enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

NIS Investments

2025

CONTACT

To contact the authors, please send an email to nis360@enisa.europa.eu

For media enquiries about this paper, please email press@enisa.europa.eu

AUTHORS

Eleni Philippou, Ugne Komzaite-Kraujale, Jurgita Skritaite, ENISA

ACKNOWLEDGEMENTS

The authors would like to thank the following contributors for the insights, feedback, and value they have provided to this effort: Patrick Abel, François Gratiolet, Edwin Maaskant, Gartner, members of the NIS Cooperation Group, NLOs Group, colleagues from the European Commission and ENISA.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA unless otherwise stated. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) No 2019/881. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or in part must indicate ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-777-1 ISSN 2600-4712 DOI 10.2824/7442427

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The **annual NIS Investments report** presents the findings of a study conducted by ENISA to explore **how cybersecurity policy translates in practice across organisations in the EU** and **its effects on their investments, resources, and operations.**

Data for this edition was collected from **1 080** professionals representing **organisations**[1] **across the EU** and **the NIS sectors of high criticality.** The sample consisted **mainly of large enterprises** (83%), complemented by a smaller share of SMEs (17%) to allow for comparative insights between organisations of different sizes.

The data supports analysis of how cybersecurity policy plays out in practice. It also considers broader contextual factors — such as the threat landscape and market dynamics — that may influence how organisations prioritise and implement cybersecurity practices. In addition, the dataset contributes to wider analytical work, including ENISA NIS360, which assesses sectoral criticality and maturity, as well as the EU Cybersecurity Index and the State of Cybersecurity in the Union report.

[1] Private companies, public sector entities and operators within the scope of the NIS Directive, whether publicly or privately owned.

Key insights from this year's report are summarised below:

Insight #1: Investment focus shifts from people to technology and services

Cybersecurity investment remains broadly in line with the levels reported in last year's study (9% of IT budgets; median 1.5 million euros), though spending is increasingly focused on technology and outsourcing rather than internal cybersecurity teams.

Insight #2: The cyber talent crunch shows no signs of easing

Organisations across the EU continue to face difficulties in attracting (76%) and retaining (71%) cybersecurity professionals, intensified by a shortage of skilled professionals and fierce competition for limited talent. High turnover reinforces this gap, raising risk and reshaping staffing strategies.

Insight #3: Compliance is the main investment driver but not the only outcome

Compliance remains the main driver of cybersecurity investment (70%) yet its benefits extend beyond regulation — strengthening risk management (41%), detection (35%) and response (26%). Looking ahead, organisations plan to focus more on upgrading tools, improving recovery and building internal skills, indicating that policy is steering progress in the right direction.

Insight #4: NIS2 is raising the bar, yet implementation remains a challenge

Implementing NIS2 is considered a challenge. Organisations say their key challenges are in the areas of patching (50%), business continuity (49%) and supply-chain risk (37%). This suggests that NIS2 is raising the bar by prompting entities to focus on strengthening some of the most demanding yet essential areas of cyber resilience.

Insight #5: Patching still takes months; many still don't test their security

Timely patching and regular assessments remain challenging even amid regulatory efforts: 30% of organisations have not conducted a cybersecurity assessment in the past 12 months, 28% take more than three months to patch critical vulnerabilities.

Insight #6: Supply chain risk: stronger controls, deeper dependence

While supply-chain risk management is improving, increasing reliance on outsourced ICT and security services introduces new vulnerabilities — particularly when suppliers are resource-constrained SMEs. Reflecting this, supply chain and third-party compromises are the second most frequently cited top concern for the future (47%).

Insight #7: DoS caused the noise, ransomware causes the nightmares

While DoS attacks put the most strain on daily operations last year, ransomware (55%), supply-chain attacks (47%) and phishing (35%) dominate organisational concerns looking ahead. Preparedness is uneven, with SMEs reporting the lowest confidence in their ability to anticipate, withstand and recover from cyber incidents — across all scenarios.

SECTION I

KEY INSIGHTS

INSIGHT #1

INVESTMENT FOCUS SHIFTS FROM PEOPLE TO TECHNOLOGY AND SERVICES

Over the past year, organisations have maintained cybersecurity investment at levels comparable to the previous year; however, this spending appears to be directed more toward technology and outsourcing rather than expanding internal cybersecurity teams.

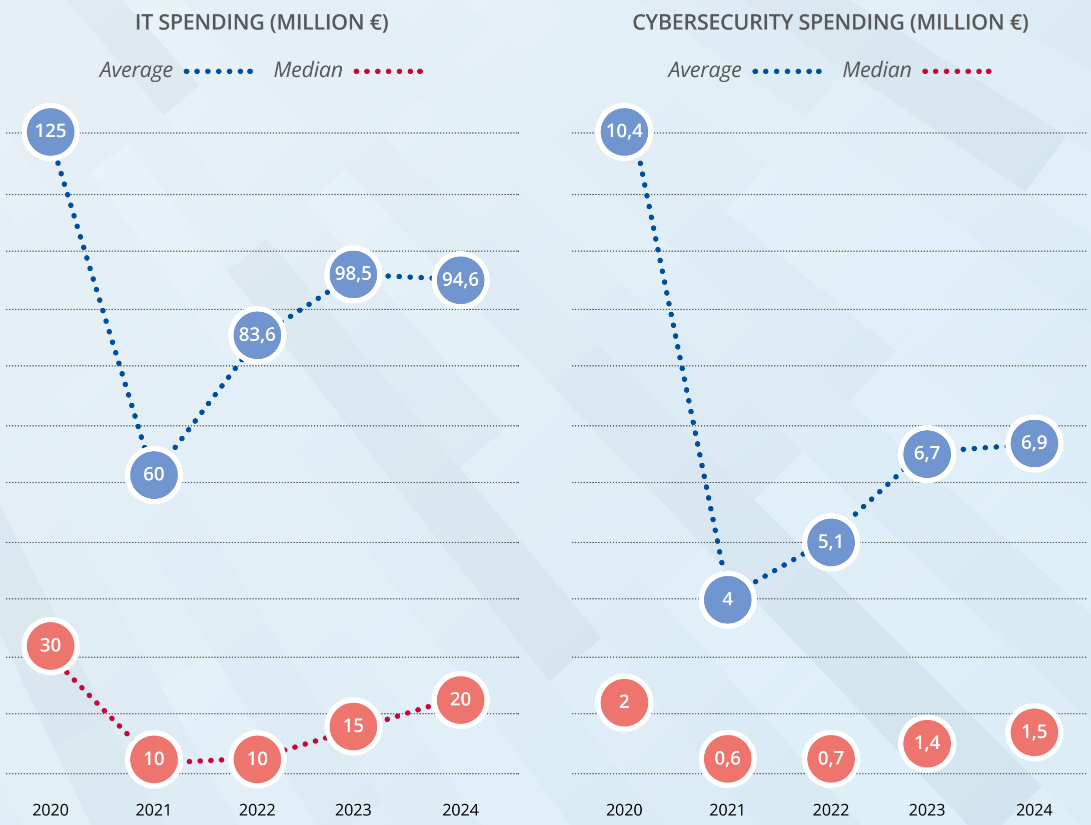
Over the past year, organisations have **maintained their cybersecurity**[2] **investments at levels comparable to the year before,** reflecting ongoing prioritisation of information security. In this report, budgets and investment are used interchangeably, covering *CAPEX and OPEX on hardware, software, personnel, contractors, and outsourcing.*

Cybersecurity investment and staffing were analysed in absolute terms and relative to overall spending on IT using ratios. **Absolute** values provide a **sense of magnitude,** showing the total resources (money or people) dedicated to cybersecurity. **Ratios** complement this by providing a consistent **basis for comparing** investment and staffing across organisations of different sizes and over time, supporting meaningful year-on-year analysis.

Overall **cybersecurity spending** has increased modestly in terms of absolute values, both in terms of the median and average, reflecting a gradual growth in cybersecurity budgets. By contrast, IT spending shows a divergent pattern: the average has decreased while the median has increased. This suggests that although very large IT spenders have reduced their investment —pulling the average down— most organisations have actually increased IT spending over the year.

A similar dynamic is observed in staffing. For **cybersecurity personnel**, the average number of full-time equivalent (FTEs) decreased slightly while the median increased modestly, indicating that most organisations have largely stable team sizes. For IT personnel, the average FTEs declined while the median rose, reflecting reductions among very large organisations but modest growth for the majority (Fig 2).

FIG. 1 - IT & CYBERSECURITY SPENDING (ABSOLUTE VALUES)



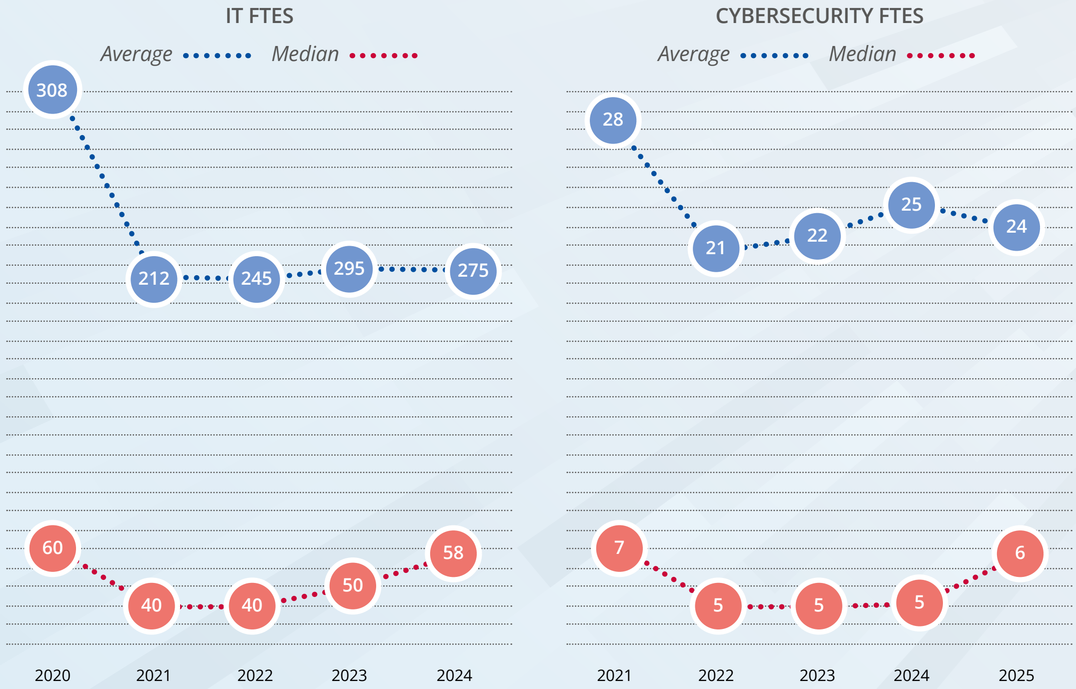
IT SPENDING (MILLION €)

CYBERSECURITY SPENDING (MILLION €)

A similar dynamic is observed in staffing. For **cybersecurity personnel**, the average number of full-time equivalent (FTEs) decreased slightly while the median increased modestly, indicating that most organisations have largely stable team sizes. For IT personnel, the average FTEs declined while the median rose, reflecting reductions among very large organisations but modest growth for the majority (Fig 2).

[2] In this report, 'cybersecurity' and 'information security (IS)' are used interchangeably to refer to all activities, staff and resources dedicated to protecting an organisation's information systems and digital assets.

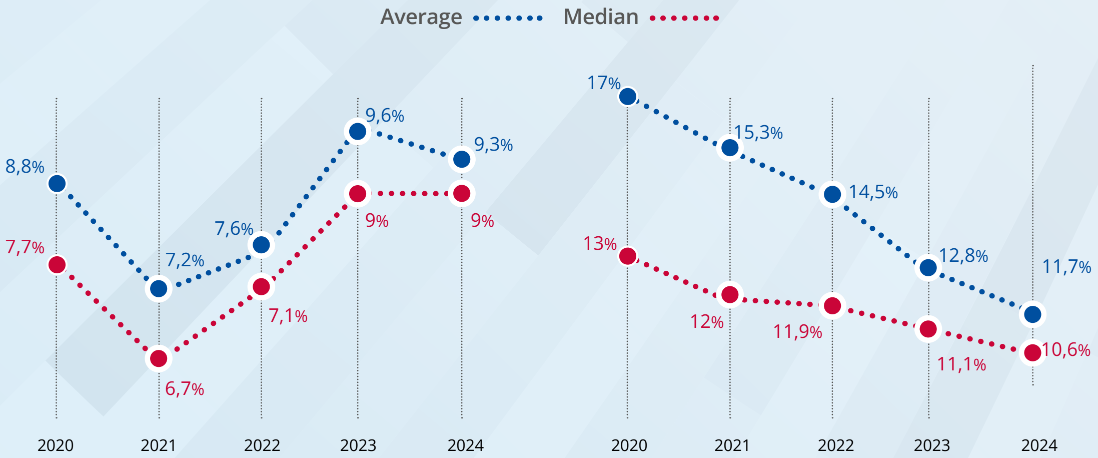
FIG. 2 - IT & CYBERSECURITY FTES (ABSOLUTE VALUES)



In terms of ratios, **median cybersecurity spending as a proportion of IT spending remained stable,** reflecting that most organisations maintained or modestly increased their budgets. The **average ratio dropped slightly,** driven by reductions among very large spenders (Fig. 3). Overall, cybersecurity budgets accounted for 9% of total IT budgets, with independent studies suggesting that spending on cybersecurity is likely to continue rising[3].

Regarding staffing, **cybersecurity FTEs now represent only 10,6% of total IT FTEs** (Fig.3), marking the lowest proportion observed to date.

FIG. 3 - CYBERSECURITY AS A SHARE OF IT BUDGET (LEFT) & CYBERSECURITY AS A SHARE OF IT FTES (RIGHT)



The decline in the FTE ratio largely reflects faster growth in IT teams rather than reductions in cybersecurity staff and may also indicate that **organisations face constraints in expanding cybersecurity teams** due to persistent skills shortages. It also highlights that **cybersecurity budgets are currently being directed more toward technology and outsourcing** (the remaining areas of our budget definition) rather than internal team growth. This shift may reflect strategic choices to maximise impact with limited human resources, responses to talent constraints or greater reliance on external providers — trends that warrant further investigation in the coming year.

[3] According to the Gartner 2025 CIO and Technology Executive Survey, cybersecurity remains the top area where 87% of the surveyed enterprises planned to increase their funding in 2025 from 2024. A similar trend is also forecasted by IDC's Worldwide Security Spending Guide — worldwide security spending to increase by 12.2% in 2025 as global cyberthreats rise.

INSIGHT #2

THE CYBER TALENT CRUNCH SHOWS NO SIGNS OF EASING

Across the EU, the organisations surveyed face a dual challenge: a structural shortage of cybersecurity professionals with the required skills and intense competition over the limited pool of talent. This combination contributes to high turnover, creating a cycle that further deepens the shortage, increasing cybersecurity risk while also influencing staffing strategies and drawing attention to the skills most in demand.

Across the study, organisations were found to be struggling to attract and retain the cybersecurity talent they need. This challenge is driven by two linked forces. Firstly, the talent pool is constrained by a structural shortage of cybersecurity specialists with the required skills. Secondly, fierce competition over the limited pool of talent makes it harder to attract and retain those who are available.

The supply-side gap: structural shortage of cybersecurity skills

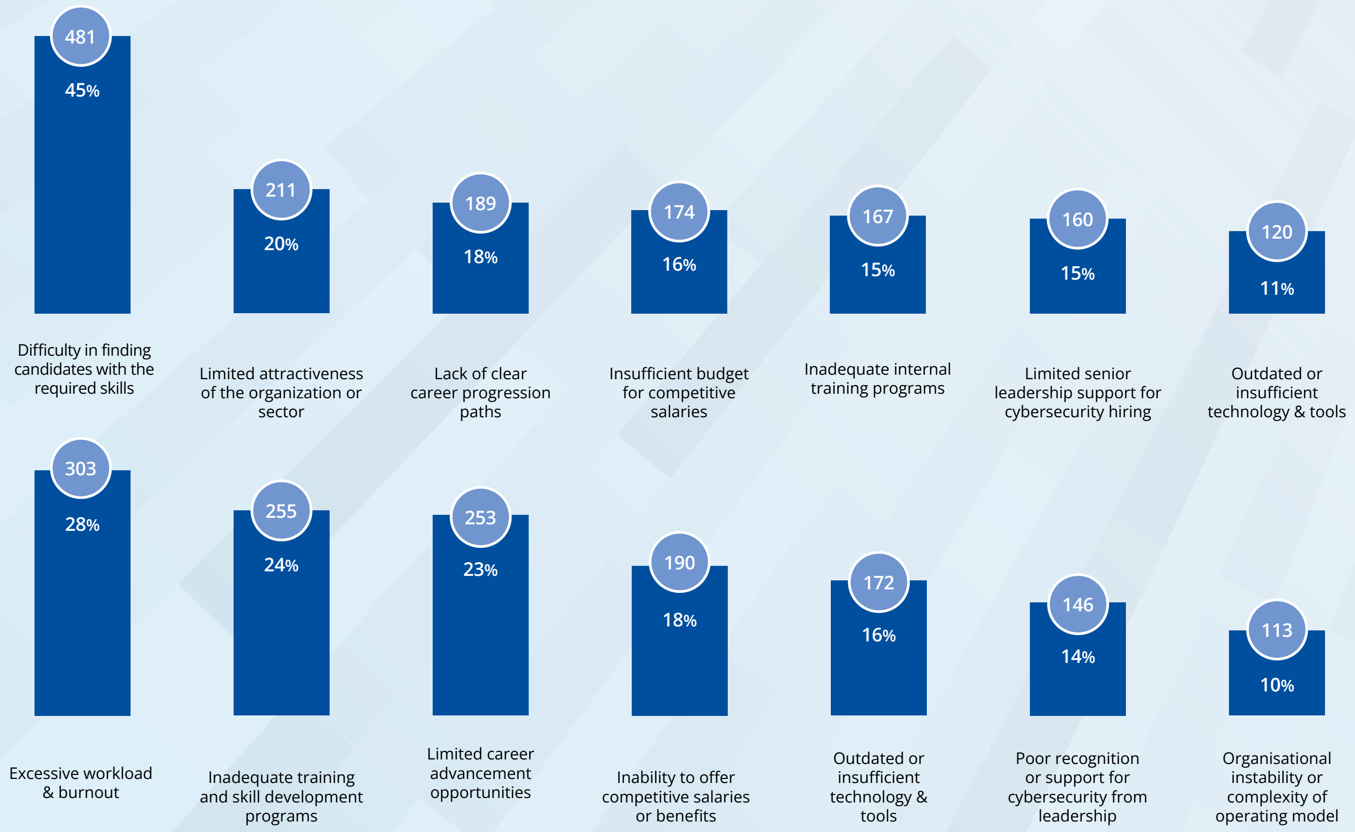
The main barrier to hiring is difficulty finding candidates with the required skills (45%), which highlights a persistent shortage of cybersecurity specialists across Europe. This reflects a deeper issue: in many cases, the skilled professionals simply do not exist. Within the EU, the estimated shortage reached 299,000 in 2024, representing a 9% increase from 2023[4]. Across the wider European region, the gap stood at 424,000, while the global shortfall climbed to 4.8 million[5].

At the same time, many employees in cybersecurity-related roles lack formal qualifications or certified training, and a significant share have transitioned from other professions, indicating that upskilling and reskilling account for much of today's workforce[6]. This mismatch between demand and available expertise helps explain why scarcity of skills is the dominant challenge in hiring.

The demand-side pressure: competition and organisational constraints

Even when skilled candidates do exist, organisations face fierce competition to attract and retain them. Organisations point to several barriers to attracting cybersecurity talent, including the unattractiveness of a sector or organisation (20%), limited career paths (18%) and uncompetitive salaries (16%), while the main pressures on retention are workload or burnout (28%), training and the development of skills (24%) and career advancement (23%) (Figure 4). As a result, many entities find themselves caught in a cycle of high turnover and persistent vacancies.

FIG. 4 - CHALLENGES TO ATTRACTING & RETAINING CYBERSECURITY TALENT



[4] European Commission *Communication on the European Cybersecurity Skills Academy* COM(2025) 10 final January 2025.
[5] ISC2 *Cybersecurity Workforce Study 2024* September 2024.
[6] According to ISC2 *Cybersecurity Workforce Study 2024,* 76% of employees in cybersecurity-related roles lacked formal qualifications or certified training, while 66% of cybersecurity roles in education, health and social work, were filled by people changing their careers from non-cyber positions.

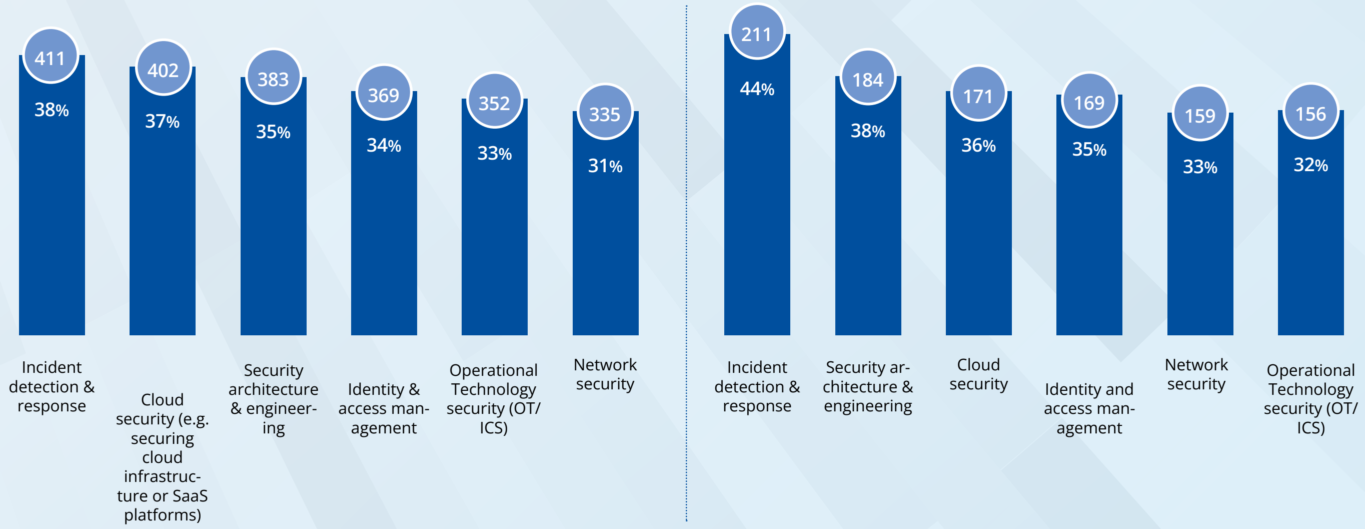
The consequences of these constraints are increasingly visible. **Understaffed or overstretched cybersecurity teams are considered a contributing factor to elevated operational risk,** with 81% of companies surveyed viewing hiring difficulties as a key factor raising their exposure to cyberattacks[7]. Beyond immediate risk, teams that are under-resourced against rising obligations and threats face higher workload, while having insufficient protected training time and constrained opportunities for progression, all factors contributing to high turnover. Stress, time constraints for professional development and limited advancement are recurring drivers of staff turnover in cybersecurity roles[8]. This creates a reinforcing loop: the lack of skilled professionals drives turnover, and turnover deepens the shortage.

SMEs

SMEs continue to face distinct challenges in building and maintaining cybersecurity capacity. Limited budgets hinder their ability to attract experienced professionals and to retain them through benefits, ongoing training and career development, and SMEs are less likely than large organisations to have dedicated staff or formal processes for managing cyber risk[9]. In fact, 94% of SMEs report difficulties attracting and 90% retaining cybersecurity personnel (vs 83% and 80% among large enterprises), which in turn undermines their ability to meet 2025 objectives[10]. Taken together, these constraints leave IS teams proportionally thinner even as budgets remain a high share of total IT expenditure.

These constraints shape where demand is the strongest, with pronounced needs identified in incident detection and response (38%), cloud security (37%), security architecture and engineering (35%), identity and access management (34%), operational technology and security of industrial control systems (33%) and network security (31%). Among organisations that struggle to hire, the same skills remain the most sought after — with 44% of entities citing difficulty in finding candidates with the required expertise also identifying these domains as their highest priority, 38% security architecture and engineering, 36% cloud security, 35% identity and access management, 33% network security and 32% OT/ICS security (Fig. 5).

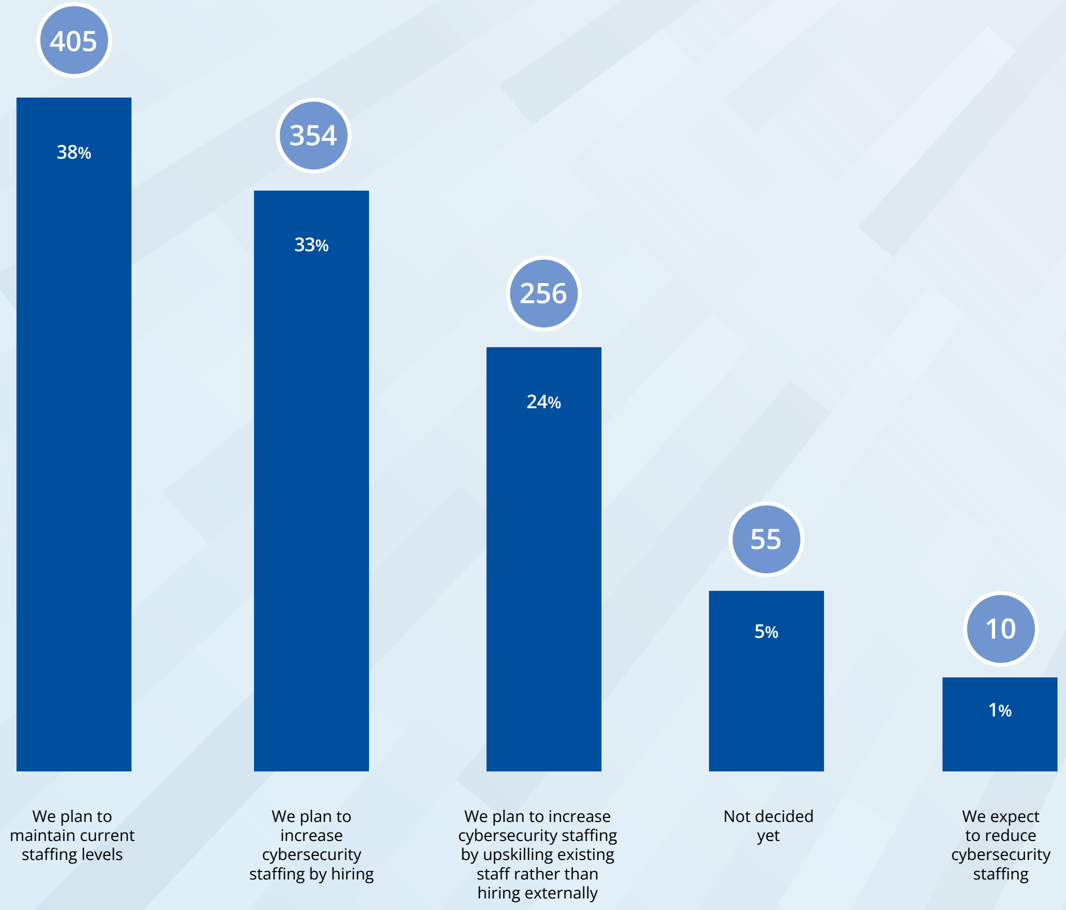
FIG. 5 - MOST IN-DEMAND CYBERSECURITY SKILLS CURRENTLY (ALL ORGANISATIONS – LEFT, ORGANISATIONS ALSO REPORTING DIFFICULTY FINDING CANDIDATES WITH THE RIGHT SKILLS – RIGHT)



[7] European Commission *Digital Skills & Jobs Platform* 'EU faces growing cybersecurity skills gap, new Eurobarometer reveals' 22 May 2024.
[8] ibid.
[9] European Union Agency for Cybersecurity (ENISA) *2024 Report on the State of Cybersecurity in the Union – Condensed Version* November 2024.
[10] According to the 2025 *Gartner CIO Talent Planning Survey,* 46% of SME IT leaders say cybersecurity skills gaps will significantly affect their ability to meet 2025 objectives.

Looking ahead, **staffing intentions point to stability rather than rapid expansion.** Most organisations expect to maintain their current cybersecurity headcount (38%), while about one quarter aim to enhance capacity through upskilling existing staff (24%), only one third plan to hire additional personnel (33%). Only a small share remains undecided (5%) or anticipate reductions (1%) (Fig. 6). This distribution suggests a market consolidating around measured growth, with a strong emphasis on the development of internal capabilities. The focus on upskilling aligns with ongoing EU efforts to expand the training ecosystem, support micro-credential recognition, and promote skills-first[11] career pathways[12] — ensuring that investments in workforce development directly translate into compliance readiness and operational resilience.

FIG. 6 - CYBERSECURITY STAFFING STRATEGY (NEXT 12 MONTHS)



[11] Skills-first refers to an approach where demonstrable skills and competencies are prioritised over formal qualifications, such as degrees.
[12] European Commission *A European approach to micro-credentials for lifelong learning and employability* December 2024.
[13] European Parliament and Council Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2) 14 December 2022.
[14] European Parliament and Council Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elemnts (Cyber Resilience Act) 23 October 2024.
[15] European Parliament and Council Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) 14 December 2022.

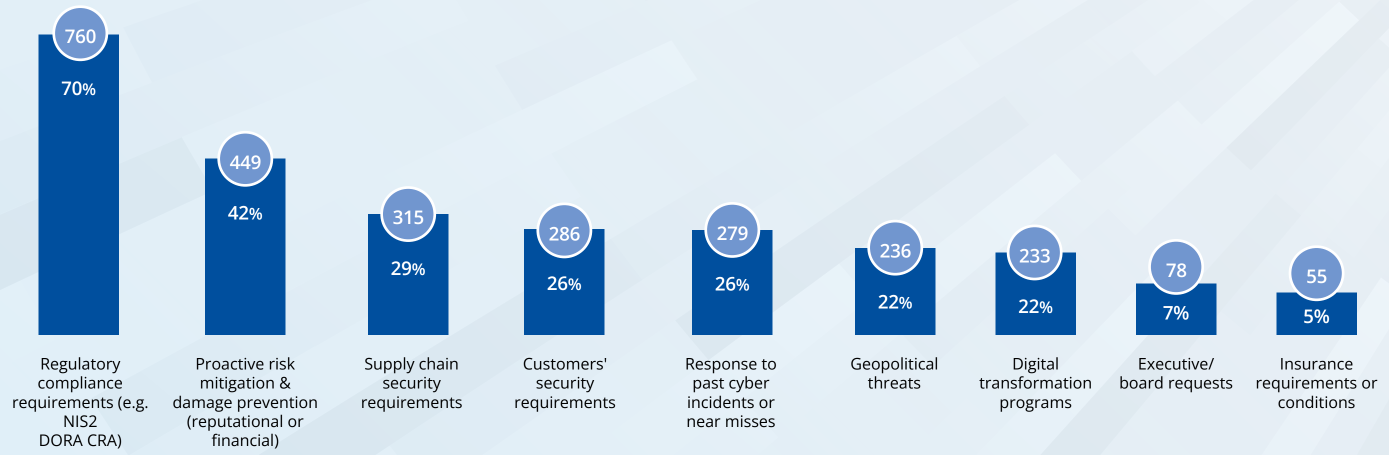
INSIGHT #3

COMPLIANCE IS THE MAIN INVESTMENT DRIVER BUT NOT THE ONLY OUTCOME

Regulatory compliance was the main driver of cybersecurity investment over the past year, with compliance-driven spending delivering benefits beyond improved compliance, including stronger risk management, faster incident detection and enhanced response and recovery capabilities. Looking ahead, organisations are shifting priorities towards upgrading tools, improving recovery, raising awareness and strengthening internal skills, suggesting that policy is helping move cybersecurity in the right direction.

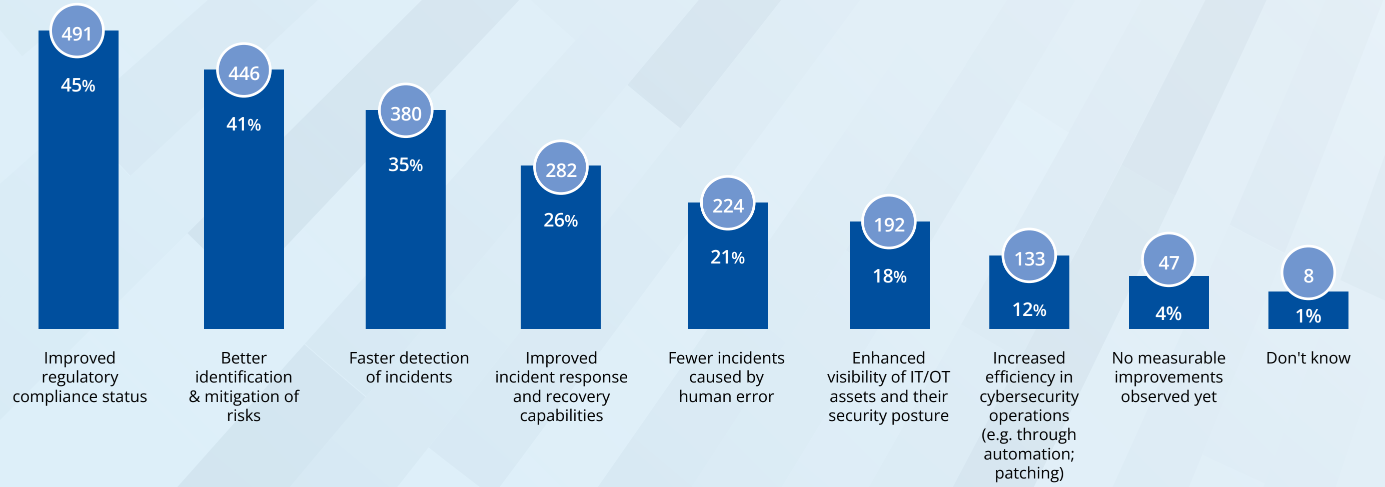
70% of surveyed organisations identified regulatory compliance with the requirements stemming from frameworks such as the NIS2 Directive[13] , the CRA[14] , or DORA[15] , as the main driver of their cybersecurity investment over the past year (Fig. 7). This underscores that **alignment with legal and regulatory requirements was the key factor influencing spending decisions** across both public and private sectors.

FIG. 7 - KEY CYBERSECURITY INVESTMENT DRIVERS FOR 2024



Nearly half of the organisations surveyed (45%) identified improved regulatory compliance as a key outcome of their cybersecurity investment in the past year (Fig. 8). A further 41% cited stronger risk-management processes, 35% reported faster or more accurate incident detection and 26% noted improved response capabilities. These outcomes suggest that, **despite spending being predominantly compliance-driven, the results attained** by many **go beyond audit readiness — strengthening risk identification and management, enabling faster incident detection and improving response and recovery capabilities.** This pattern mirrors broader European evidence that regulation-driven investment — particularly under NIS2 and related frameworks — has helped to raise baseline security standards and integrate cybersecurity more firmly into risk and governance structures[16].

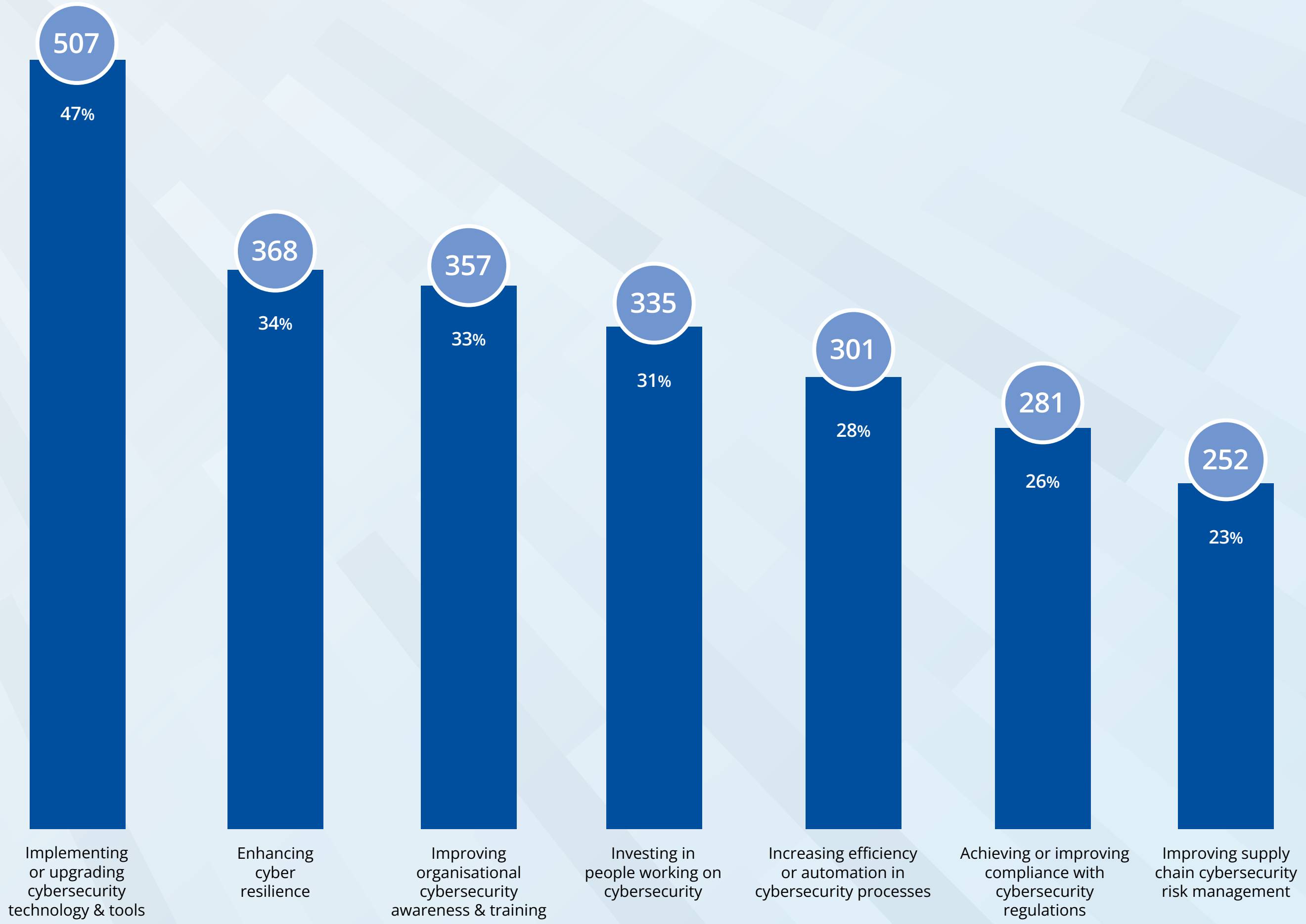
FIG. 8 - OUTCOMES ATTAINED VIA CYBERSECURITY INVESTMENT IN 2024



[13] European Parliament and Council Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2) 14 December 2022.
[14] European Parliament and Council Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elemnts (Cyber Resilience Act) 23 October 2024.
[15] European Parliament and Council Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) 14 December 2022.
[16] European Union Agency for Cybersecurity (ENISA) *2024 Report on the State of Cybersecurity in the Union* 3 December 2024.

Looking ahead, **targeted outcomes of cybersecurity investment suggest a shift.** While compliance was the key driver in 2024, many organisations now plan to direct future resources **towards strengthening their overall cybersecurity posture.** The most common priorities include upgrading cybersecurity tools (47%), improving resilience (34%), expanding training and awareness programmes (33%), and investing in cybersecurity staff (31%) (Fig.9). Overall, this suggests that policy is steering investment in the right direction, although these remain intentions for now and the actual impact will only be clear over time.

FIG. 9 - EXPECTED OUTCOMES OF CYBERSECURITY INVESTMENT LOOKING FORWARD



This transition also reflects a wider shift in how cybersecurity is being regarded across Europe. One example comes from the banking sector where compliance now sits at a similar level to other drivers rather than clearly leading — suggesting regulation (DORA, NIS2) has set the baseline and is being absorbed into day-to-day practice — an early sign of maturity where compliance evolves into capability. Rather than viewing compliance as an end goal, organisations are increasingly treating it as a foundation for building lasting capability. Investments are gradually becoming more strategic by focusing on strengthening processes, integrating security into daily operations and by improving the ability to detect and respond to incidents. At the same time, there is growing recognition that sustained resilience depends on people as much as technology. Expanding training opportunities, supporting professional development and aligning roles with frameworks of recognised skills are emerging as key elements in maintaining maturity in security over time[17].

INSIGHT #4

NIS2 IS RAISING THE BAR YET IMPLEMENTATION REMAINS A CHALLENGE

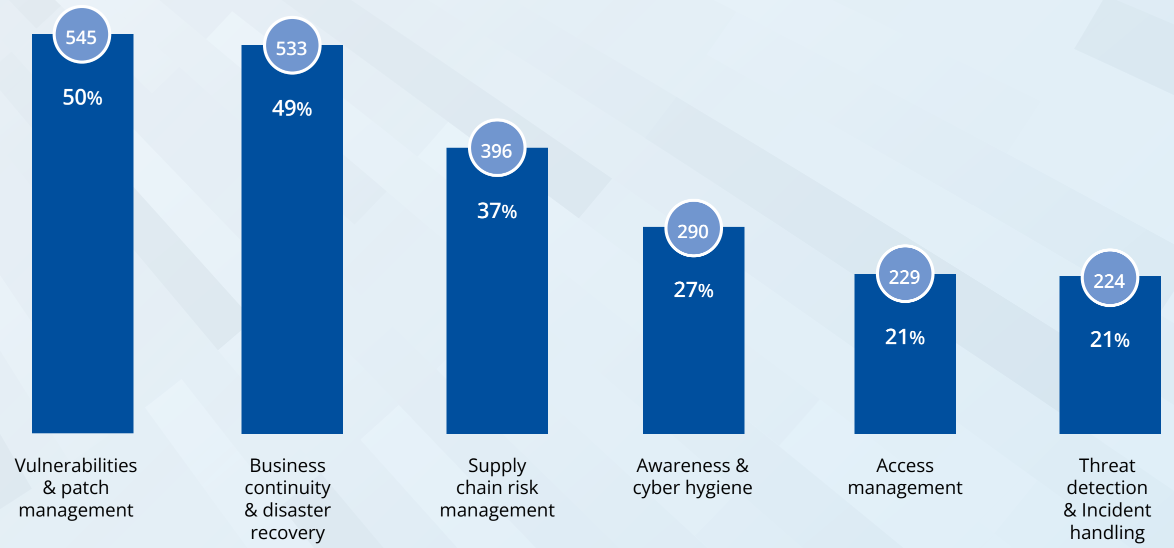
Regulation is moving the needle, yet aligning with NIS2 remains demanding. The toughest areas — vulnerability and patch management, business continuity and supply-chain risk — highlight where organisations face the greatest pressure, while barriers such as legacy systems, Operational Technology (OT) constraints, cross-jurisdictional complexity and skills shortages continue to challenge implementation. Importantly, this suggests that NIS2 is raising the bar by prompting entities to focus on strengthening some of the most demanding yet essential areas of cyber resilience.

While NIS2 is driving improvements, aligning with its requirements continues to be challenging for organisations. The **areas where organisations report the greatest difficulty** are (Fig. 10):

- Vulnerability and patch management — 50%
- Business continuity and disaster recovery — 49%
- Supply-chain risk management — 37%

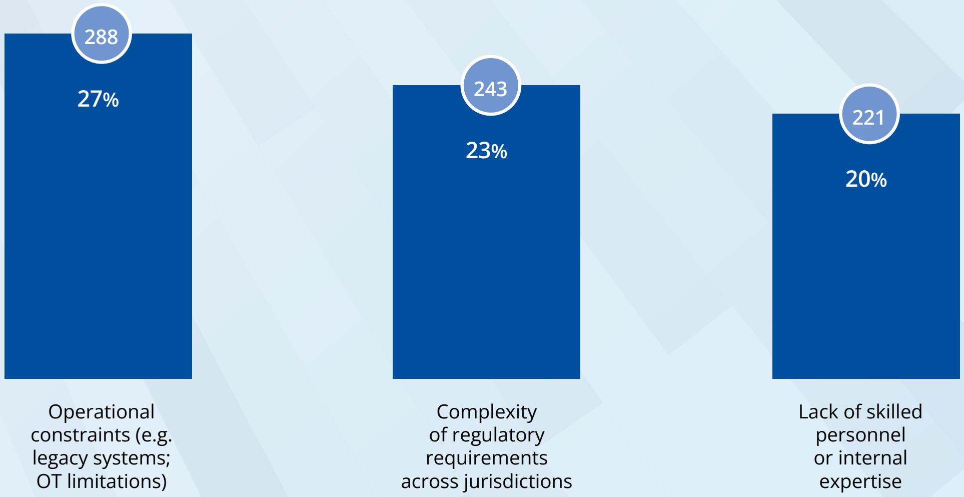
Awareness-raising, access control and incident handling are also cited as challenging by roughly one in five entities.

FIG. 10 - MOST CHALLENGING NIS2 REQUIREMENTS TO IMPLEMENT



When asked to name their **main obstacle to implementing NIS2 cybersecurity requirements,** most organisations pointed to infrastructure constraints — typically the persistence of legacy systems or limitations posed by operational technologies (27%). The next most cited challenge was the complexity of regulatory requirements across jurisdictions (23%) — particularly relevant for organisations operating across borders. Shortages of skilled personnel and internal expertise followed closely (20%), reflecting the broader gap in the workforce already evident across the cybersecurity sector (Fig. 11).

FIG. 11 - TOP THREE MOST REPORTED BARRIERS TO EFFECTIVE NIS2 CONTROLS IMPLEMENTATION

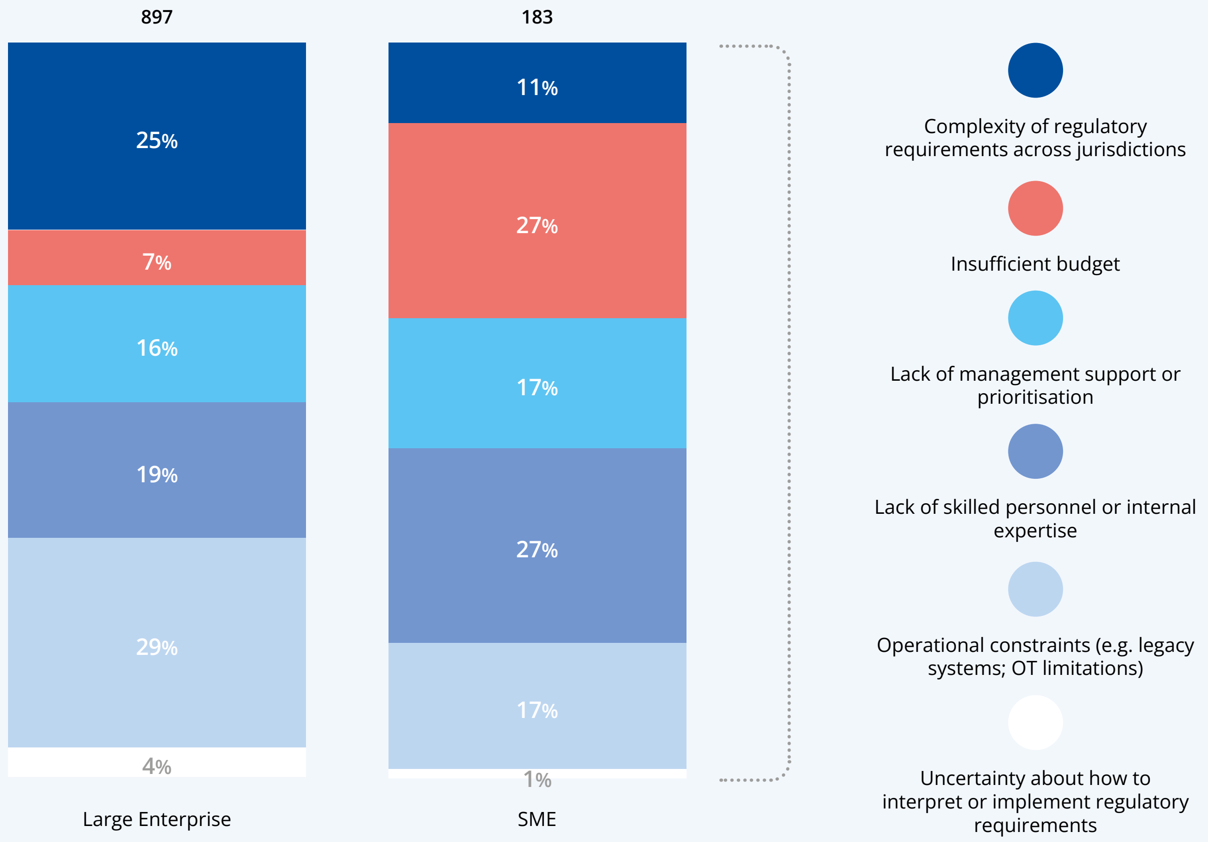


While all response options were drawn from NIS2 requirements, the fact that organisations consistently highlight the above-mentioned areas suggests that NIS2 is successfully bringing focus to some of the most demanding yet essential areas of cyber resilience — a clear sign of progress. At the same time, the obstacles identified, including OT environments, legacy systems, cross-jurisdictional complexity and skills shortages, represent persistent challenges that policymakers should take into account when assessing the effectiveness of regulatory measures and supporting efforts at implementation.

SMEs

When examining their alignment with NIS2, the barriers faced by organisations vary depending on their size, with SMEs and large companies experiencing different operational and resource challenges. Differences by the size of organisations suggest tailored responses. Large enterprises are most constrained by operational realities and regulatory complexity, whereas SMEs cite budget limitations and shortages of skilled personnel as equally critical obstacles. This points to distinct support needs: for larger entities, harmonised approaches and paths for the transition from legacy to modern technology; for SMEs, accessible guidance, affordable tooling (including managed and cloud services governed under the above frameworks) and skills development.

FIG. 12 - TOP REPORTED BARRIERS TO EFFECTIVE IMPLEMENTATION OF NIS2 CONTROLS (SME VS. LARGE)



INSIGHT #5

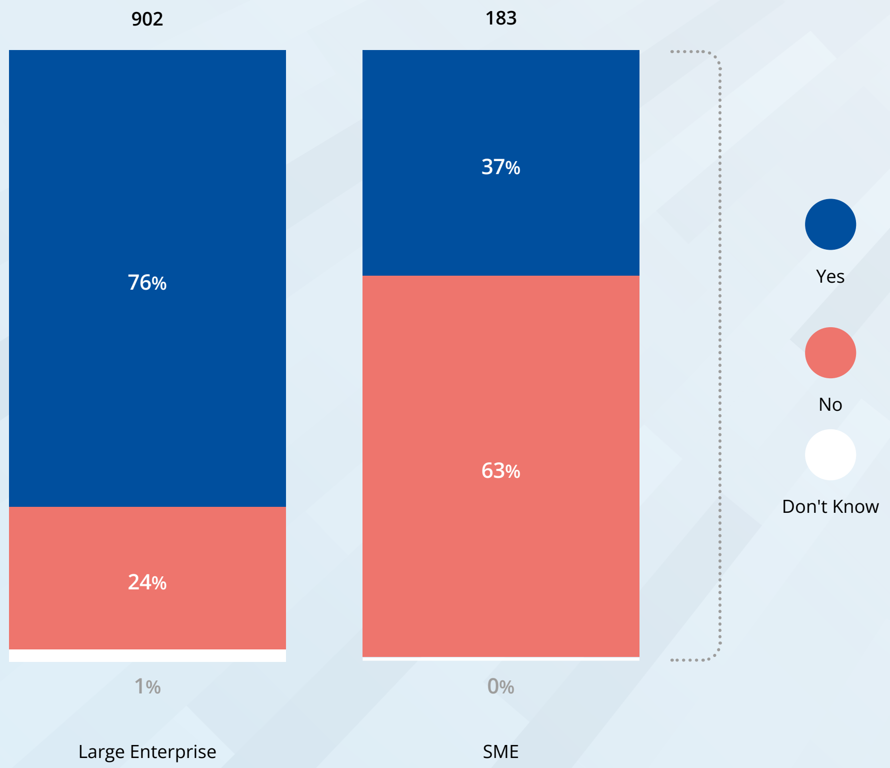
PATCHING STILL TAKES MONTHS; MANY STILL DON’T TEST THEIR SECURITY

Even as organisations work to align with regulatory requirements, many continue to struggle with basic cybersecurity practices — from conducting regular assessments to timely patching. With vulnerabilities weaponised within days and linked to most intrusions, these gaps continue to expose organisations to preventable risks — a reminder that strong cybersecurity starts with getting the fundamentals right.

Even as organisations work to align with regulatory requirements, many continue to struggle with basic cybersecurity practices. Almost one in three of the organisations (and more than one in two of the SMEs) surveyed reported **not having conducted any form of cybersecurity assessment in the previous 12 months,** potentially leaving blind spots in their understanding of exposures and gaps.

This is particularly concerning for SMEs, where 63% of the entities surveyed stated that they had not performed any form of cybersecurity assessment in the previous year.

FIG. 13 - SHARE OF ORGANISATIONS CONDUCTING CYBERSECURITY ASSESSMENTS OR TESTING IN THE PAST 12 MONTHS (SME VS. LARGE ENTERPRISE)



Patching remains a persistent issue for organisations. Timely application of security patches is a critical control to prevent exploitation of known vulnerabilities. If vulnerabilities are left unpatched for extended periods, attackers have a large window of opportunity to unauthorised access, potentially leading to data breaches, operational disruption or financial and reputational damage.

Looking at trends over time highlights the scale of the challenge: in the 2022 NIS Investments study[18], 48% of entities reported that patching took between one and six months, with a further 8% indicating it took more than six months. Today, nearly two thirds (63%) of organisations report taking a month or longer to apply critical patches to critical systems, and over a quarter (28%) indicate that it takes them more than three months to apply critical patches (Fig. 14).

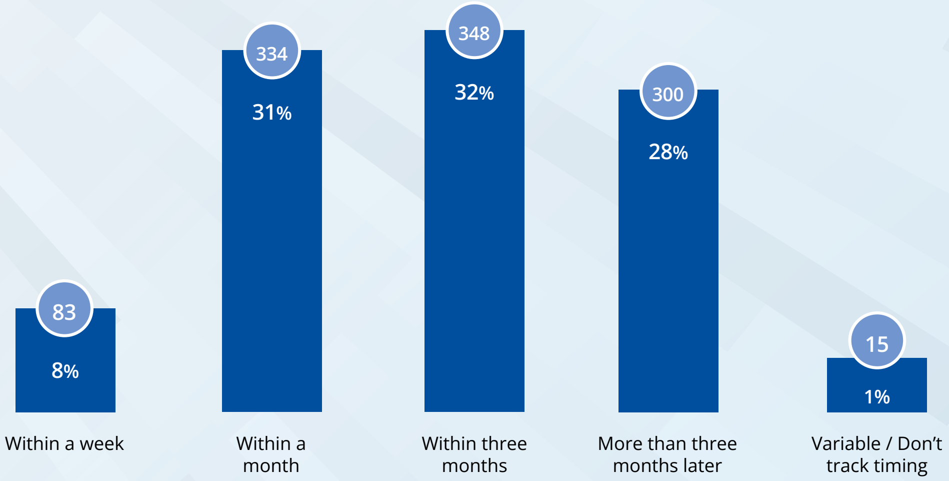
Such delays leave organisations exposed for significant periods, which increases the likelihood of successful attacks and undermines overall cyber resilience.

While high-profile zero-day exploits draw attention, the majority of vulnerabilities actively exploited in the wild remain n-day vulnerabilities — those for which a patch is available. Data from external sources[19] indicate that although around one in three known exploited vulnerabilities are weaponised at or immediately after disclosure, the remaining two-thirds are n-day vulnerabilities. This means that the **exploitation of most vulnerabilities is preventable through timely patching.** Delays in applying patches therefore leave organisations exposed to avoidable risks.

These delays are perhaps unsurprising given that one in two of the entities surveyed identified vulnerabilities and patch management among the 'most challenging' NIS2 requirements to implement. Several factors may be contributing to these delays. For some (27% of entities surveyed), infrastructure characteristics play a role — particularly the persistence of legacy systems and OT environments that cannot easily be updated or taken offline without disrupting essential operations. Other reasons may include limited staff capacity, competing operational priorities or challenges in coordination between IT and business functions. In complex environments, patching can also involve significant testing and approval processes, which further extend patching timelines.

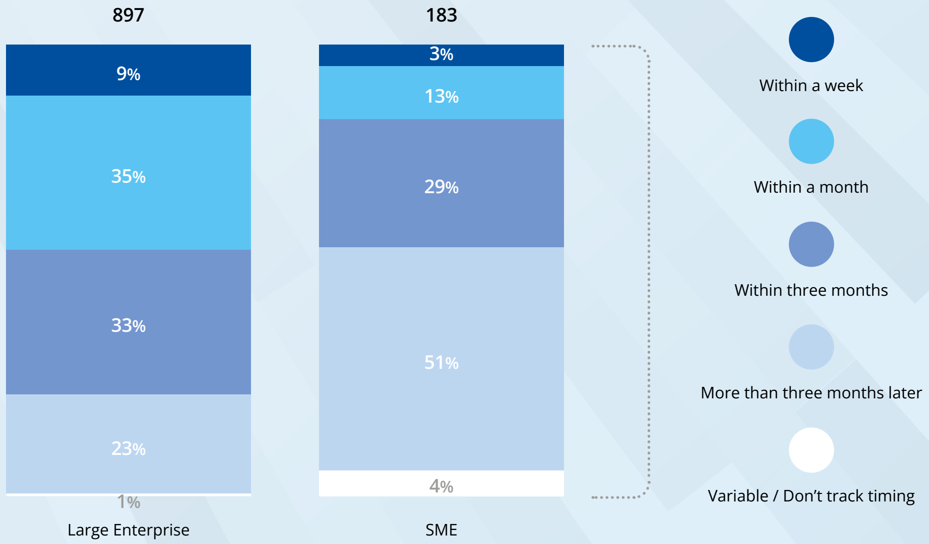
Placed in the context of the *ENISA Threat Landscape (ETL) 2025*[20], these findings are concerning: vulnerabilities remain the second most common initial infection vector, are often weaponised within days of disclosure and account for nearly 20% of intrusions.

FIG. 14 - AVERAGE TIME TO PATCH CRITICAL VULNERABILITIES ON CRITICAL ASSETS (IT OR OT)



The issue appears even more pronounced among SMEs, where more than one in two (51%) suggest it takes them more than three months to apply critical patches on critical systems.

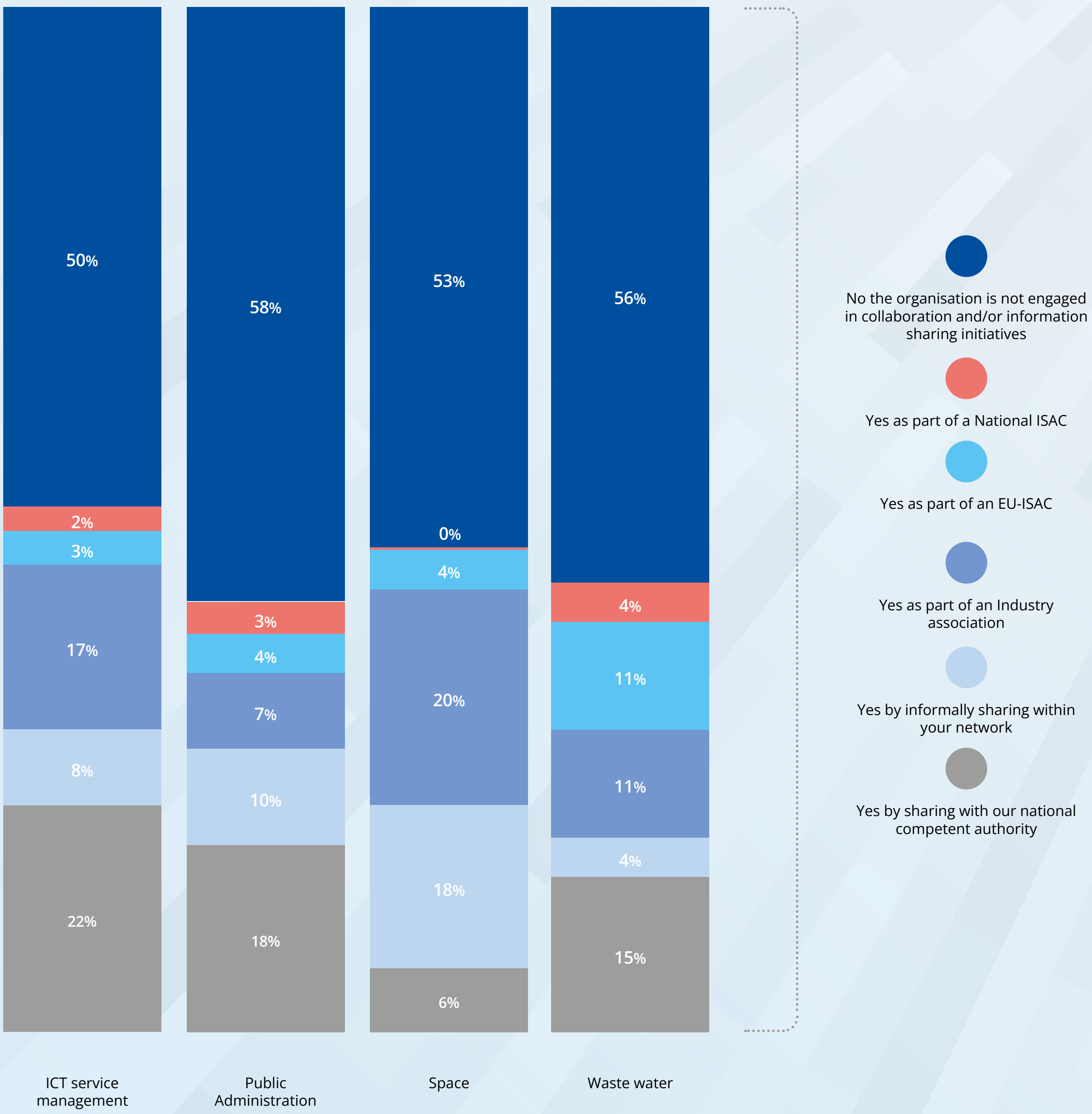
FIG. 15 - AVERAGE TIME TO PATCH CRITICAL VULNERABILITIES ON CRITICAL ASSETS (IT OR OT)



[20] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2025.* October 2025

Beyond internal risk mitigation measures, effective cybersecurity risk management also relies on timely **information sharing and collaboration** across sectors. These mechanisms are essential for early detection, collective learning and coordinated responses to emerging threats. While a majority of entities (81%) report engaging in some form of information exchange, participation is uneven across sectors. In fact, entities in sectors previously outside the scope of the NIS Directive remain notably less involved — with at least one in two reporting that they do not participate in any collaboration or information-sharing initiatives (Fig. 16).

FIG. 16 - PARTICIPATION IN INFORMATION SHARING INITIATIVES, NEW SECTORS



INSIGHT #6

SUPPLY CHAIN RISK: STRONGER CONTROLS, DEEPER DEPENDENCE

Organisations are becoming more systematic in managing supply chain and third-party risk — yet their expanding reliance on outsourced ICT and security services is simultaneously creating new layers of dependence and potential exposure. The risk is particularly pronounced when suppliers are SMEs, whose limited resources and capabilities can amplify exposure throughout the chain.

Organisations continue to strengthen their third-party and supply chain security with the majority (90%) reporting they implement specific controls in that respect. The most common measures are requiring suppliers to comply with security standards and maintain certifications (63%), conducting supplier risk assessments or audits (54%) and including cybersecurity requirements in supplier contracts (48%).

These measures demonstrate both awareness and action. Organisations are taking concrete steps to manage third-party and supplier risk. The same top three measures were already highlighted in our 2024 edition[21]. Requiring suppliers to maintain certifications and implement standards has been the most frequently cited measure to managing third-party and supply chain risks since 2022[22].

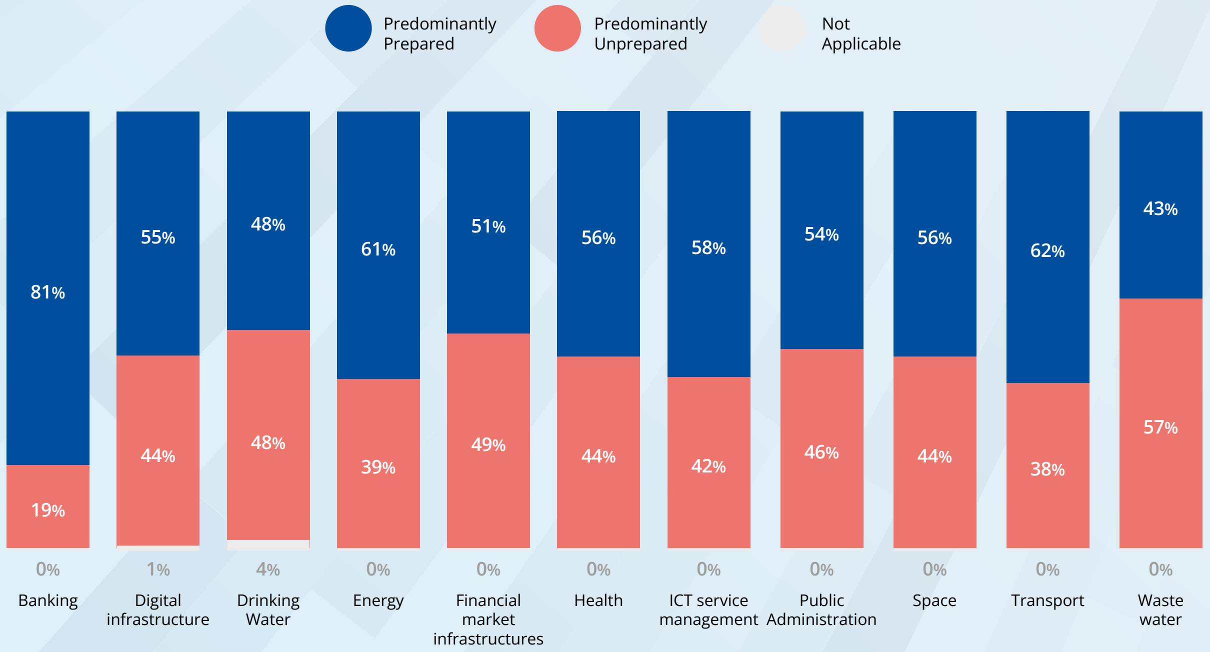
Despite these efforts, **supply chain and third-party attacks have emerged as the second most frequently cited top concern for the future (47%).** This combination of growing action and growing concern tells an important story: organisations recognise that their exposure is expanding faster than their ability to control it. This likely reflects increased outsourcing of both ICT functions[23] and cybersecurity services and thus increased dependence[24].

This dependence brings new challenges:

- **Limited visibility:** Organisations often lack a clear view of the security maturity of their suppliers and sub-suppliers.
- **Difficult enforcement:** Ensuring that suppliers and third-party providers meet security expectations is increasingly complex, particularly in the absence of harmonised baseline requirements.
- **Concentration risk:** Reliance on a small number of dominant service providers can create systemic points of failure.
- **Shared responsibility in the cloud:** While major cloud providers usually maintain strong security postures, individual organisations retain limited control over configurations and must navigate overlapping responsibilities within complex SaaS environments.

The consequences of these dynamics are visible in our data. Although concern about third-party and supply chain attacks is high across all sectors, only the banking sector reported feeling adequately prepared to deal with such incidents. This is consistent with the stronger regulatory emphasis placed on third-party risk management in banking, notably through DORA and ECB supervisory initiatives[25]. Across other sectors, **over one-third of organisations said they do not feel ready to respond to supply-chain-related incidents or third-party compromises** (Fig. 17).

FIG. 17 - PREPAREDNESS TO DEAL WITH SUPPLY CHAIN OR THIRD-PARTY COMPROMISES



[21] European Union Agency for Cybersecurity (ENISA) *NIS Investments 2024: Cybersecurity Policy Assessment* November 2024.
[22] European Union Agency for Cybersecurity (ENISA) *NIS Investments* November 2022.
[23] Eurostat ICT specialists – statistics on hard-to-fill vacancies in enterprises (Statistics Explained) Accessed November 2025.
[24] World Economic Forum Global Cybersecurity Outlook 2025 13 January 2025.
[25] European Central Bank (ECB) Banking Supervision *Outsourcing trends in the banking sector* Supervision Newsletter 19 February 2025.

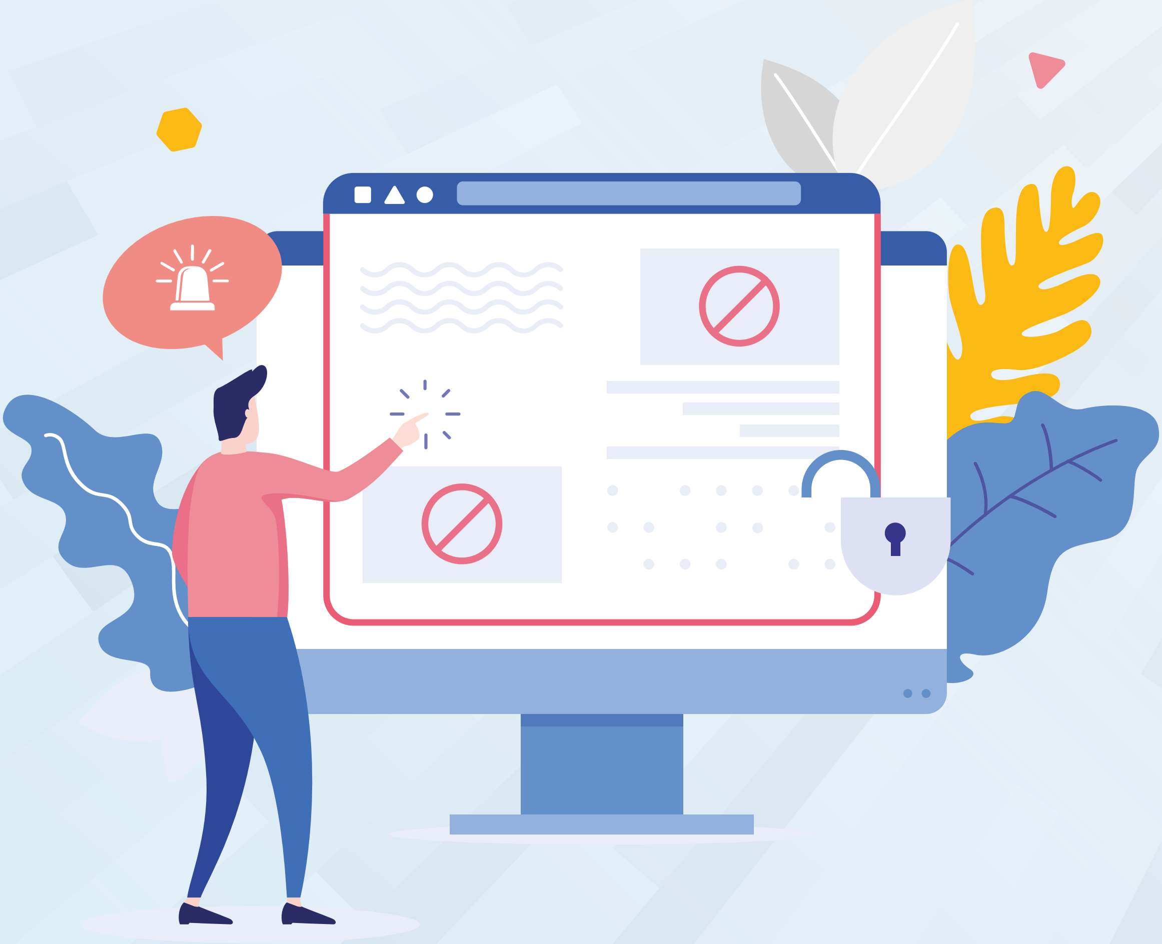
The challenge becomes particularly evident when looking at the ICT service management sector, which includes managed service providers (MSPs) and managed security service providers (MSSPs). These entities often act as third-party service providers for multiple clients across sectors. According to our survey, 43% of these entities reported that they had not undergone any form of cybersecurity testing in the past year, and 45% indicated that it takes them more than three months to apply critical patches to critical systems. Weaknesses in their patching and testing practices suggest that even well-prepared organisations may still be exposed to risk through their third-party service providers.

The implications are serious, not least because supply chain and third-party attacks are inherently difficult to detect and mitigate — taking an average of 267 days to detect and contain[26] — the longest among all threat types and are the second most costly initial attack vector. They exploit trusted relationships, bypass traditional defences and can spread through legitimate channels such as software updates or vendor integrations. Reflecting these challenges, our study found that over a third of entities surveyed (37%) identified supply-chain risk management as the most difficult NIS2 requirement to implement.

SMEs

The risk is even greater when SMEs are involved. When the supplier is an SME, resource and staffing constraints can significantly increase the likelihood of exploitable weaknesses. Conversely, when the organisation itself is an SME relying on an insecure supplier, the financial and operational impact of a cyber incident could be disproportionately severe, potentially threatening business continuity altogether.

INSIGHT #7

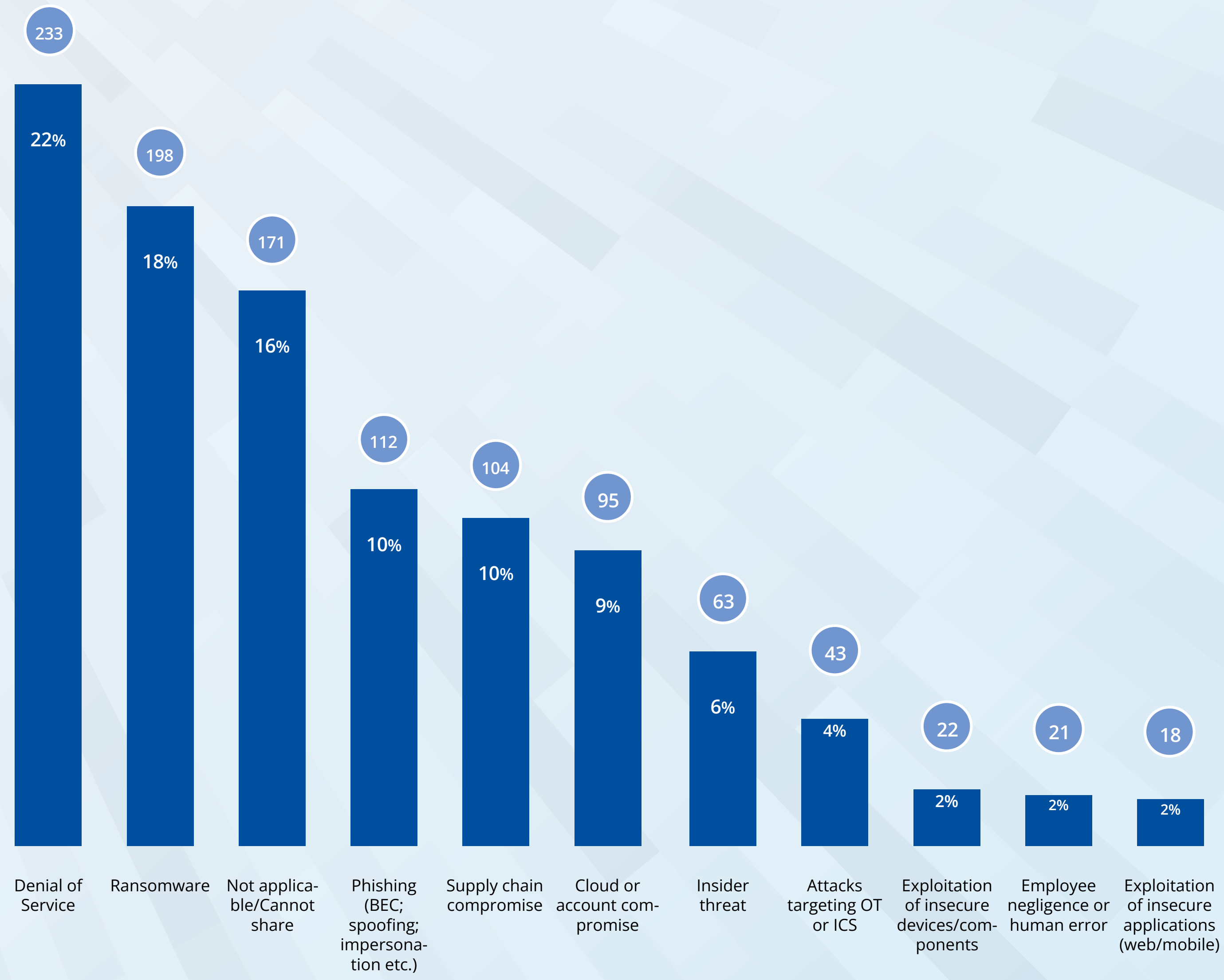


DOS CAUSED THE NOISE, RANSOMWARE CAUSES THE NIGHTMARES

While DoS attacks put the most strain on daily operations last year, future concerns centre on ransomware, supply-chain and third-party compromises and phishing. Confidence in preparedness to anticipate, withstand and recover from cyber-attacks of different types varies; entities feel most ready for ransomware, less so for supply-chain threats, and SMEs trail behind across all scenarios.

Over the past year, entities experienced a range of cyberattacks affecting their day-to-day operations (Fig. 18), with DoS (22%), ransomware (18%), phishing (10%), and supply chain and third-party compromises (10%) emerging as the most commonly reported.

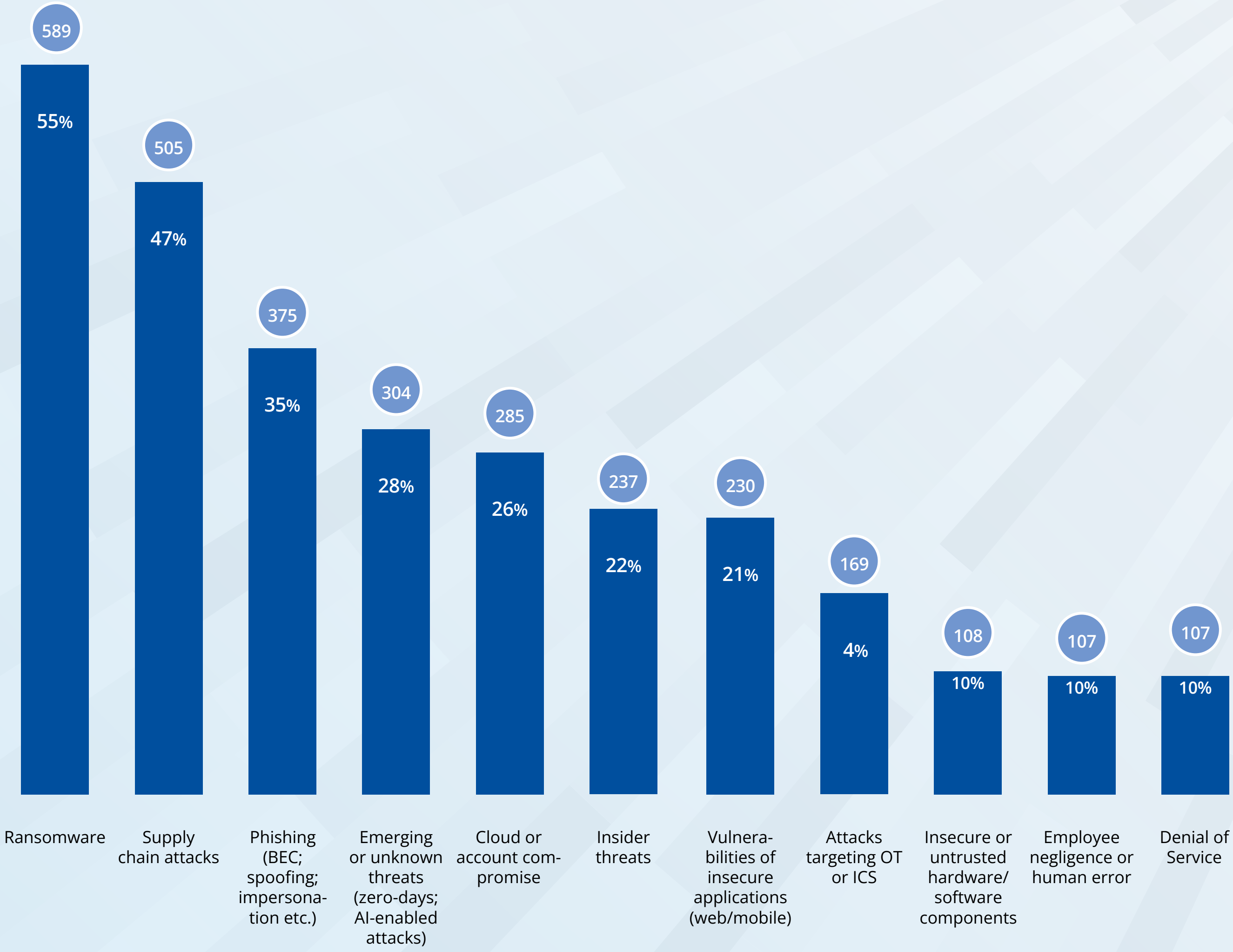
FIG. 18 - CYBERATTACKS THAT AFFECTED DAY-TO-DAY OPERATIONS THE MOST (PAST 12 MONTHS)



The prominence of DoS attacks among the above, aligns with ETL[27] data showing that DDoS accounted for 80% of recorded incidents between July 2024 and June 2025. This high frequency and persistence helps to explain why organisations reported effects on day-to-day operations. Repeated attempts likely required mitigation efforts that caused temporary service slowdowns and diverted resources. As a result, organisations experienced a tangible operational strain from managing recurring attacks, rather than from the technical or strategic severity of any single incident.

[27] European Union Agency for Cybersecurity (ENISA) *ENISA Threat Landscape* 2025 October 2025

FIG. 19 - CYBERSECURITY THREATS ORGANISATIONS ARE MOST CONCERNED ABOUT (NEXT 12 MONTHS)



Looking ahead, the threats that organisations are **most concerned about** do not always mirror past experience (Fig. 19). Most organisations (55%) reported **ransomware** as the attack that most concerns them in the coming year even though many (83%) feel relatively well-prepared to anticipate, withstand and recover from such attacks. This concern is supported by data in the ETL report, which shows that ransomware continues to dominate cybercriminal activity, with decentralised operations, aggressive extortion tactics and the proliferation of cybercrime-as-a-service models creating a resilient, professionalised ecosystem and lowering barriers to entry.

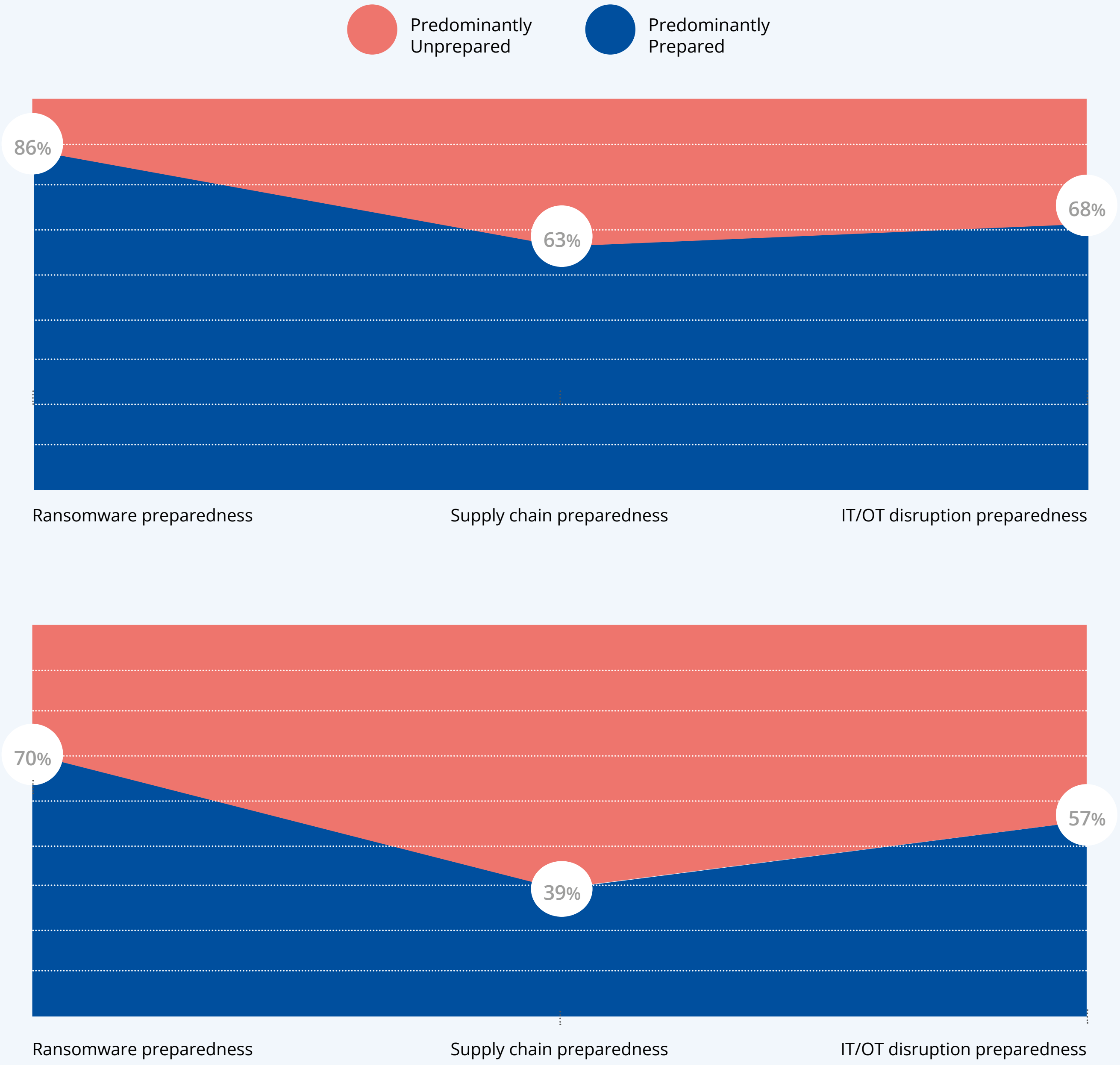
Supply chain attacks are the second most frequently cited top concern, with almost one in two (47%) entities surveyed identifying them as their primary concern looking ahead. Confidence in preparedness, however, is lower (only 59% of entities). The concern of organisations is justified. According to the latest ETL report state-aligned threat groups are intensifying long-term cyber-espionage campaigns, often leveraging supply-chain compromises and stealthy malware frameworks to target multiple organisations simultaneously. Unlike ransomware, these attacks exploit the interconnected nature of systems and third-party dependencies, meaning even well-prepared organisations remain vulnerable if their suppliers or service providers are insecure.

Last but not least, **phishing** was the third most frequently cited top concern, with 35% of the entities surveyed entities identifying it as their primary concern looking ahead. Based on the ETL, phishing remains the most common intrusion vector (60%), increasingly industrialised through phishing-as-a-service platforms and AI-supported campaigns. Despite awareness and training programmes, phishing continues to challenge the operational resilience of organisations.

SMEs

Perceptions of preparedness differ notably between SMEs and large enterprises. Across all the types of attacks examined, SMEs consistently report lower confidence in their ability to respond effectively compared with larger organisations (Fig. 20). This disparity likely reflects constraints highlighted in earlier insights — including limited budgets, staffing shortages and resource limitations — which can reduce SMEs' capacity to implement robust cybersecurity measures and respond swiftly to incidents.

FIG. 20 - PERCEIVED PREPAREDNESS AGAINST SPECIFIED SCENARIOS - LARGE (TOP) VS. SME (BOTTOM)



SECTION II

ABOUT THIS REPORT

2. ABOUT THIS REPORT

This report presents the findings of the sixth edition of the annual NIS Investments study conducted by ENISA. The study focuses on:

How EU cybersecurity policies influence organisations' investment decisions, resources, and operations.

It also considers other factors, such as the threat landscape or market pressures, that may influence behaviours shaping cybersecurity practices.

The aim is to provide insights that help policymakers and practitioners at both national and EU levels understand how cybersecurity policy plays out in practice, highlight areas where challenges exist, and take into account factors beyond policy that may also influence organisational behaviour.

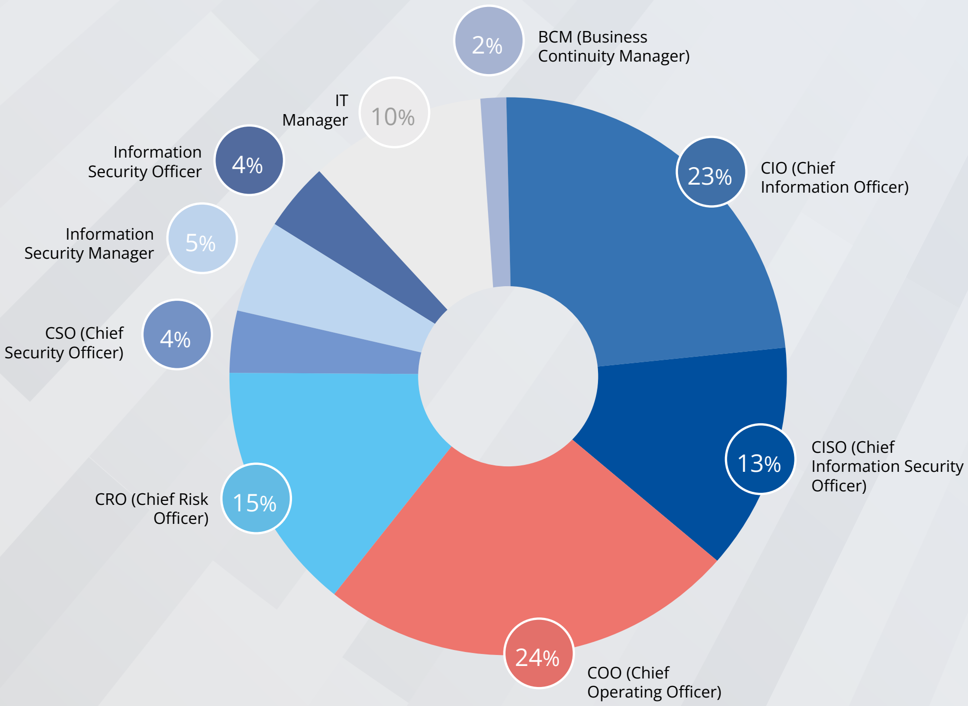
2.1. Respondent profiles and data collection

This edition was informed by a survey of **1 080 professionals** representing organisations[28] across **all 27 EU Member States** and **all sectors and subsectors of high criticality covered by the NIS2 Directive.** Respondents were predominantly senior personnel, well-acquainted with their organisation's cybersecurity budgets, resourcing, overall posture, key challenges and threat experience.

Respondents to this survey were mostly COOs, CIOs, CROs, CISOs and CSOs

Data was collected through dedicated phone interviews using structured questionnaires specifically developed for this study. To enable the tracking of trends over time, certain core indicators have remained fixed across editions, while other questions are updated each year to reflect evolving priorities, emerging threats and new areas of interest. The questionnaires included both quantitative questions — requesting ballpark figures or high-level estimates — and closed qualitative questions to capture insights on practices and challenges. The survey was conducted from May to August 2025.

FIG. 21 - BREAKDOWN OF RESPONDENT PROFILES



2.2. Sectors in focus

This study focused on organisations from all high-criticality sectors and subsectors identified under the **NIS2 Directive - Annex I.** The share of entities surveyed per sector is presented below:

1080
Organisations surveyed

27
EU member states represented

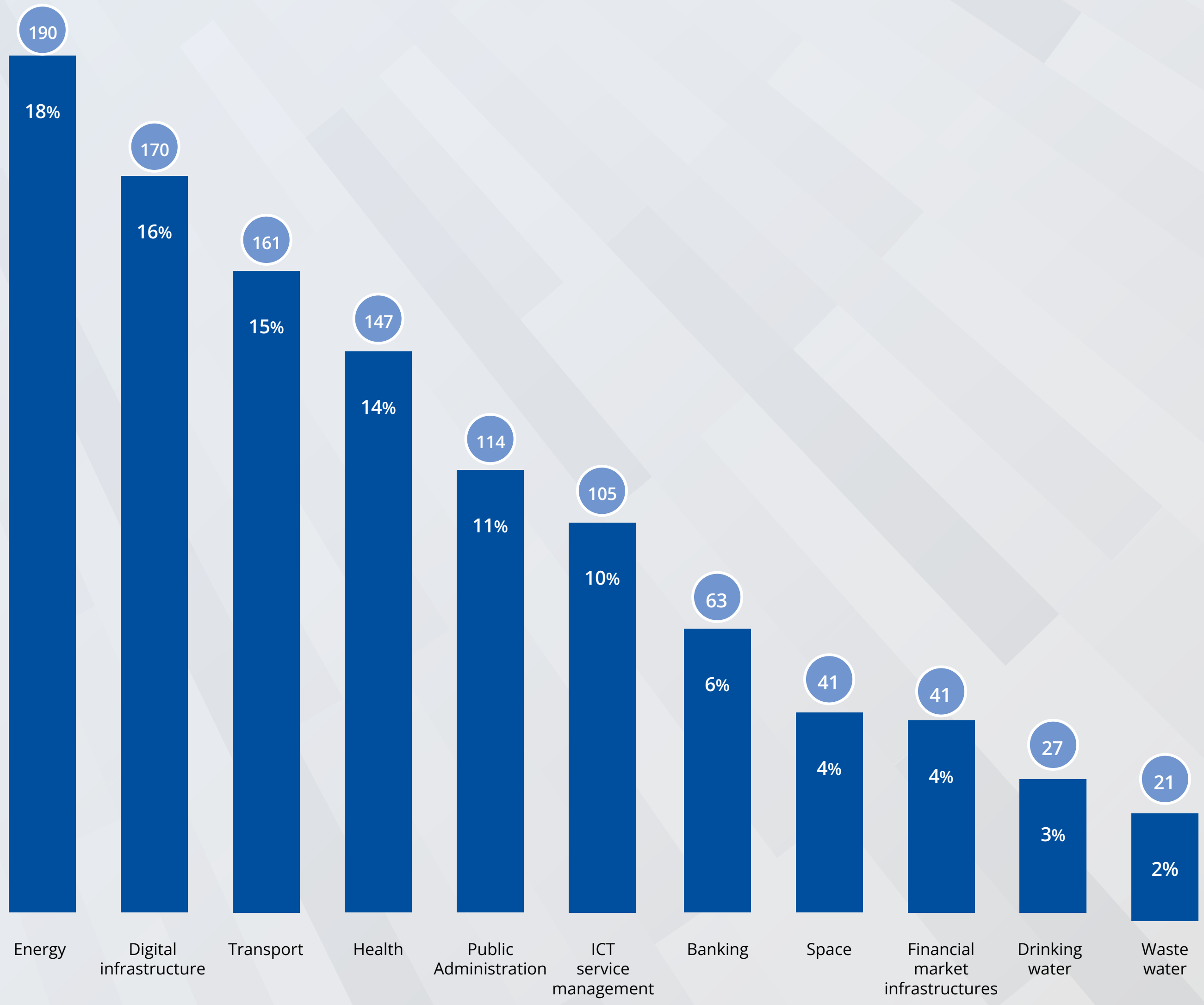
NIS2
Network & Information Systems Directive

22
(Sub) sectors of high criticality in scope

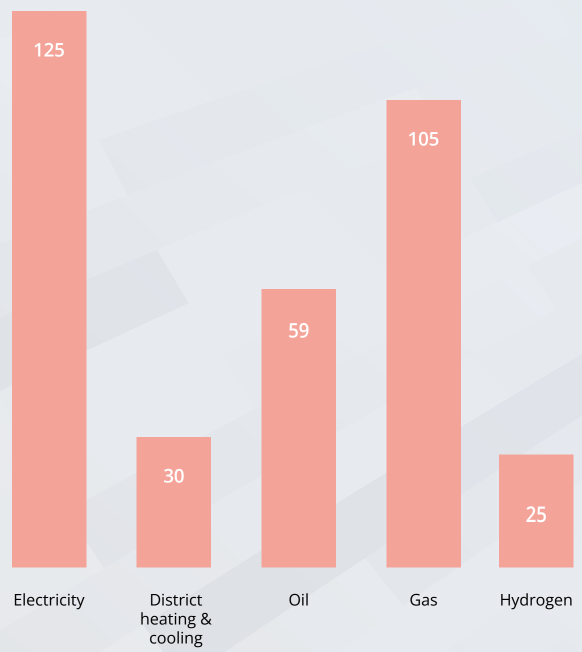
83%
Large enterprises

17%
SMEs

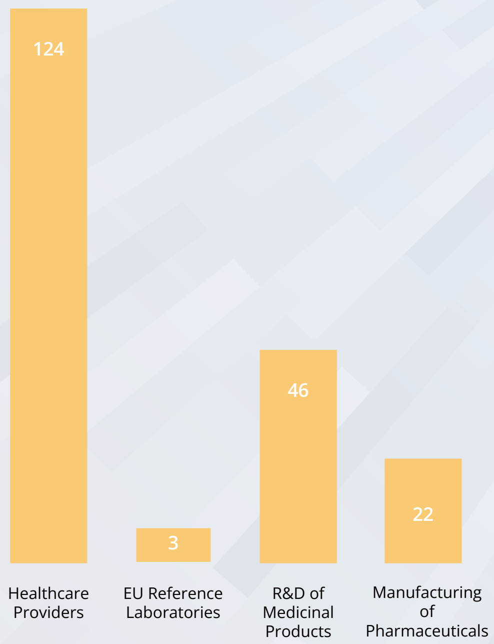
FIG. 22 - SECTORS REPRESENTED IN THIS YEAR'S ENISA NIS INVESTMENTS SURVEY



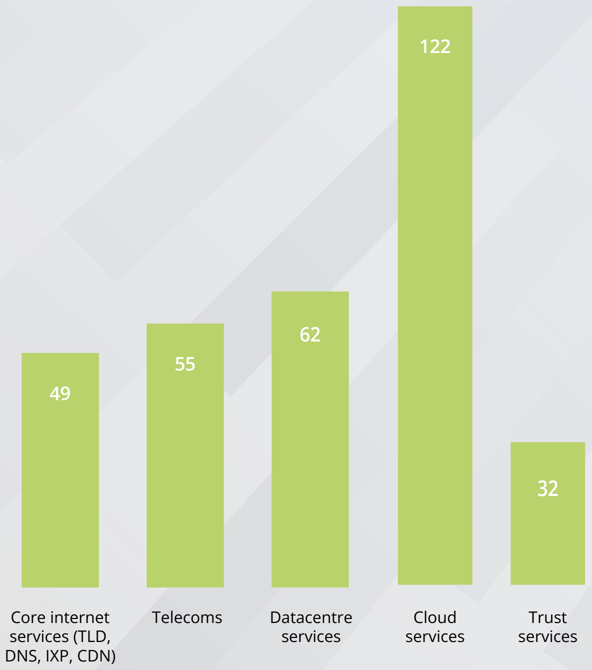
ENERGY SUBSECTOR BREAKDOWN
*(190 companies surveyed;
many operate across subsectors)*



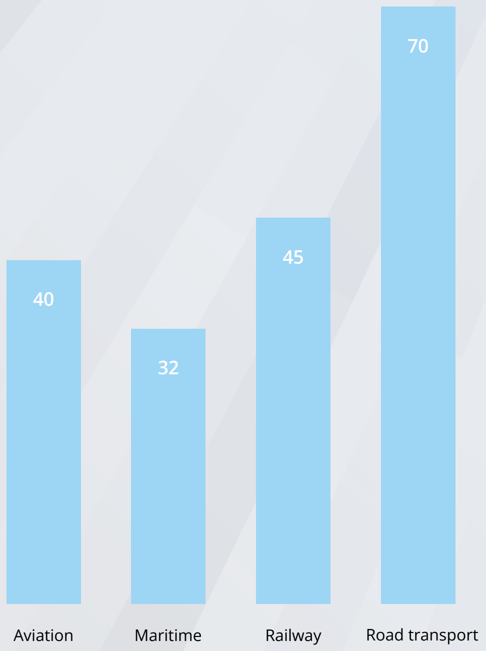
HEALTH SUBSECTOR BREAKDOWN
*(147 companies surveyed;
many operate across subsectors)*



DIGITAL INFRASTRUCTURE SERVICES BREAKDOWN
*(170 companies surveyed;
many operate across subsectors)*



TRANSPORT SUBSECTOR BREAKDOWN
*(161 companies surveyed;
many operate across subsectors)*



2.3. Sampling approach

As with previous editions, the composition and size of the sample varies from year to year, which may influence results and observations.

Each annual study involves a different set of organisations, and the sample size may also differ. To maintain comparability with previous reports, we aim to recruit organisations with similar characteristics each year, including sector, headcount and geographic footprint; participation, however, remains voluntary. The target population — all organisations accessible and willing to participate in our study across the EU — is divided into strata based on Member States. Within each Member State, entities are further stratified by sector, according to predefined percentages reflecting the study's focus areas.

Within each sector-specific stratum, a tiered approach is applied to select participants:

1. **Initial focus on large enterprises.** We prioritise organisations with a significant operational footprint (very large and large). This approach ensures that the study captures practices and experiences from entities with the most complex operations, interdependencies and cybersecurity requirements — typically those facing higher levels of risk and holding greater systemic importance within their sectors. These organisations are often among the most critical to the functioning of the economy and society overall, making their cybersecurity posture a key indicator of broader resilience.
2. **Subsequent inclusion of medium-sized enterprises:** Once the sample of larger organisations is addressed, we extend the survey to include smaller but still significant entities (under the NIS2 Directive). This broadens our understanding of cybersecurity practices across a wider range of organisational types, highlighting differences in approach, resources and risk exposure.
3. **Repeat participation:** In countries with fewer large or medium-sized organisations, some participants may have participated in surveys for earlier editions of this study. This repeat participation helps maintain **consistency and comparability over time,** allowing us to track trends and changes in practices while ensuring sufficient representation in smaller markets.

It is important to note that:

- The distribution of surveyed organisations is **not proportional to overall sector coverage across the EU,** but rather follows minimum thresholds set by ENISA based on the study's focus areas.
- The sample was **not adjusted to reflect market size across Member States,** as this would have disproportionately weighted larger markets like Germany or France and offered limited insight into smaller ones such as Cyprus or Malta. Instead, a stratified approach was used to ensure representation from all Member States, providing a more balanced picture of cybersecurity practices, challenges and policy implementation across the EU.
- **All responses collected through the survey are visualised and presented in the accompanying Survey data companion document. While this report highlights the main findings, the companion document offers a deeper look—allowing readers to explore how these insights play out across different Member States and sectors.**

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union

ISBN 978-92-9204-777-1