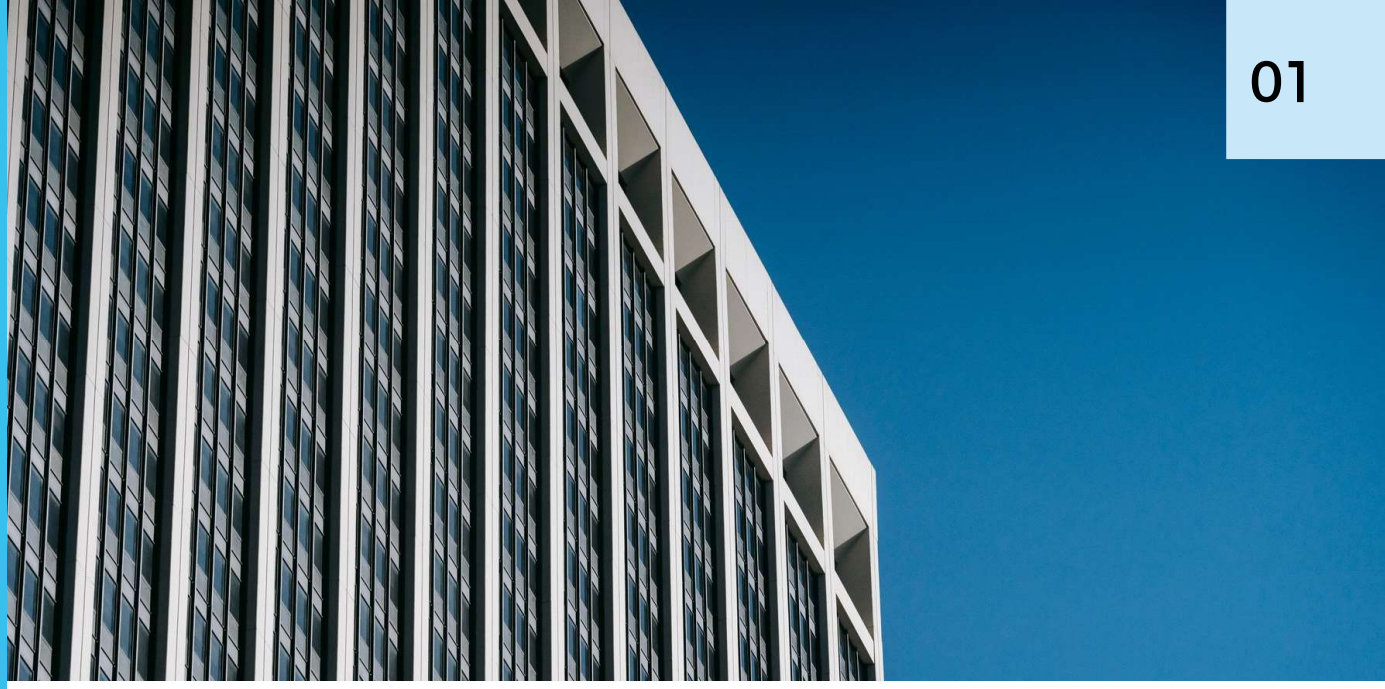
European Cybersecurity Professionals survey

2024

ATAYA&PARTNERS
ECSO EUROPEAN CYBER SECURITY ORGANISATION
HightechPartners
Solvay Brussels School Economics & Management



Summary

The report offers a thorough examination of the **cybersecurity landscape in Europe**, spotlighting the increasing **impact of digitalization on businesses** and the pressing **need for a proficient workforce** to tackle associated challenges.

It explores the hurdles confronting organizations in cybersecurity, notably the **scarcity of skilled professionals** and its repercussions on employee turnover. As digitalization advances, companies face progressively intricate cyber threats, demanding swift action and expertise. To gauge the depth of these challenges, the report outlines a **survey** aimed at dissecting the European market for cybersecurity professionals and Chief Information Security Officers (CISOs), probing into **factors driving job changes** within this domain.

The survey's insights provide valuable glimpses into the **career aspirations** of cybersecurity experts, **training requirements**, and **strategies to attract and retain talents** critical for safeguarding businesses against evolving cyber risks. By **analysing previous survey data**, the report furnishes a comparative analysis of **emerging trends** and **challenges** in European cybersecurity, empowering organizations to devise robust and proactive strategies in this pivotal realm.

Table of Content

HIGHTECH PARTNERS

Hightech Partners is a pan-European company founded and established in Brussels in 1985 offering digital talent acquisition and leadership consulting services. Thanks to its expertise, Hightech Partners plays an important role in the digital transition and in the European technology industry, by linking executive and non-executive directors with companies undergoing digital transformation. Co-founder and shareholder of the ITP Worldwide Network and member of the Association of Executive Search & Leadership Consulting (AESC), Hightech Partners enjoys an international presence.

In order to respond appropriately to its clients' needs, Hightech Partners uses its own ARP approach: Acquire, Reskill and Partner. The company is therefore active across the entire spectrum of digital talent acquisition and development. Hightech Partners also offers companies human capital and leadership assessments and coaching, to enable its clients to realise their full potential in their digital strategy. The company's core values are trust, energy, empathy, agility, passion and integrity.

CYBERSECURITY WORKFORCE CHALLENGES

Increasing digitalization

The increasing digitalization within companies presents both **opportunities** and **challenges**, particularly in the realm of **cybersecurity**.

As organizations adopt new technologies and digital tools, they face the critical task of **ensuring the security** of their digital assets and **the privacy** of their employees and customers.

Cyber threats are becoming increasingly **complex** and ingenious. As digital transformation progresses, there is a **growing need** for **employees with the necessary skills** to understand and navigate the complexities of cybersecurity.

> **“**
> **Europe lacks skilled cybersecurity workforce**

Talent shortage

Europe is **lacking skilled workforce** to meet this demand and protect companies.

This talent shortage leads to a **high employee turnover** due to **stress, burnout**, and **security fatigue** among cybersecurity professionals.

The **challenge** for organizations is not just finding the right talent but also ensuring the **retention of existing cybersecurity experts.**

SURVEY OBJECTIVES

The objective of this survey is to analyse the European market of Cybersecurity professionals and Chief Information Security Officers (CISOs) to better understand the current state of cybersecurity skills shortage and its impact on organizations.

Gain insights

This report aims to gain insights on the career aspirations of these professionals, specifically grasping the reasons behind their job changes. Moreover, this report seeks to evaluate the necessity of investing in trainings to enhance professional with new certifications and skills.

Surveys

Two surveys were conducted to draw conclusions, targeting both CISOs and other cybersecurity professionals.
These surveys encompassed a wide range of topics, including professional experience, stress levels, career transitions, training needs, skill sets, and compensation.
These insights provide a comprehensive view of the cybersecurity landscape in Europe, offering valuable data for organizations looking to navigate the complexities of cybersecurity in the digital age.

Analysis

This report presents a thorough analysis of the responses from the two surveys, focusing on the key findings and comparing them with the results from the previous year's survey.
The insights gained from these surveys are crucial for organizations aiming to build a robust cybersecurity strategy, ensuring they can attract, retain, and develop the necessary talent to protect against the ever-evolving cyber threats.

ROLES IN CYBERSECURITY

For a thorough understanding of this report, it is essential to first define the various roles of the cybersecurity professionals discussed in the investigation.

According to the European Union Agency for Cybersecurity, professionals in the cybersecurity sector can be categorized into 12 different profiles:

CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO, also known as Head of Information Security, manages the development and execution of an organization's cybersecurity strategy to guarantee the adequate security and protection of digital systems, services, and assets.

Mission

- Establish, maintain, and communicate the vision, strategy, policies, and procedures regarding cybersecurity.
- Report cybersecurity risks and issues to the C-level management and authorities.

Deliverables

- Cybersecurity Strategy
- Cybersecurity Policy

Key knowledge

- Incident handling standards, methodologies, frameworks, tools, communication, and recommendations
- Operating systems and computer networks security
- Cyber threats
- Cybersecurity attack procedures
- Computer systems vulnerabilities
- Cybersecurity related laws, regulations and legislations
- Secure Operation Centres (SOCs) operation
- Computer Security Incident Response Teams operation

Main tasks

- Assess, influence and enhance an organisation’s cybersecurity posture
- Analyse and implement cybersecurity policies, certifications, standards,
- methodologies and frameworks
- Comply with cybersecurity-related laws, regulations and legislations
- Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
- Review and enhance security documents, reports, SLAs and ensure the security objectives
- Establish a cybersecurity plan
- Communicate, coordinate and cooperate with internal and external stakeholders
- Anticipate cybersecurity threats, needs and upcoming challenges

Definitions sourced from ENISA (European Union Agency for Cybersecurity. European Cybersecurity Skills Framework Role Profiles. (2022, September). [Report/Study]. DOI: 10.2824/859537.

CYBER INCIDENT RESPONDER

The Cyber Incident Responder, also known as Cyber Crisis Expert or Security Operations Centre Analyst, monitors the organisation's cybersecurity posture, manages any disruptions that occurs during cyber-attacks, and ensures the uninterrupted functioning of ICT systems.

Mission

- Monitor and assess systems' cybersecurity state.
- Identify and evaluate cyber incident causes and mitigate their impact.
- Follow the Incident Response Plan in case of an attack: restore systems' and processes' functionalities, collect evidences and document actions taken.

Key knowledge

- Incident handling standards, methodologies, frameworks, tools, communication, recommendations and best practices
- Operating systems and computer networks security
- Cyber threats
- Cybersecurity attack procedures
- Computer systems vulnerabilities
- Cybersecurity related laws, regulations and legislations
- Secure Operation Centres (SOCs) operation
- Computer Security Incident Response Teams (CSIRTs) operation

Deliverables

- Incident Response Plan
- Cyber Incident Report

Main tasks

- Contribute to the development, maintenance and assessment of the Incident Response Plan
- Identify, analyse, mitigate and communicate cybersecurity incidents
- Assess and manage technical vulnerabilities
- Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident
- Establish procedures for incident results analysis and incident handling reporting
- Document incident results analysis and incident handling actions
- Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs)
- Cooperate with key personnel for reporting of security incidents according to applicable legal framework
- Collect, analyse and correlate cyber threat information originating from multiple sources
- Work on operating systems, servers, clouds and relevant infrastructures

CYBER LEGAL, POLICY AND COMPLIANCE OFFICER

The Cyber Legal, Policy and Compliance officer has alternative titles, such as Data Protection Officer, Cyber Legal Advisor, Information Governance officer, Data Compliance Officer, and Governance Risk Compliance Consultant. They mainly manages compliance with cybersecurity-related standards, legal and regulatory frameworks that are based on the organisation's strategy and legal requirements.

Mission

- Monitor and ensure compliance with cybersecurity- and data-related legal, regulatory frameworks.
- Provide legal advice in the development of the organisation's cybersecurity governance processes.

Key knowledge

- Cybersecurity related laws, regulations and legislations
- Cybersecurity and privacy impact assessments standards, methodologies and frameworks
- Cybersecurity policies
- Legal, regulatory and legislative compliance requirements, recommendations and best practices

Deliverables

- Compliance Manual
- Compliance Report

Main tasks

- Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures
- Ensure that data owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities
- Act as a key contact point to handle queries and complaints regarding data processing
- Assist in designing, implementing, auditing and compliance testing activities to ensure cybersecurity and privacy compliance
- Monitor audits and data protection related training activities
- Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization
- Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties

CYBER THREAT INTELLIGENCE SPECIALIST

The Cyber Threat Intelligence Specialist collects and analyses data and information to provide target stakeholders with actionable intelligence reports.

Mission

- Manage cyber threat intelligence life cycle
- Production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level.
- Identify the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors and their trends, monitor threat actors' activities and observe how non-cyber events can influence cyber-related actions.

Key knowledge

- Operating systems and computer networks security
- Cybersecurity controls and solutions
- Computer programming
- Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks
- Responsible information disclosure procedures
- Advanced and persistent cyber threats (APT)
- Threat actors Tactics, Techniques and Procedures (TTPs)

Deliverables

- Cyber Threat Intelligence Manual
- Cyber Threat Report

Main tasks

- Develop, implement and manage the organisation's cyber threat intelligence strategy
- Identify and assess cyber threat actors targeting the organisation
- Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence
- Leverage intelligence data to support and assist with threat modelling,
- recommendations for Risk Mitigation and cyber threat hunting
- Articulate and communicate intelligence openly and publicly at all levels
- Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders

CYBERSECURITY ARCHITECT

The Cybersecurity Architect, also known as Data Security Architect, plans and designs security-by-design solutions that entails infrastructures, systems, assets, software, hardware, and services.

Mission

- Design solutions based on security-by-design and privacy-by-design principles.
- Create and continuously improve architectural models and develop appropriate architectural documentation and specifications.

Deliverables

- Cybersecurity Architecture Diagram
- Cybersecurity Requirements Report

Key knowledge

- Cybersecurity standards, methodologies and frameworks
- Secure development lifecycle
- Security architecture reference models
- Cybersecurity risks & threats
- Legacy cybersecurity procedures Privacy-Enhancing Technologies (PET)
- Privacy-by-design standards, methodologies and frameworks

Main tasks

- Design a secure architecture to implement the organisation's strategy to address security and privacy requirements
- Produce architectural documentation and specifications
- Adapt the organisation's architecture to emerging threats
- Conduct user and business security requirements analysis
- Guide and communicate with implementers and IT/OT personnel

CYBERSECURITY AUDITOR

The Cybersecurity Auditor ensures compliance with statutory, regulatory, policy information, security requirements, and industry standards.

Mission

- Assess the organisation's compliance with legal and regulatory frameworks policies.
- Evaluate, test and verify cybersecurity-related products (systems, hardware and software), functions and policies ensuring, compliance with guidelines, standards and regulations

Deliverables

- Cybersecurity Audit Plan
- Cybersecurity Audit Report

Key knowledge

- Legal, regulatory, and legislative compliance requirements, and recommendations
- Conformity assessment standards, methodologies and frameworks
- Auditing & Cybersecurity standards, methodologies and frameworks

Main tasks

- Develop the organisation's auditing policy, procedures, standards, and guidelines
- Establish the methodologies and practices used for systems auditing
- Define audit scope, objectives, and criteria to audit against
- Review target of evaluation, security objectives and requirements based on the risk profile
- Audit compliance with cybersecurity-related applicable laws and regulations
- Maintain and protect the integrity of audit records
- Monitor risk remediation activities

CYBERSECURITY EDUCATOR

The Cybersecurity Educator or Awareness specialist improves cybersecurity knowledge and skills within organizations.

Mission

- Design, develop, and conduct awareness, training and educational programmes about cybersecurity and data protection.
- Promote cybersecurity and create a cybersecurity culture into the organization.

Deliverables

- Cybersecurity Awareness Program
- Cybersecurity Training Material

Key knowledge

- Cybersecurity & Pedagogical standards, methodologies and frameworks
- Cybersecurity education and training standards, methodologies and frameworks
- Cybersecurity related laws, regulations and legislations

Main tasks

- Develop, update and deliver cybersecurity and data protection educational material for training and awareness based on content, method, tools, trainees need
- Monitor, evaluate and report training effectiveness
- Provide guidance on cybersecurity certification programs for individuals
- Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building

CYBERSECURITY IMPLEMENTER

Also known as the Cybersecurity solutions Expert or Development, Security & Operations (DevSecOps) Engineer, the Cybersecurity Implementer develops, deploys and operates cybersecurity solutions on infrastructures and products.

Mission

- Develop, implement, maintain, upgrade, test cybersecurity products
- Ensure adherence to specifications and conformance requirements and resolve technical issues required in the organisation's cybersecurity-related, infrastructures and products.

Deliverables

- Cybersecurity Solutions

Key knowledge

- Secure development lifecycle
- Computer programming
- Operating systems and computer networks security
- Cybersecurity controls and solutions
- Offensive and defensive security practices
- Secure coding recommendations and best practices
- Testing standards, methodologies and frameworks
- Cybersecurity-related technologies

Main tasks

- Provide cybersecurity-related support to users and customers
- Integrate cybersecurity solutions and ensure their sound operation
- Securely configure systems, services and products
- Maintain and upgrade the security of systems, services and products
- Implement and ensure cybersecurity procedures and controls
- Document and report on the security of systems, services and products
- Work close with the IT/OT personnel on cybersecurity-related actions
- Implement, apply and manage patches to products to address technical vulnerabilities

CYBER RESEARCHER

The Cybersecurity Researcher conducts research on the cybersecurity domain and incorporates results in cybersecurity solutions.

Mission

- Conduct fundamental and applied research and facilitate innovation in the cybersecurity domain through cooperation with other stakeholders.
- Identify trends and scientific findings in cybersecurity

Key knowledge

- Cybersecurity-related research, development and innovation (RDI)
- Cybersecurity standards, methodologies and frameworks
- Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies
- Responsible information disclosure procedures

Deliverables

- Publication in cybersecurity

Main tasks

- Conduct research, innovation and development work in cybersecurity-related topics
- Manifest and generate research and innovation ideas
- Conduct experiments and develop a proof of concept, pilots and prototypes for
- cybersecurity solutions
- Select and apply frameworks, methods, standards, tools and protocols including a building and testing a proof of concept to support projects
- Contribute towards cutting-edge cybersecurity business ideas, services and solutions
- Assist in cybersecurity-related capacity building including awareness, theoretical training, practical training, testing, mentoring, supervising and sharing
- Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions
- Lead or participate in the innovation processes and projects including project management and budgeting
- Publish and present scientific works and research and development results

CYBERSECURITY RISK MANAGER

The Cybersecurity Risk Manager ensures the organization's cybersecurity-related risks are aligned to its strategy in addition to developing, maintaining and communicating the risk management processes and reports.

Mission

- Continuously manage (identify, analyse, assess, estimate, mitigate) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment.
- Establish a risk management strategy for the organisation and ensure that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.

Key knowledge

- Risk management standards, methodologies, frameworks, and tools
- Risk management recommendations and best practices
- Cyber threats & risks
- Computer systems vulnerabilities

Deliverables

- Cybersecurity Risk Assessment Report
- Cybersecurity Risk Remediation Action Plan

Main tasks

- Develop an organisation's cybersecurity risk management strategy
- Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems
- Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy
- Monitor effectiveness of cybersecurity controls and risk levels
- Ensure that cybersecurity risks remain at an acceptable level for the organisation's assets
- Develop, maintain, report and communicate complete risk management cycle

DIGITAL FORENSICS INVESTIGATOR

The Digital Forensics Investigator, also known as Cybersecurity & Forensics Specialist makes sure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.

Mission

- Connect artefacts to natural persons, capture, recover, and preserve data, including manifestations, inputs, outputs and processes of digital systems under investigation.
- Presents an unbiased qualitative view without interpreting the resultant findings.

Deliverables

- Digital Forensics Analysis Results
- Electronic Evidence

Key knowledge

- Digital forensics standards, methodologies, frameworks, and best practices
- Digital forensics analysis and testing procedures
- Criminal investigation procedures, standards, methodologies and frameworks
- Cybersecurity related laws, regulations and legislations
- Malware analysis tools
- Computer systems vulnerabilities and cyber threats
- Cybersecurity attack procedures
- Operating systems and computer networks security

Main tasks

- Develop digital forensics investigation policy, plans and procedures
- Identify, recover, extract, document, analyse, and preserve digital evidence, and make it available to authorised stakeholders
- Inspect environments for evidence of unauthorised and unlawful actions
- Systematically and deterministic document, report and present digital forensic analysis findings and results

PENETRATION TESTER

The Penetration Tester, also known as Ethical Hacker, Offensive Cybersecurity Expert or Red Team Expert assesses the effectiveness of security controls, reveals cybersecurity vulnerabilities, and determines their criticality if they were exploited by threat actors.

Mission

- Plan, design, and execute penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures.
- Identify vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products.

Deliverables

- Vulnerability Assessment Results Report
- Penetration Testing Report

Key knowledge

- Cybersecurity attack procedures
- Information technology (IT) and operational technology (OT) appliances
- Offensive and defensive security procedures
- Operating systems and computer networks security
- Penetration testing standards, procedures, tools, methodologies and frameworks
- Computer programming
- Computer systems vulnerabilities

Main tasks

- Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities
- Test systems and operations compliance with regulatory standards
- Select and develop appropriate penetration testing techniques
- Establish procedures for penetration testing result analysis and reporting
- Document and report penetration testing results to stakeholders

METHODOLOGY

Data Gathering

The surveys were carried out using two online questionnaires of 29 questions, with 7 themes: Demographics, Education, Employment & Career, Certifications, Skills, Stress, Compensation.
The questions were of various nature, including single and multiple choice, quantitative, qualitative, simple Yes/No and 1 to 5 scales.
The surveys were shared and promoted with the help of ECSO, and a total of 130 answers were collected.

Data analysis

The Data was analyzed both per question and per respondent. All analysis was performed in Excel. The data has been carefully refined to generate graphs that prioritize clarity and readability. This process required striking a balance between the amount of information presented and its ease of understanding. By focusing on a coherent visual narrative, we ensured that the graphs convey key trends and patterns without overwhelming viewers, making the data both accessible and informative.
Special care was taken to ensure that the analysis could be replicated in future surveys, so as to enable comparison over several years.

Limits of the data

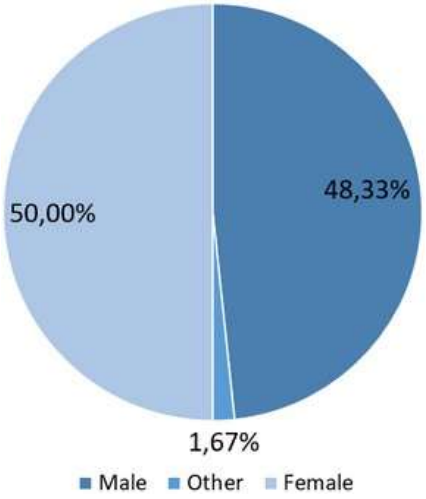
While growing with every new yearly survey, the small number of data points means that any interpretation or inference must be examined critically. No trend is definitively shown, and when possible, several possible hypotheses for an explanation will be offered.
In an effort to normalize the data, some of it had to be discarded.

SURVEY ANALYSIS

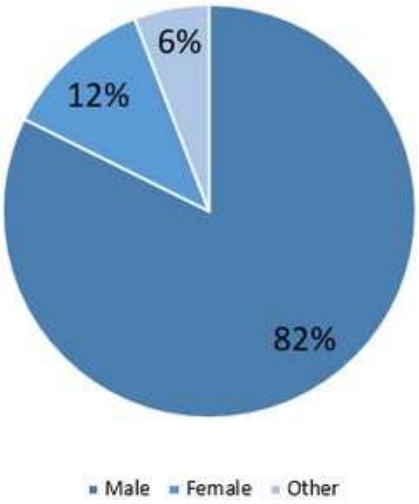
DEMOGRAPHICS

GENDER DISTRIBUTION

CYBER PROFESSIONALS 2024

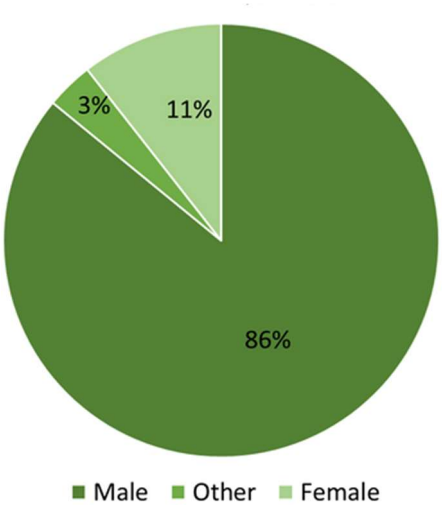


CYBER PROFESSIONALS 2023

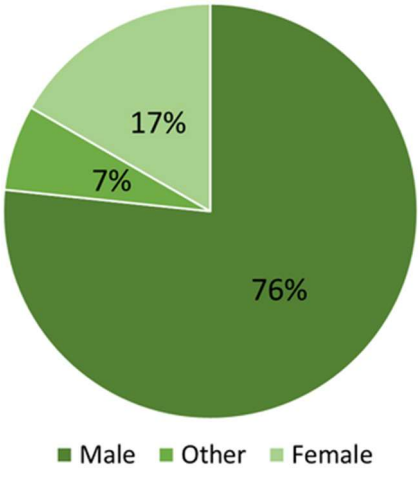


Although there is a discernible trend of **decreasing gender imbalance** in the cybersecurity domain, it's essential to interpret sudden changes in data with caution. The drastic shift observed in the gender distribution between 2023 and 2024, from 82% male to 48.33% male, 12% female to 50%, and 6% other to 1.6%, likely reflects the influence of relatively small sample sizes rather than a rapid transformation in the industry's gender demographics. Despite the increase in the proportion of female professionals in 2024, the proportion of female CISOs remains significantly lower, reflecting the usual barriers to female representation in executive roles.

CISO 2024

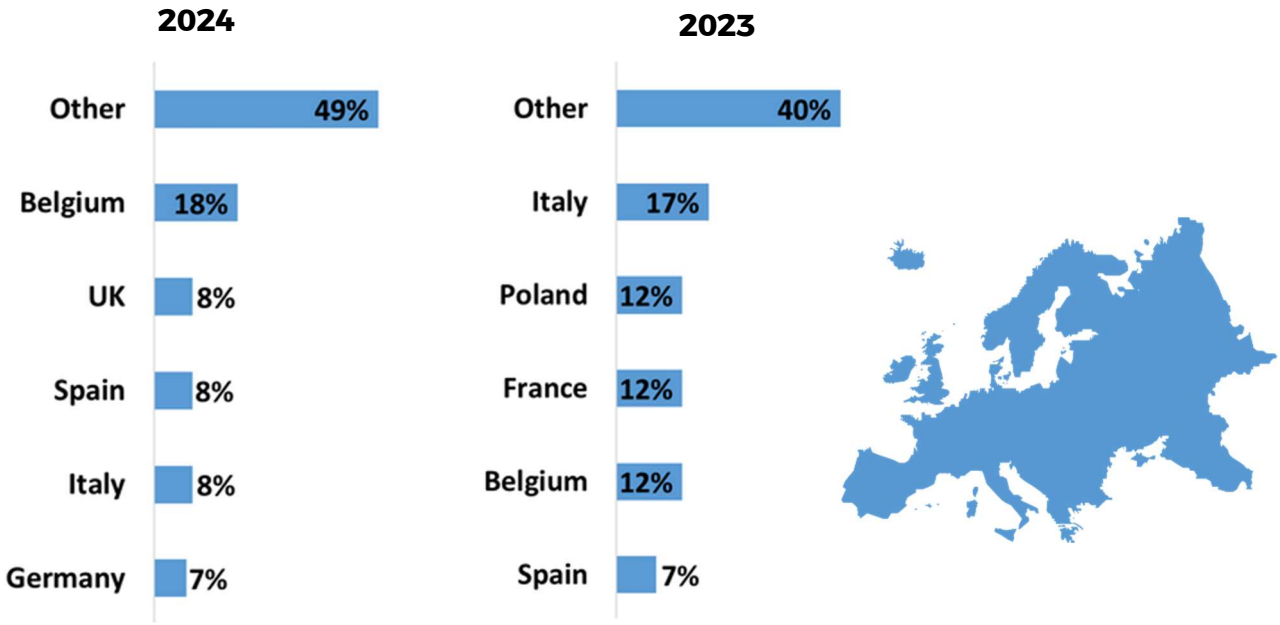


CISO 2023



GEOGRAPHIC DISTRIBUTION

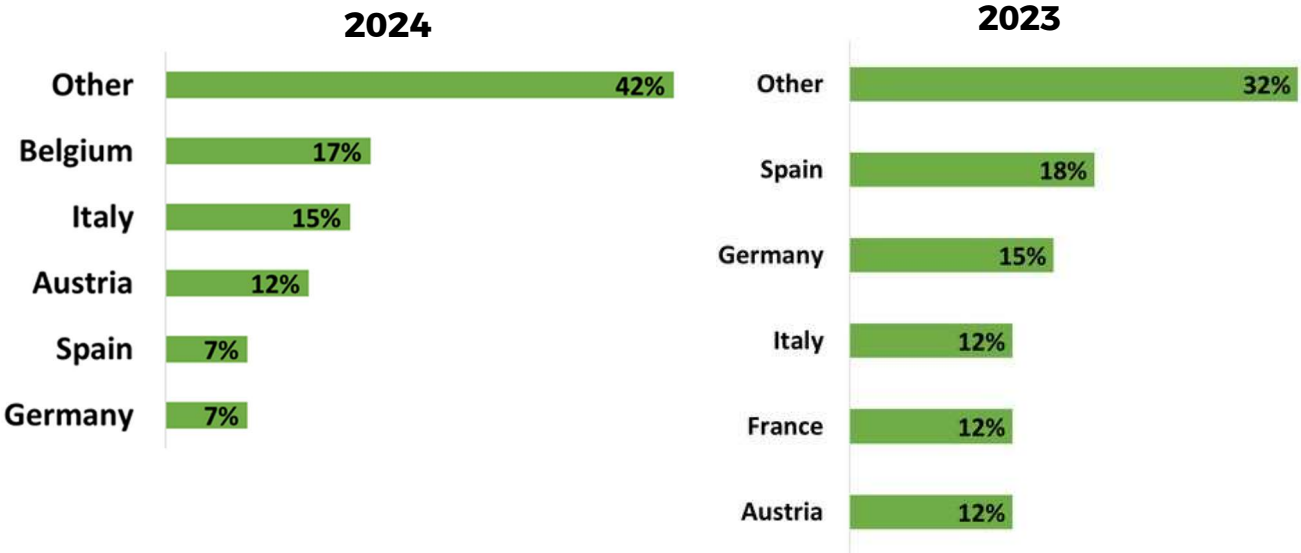
CYBER PROFESSIONALS



In 2024, Belgium emerged as the most represented country among cybersecurity professionals, surpassing Italy, which held the lead in 2023. Spain, consistently in the top 5, maintained its presence alongside Belgium. This shift in representation could be attributed to the reputation of Brussels and Madrid as notable cybersecurity hubs, attracting professionals from various backgrounds and regions.

"Other" countries include Latvia, Denmark, and Portugal, which underscores the geographic diversity within the cybersecurity domain. This highlights the global nature of cybersecurity and the widespread engagement in addressing cybersecurity challenges across diverse regions.

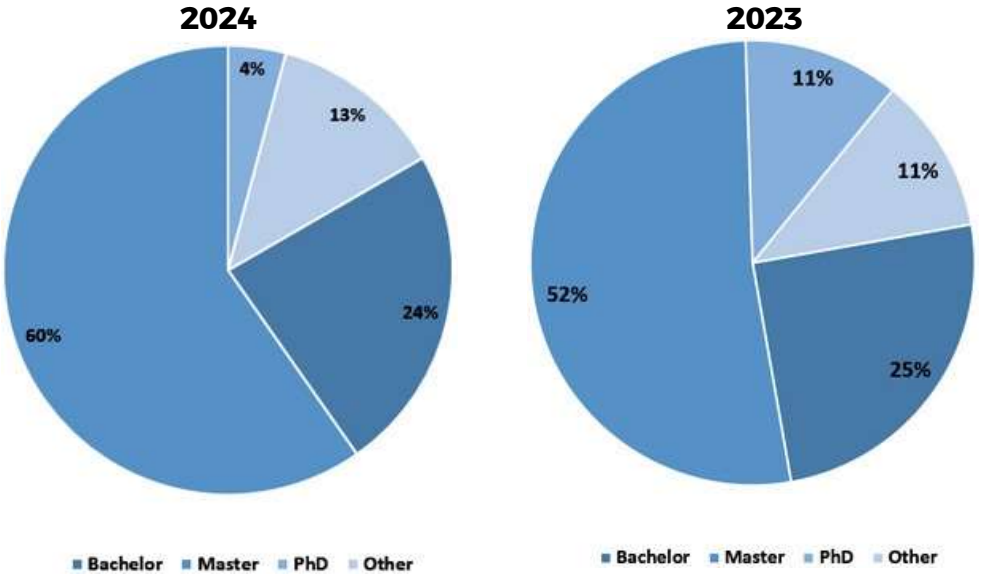
CISOS



EDUCATION

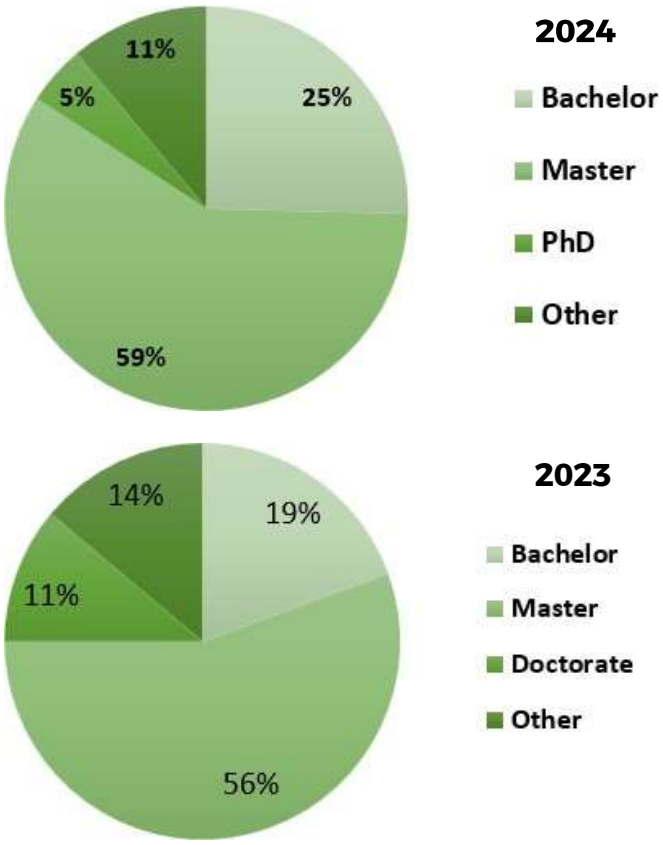
LATEST DEGREE OBTAINED

CYBER PROFESSIONALS



A majority of Cyber Professionals held a **Master's degree in 2024**. This was true of 2023 as well, although an **8p.p. increase** is observed. This could reflect a real **trend of increased academic barriers** to entry to the profession, improvement of Cybersecurity education. A rather large "other" category includes several high school graduates and a vocational school graduate.

CISOS



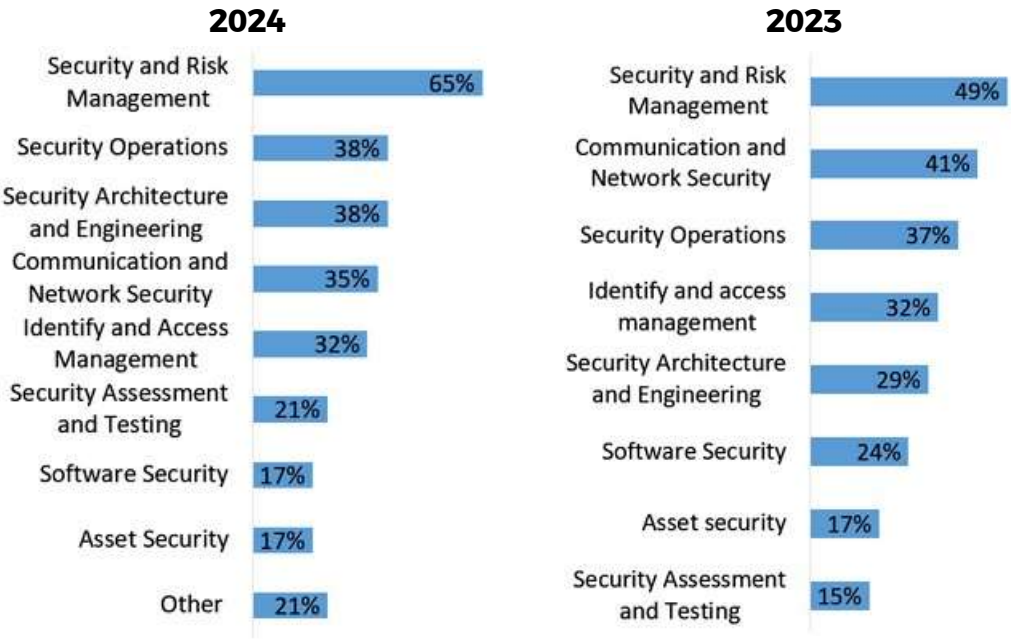
PHD's are not necessarily more prevalent in CISO positions

The majority of CISO's held a **Master's degree in 2024**, but the **share** of Master's and Bachelor's degrees sligthly **declined** compared to 2023. **PhD's have risen strongly** by 6p.p., possibly indicating an **increasing demand** for a high quality theoritical knowledge.

EXPERTISE

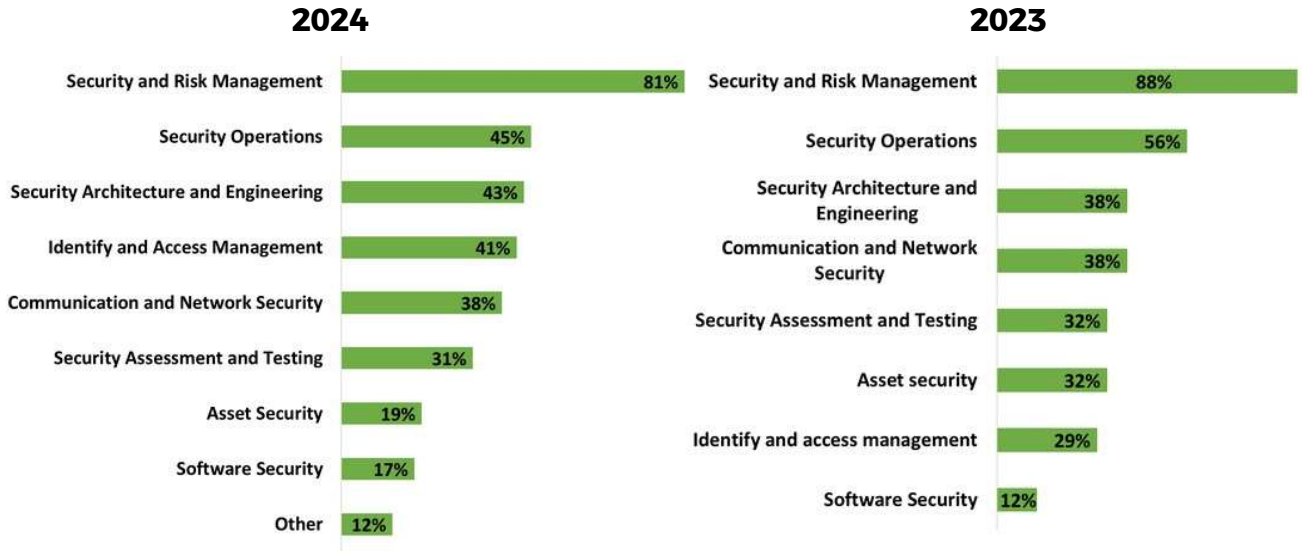
SELF-REPORTED FIELDS OF EXPERTISE

CYBERPROFESSIONALS



Self reported expertise assessments are a good way to judge what aspects of their work professionals are most comfortable with. Note that several answers were accepted, so this is a list of the most selected, not a ranked list of importance. In 2024, **Risk management** was the leading subject, with a wide margin. This was also true for 2023, though the lead was not as pronounced. This might stem from the rising awareness of cybersecurity challenges, reflecting that a growing number of professionals are being trained in this field.

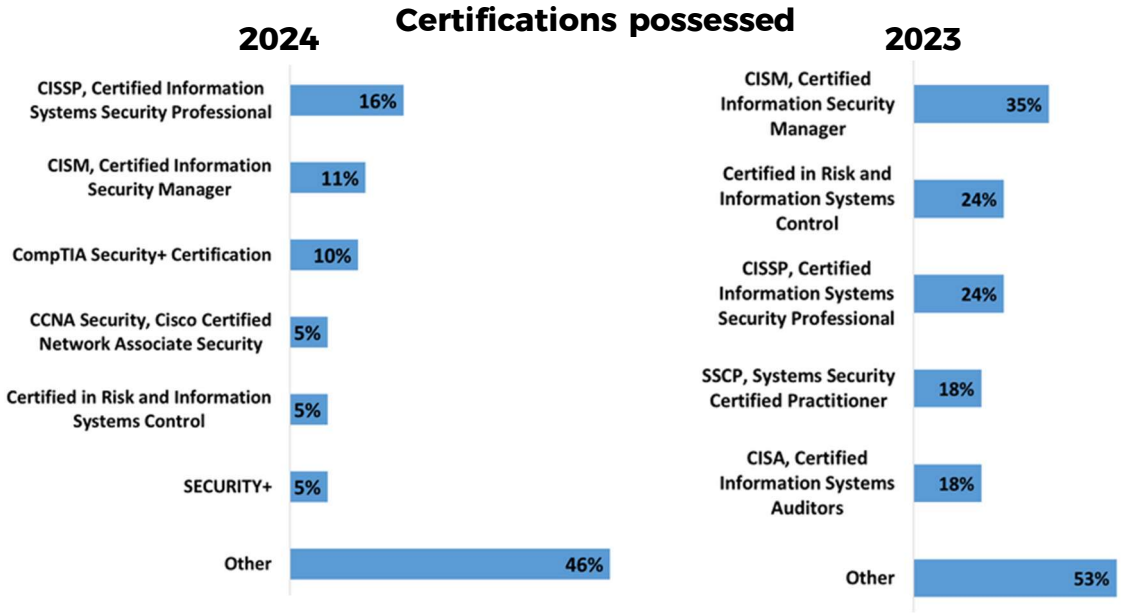
CISOS



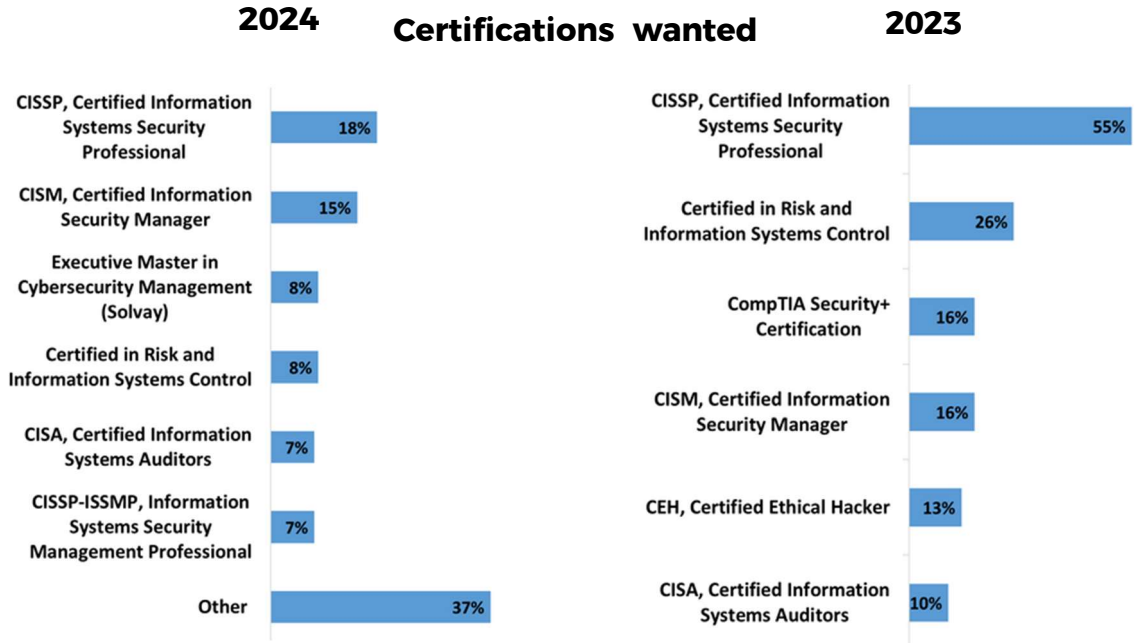
Security and Risk Management remained the **most self reported** field of expertise **in 2024**. Compared to the previous year, there was an **increase of 12p.p** in self reported expertise **in Identify and Access Management**, while **expertise in Asset security dropped by 13p.p**.

CERTIFICATIONS

CYBER PROFESSIONALS



The **most popular** certification as of 2024 is **CISSP**, with a 16% answer rate, which is not suprising as it is one of the most recognized certifications in the field. Notably, no single certification appears to fit every role and professional need, evidencing the variety of Cybersecurity professions.
Many popular certifications were not represented at all within our sample, showing perhaps a concentration in specific industries where they are desireable.

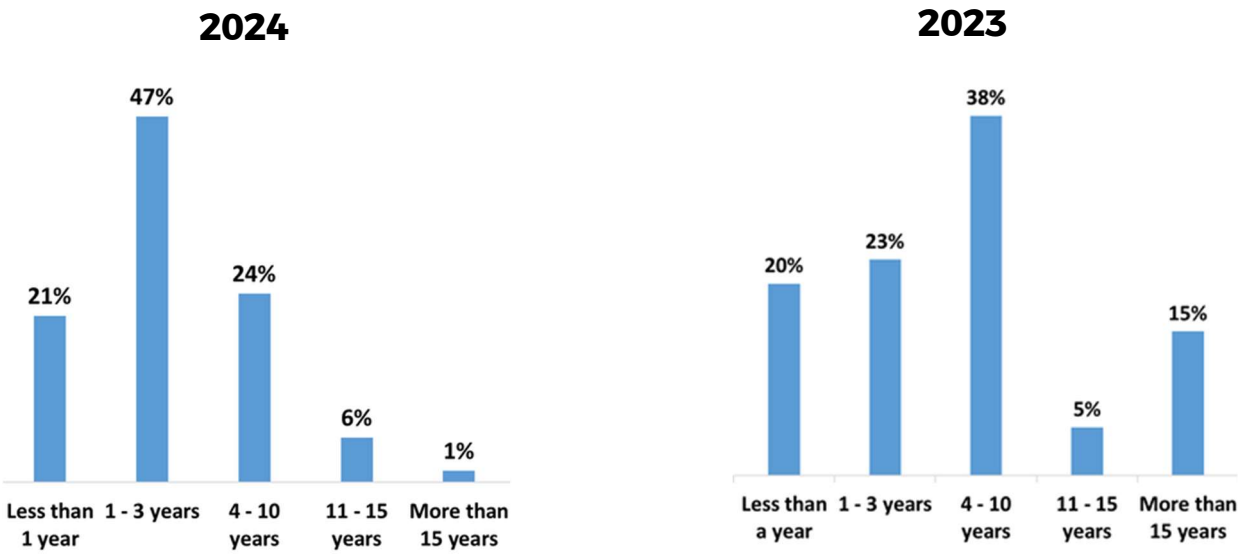


Interesting to note is that both in 2023 and 2024, **CISSP** was the most desired certification, as well as the most held in 2024. It seems CISSP is primed to continue growing, and special interest will be shown to it in future surveys.
Overall, Certifications wanted and certifications held look remarkably similar.

SENIORITY

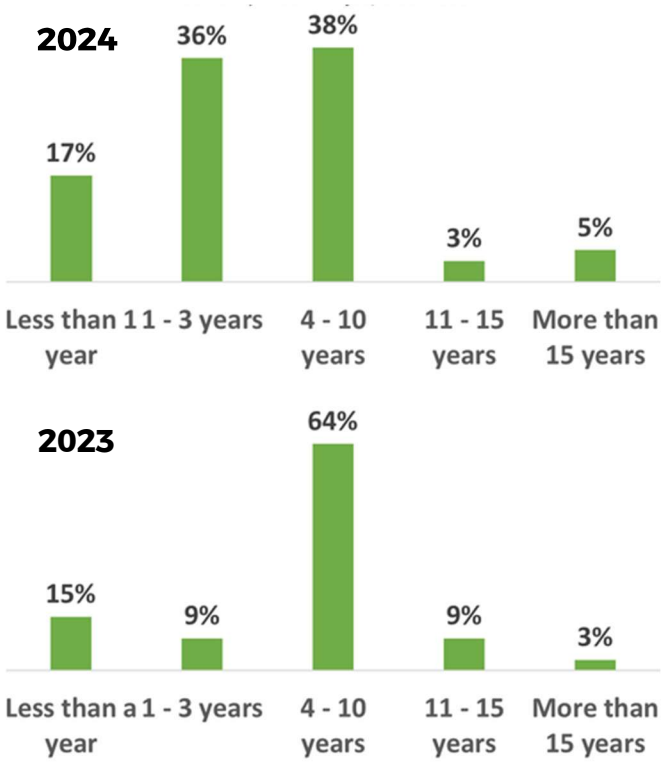
SENIORITY IN CURRENT ROLE

CYBER PROFESSIONALS



In 2024, nearly **70% of professionals** employed in the cybersecurity field have held their current positions for **fewer than four years**, a notable increase from the over 40% reported in 2023. This data underscores the dynamic nature of the cybersecurity industry, where professionals frequently transition between roles. The pronounced change observed between 2023 and 2024 could stem from two primary factors. Firstly, the possibility of small sample sizes influencing the data cannot be overlooked, as variations in sample composition may lead to fluctuations in reported figures. Alternatively, this shift may indeed reflect changes in the job market dynamics. A "hotter" job market could **incentivize** professionals to seek out **new opportunities** more frequently, resulting in a higher **turnover rate** and shorter tenures in their current positions.

CISOS



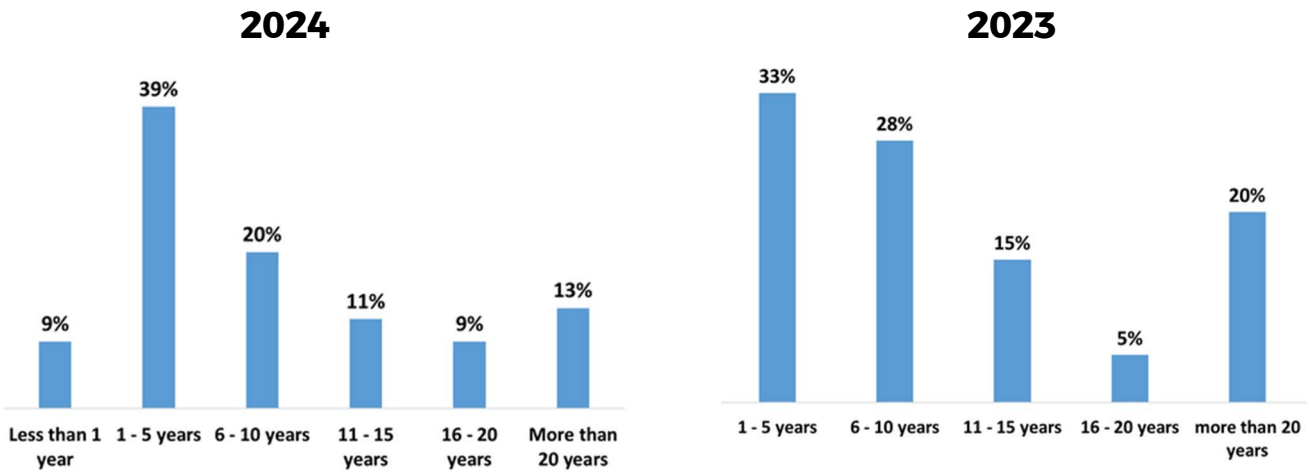
The data from 2023 indicates that only 24% of CISOs had been employed for less than three years. However, in just one year, **this figure nearly doubled**, with **53% of CISOs** in 2024 having been employed for **less than three years**.

This trend reflects a notable shift in the cybersecurity landscape and underscores the **increasing emphasis** that companies place **on the security** of their information systems. The rising prevalence of CISOs with shorter tenures and the very few CISOs with more than 15 years of experience suggest a **growing recognition** of the importance of having a dedicated security executive position within organizations.

SENIORITY

SENIORITY IN THE INDUSTRY

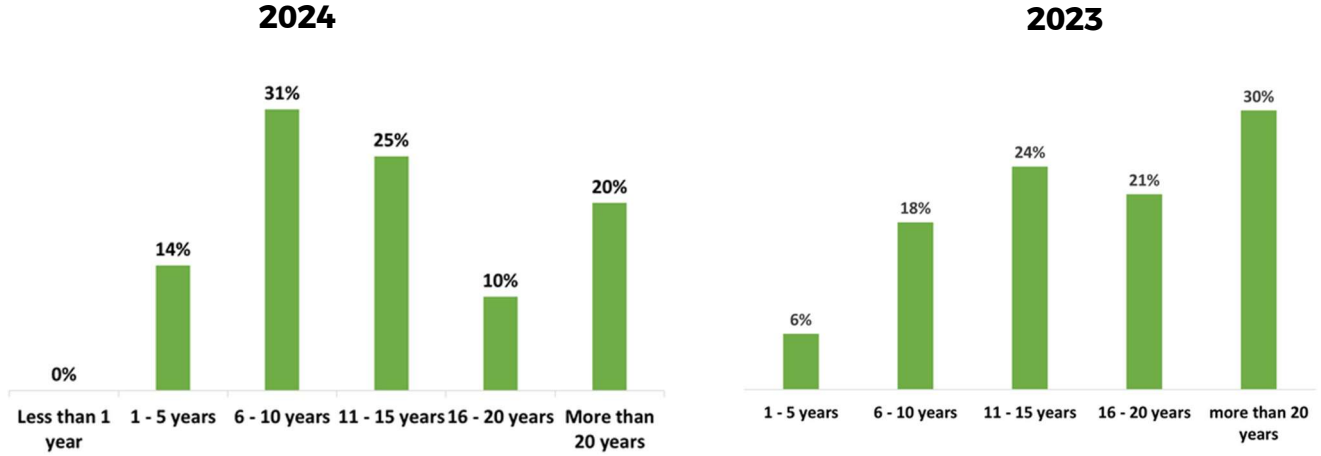
CYBER PROFESSIONALS



The data reveals that a **significant number** of cybersecurity professionals **have extensive experience in the field**, with a notable cohort having been involved for more than 20 years in both 2023 and 2024. Particularly striking is the proportion of CISOs with high seniority, with **30% of respondents** having held their positions for **more than 15 years**, and a substantial **86% for over 5 years**.

Despite some fluctuations from year to year, the overall structure remains consistent. There is a prominent **spike in junior employees**, followed by a gradual decrease in population as experience increases, until another peak representing very senior professionals. This suggests a pattern of career progression within the cybersecurity industry, where professionals enter the field at various levels of experience, gain expertise over time, and ascend to senior roles.

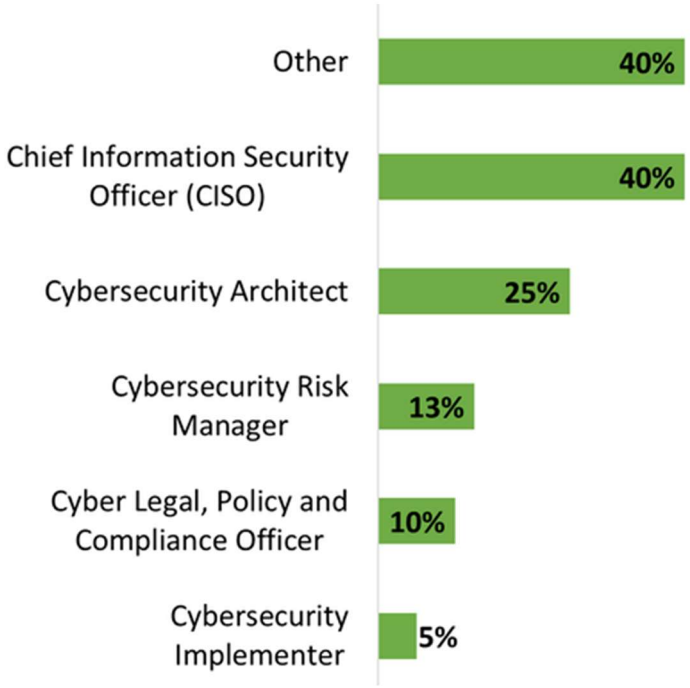
CISOS



SENIORITY

PREVIOUS ROLE

CISOS

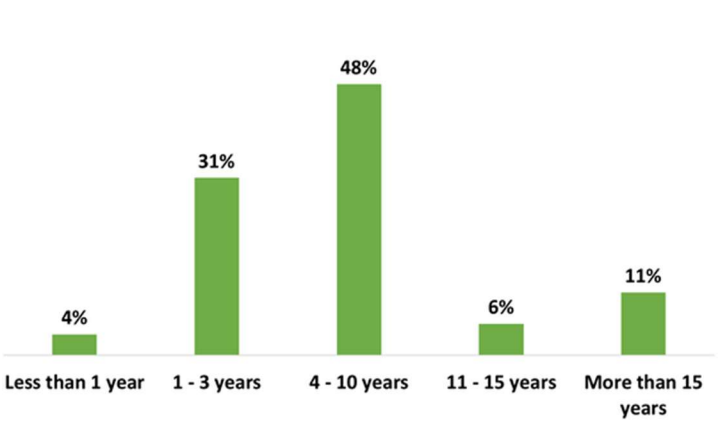


The data indicates that a significant proportion of CISOs respondents had **previously held the role of CISO in another firm.** This suggests a common trend of mobility and experience among CISO professionals, where individuals bring their expertise from previous positions to new organizations.

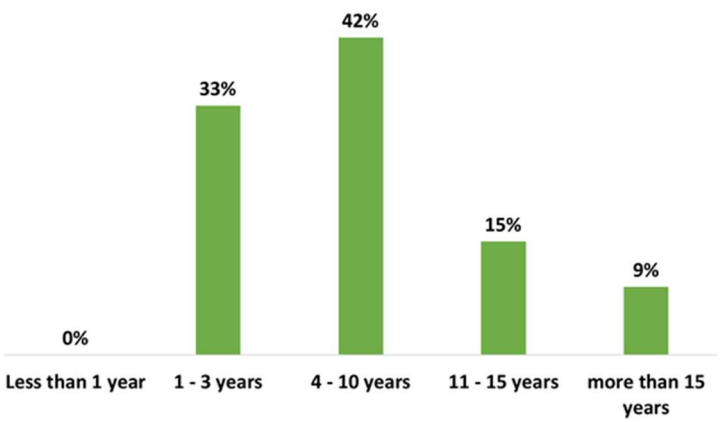
Moreover, the data highlights that CISOs often served as professionals with a broad view of cybersecurity across the firm, such as architects and risk managers. This diverse experience equips CISOs with a comprehensive understanding of cybersecurity challenges and strategies, enabling them to effectively oversee security measures and initiatives within their organizations.

TENURE OF PREVIOUS ROLE

2024



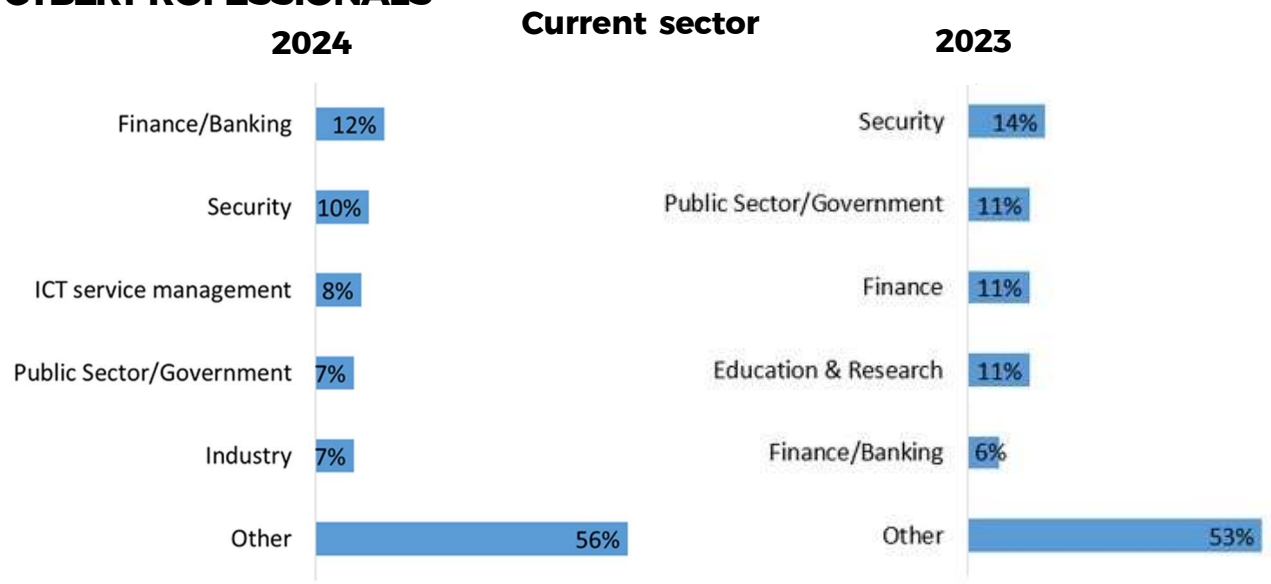
2023



The analysis of the tenure of CISOs in their previous roles highlights a significant trend: a considerable number of these professionals had previously held the role of CISO in another organization. This reflects a **pattern of career mobility** and accumulated experience within the industry, where CISOs **transfer their specialized knowledge** and skills from one company to another. The data notably shows that most CISOs had tenure ranging from four to ten years in their previous roles, as evident in the 2024 and 2023 graphs where 48% and 42% of them, respectively, fall within this duration. This duration of tenure underscores a **stable period** during which these leaders not only manage but also refine cybersecurity practices effectively.

SECTOR

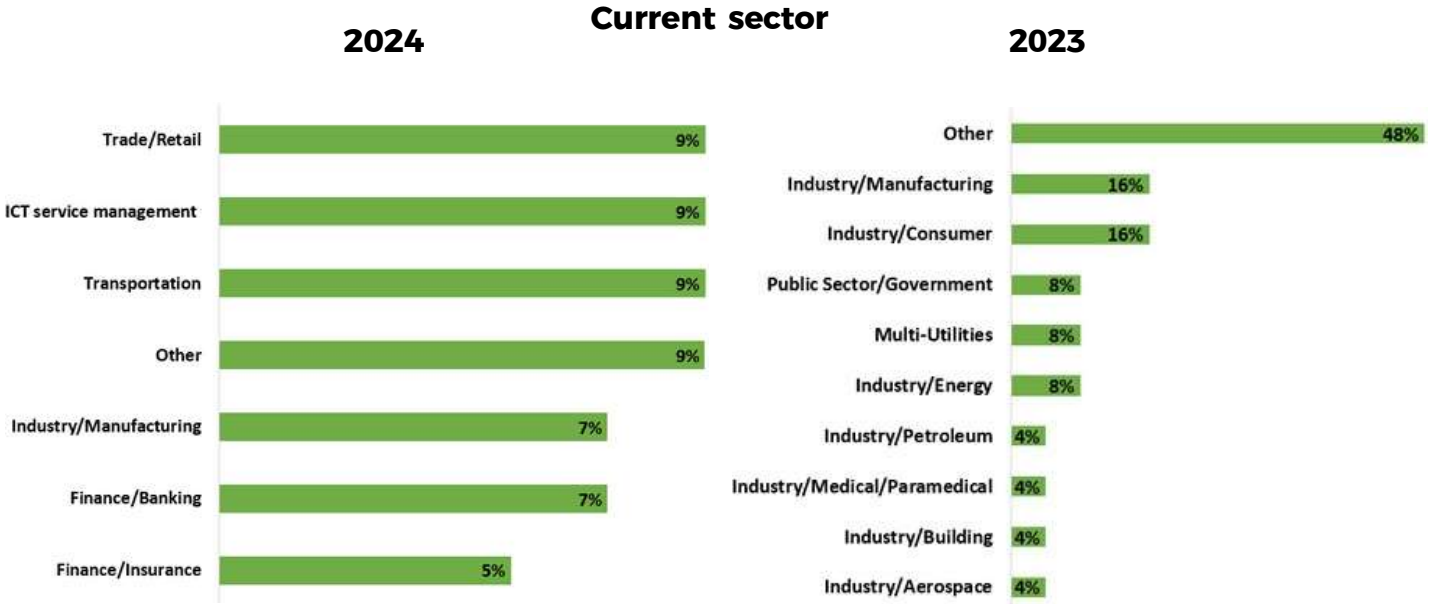
CYBER PROFESSIONALS



The data for 2024 reveals that the **Finance and Banking** sector employed the highest number of cybersecurity professionals. This could be explained by the fact that this sector is particularly regulated and by the future **Digital Operational Resilience Act (DORA)** that will apply as of 17 Janurary 2025.

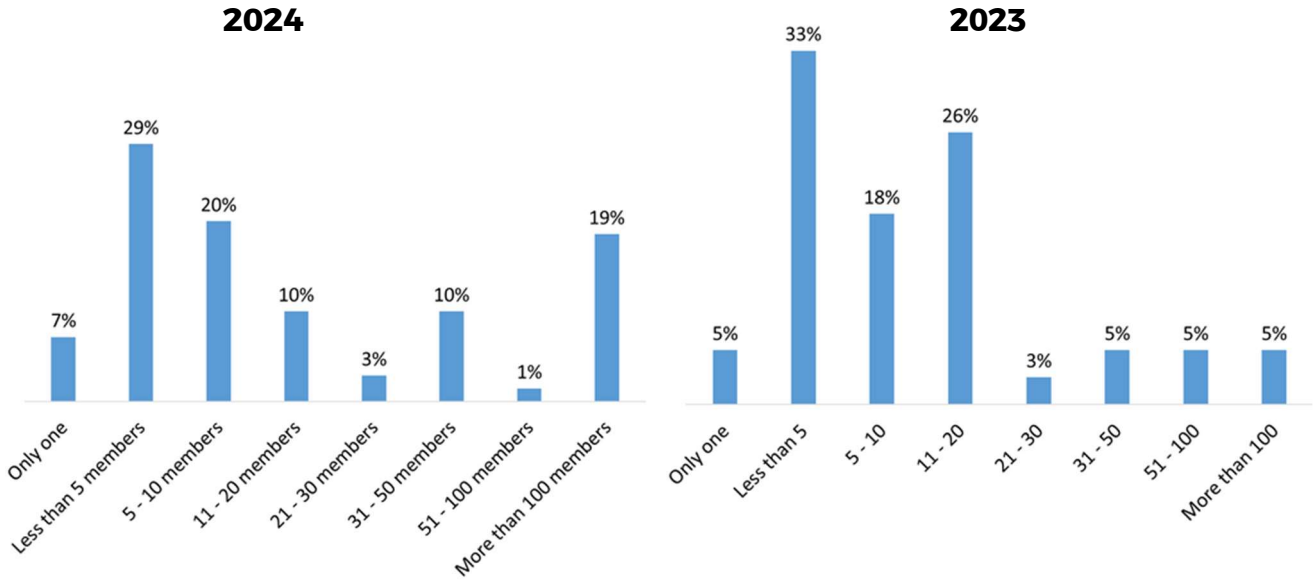
The **security sector**, which held the leading position in 2023, appeared in second position. However, it's important to note that a significant portion of cybersecurity professionals work in various other sectors, collectively categorized as "other." This highlights the pervasive nature of cybersecurity across diverse industries and underscores its **essential role** in safeguarding sensitive information and infrastructure. Among these "other" sectors, notable mentions include **consulting, real estate, and oil & gas**.

CISOS



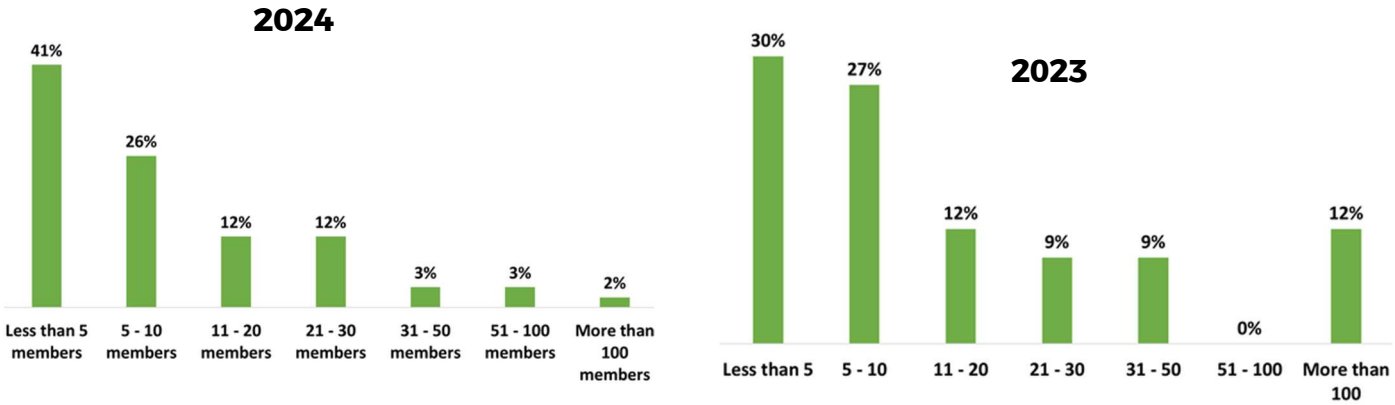
SIZE OF THE TEAM

CYBER PROFESSIONALS



A significant proportion of participants are part of small teams comprising 20 members or fewer. Conversely, teams consisting of 21 to 100 members are less common. Surprisingly, teams exceeding 100 members are more prevalent than anticipated. This distribution suggests a somewhat **consolidated landscape** within the cybersecurity industry. Many small teams coexist alongside a few very large ones, creating a **noticeable gap** in team sizes without many intermediate options. However, it's essential to consider potential factors that could influence these findings. Firstly, the presence of multiple respondents from a single large team could potentially skew the perception of the frequency of such large teams. Additionally, there may be instances of confusion between **team size** and **company size**, which could further complicate the interpretation of the data.

CISOS

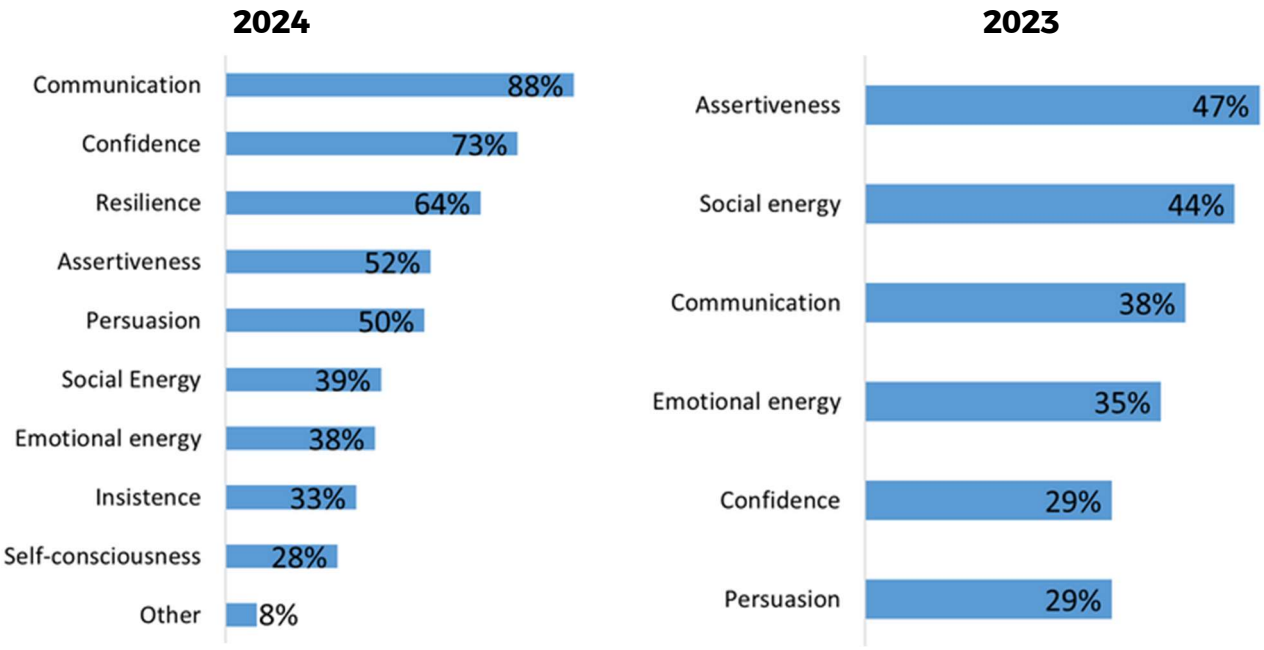


The data reveals that CISOs were more likely to have **smaller teams** compared to other cybersecurity professionals. Many CISOs reported having teams consisting of **fewer than five members**. One possibility is that some CISOs may not consider the entire cybersecurity workforce within their organization as part of their team. Instead, they may focus on their **direct reports** or **immediate team members**. Another possibility is that the sample of CISOs surveyed primarily represented smaller firms.

SKILLS

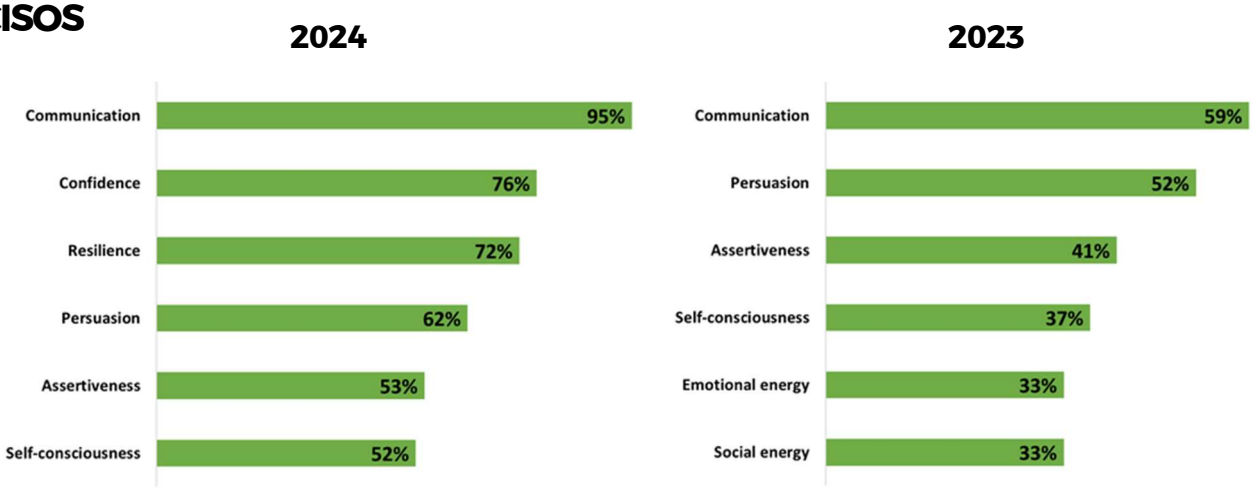
ESSENTIAL SOFT SKILLS

CYBER PROFESSIONALS



The data suggests that effective communication, confidence, and resilience are highly valued traits among cybersecurity professionals. Effective **communication** is crucial for conveying information accurately, whether it's sharing threat intelligence or explaining security protocols to non-technical stakeholders. **Confidence** is necessary for making decisions under pressure and instilling trust in team members and stakeholders. **Resilience** is vital for bouncing back from setbacks, adapting to new threats, and persevering in the face of challenges.

CISOS

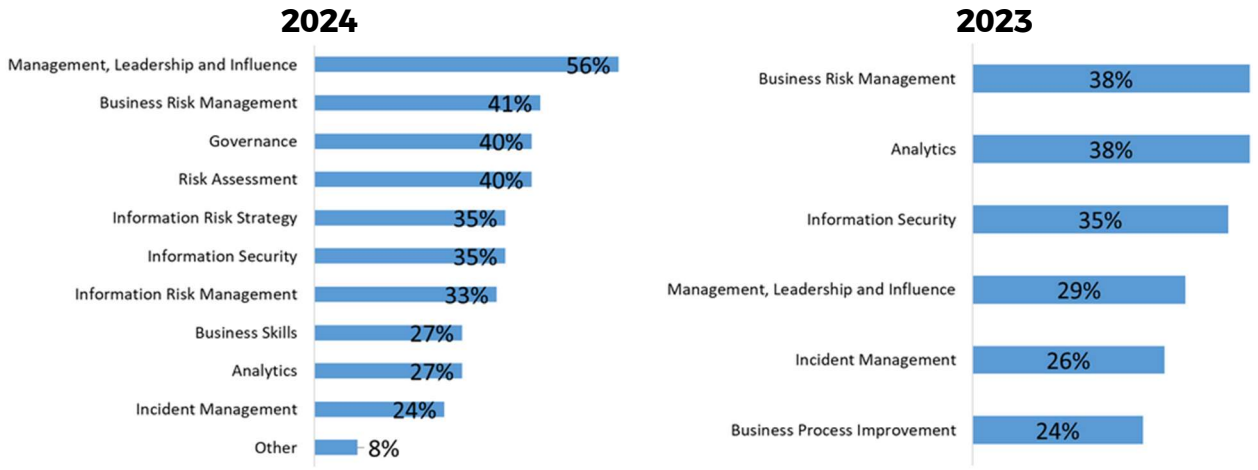


A higher emphasis was put on **self-consciousness** for CISOs, reflecting the importance of understanding their own biases, strengths, and limitations in decision-making processes, thereby fostering more effective leadership and strategic risk management within their organizations.

SKILLS

ESSENTIAL HARD SKILLS

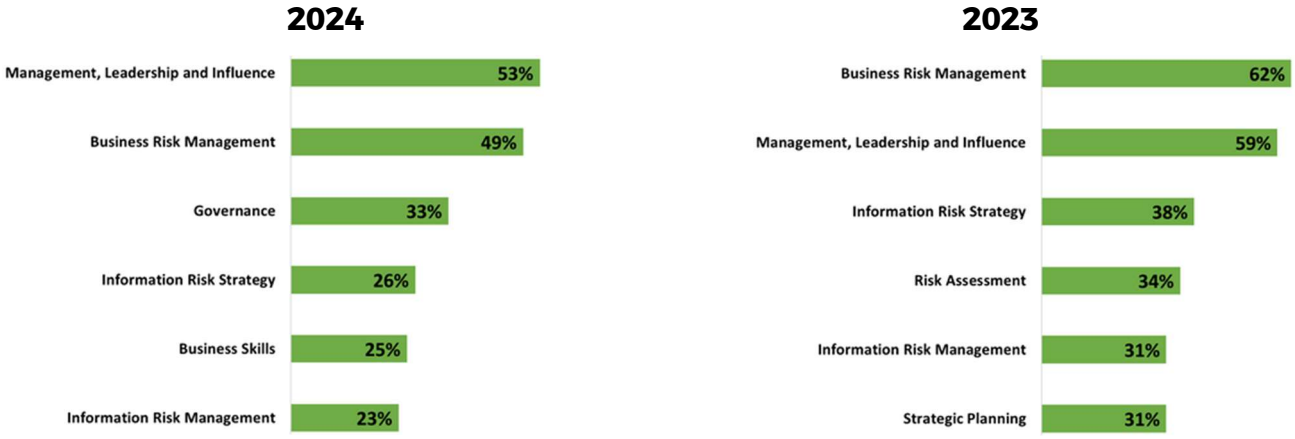
CYBER PROFESSIONALS



The prioritization of management, leadership, and influence as the most desired hard skills reflects a growing trend towards career progression into **management roles**. This is evidenced by the data showcased on the next page. The ability to effectively manage and mitigate business risks remains critical for safeguarding organizational assets and maintaining operational resilience.

Additionally, the frequent selection of governance, risk assessment, and risk strategy underscores the importance of a comprehensive approach to risk management within the cybersecurity profession. **Governance frameworks** provide the necessary structure and guidelines for implementing effective risk management practices, while risk assessment methodologies enable organizations to identify and prioritize potential threats. **Strategic risk management** ensures alignment with broader business objectives, optimizing the impact of cybersecurity initiatives.

CISOS



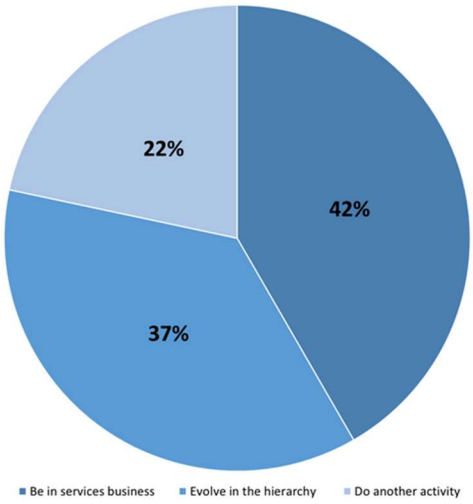
Desired skills are largely similar between cybersecurity professionals and Chief Information Security Officers. This suggests that while their responsibilities may differ, many of the most important challenges faced by both groups remain consistent.

CAREER

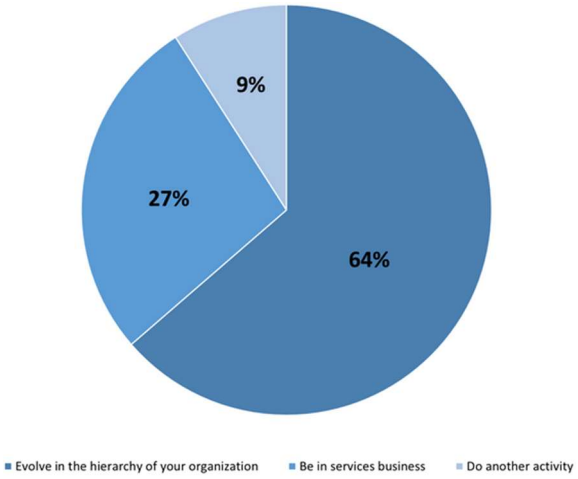
LIKELY NEXT CAREER MOVE

CYBER PROFESSIONALS

2024



2023



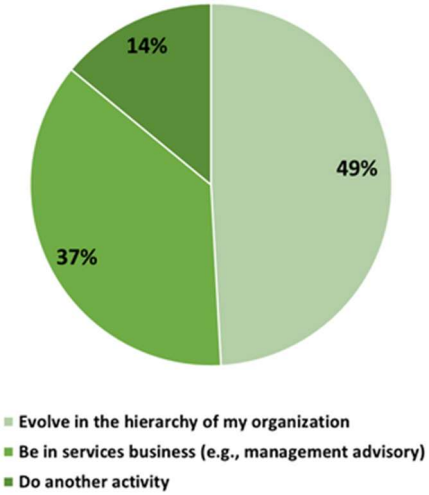
The data reveals a noteworthy shift in the career trajectories of cybersecurity professionals. A substantial proportion, accounting for 22%, now view **leaving the cybersecurity field** altogether as a natural progression, marking a significant increase from the 9% reported in 2023. This trend suggests that some professionals may be **seeking opportunities outside** of cybersecurity, either due to personal career interests or perceived limitations within the field.

Conversely, for over a third of respondents (37%), **advancing within the hierarchy** is deemed the natural course of action. This indicates a desire among many professionals to climb the ranks within the cybersecurity domain, likely aspiring to take on greater responsibilities and leadership roles.

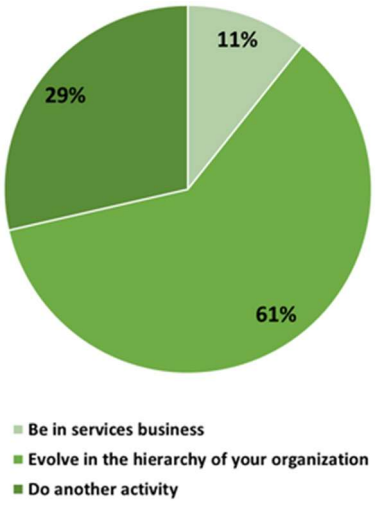
Interestingly, the largest number of respondents see a **move into business services** as the most natural progression. This suggests a growing recognition of the interconnectedness between cybersecurity and broader business functions. Transitioning into business services may allow professionals to **leverage their cybersecurity expertise** in new ways, such as consulting or advising on cybersecurity-related matters within different industries or sectors.

CISOS

2024



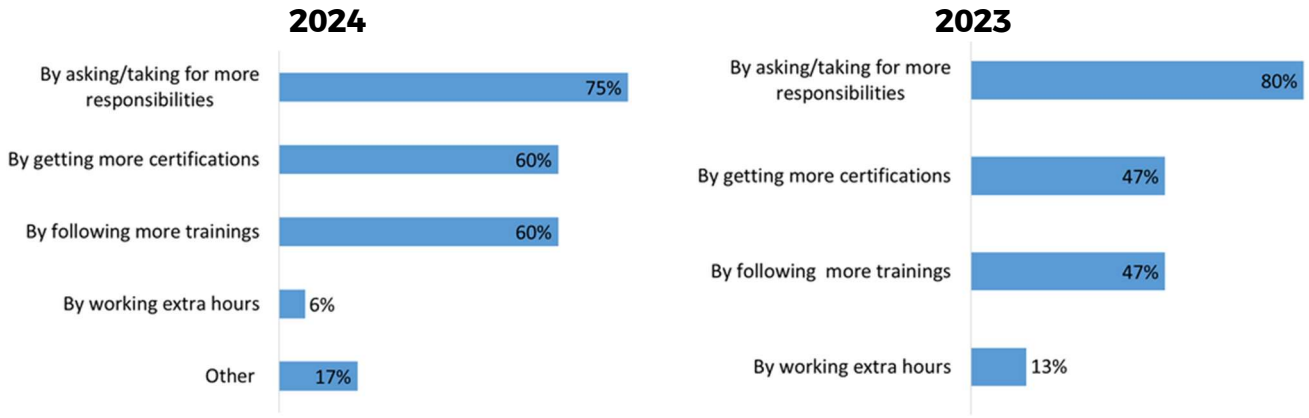
2023



In 2024, a significant number of CISOs were inclined towards transitioning into **service businesses**, possibly motivated by aspirations for broader managerial and executive roles. This shift contrasts with the previous year, where more CISOs expressed a desire to **change activities**, indicating a possible evolution in the perception and rewards associated with the CISO role or reflecting the unique challenges faced by CISOs in 2023.

ACTIONS TO INCREASE CHANCES OF PROMOTION

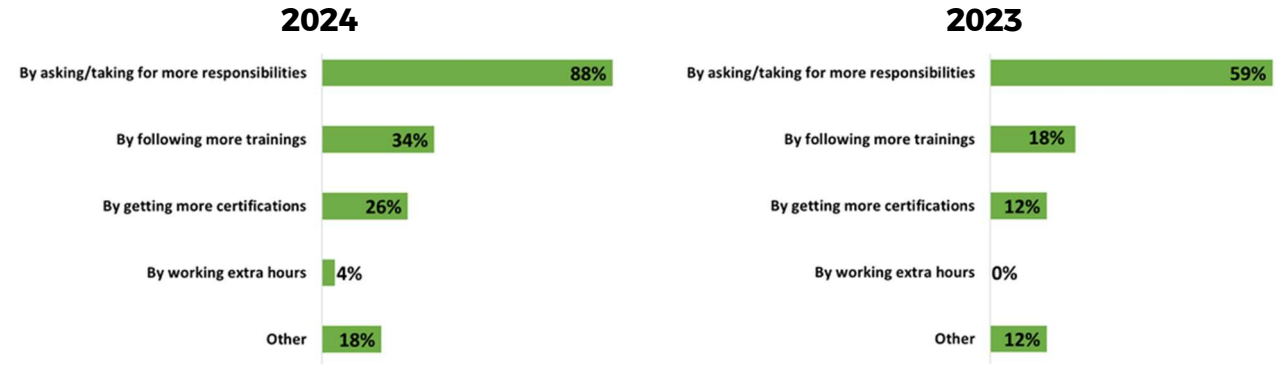
CYBERPROFESSIONALS



The data suggests that the primary strategy for increasing chances of promotion among cybersecurity professionals remains **taking on more responsibility**. This indicates a recognition among professionals that demonstrating capability and reliability in handling greater tasks and projects is a key factor in advancing their careers.

Furthermore, the popularity of acquiring **more certifications** and pursuing additional training underscores the ongoing commitment of professionals to enhancing their skills and knowledge. It's notable that only a very small percentage of professionals intend to work **extra hours** to improve their chances of promotion. This could suggest a belief that working longer hours may not necessarily increased chances of promotion, or a preference for maintaining a healthy work-life balance. The overall similarity of responses to last year's surveys shows **consistency** in how cybersecurity professionals perceive and pursue opportunities for career advancement.

CISOS

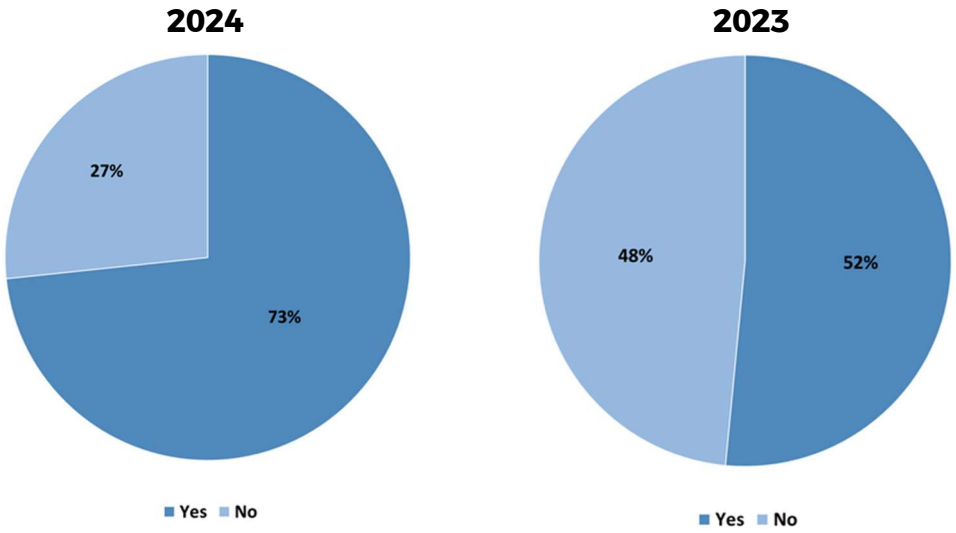


Compared to 2023, more CISO's are finding training and certification important. Taking on more responsibility remains the primary strategy for promotion, even more so than last year. This may reflect a certain **increase in competition** for access to CISO and executive management roles. The chances of a CISO moving up in the company seem to require more effort in 2024.

CAREER

ATTENDANCE TO FORMAL TRAINING

CYBERPROFESSIONALS

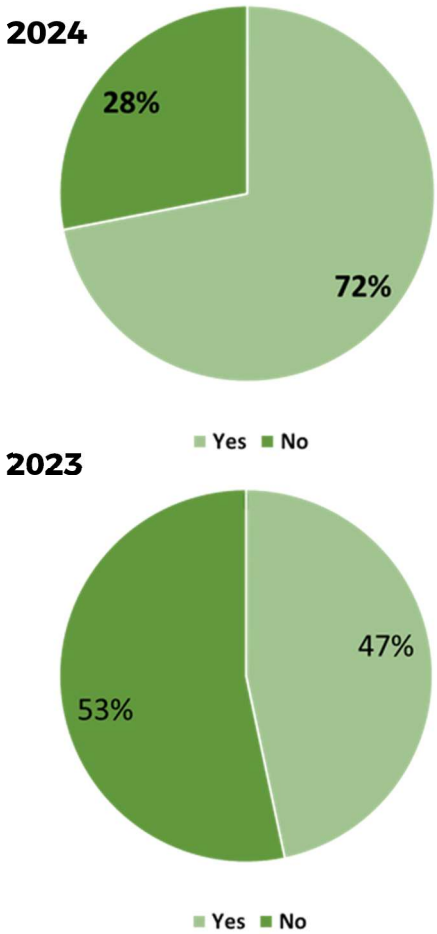


The significant increase in the proportion of cybersecurity professionals attending some form of **training** in the last three years, particularly compared to the previous year, suggests a notable shift in the industry's approach to **skill development** and education. It's possible that training became more popular in 2023 due to various factors such as increased awareness of the importance of ongoing learning, advancements in training opportunities and resources, or shifts in **organizational priorities** towards investing in employee development.

CISOS

The data reveals a significant increase in the share of CISOs who attended **formal training** in the past three years, particularly in 2024. This surge may indicate a heightened awareness and recognition of the importance of **continuous learning** and professional development within the cybersecurity field.

The notable uptick in CISOs participating in formal training programs suggests a shift towards prioritizing skill enhancement and staying abreast of the latest developments in cybersecurity practices and technologies. This increased investment in training may be driven by the **evolving nature of cyber threats** and the need for CISOs to maintain a competitive edge in addressing complex security challenges.

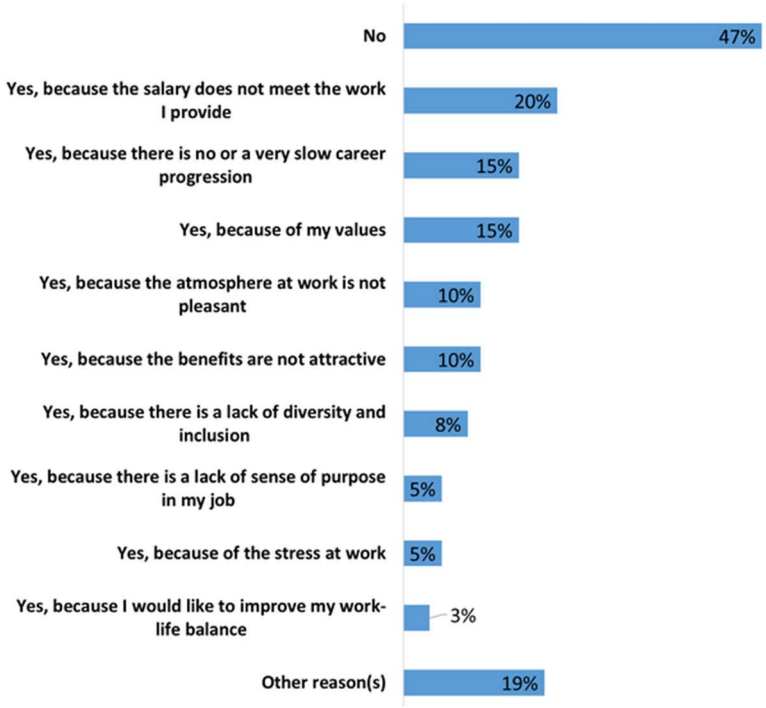


CAREER

INTENTION TO CHANGE CAREER PATH

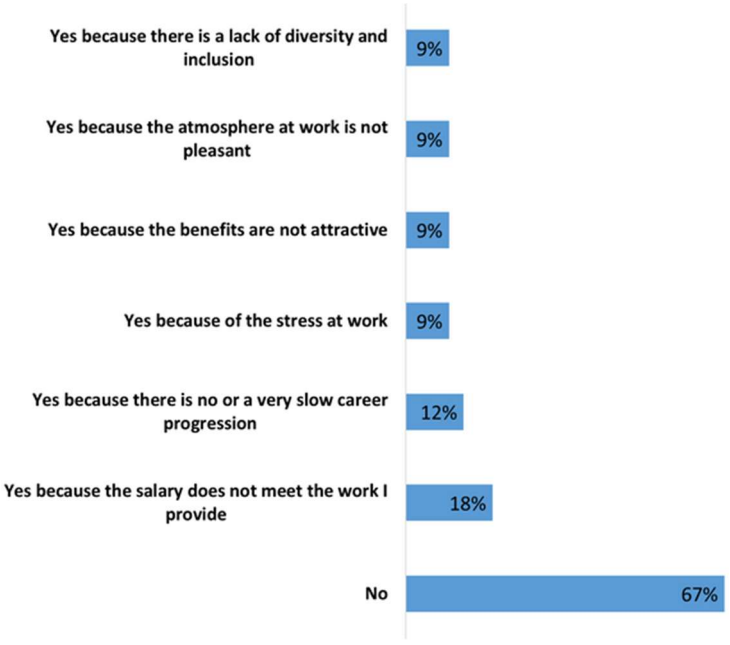
CYBER PROFESSIONALS

2024



Intention to change career path

2023



While a **significant proportion**, 47%, still intend to **remain in the cybersecurity industry**, there has been a decrease compared to the previous year's data, 67%. This shift indicates a **growing willingness** among professionals to **explore alternative career paths** or opportunities outside of the cybersecurity field.

Among those considering leaving the industry, **insufficient compensation** emerges as the primary factor, with approximately 20% citing it as a reason for their potential departure. This underscores the importance of competitive compensation packages in retaining top talent within the cybersecurity sector.

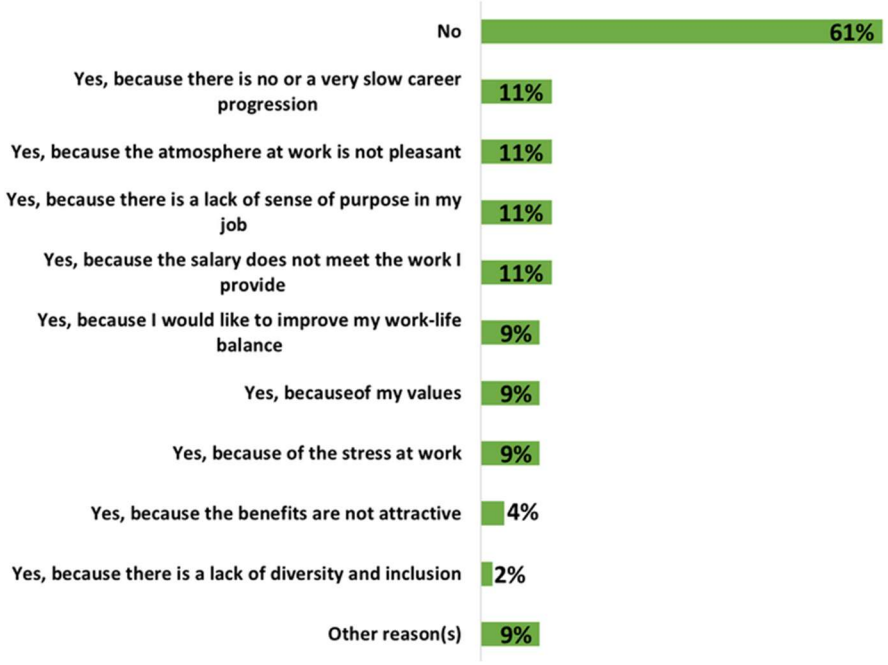
Furthermore, concerns related to **career progression, industry values, and work atmosphere** contribute to professionals' decisions to potentially leave the field. **Approximately 15% cite slow career progression**, while an equal percentage find that the industry does not align with their **values**. Additionally, 10% mention an unpleasant work atmosphere as a factor influencing their decision to seek opportunities elsewhere.

INTENTION TO CHANGE CAREER PATH

CISOS

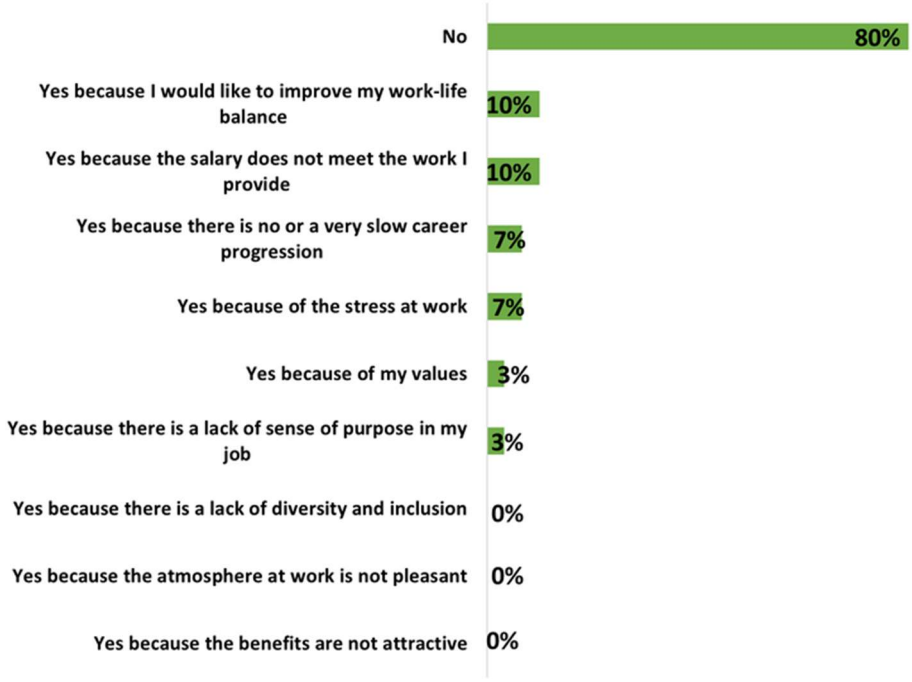
As with the professional survey, respondents could pick either "no", or several possible reasons leading to a possible career change. It appears that CISOs are **more inclined to remain in the cybersecurity industry** going forward, although a decrease in retention was also observed.

2024



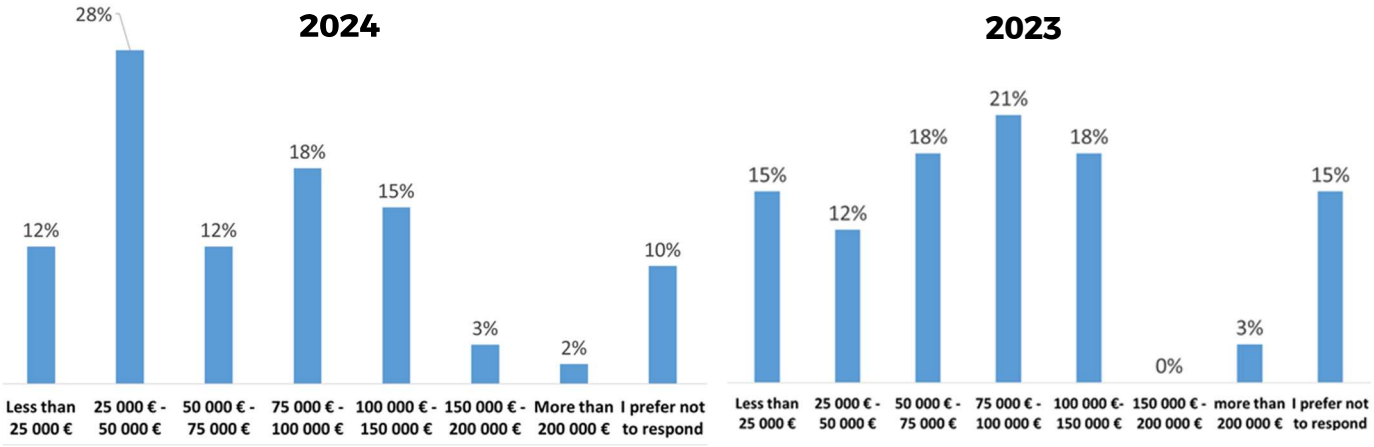
Salary and **slow career progression** emerged as significant factors influencing retention decisions among CISOs, reflecting broader concerns within the industry regarding compensation and opportunities for advancement. Additionally, **work-life balance**, **stress**, and **compensation** related matters were commonly cited by CISOs as reasons for potential departure.

Intention to change career path 2023



COMPENSATION

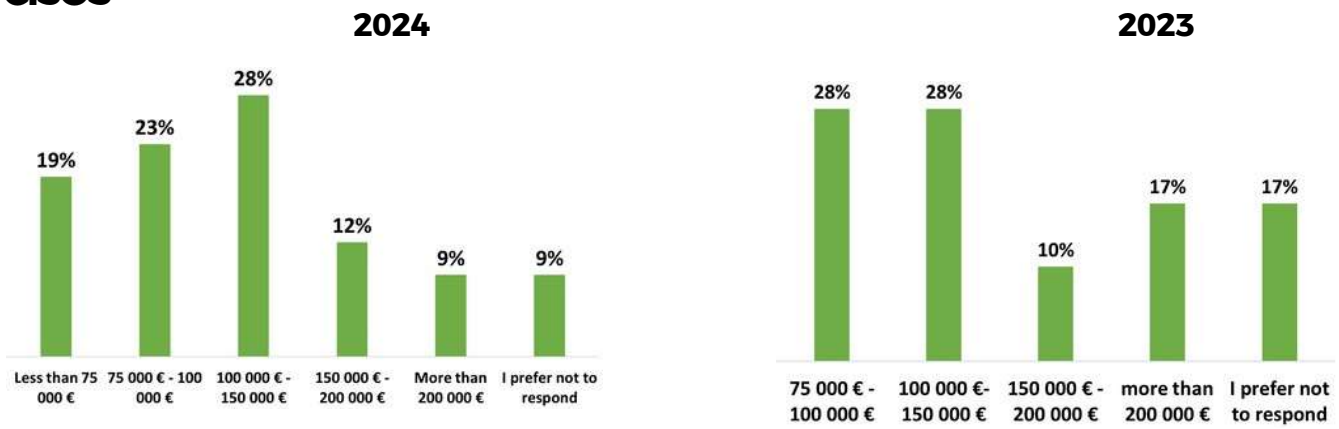
CYBER PROFESSIONALS



In examining the salary distribution, notable shifts are observed, particularly a significant **increase in the €25-50k bracket.** However, overall, the distribution appears to have maintained a degree of stability. A substantial portion of positions offer salaries of €50k or less, followed by something resembling a normal distribution centered on the €75k-100k bracket.

Furthermore, the prevalence of extremely high-paying positions, exceeding €200k, has shown consistency over the observed period. This suggests a sustained presence of such roles within the cybersecurity industry.

CISOS

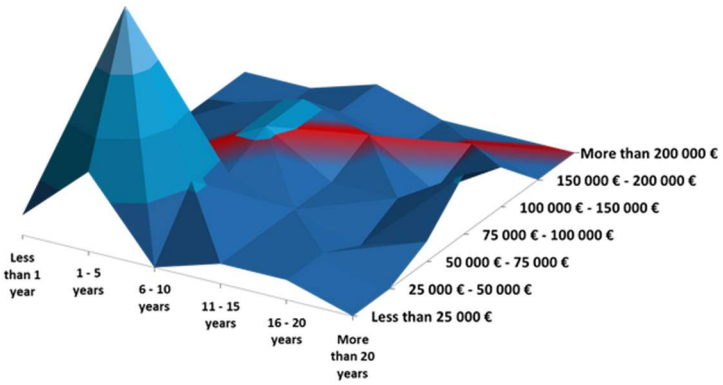


IIn comparison, CISOs' salaries are **much higher** than those of other professionals, with almost **50%** reporting an annual salary **over €100k** and only one in 5 earning less than €75k.

COMPENSATION

CYBER PROFESSIONALS 2024

Compensation with regards to **seniority**

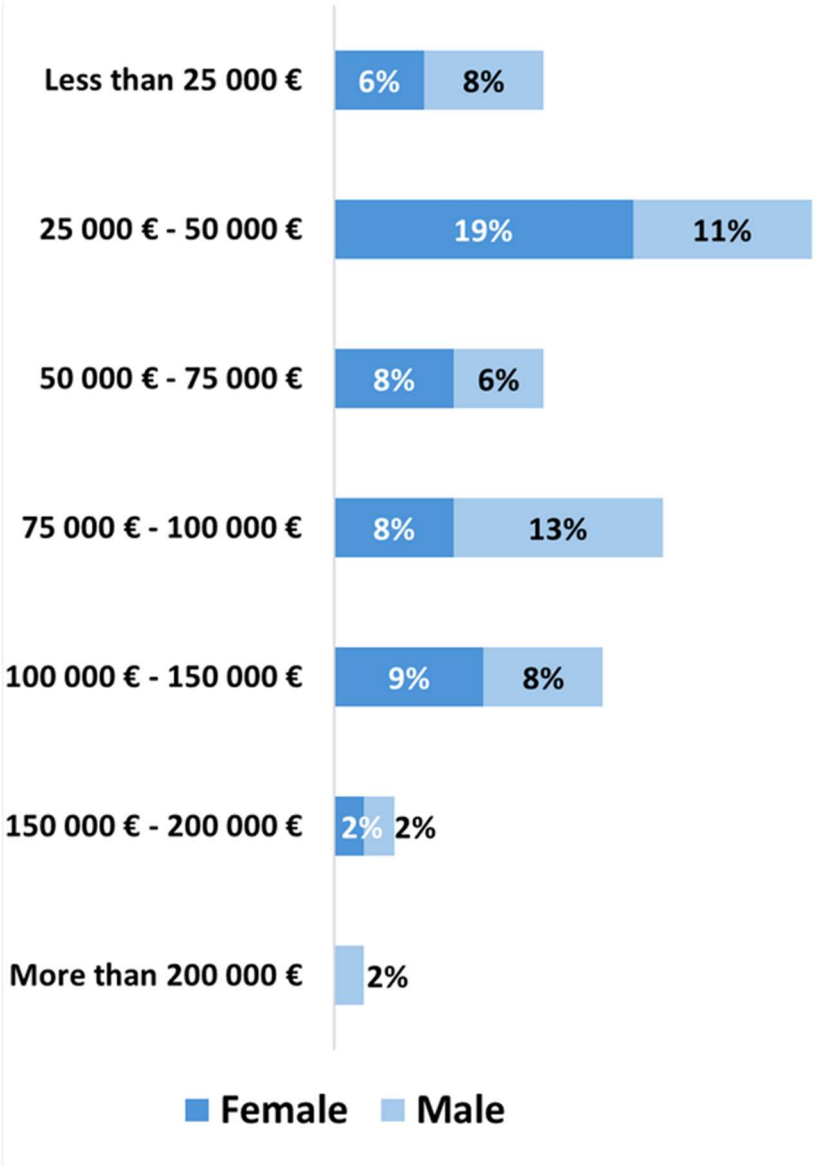


Unsurprisingly, salary correlates quite strongly with **seniority**, as indicated by the **highlighted diagonal** on the graph. This trend illustrates that more senior positions tend to command higher salaries, reflecting the increased experience and responsibilities associated with these roles.

Additionally, the graph reveals a striking concentration of individuals earning between 25-50k with 1-5 years of experience.

The gender pay gap doesn't stand out as much as one might have anticipated. In fact, within each salary tier, there's a reasonable **balance between male and female employees**, demonstrating progress toward equity.

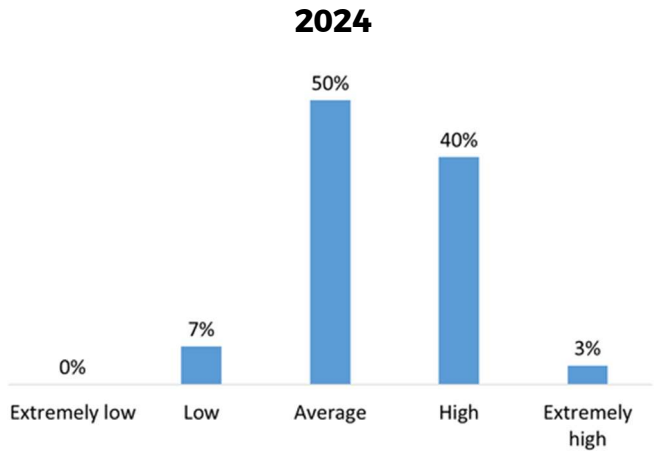
The only notable exception lies in the **highest salary** bracket, encompassing earnings above €200,000. In this category, women are completely absent, which could potentially highlight the persistent influence of the well-known **glass ceiling principle** that prevents women from breaking into the uppermost echelons of corporate compensation despite their qualifications and achievements.

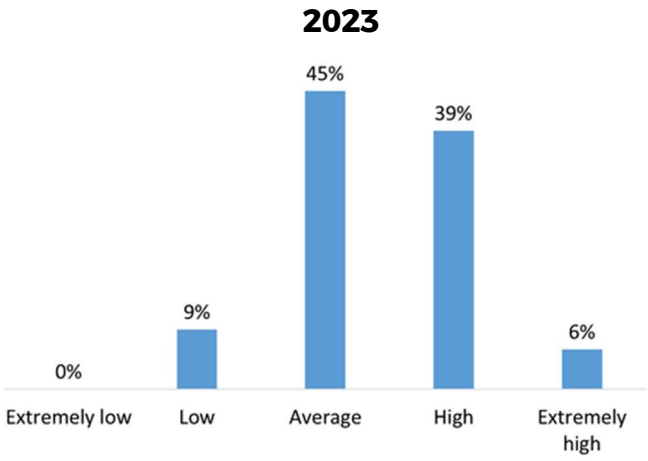


STRESS

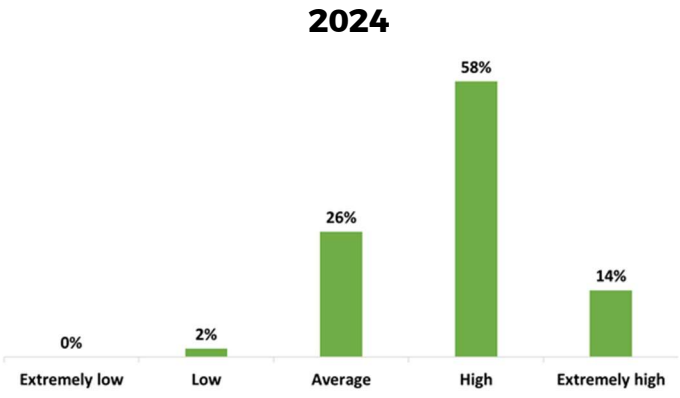
PERCEPTION OF STRESS IN THE JOB

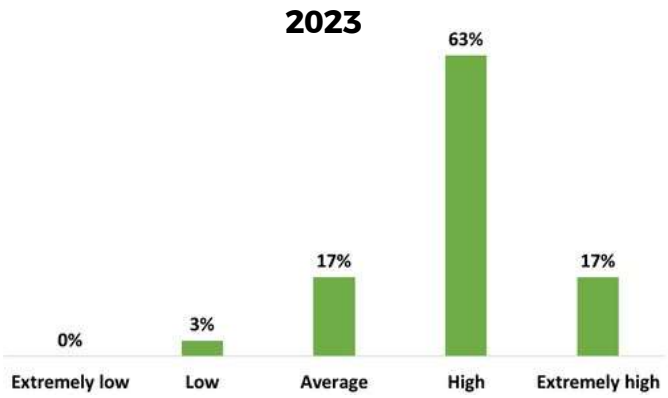
CYBER PROFESSIONALS





CISOS





Stress is indeed a common byproduct of work, particularly in **high-pressure environments** such as the cybersecurity industry where professionals often contend with the **constant threat of cyber attacks** and the **need to safeguard sensitive** information and systems.

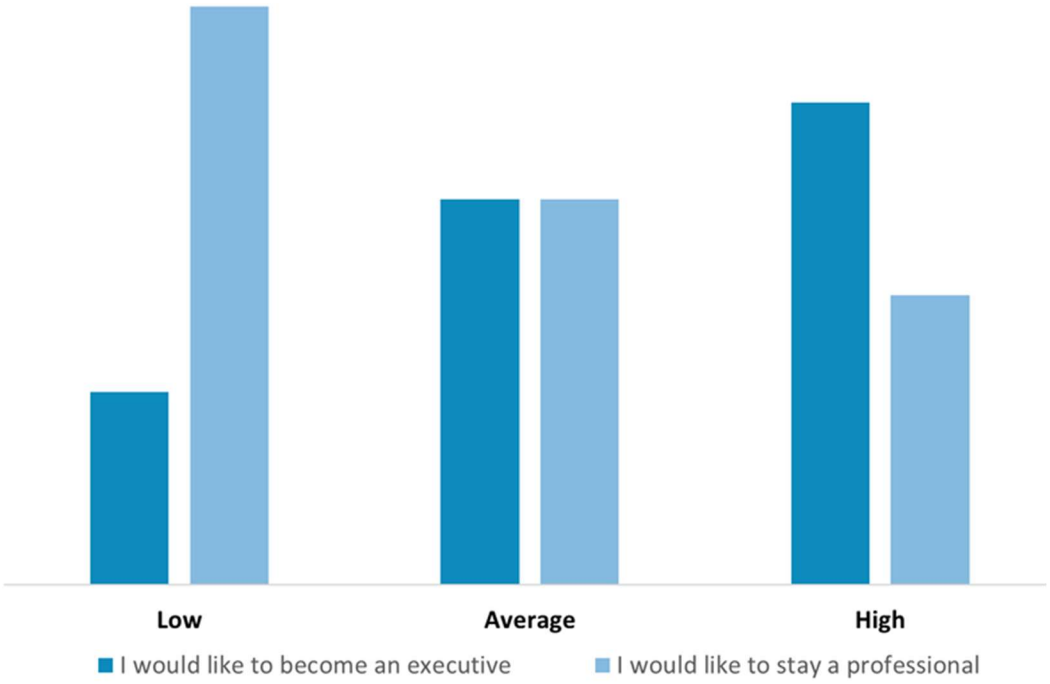
The data indicating that a **vast majority** of respondents in both 2023 and 2024 qualify their **stress levels as either average or high** underscores the persistent nature of stress within the cybersecurity profession. While some level of stress may be inherent to the nature of the work, prolonged or excessive stress can have detrimental effects on individuals' well-being, productivity, and job satisfaction.

Addressing stress in the workplace is **crucial** for promoting the health and resilience of cybersecurity professionals. This requires **proactive efforts** from organizations to implement strategies and initiatives aimed at reducing stressors and fostering a supportive work environment. This could include measures such as promoting work-life balance, providing resources for stress management and mental health support, fostering a culture of open communication and collaboration, and implementing policies to address excessive workloads or unrealistic expectations.

STRESS

PERCEPTION OF STRESS IN THE JOB

Individuals experiencing elevated stress levels are more inclined to pursue executive roles than remain in professional positions.



The data indicates a noteworthy **relationship between stress levels and career aspirations** among cybersecurity professionals. Those who report lower levels of stress tend to demonstrate a preference for staying in their current professional roles, possibly signifying a sense of contentment or satisfaction with their existing responsibilities and career paths. These individuals appear to find **stability and fulfillment** in their current positions, which likely meet their professional needs without overburdening them.

Conversely, individuals experiencing heightened stress levels seem more driven to pursue advancement into **executive positions**. This ambition for upward mobility could reflect a desire to **reshape their professional environment** or achieve greater influence, suggesting that the pressure they're currently under may be pushing them to seek roles with broader strategic control. This dynamic underscores **how stress can influence career ambitions differently**, shaping career trajectories and workplace priorities across the cybersecurity sector.

CONCLUSION

In conclusion, this report delivers a comprehensive overview of the cybersecurity landscape in Europe, emphasizing the critical role that digitalization plays in shaping the sector. The findings underscore the urgent need for a skilled workforce capable of confronting increasingly sophisticated cyber threats. The challenges faced by organizations, particularly the scarcity of skilled professionals, are highlighted through detailed survey analysis, revealing their impact on employee turnover and organizational stability.

By analyzing previous survey data alongside current findings, the report offers a comparative analysis that equips organizations to proactively strategize against evolving cyber risks. This approach provides a robust foundation for devising effective solutions and reinforces the importance of continuous skill development, workforce planning, and strategic investment in cybersecurity. Ultimately, this report serves as a strategic guide, enabling organizations to navigate the complex and dynamic cybersecurity landscape with confidence.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to Raffaele Jacovelli, Managing Director at Hightech Partners, for enabling us to participate in the analysis of the European survey of cybersecurity professionals.

We are especially grateful to our academic supervisor, Nicolas Ameye, for his invaluable guidance and unwavering support throughout this endeavor. His expertise and advice were pivotal in shaping the quality and direction of this report, and we deeply appreciate his commitment to our work.

THANK YOU!

ATAYA&PARTNERS

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

HightechPartners
TALENT | TECH | TRANSFORMATION