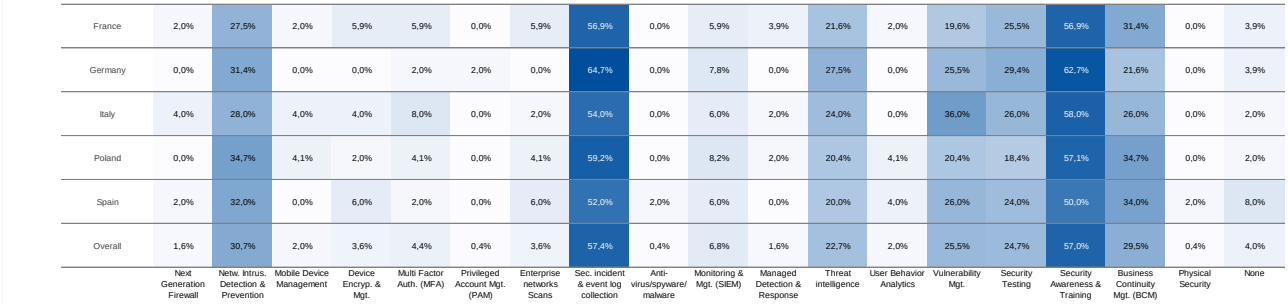
- **Security incident & event log collection** (64%), with an obvious relation to security incident reporting requirement provisions of the Directive.
- **Security Awareness & training** (63.6%)

Figure 35: Technologies and services procured to implement the NIS Directive



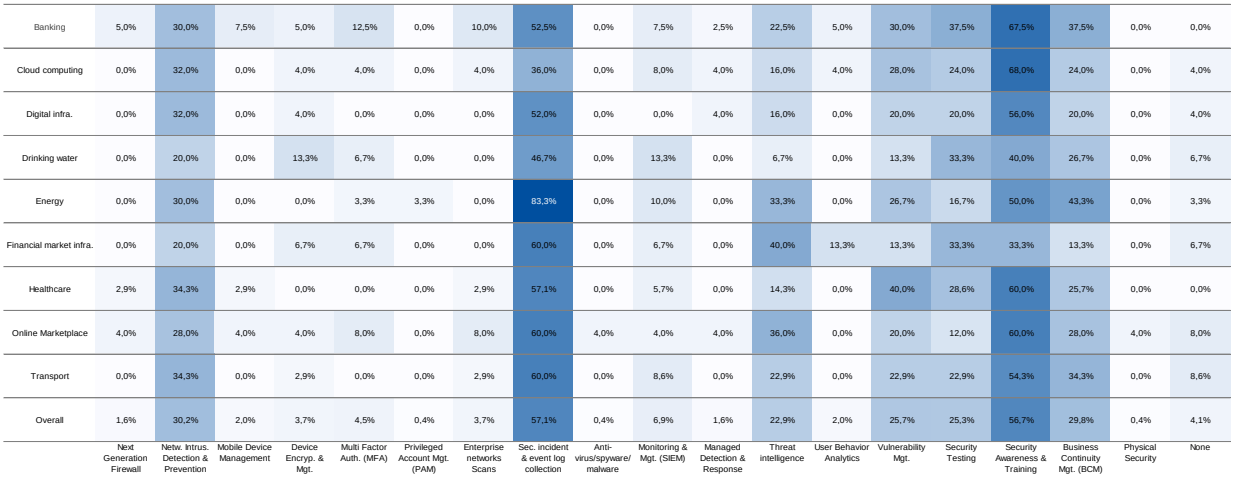
n = 225
Q: Which of the following technologies or services did you procure because of the NIS Directive implementation?
Scope: Organizations with existing or planned NIS program that planned further investments to NIS Directive-related
Note: Total does not add up to 100% since multiple answers could be selected by survey respondents

Figure 36: Technologies and services procured to implement the NIS Directive per country



	Next Generation Firewall	Netw. Intrus. Detection & Prevention	Mobile Device Management	Device Encryp. & Mgt.	Multi Factor Auth. (MFA)	Privileged Account Mgt. (PAM)	Enterprise networks Scans	Sec. incident & event log collection	Anti-virus/spyware/ malware	Monitoring & Mgt. (SIEM)	Managed Detection & Response	Threat intelligence	User Behavior Analytics	Vulnerability Mgt.	Security Testing	Security Awareness & Training	Business Continuity Mgt. (BCM)	Physical Security	None
France	2,0%	27,5%	2,0%	5,9%	5,9%	0,0%	5,9%	56,9%	0,0%	5,9%	3,9%	21,6%	2,0%	19,6%	25,5%	56,9%	31,4%	0,0%	3,9%
Germany	0,0%	31,4%	0,0%	0,0%	2,0%	2,0%	0,0%	64,7%	0,0%	7,8%	0,0%	27,5%	0,0%	25,5%	29,4%	62,7%	21,6%	0,0%	3,9%
Italy	4,0%	28,0%	4,0%	4,0%	8,0%	0,0%	2,0%	54,0%	0,0%	6,0%	2,0%	24,0%	0,0%	36,0%	26,0%	58,0%	26,0%	0,0%	2,0%
Poland	0,0%	34,7%	4,1%	2,0%	4,1%	0,0%	4,1%	59,2%	0,0%	8,2%	2,0%	20,4%	4,1%	20,4%	18,4%	57,1%	34,7%	0,0%	2,0%
Spain	2,0%	32,0%	0,0%	6,0%	2,0%	0,0%	6,0%	52,0%	2,0%	6,0%	0,0%	20,0%	4,0%	26,0%	24,0%	50,0%	34,0%	2,0%	8,0%
Overall	1,6%	30,7%	2,0%	3,6%	4,4%	0,4%	3,6%	57,4%	0,4%	6,8%	1,6%	22,7%	2,0%	25,5%	24,7%	57,0%	29,5%	0,4%	4,0%

Figure 37: Technologies and services procured to implement the NIS Directive per sector



	Next Generation Firewall	Netw. Intrus. Detection & Prevention	Mobile Device Management	Device Encryp. & Mgt.	Multi Factor Auth. (MFA)	Privileged Account Mgt. (PAM)	Enterprise networks Scans	Sec. incident & event log collection	Anti-virus/spyware/ malware	Monitoring & Mgt. (SIEM)	Managed Detection & Response	Threat intelligence	User Behavior Analytics	Vulnerability Mgt.	Security Testing	Security Awareness & Training	Business Continuity Mgt. (BCM)	Physical Security	None
Banking	5,0%	30,0%	7,5%	5,0%	12,5%	0,0%	10,0%	52,5%	0,0%	7,5%	2,5%	22,5%	5,0%	30,0%	37,5%	67,5%	37,5%	0,0%	0,0%
Cloud computing	0,0%	32,0%	0,0%	4,0%	4,0%	0,0%	4,0%	36,0%	0,0%	8,0%	4,0%	16,0%	4,0%	28,0%	24,0%	68,0%	24,0%	0,0%	4,0%
Digital infra.	0,0%	32,0%	0,0%	4,0%	0,0%	0,0%	0,0%	52,0%	0,0%	0,0%	4,0%	16,0%	0,0%	20,0%	20,0%	56,0%	20,0%	0,0%	4,0%
Drinking water	0,0%	20,0%	0,0%	13,3%	6,7%	0,0%	0,0%	46,7%	0,0%	13,3%	0,0%	6,7%	0,0%	13,3%	33,3%	40,0%	26,7%	0,0%	6,7%
Energy	0,0%	30,0%	0,0%	0,0%	3,3%	3,3%	0,0%	83,3%	0,0%	10,0%	0,0%	33,3%	0,0%	26,7%	16,7%	50,0%	43,3%	0,0%	3,3%
Financial market infra.	0,0%	20,0%	0,0%	6,7%	6,7%	0,0%	0,0%	60,0%	0,0%	6,7%	0,0%	40,0%	13,3%	13,3%	33,3%	33,3%	13,3%	0,0%	6,7%
Healthcare	2,9%	34,3%	2,9%	0,0%	0,0%	0,0%	2,9%	57,1%	0,0%	5,7%	0,0%	14,3%	0,0%	40,0%	28,6%	60,0%	25,7%	0,0%	0,0%
Online Marketplace	4,0%	28,0%	4,0%	4,0%	8,0%	0,0%	8,0%	60,0%	4,0%	4,0%	4,0%	36,0%	0,0%	20,0%	12,0%	60,0%	28,0%	4,0%	8,0%
Transport	0,0%	34,3%	0,0%	2,9%	0,0%	0,0%	2,9%	60,0%	0,0%	8,6%	0,0%	22,9%	0,0%	22,9%	22,9%	54,3%	34,3%	0,0%	8,6%
Overall	1,6%	30,2%	2,0%	3,7%	4,5%	0,4%	3,7%	57,1%	0,4%	6,9%	1,6%	22,9%	2,0%	25,7%	25,3%	56,7%	29,8%	0,4%	4,1%

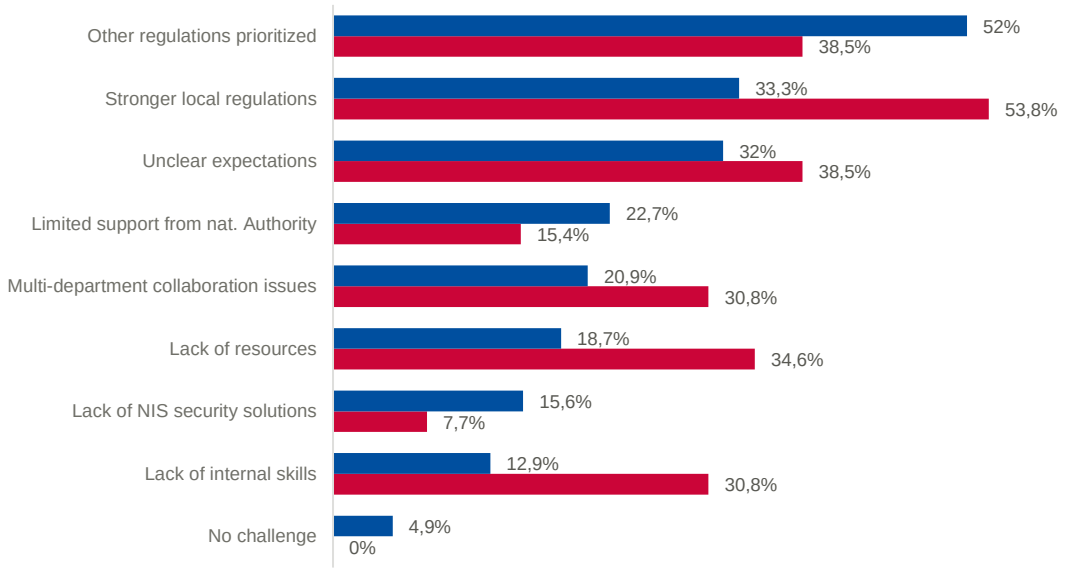
3.5 NIS DIRECTIVE IMPLEMENTATION CHALLENGES

Almost all OES and DSPs surveyed reported having faced at least one serious challenge while implementing the NIS Directive. Irrespective of organisations' current implementation state, the challenges that were most cited were the following:

- The prioritisation of other regulations e.g. GDPR.
- The existence of stronger local regulations e.g. France's "Loi de Programmation Militaire" (LPM).
- The lack of clarity of the NIS Directive expectations after transposition into national law.

However, as regards the organisations that *do not have* a dedicated NIS Directive implementation project, then internal challenges rise to prominence: the lack of resources (34.6% of such respondents), lack of skills (30.8%) or lack of collaboration (30.8%).

Figure 38: Main challenges in implementing the NIS Directive amongst surveyed organisations



n = 251
Q: In your opinion, what are the main challenges to implement the NIS Directive in your organization?
Note: Totals do not add up to 100% since multiple answers could be selected by survey respondents

For all countries in scope of the survey, the prioritisation of other regulations is the most frequently cited challenge to implement the NIS Directive, with the exception of France, for which organisations cited the existence of stronger regulations, such as the LPM.

The lack of clarity in the expectations of national competent authorities is also a relatively common denominator in all countries, with around 30% of organisations on average citing it as a challenge to implement the NIS Directive.

Figure 39: NIS Directive implementation challenges per country

	Unclear implications	Lack of skills	Lack of resources	Collaboration issues	Limited support from nat. authority	Other regulations prioritized	Stronger local regulations
France	23,9%	13,0%	23,9%	23,9%	8,7%	52,2%	58,7%
Germany	30,6%	20,4%	16,3%	26,5%	18,4%	49,0%	20,4%
Italy	37,0%	8,7%	17,4%	21,7%	28,3%	52,2%	41,3%
Poland	36,6%	7,3%	17,1%	14,6%	31,7%	56,1%	22,0%
Spain	32,6%	14,0%	18,6%	16,3%	27,9%	51,2%	23,3%
Grand Total	32,0%	12,9%	18,7%	20,9%	22,7%	52,0%	33,3%

For the large majority of sectors, other regulations pose the main challenge faced when implementing the NIS Directive, whether due to their prioritisation or the existence of stronger local rules / regulatory requirements.

A sizeable share of Digital infrastructure, Financial Market Infrastructure and to a lesser extent Online Marketplace organisations state the scarcity of resources devoted to the NIS Directive as challenge to its implementation.

Finally, the implications of the NIS Directive seem well grasped by Cloud computing organisations, as less than one in ten cite it as a challenge to set up the Directive, compared to nearly a third of all NIS affected organisations across the rest of the sectors.

Figure 40: NIS Directive implementation challenges per sector

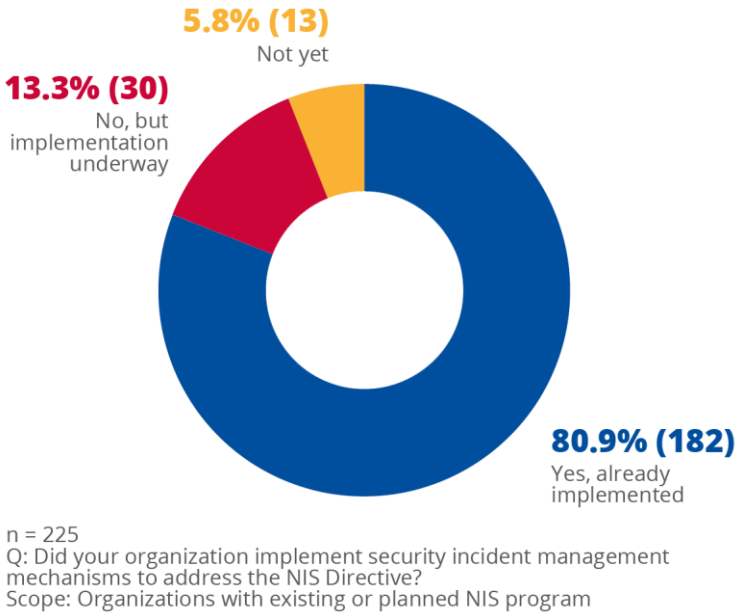
	Unclear implications	Lack of skills	Lack of resources	Collaboration issues	Limited support from nat. authority	Other regulations prioritized	Stronger local regulations
Banking	38,5%	10,3%	10,3%	15,4%	7,7%	51,3%	28,2%
Cloud computing	9,5%	19,0%	14,3%	14,3%	14,3%	57,1%	33,3%
Digital infra.	38,9%	27,8%	50,0%	11,1%	33,3%	44,4%	50,0%
Drinking water	36,4%	18,2%	27,3%	18,2%	18,2%	54,5%	18,2%
Energy	23,3%	3,3%	3,3%	26,7%	26,7%	50,0%	26,7%
Financial market infra.	42,9%	7,1%	50,0%	21,4%	35,7%	42,9%	7,1%
Healthcare	30,3%	15,2%	9,1%	33,3%	33,3%	51,5%	48,5%
Online Marketplace	27,3%	9,1%	31,8%	4,5%	22,7%	59,1%	54,5%
Transport	38,7%	12,9%	6,5%	25,8%	22,6%	51,6%	22,6%
Overall	31,5%	12,8%	17,8%	20,1%	22,8%	51,6%	33,3%

3.6 INFORMATION SECURITY INCIDENTS

3.6.1 Information security incident reporting

Survey data reveals that the NIS Directive requirements regarding information security incident management mechanisms are in place for most OES and DSP organisations: more than 80% have already implemented these mechanisms, with an additional 13.3% of surveyed organisations declaring to have their implementation underway with little variation between the MS in scope of the survey. This widespread adoption can be at least partly explained by the relative low number of personnel involved: more than 70% of affected organisations allocate up to 4 people to this task.

Figure 41: Implementation of information security incident management mechanisms among surveyed organisations

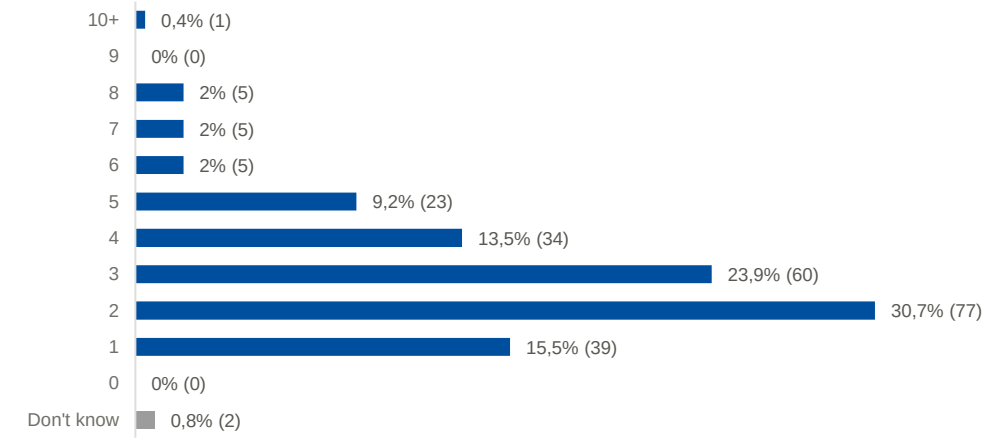


Mechanisms for information security incident management are largely in place for the majority of sectors.

Figure 42: Implementation of information security incident management mechanisms per sector

	Not implemented	Underway	Implemented
Banking	5,1%	2,6%	92,3%
Cloud computing	4,8%	23,8%	71,4%
Digital infra.	27,8%	27,8%	44,4%
Drinking water	0,0%	36,4%	63,6%
Energy	0,0%	0,0%	100,0%
Financial market infra.	14,3%	0,0%	85,7%
Healthcare	0,0%	12,1%	87,9%
Online Marketplace	0,0%	18,2%	81,8%
Transport	6,5%	16,1%	77,4%
Overall	5,5%	12,8%	81,7%

Figure 43: Staff responsible for information security incident reporting among surveyed organisations (FTEs)

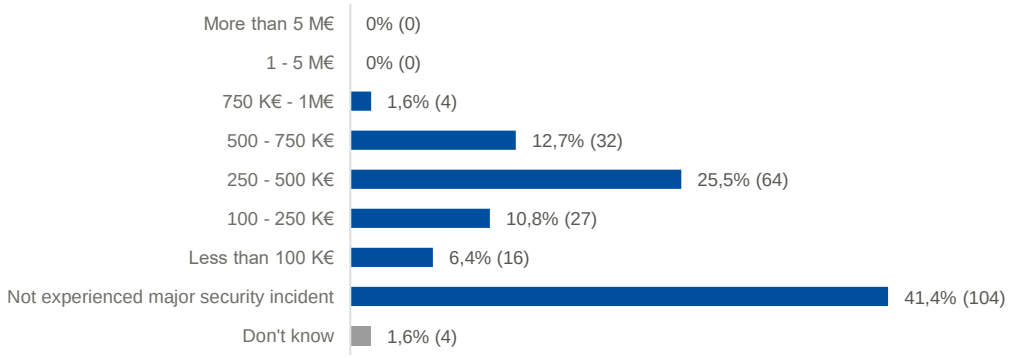


n = 251
Q: How many resources (FTEs) are responsible for the security incident reporting to your national authority in 2019?

3.6.2 Cost of major information security incidents

Among surveyed organisations, 58.6% did report major information security incidents. Among those organisations, the majority of respondents reported associated costs between 250 and 500 K€, without significant discrepancy when comparing between the EU MS in scope of the survey.

Figure 44: Major information security incident financial impact among surveyed organisations



n = 251
Q: What are the estimated damages incurred by the last major security incident(s) experienced by your organization?

Cloud computing, Digital infrastructure, Drinking water distribution and Transport are the sectors least affected major information security incidents based on the survey responses, while the sectors most affected are the Banking and Healthcare sectors.

The severity of the incidents appeared higher in organisations from Banking and Online marketplaces: respectively 32.5% and 28% of those organisations experienced incidents incurring more half a million euros of costs, versus less than 15% on average.

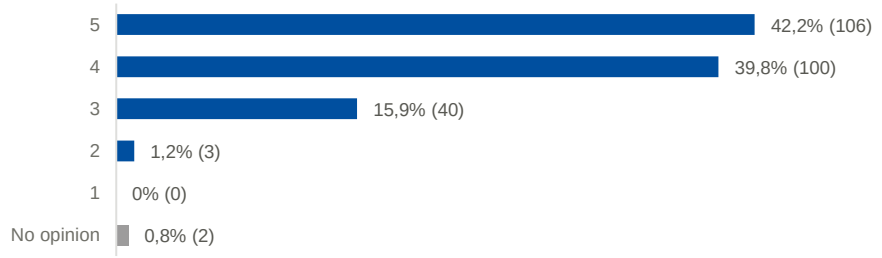
Figure 45: Major information security incident financial impact per sector

	<100 K€	101 - 250 K€	251 - 500 K€	500 - 750 K€	751 K€ - 1 M€	No major incident	Doesn't know
Banking	5,0%	2,5%	32,5%	27,5%	5,0%	25,0%	2,5%
Cloud computing	0,0%	8,0%	20,0%	16,0%	0,0%	56,0%	0,0%
Digital infra.	20,0%	4,0%	8,0%	12,0%	0,0%	56,0%	0,0%
Drinking water	6,7%	26,7%	13,3%	0,0%	0,0%	53,3%	0,0%
Energy	0,0%	0,0%	36,7%	20,0%	0,0%	43,3%	0,0%
Financial market infra.	6,7%	26,7%	13,3%	6,7%	0,0%	40,0%	6,7%
Healthcare	5,7%	28,6%	37,1%	5,7%	0,0%	22,9%	0,0%
Online Marketplace	8,0%	12,0%	12,0%	20,0%	8,0%	36,0%	4,0%
Transport	5,7%	5,7%	34,3%	0,0%	0,0%	51,4%	2,9%
Overall	6,1%	11,0%	25,7%	13,1%	1,6%	40,8%	1,6%

3.7 PERCEPTION OF THE NIS DIRECTIVE IMPACT

Survey data shows that the large majority of affected organizations tend to have a positive assessment of the NIS Directive contribution to their security posture. On a scale from 1 (low) to 5 (high), 82% of surveyed organisations gave the NIS Directive a mark of 4 or above. This positive assessment can be found irrespective of the EU MS or the sector concerned.

Figure 46: Appreciation of survey respondents of the NIS Directive impact on their information security posture



n = 251

Q: Please rate the impact of NIS Directive on your organization's security posture, where 1=Negative Impact; 3=Neutral and 5=Positive impact

Figure 47: Appreciation of the survey respondents of the NIS Directive impact on their information security posture per country

France	0,0%	0,0%	11,8%	37,3%	49,0%	2,0%
Germany	0,0%	0,0%	9,8%	60,8%	29,4%	0,0%
Italy	0,0%	0,0%	22,0%	36,0%	42,0%	0,0%
Poland	0,0%	2,0%	20,4%	30,6%	46,9%	0,0%
Spain	0,0%	4,0%	16,0%	34,0%	44,0%	2,0%
Grand Total	0,0%	1,2%	15,9%	39,8%	42,2%	0,8%
	1	2	3	4	5	No opinion

Figure 48: Appreciation of the survey respondents of the NIS Directive impact on their information security posture per sector

Banking	0,0%	0,0%	12,5%	42,5%	45,0%	0,0%
Cloud computing	0,0%	0,0%	24,0%	52,0%	24,0%	0,0%
Digital infra.	0,0%	8,0%	24,0%	40,0%	24,0%	4,0%
Drinking water	0,0%	0,0%	26,7%	40,0%	33,3%	0,0%
Energy	0,0%	0,0%	10,0%	16,7%	73,3%	0,0%
Financial market infra.	0,0%	0,0%	6,7%	33,3%	53,3%	6,7%
Healthcare	0,0%	0,0%	11,4%	40,0%	48,6%	0,0%
Online Marketplace	0,0%	0,0%	16,0%	48,0%	36,0%	0,0%
Transport	0,0%	2,9%	17,1%	45,7%	34,3%	0,0%
Overall	0,0%	1,2%	15,9%	40,0%	42,0%	0,8%
	1	2	3	4	5	No opinion

4. CONCLUSIONS

The data collected and processed for this report produced a number of interesting findings leading to some conclusions on the nature of NIS investments across different sectors and countries, as well as how the relevant spend among EU OES and DSPs has been influenced over the last few years by the NIS Directive. A summary of the main conclusions is presented below.

When analysing information security spending in a global, cross-industry scale (section 2.1), it can be observed that **organisations average around 6% of their overall IT budget to information security**, a percentage that has remained fairly stable since 2016. Discrepancies do exist when comparing organisations in different countries with **EU organisations allocating on average 41% less to information security than their American counterparts**. Discrepancies in information security spending are even more apparent between different sectors with certain sectors investing in information security a percentage of their IT budget up to 5-6 times higher than that invested by sectors with the lower information security spending profiles.

Section 2.2 illustrates how the information security budgets are spent and reveals that the average spending profile of EU and US organisations is very similar though **spending can significantly vary across different sectors**. Solutions related to Vulnerability Management and Analytics were found to comprise from 8% up to 35% of the organisations' overall information security budget when comparing different sectors. Smaller variations of the relevant percentage across sectors can be observed when looking at other information security products and services, such as Identity and Access Management (7% - 15%) and Network Security (11% - 28%). Section 2.4 presents the outlook of the information security market and identifies Cloud Access Security Brokers (CASB) as the fastest growing security segment is, reflecting the increased adoption of cloud in all sectors. Another key growing domain is Identity and Access Management, including Access Management (AM), Identity Governance and Administration (IGA), Privileged Access Management (PAM), and User Authentication. Indeed, organisations need to provide secure access to their remote workforce users, including IT users with privileged access, a requirement that has been further emphasised with the new modus operandi resulting from the on-going pandemic.

Figure 7 shows that **the main area of spending for information security is Personnel (37%)**, followed by Software (27%) and Hardware (21%). In terms of personnel, as of 2020, **information security staff represents 5,6% of total IT staff**, measured in terms of FTEs (information security personnel includes in-house and contract full-time equivalents supporting the IT security domains), as further detailed in section 2.3. While this percentage has remained relatively stable over the past 5 years there has been a **change in the security skills that are in demand**. Skills that were in high demand in previous years such as Manual Penetration Testing, Tier 1/2 SOC Analysis or Technology Management are now decreasing in value and are being replaced by skills in Risk Management, Service Management, Incident Response, Threat Intelligence, Data Science and Analysis or Coding.

The EU organisations surveyed (OES and DSPs) declared a broad range of information security budgets, ranging from less than 100 K€ to above 100 M€, with **the highest percentage of information security budget range among the surveyed organisations being 10 – 25 M€**. There is a **strong correlation between overall IT budget and Information Security budget**, as organisations with a higher IT budget will also spend more in information security (section 3.1).

Section 3.2 presents additional information related to the NIS Directive implementation and shows that, as of November 2020, **more than 80% of surveyed organisations declared that their NIS Directive implementation program is either completed or in progress** and 8% of surveyed organisations plan to implement the NIS Directive but have not started yet. When comparing across the different sectors of the NIS Directive, some sectors appear to be more relatively ahead in terms of its implementation. Furthermore the percentage of surveyed organisations that declared they will not directly implement the NIS Directive, but will instead leverage its principles as best practices, varies substantially across the different sectors. An interesting find is that 10**% of all surveyed organisations are not following an NIS Directive implementation program but are using the NIS Directive as best practice**. The start year of the NIS Directive implementation program varies between the MS in scope of the survey, a fact that can be attributed to different timelines in the transposition of the NIS Directive into national laws. However, **implementation projects of the NIS Directive typically last between 14 and 18 months**, with little discrepancies between countries or sectors.

The average budget for NIS Directive implementation projects is approximately 175 K€, with 42.7% of affected organisations allocating between 100 and 250 K€, representing a relatively low share of the organisations' overall information security budgets (section 3.3.1). This budget remains similar when examining across different MS but varies slightly when comparing different sectors. **The majority of organisations did not require additional staff to implement the NIS Directive (50.7%)**. Among those that did, ~29% filled that need by hiring new internal staff with the large majority recruiting up to 4 people. Discrepancies can be observed both across different MS, as well as across sectors (section 3.3.2).

Data presented in section 3.4 shows that the most frequently cited domains impacted by the NIS Directive implementation are **Governance, Risks and Compliance (64.5%)**, **Network Security (48.6%)** and **Business Continuity Management (33.1%)**. NIS Directive investments did not seem to focus on new technologies. The services most cited in the survey as NIS investment targets were Security incident & event log collection (64%) and Security Awareness & training (63.6%).

Section 3.5 indicates that almost all OES and DSPs surveyed reported having faced at least one serious challenge while implementing the NIS Directive. Irrespective of organisations' current implementation state, the challenges that were most cited were the **prioritisation of other regulations**, the **existence of stronger local regulations** and the **lack of clarity** of the NIS Directive expectations after transposition into national law. However, for organisations that *do not* have a dedicated NIS Directive implementation project internal challenges such as the **lack of resources (34.6% of such respondents)**, **lack of skills (30.8%)** and **lack of collaboration (30.8%)** appear to be most important. Overall, **82% of surveyed organisations acknowledge a positive impact of the NIS Directive on their security program**.

Finally, section 3.6 presents data collected on information security incidents. According to the data, **81% of the surveyed organisations have established a mechanism to report information security incidents** to their national authority, with the majority of surveyed organisations allocating up to 4 resources for incident reporting. Nearly **60% of surveyed organisations reported major information security incidents** with **43% of them having experienced information security incidents with a direct financial impact up to 500 k€**.

The data and accompanying analysis presented in this report offers some insights on NIS investments among EU OES and DSPs and how these investments have been influenced by the NIS Directive. Hopefully, this data will prove useful to policy makers at an EU and National level to better understand the impact of the NIS Directive and its implementation and reflect upon it to identify and focus future policy initiatives.

A ANNEX: SURVEY DEMOGRAPHICS

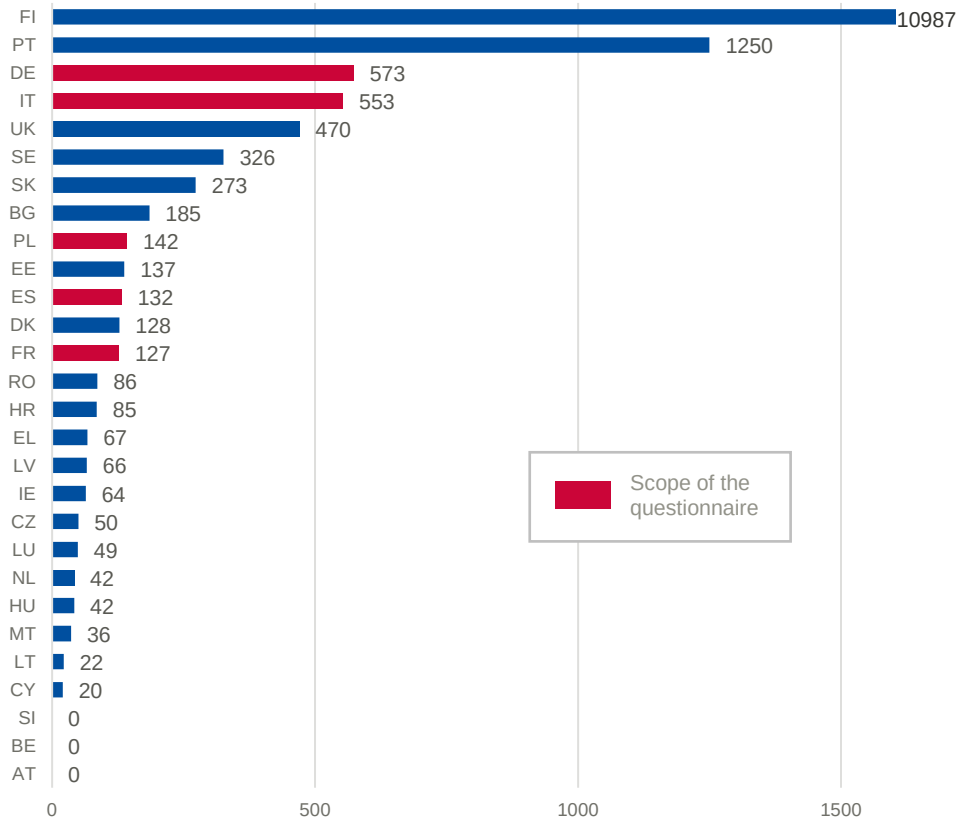
This Annex present additional information on the demographics of the survey used to collect the data presented in Chapter 3.

A.1 SELECTION OF MEMBER STATES TO FOCUS SURVEY

In order to secure a representative size of sample per country and respect the timeline associated with this report, the survey was performed on five Member States (Germany, France, Italy, Spain and Poland) selected based on the following criteria:

- National GDP.
- Estimated Information Security market size.
- Number of declared organizations in the scope of the NIS Directive (see figure below).
- Inclusion of one country representative of more recent Member States.

Figure 49: OES identified by Member States across all sectors[10]



[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019DC0546&from=EN

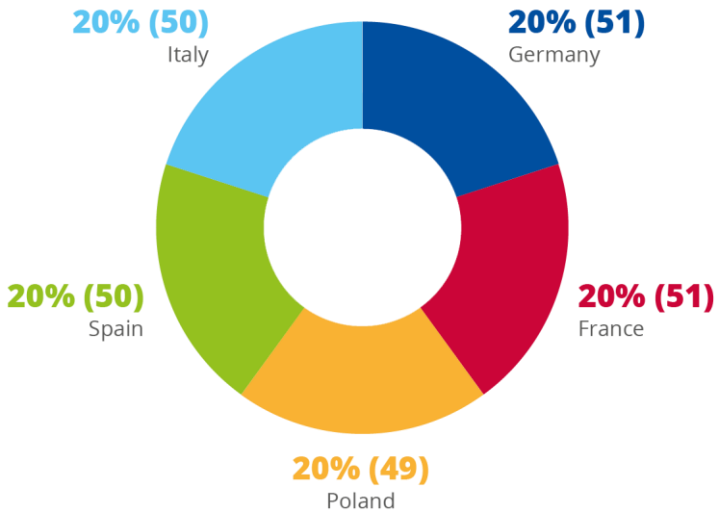
A.2 SURVEY RESPONDENT DEMOGRAPHICS

251 EU organisations identified as either operators of essential services (OES) or digital service providers (DSP) participated in the survey.

A.3 LOCATION OF SURVEYED ORGANISATIONS

Five Member States were selected for this survey: Germany, France, Italy, Spain and Poland. They were selected with regards to the size of their information security market as well as the number of OES and DSPs identified. The selection of surveyed organisations was designed to respect a balanced geographical distribution between the selected countries.

Figure 50: Distribution of surveyed organisations by country of origin



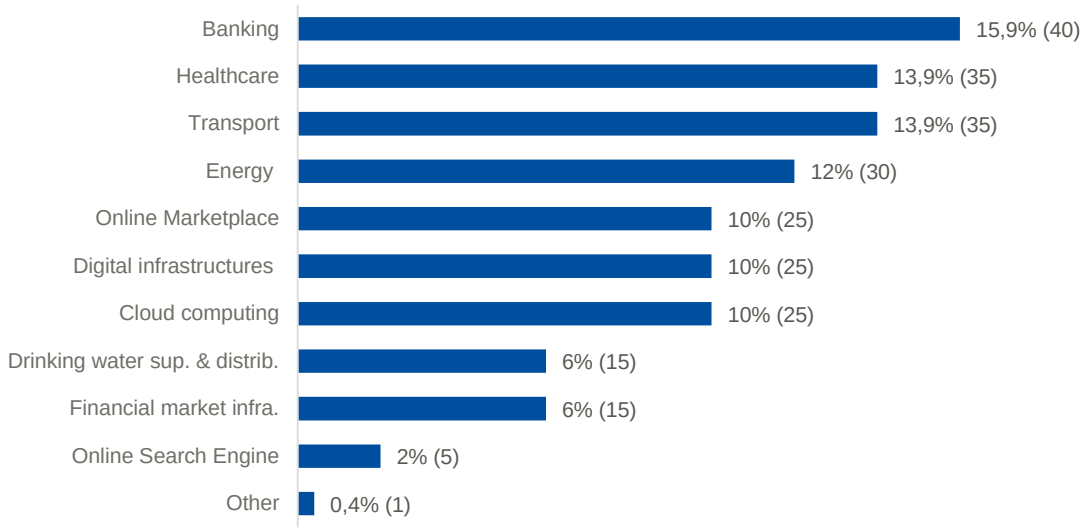
n = 251
Q: In which country is your organization located?

A.4 SECTORS OF SURVEYED ORGANISATIONS

The selection criteria for surveyed organisation were designed to align as closely as possible with the sectors in scope of the NIS Directive, namely:

- Online Search Engine
- Financial market infrastructures (trading venues, central counterparties)
- Drinking water supply and distribution
- Cloud computing
- Digital infrastructures (internet exchange points, domain name system service providers, top level domain name registries)
- Online Marketplace
- Energy (electricity, oil and gas)
- Transport (air, rail, water and road)
- Healthcare
- Banking

Figure 51: Distribution of surveyed organisations per sector

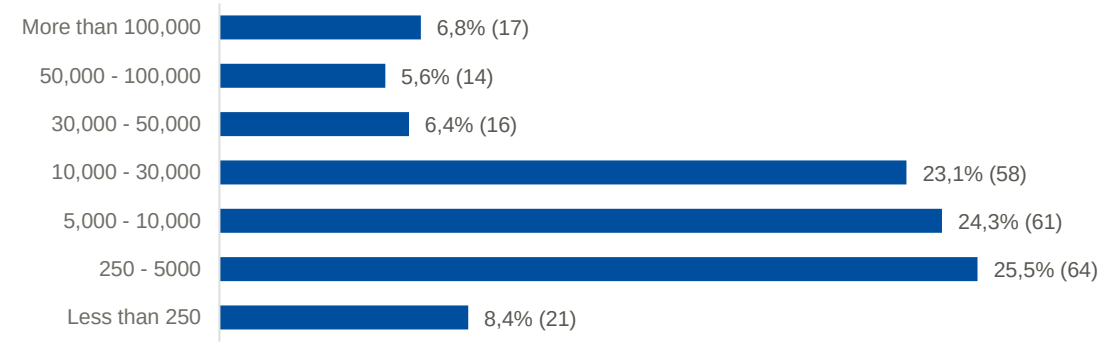


n = 251
Q: Which of below best describes the industry in which your organization operates?

A.5 STAFFING AND REVENUE OF SURVEYED ORGANISATIONS

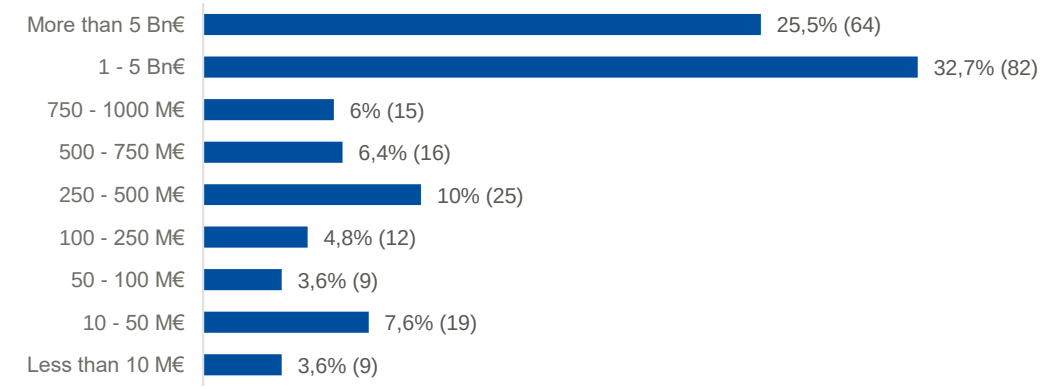
No specific quotas were set as to the size or revenues of the surveyed organisations as long as they were considered in scope of the NIS Directive.

Figure 52: Distribution of surveyed organisations by headcount



n = 251
Q: What is the estimated number of your organization's full-time employees in 2019?

Figure 53: Distribution of surveyed organisations by revenue (2019)



n = 251
Q: What is your organization's estimated revenue range in 2019?

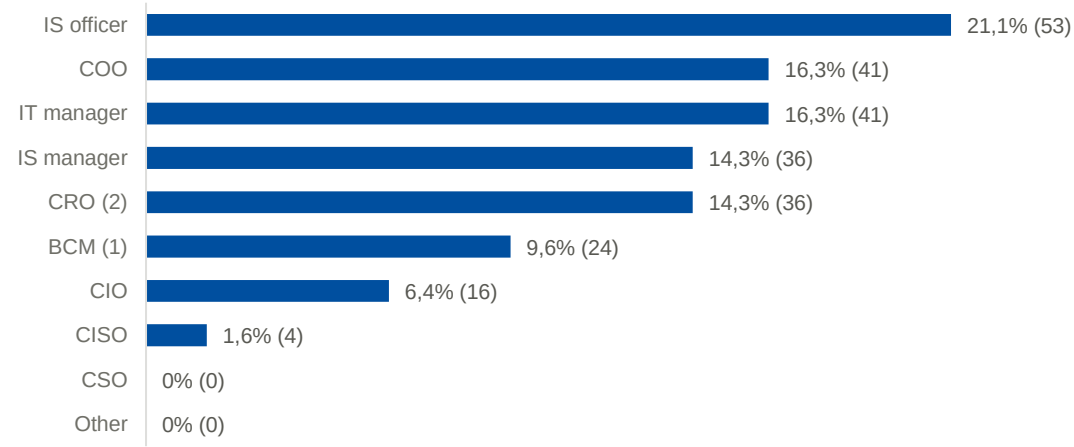
A.6 ROLE OF SURVEYED INDIVIDUALS

Collecting precise facts and figures for this study required the ability to reach out to individuals in each organisation that are knowledgeable in the field of cybersecurity and specifically in the implementation of the NIS Directive.

Consequently, most of the individuals that were qualified to take part in the survey have direct or indirect links with Information Security departments.

It should be noted that the prevalence of COO (Chief Operating Officer) among respondents can be explained by the fact that in many organisations Information Technology falls under their responsibility.

Figure 54: Distribution of surveyed individuals by role

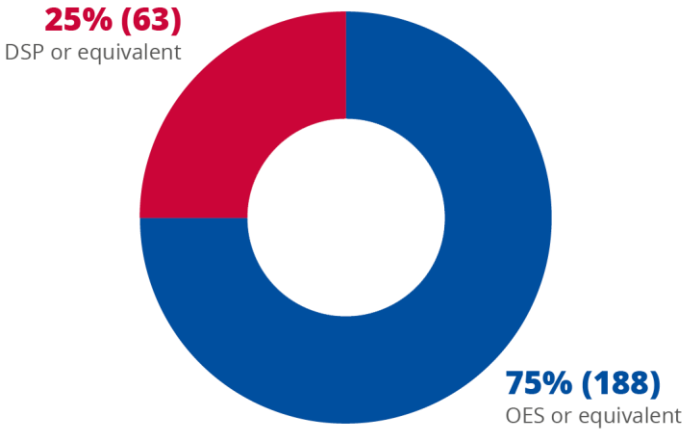


n = 251
Q: Which of the function below best match your role in your organization?
(1) = Business Continuity Manager; (2) = Chief Risk Officer

A.7 TYPES OF SURVEYED ORGANISATIONS

The most important selection criteria for this survey was the applicability of the NIS Directive. The 251 organizations included in the survey results all declared to be considered Operator of Essential Services (OES) or Digital Service Providers (DSP) by their respective national competent authorities.

Figure 55: Distribution of surveyed organisations by type of NIS Directive entity



n = 251
Q: Is your organization considered as an "Operator of Essential Services" (OES), a "Digital Service Provider" (DSP) or equivalent by your country's national authority?

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 database definitions.

B.1 FINANCIALS

- **Operational Expense** is defined as: the total expense associated with the business units supported by the IT organization.
  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 amortization expenses. For insurance, this includes underwriting expenses, loss and loss-adjustment expenses; for banking organizations, it includes interest expenses and noninterest expenses; for government and non-profit organizations, 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 it is not limited to the IT organization. It includes estimates by enterprises on decentralized IT spending and or "shadow IT."
  It is calculated on an annualized 'cash flow view' basis, and, therefore, contains capital spending and operational expenses, but not depreciation or amortization.

B.2 INDUSTRIES

- **Banking and Financial Services** –Organizations from which their primary revenue stream is derived from one or more of the following:
  - 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 Organizations, etc.

- **Education** - Organizations from which their primary revenue stream is derived from one or more of the following:
  - Higher Education
  - Colleges, Universities, and Junior Colleges.
  - Other (Professional Schools, Elementary and Secondary Schools, Vocational Schools, Specialty Educational Services. Automobile Driving Instruction, Child Day Care Services, Educational Curriculum Development, Exam Preparation and Tutoring, Online Education Courses, Online Training Services)

- **Energy** - Organizations from which their primary revenue stream is derived from one or more of the following:
  - 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, Petroleum Refining.
  - Oil and Gas Storage and Transportation, Natural Gas Pipelines, Oil and Gas Pipelines.

- **Natural Resources** - Organizations from which their primary revenue stream is derived from one or more of the following:
  - 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 Molding and Die Casting, Drawing and Insulating Of Diversified Metal Wire, Copper Wire Drawing, Fiber Optic Cable, Rolling, Drawing, and Extruding of Copper, Copper Powder, Paste and Flakes, Smelting and Refining of Diversified Metals.
  - Agricultural Services, Animal Services, Horses and Equines Services and Breeding, Livestock Services, Crop Services.

- **Government** Organizations from the National Governments, International Organizations performing government services, as well as Government Affiliated Organizations.

- **Healthcare Providers**
  - Healthcare Facilities, Assisted Living Facilities and Services, Nursing Homes, Retirement Communities, Hospitals and Healthcare Centers, 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, Healthcare Referral Services.
  - Medical Laboratory Services, Mental Care Facilities, Rehabilitation Services, Occupational Therapy Services, Physical Therapy Services, Speech and Language Therapy Services, Medical Practice Organizations, Physician Practice Management Organizations, Primary Care Practitioner Services, Ambulance Services.

- **Pharmaceuticals and Life Sciences**
  - 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 Organization, 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, Orthbiological Products, Protein and Genome Sequence Products, rDNA Pharmaceuticals, 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 (REITs), 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 (ERP), 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, Reupholstery and Furniture Repair
  - Environment, Conservation, and Wildlife Organizations, Humane Societies, Membership Organizations, Business Associations, Civic, Social, and Fraternal Associations, Farm Business Organizations, Labor Unions and Labor Organizations, Professional Membership Organizations, Political Organizations

- **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, 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, 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-Ins Software, Search Engine Software, Web Site Management Software, Website Infrastructure Software. Application Hosting Services, Application Service Providers (ASPs), Custom Web Site Design and Business Solutions, Online Research Services, Online Small Business Portals, Online Supply Customer Relationship Management (CRM) 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 (CTI) Software, Design Automation Software, Maintenance Encryption Software, Network Administration, Operating System Software,

- **Telecommunications**
  - Communications Equipment, Communications Processing Equipment, Communications Towers, Telephone and Telecommunications Equipment, Telecommunications Equipment, Integrated Services Digital Network (ISDN) Equipment, Private Branch Exchange (PBX) Network Equipment, Switchboard Equipment, Telephone Switching Equipment, Telephone Equipment, Paging Systems, Teleconferencing Equipment, Wireless Telephone Equipment. Wireline Telephone Equipment, Answering Machines, Cordless Telephones
  - Telecommunication Services, Diversified Telecommunication Services, Alternative Carriers, Broadband Telecommunications Services, Asynchronous Transfer Mode Network Services (ATM), Digital Telecommunications Services, Digital Subscriber Line Services (DSL), Integrated Services Digital Network Services (ISDN), Point to Point Digital Telecommunications Services, Fiber Telecommunications Services, Virtual Private Network Services (VPN),

- **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 Service, Limousine, Taxicab,
- **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, Water Distribution.

B.3 SECURITY DOMAINS

Security Domains	Description	Key NIS related solutions & services
Network Security	Protection of telecommunications infrastructure from threats resulting in compromised data in flight or loss of network availability	Next generation firewalls Network intrusion detection & prevention (NIDS and NIPS)
Endpoint Security	Protection of endpoint systems, including servers, end-user laptops and desktops	Anti-virus/anti-spyware/anti-malware software on PCs and servers Mobile device management (MDM) Device encryption and management
Data Security	Protection from compromised data, exposed data, loss of data fidelity or lost data resulting from compromised systems, systems failure or inappropriate user behaviour	No core focus on NIS
Identity & Access Management	Protection from unauthorized access to data, applications, and devices, resulting from compromised identities and credentials	Strong or multi factor authentication (MFA) / two-factor (2FA) Privileged Account Management (PAM)
Vulnerability Management	Proactive mitigation of risk due to weaknesses, and protection from data exposure and production loss resulting from comprised systems and IT infrastructure	Scan enterprise networks (IP ranges) & Asset Management
Security Analytics	Use of data analytics captured from security information and events management (SIEM) systems to proactively mitigate risk due to weaknesses in the IT infrastructure	Security incident and event log collection Monitoring & management (SIEM) Managed log retention & analysis User behavior analytics (UEBA) Threat intelligence services Fraud detection and response services Cyber incident response services
Application Security	Software applications to provide protection from data exposure resulting from transaction compromise or failure	No core focus on NIS
Governance, Risk & Compliance	Protection from security risks through the management and achievement of security objectives commensurate with and necessary for the achievement of business objectives	Governance & risk management Service protection policies and processes Security training & awareness Supply chain security Business continuity

- **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 IAM related activities are: user account provisioning, password management, user access administration (e.g., changes in roles, position or status (JML)), directory integration, single sign-on (SSO), Active Directory, remote access services, strong or multi factor authentication / two-factor (2FA) / three-factor (3FA), hard and soft token based authentication services, Public Key Infrastructure (PKI) and Federation type services, privileged user management (PUM), Identity and access governance (IAG) (inclusive of 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 unauthorized 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 (WAF)s / RASP, Network Intrusion Detection & Prevention (NIDS and NIPS), Virtual Private Networking (VPN) concentrators, Hardware Security Modules (HSMs), Proxy Servers, Secure Email and/or Web Gateways, Unified Threat Management (UTM) appliances, Network Access Control (NAC) services, and Distributed Denial of Service (DDoS) protection and prevention services.

- **End Point 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 end point 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 (MDM), device encryption and management, Host Intrusion Detection & Prevention (HIPS), 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 unauthorized 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 & classification, encryption/decryption of data "at rest," "in motion" or "in use" (incl. endpoint & bulk storage data encryption/decryption), digital certificate lifecycle management for digital signature based services, privacy enforcement techniques (data masking), database audit and protection (DAP) techniques, data loss prevention (DLP) services and data destruction, 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 prioritization; 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 centralized 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 & 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 unauthorized access, theft, modification of 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 & dynamic application testing techniques (SAST/DAST/IAST) and application security frameworks, and/or via data obfuscation, filtering & masking, secure coding practices and software composition analysis (SCA) etc.

- **Governance, Risk, and Compliance Management** (**GRC**) in general 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 organization 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 & procedures, the communication of business values, culture & principles, security strategy & organization, training & awareness, documentation & 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 Chief IT security Officer (CISO) or equivalent, and his 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 & action tracking, and the development and execution of remediation plans.
  – Compliance Management is the process of identifying, managing and reporting compliance activities related to organizational, 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.4 SECURITY ASSET TYPES

- **Hardware** is defined as:
  – All dedicated hardware assets utilized 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, etc.
  – Include only annual asset costs that are directly or recognizably related to the defined in-scope security functions. Do not include costs of hardware assets whose prime purpose is not security. For example, there may be routers deployed that have firewall, encryption or NIPS capabilities, but you must not include any apportionment of their annual costs unless you can identify a cost to specifically enable a security function - such as a firewall "add-on" enabler cost of extra router hardware or software.
  – 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 center, 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:
  - Annual license and maintenance as well as 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, content filtering, etc.
  - Only software license costs that are directly or recognizably 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 licenses for OS, productivity suite software or enterprise packages that have security capabilities (e.g., BitLocker encryption in WinOS). No apportionment of their annual costs are 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 license charge for security functionality (e.g., Oracle Identity Manager)

- **Outsourcing** is defined as:
  - 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 (MSP)/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, DDoS etc. and cloud-based security services such as IDaaS.
  - Consulting is defined as: Security advisory services that help organizations analyse and improve the efficacy of business operations and technologies strategies.

- **Personnel** is defined as:
  - 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-06-20-028-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
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-442-8
DOI: 10.2824/50973