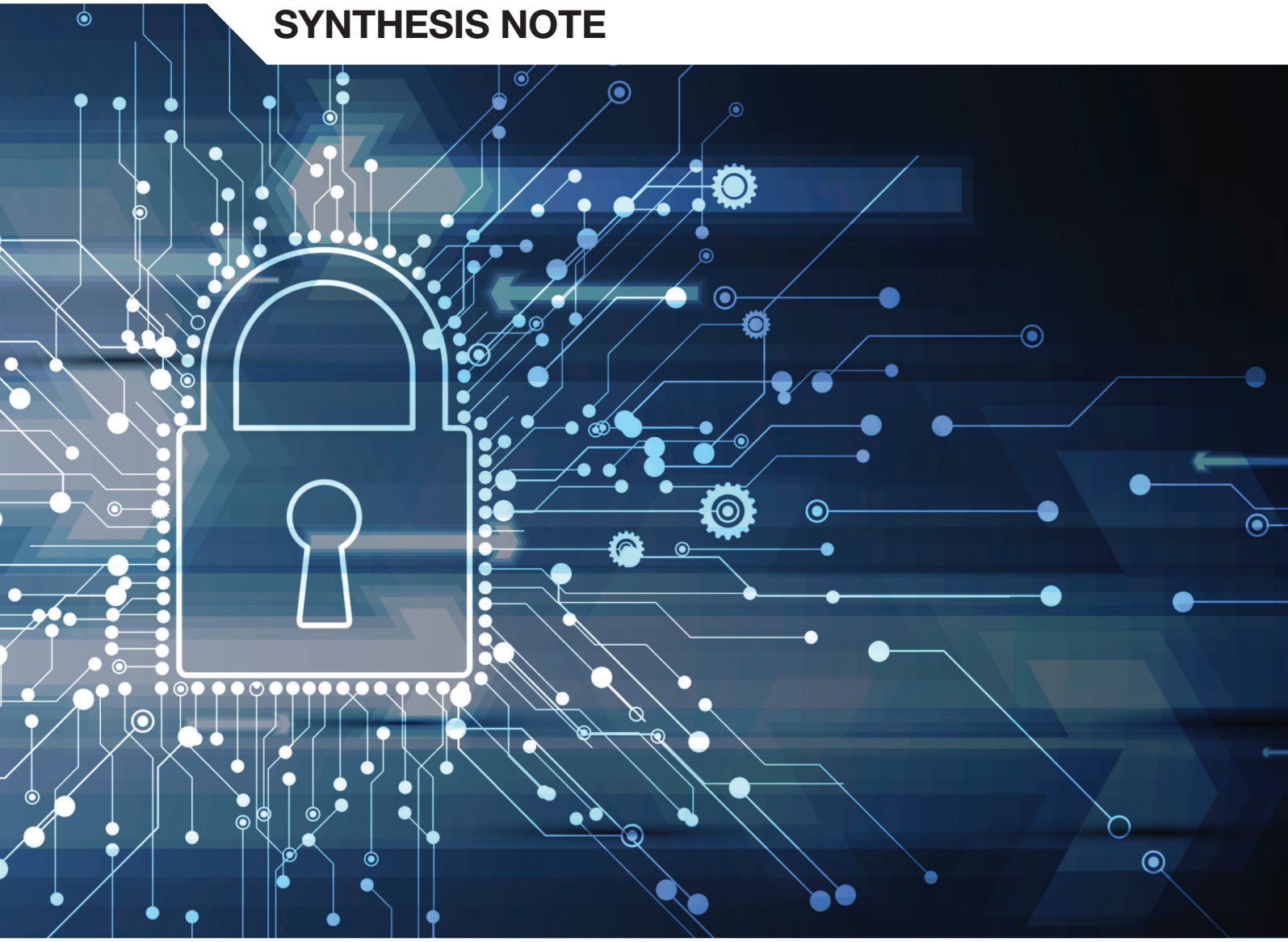
Building a Skilled Cyber Security Workforce

INSIGHTS FROM OECD COUNTRIES

SYNTHESIS NOTE



OECD

Building a Skilled Cyber Security Workforce

INSIGHTS FROM OECD COUNTRIES

SYNTHESIS NOTE

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Member countries of the OECD.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Photo credits: Cover © vs148/Shutterstock.com.

Key policy points for building a skilled cyber security workforce

- **Structured Characterisation of the Cyber Security Profession:** Develop a detailed framework that categorises various cyber security roles and their skill requirements. This should involve a collaborative effort among stakeholders to create a standardised taxonomy and roadmap. Such a framework can help in clearly understanding the profession's dynamics and designing targeted policies to address labour shortages and align training with industry needs. An example is the National Initiative for Cybersecurity Education (NICE) framework in the United States, which provides a comprehensive way to identify, recruit, and retain cyber security talent.
- **Proactive Skills Assessment and Response:** Establish centralised platforms for continuous data gathering and analysis to proactively anticipate and respond to evolving cyber security skills needs. Involving public authorities, industry bodies, and educational institutions in this process ensures a cohesive approach to understanding and adapting to the sector's rapidly changing requirements. An example is CyberSeek, an interactive tool that provides detailed data about supply and demand in the cyber security job market.
- **Enhanced Career Guidance and Awareness:** Strengthen career guidance initiatives to help individuals understand the diverse opportunities in cyber security and the educational paths leading to them. Additionally, raise awareness among employers, especially SMEs, about the value of a skilled cyber security workforce, encouraging adherence to established cyber security frameworks and standards. Programmes like Cyber security Career Awareness Week in England (United Kingdom) can play a crucial role in this regard.
- **Promotion of Cyber Security as a Career Choice:** Government-led campaigns and educational initiatives should highlight cyber security as a compelling career path. This includes showcasing diverse roles within the sector and providing interactive learning experiences to attract more individuals into the field. France's "The Tomorrow Cyber Specialist" initiative serves as an excellent model for such campaigns.
- **Gender Diversity and Inclusion Initiatives:** Implement targeted programmes like mentorship schemes to support women entering the cyber security field. Programmes like the Women in Cybersecurity (WiCyS) Cybersecurity Mentorship Pilot Programmes are instrumental in developing skills, building networks and enhancing confidence among aspiring female professionals. Showcasing successful women in cyber security can also motivate more women to join the sector.
- **Building Strong Digital Foundations:** Provide accessible digital literacy programmes, especially for disadvantaged groups, to lay the groundwork for advanced cyber security training. In Colombia, NODO, a flexible ICT learning centre, offers free core courses and various learning pathways with modules ranging from basic to advanced topics. Students can take levelling classes based on their skills for a smooth learning progression, emphasising real-life application.
- **Expanding Apprenticeship and Work-Based Learning:** Collaborate with employers to design apprenticeships that offer practical experience and align with real-world job requirements. The NCSC's CyberFirst Degree Apprenticeship programme in the United Kingdom is a prime example of such an initiative, combining on-the-job training with a clear career pathway in cyber security.
- **Short, Targeted Non-Formal Programmes with Industry Collaboration:** Develop brief, focused non-formal programmes in partnership with industry leaders to rapidly address specific skill gaps. These programmes should be directly linked to particular cyber security roles and act

as supplements to formal education. The SANS Institute's Cyber Workforce Academy in England (United Kingdom) is a notable example of this approach.

- **Involvement of Industry Professionals in Education:** Facilitate the participation of industry professionals in cyber security education as teachers or curriculum advisors. By reducing regulatory barriers, these professionals can offer practical insights and current industry knowledge to students. École 42 in France, where industry experts actively contribute to curriculum development and teaching, illustrates the effectiveness of this strategy.

Building a skilled cyber security workforce: Insights from OECD countries

The advent of new technologies like cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) has brought significant benefits to an increasingly interconnected society. However, their widespread use also escalates the risk of cyberattacks. The shift to remote work during the COVID-19 pandemic further increased vulnerabilities to cyber threats, affecting businesses and individuals globally. This has increased the demand for cyber security professionals, leading to notable shortages in the cyber security labour market worldwide.

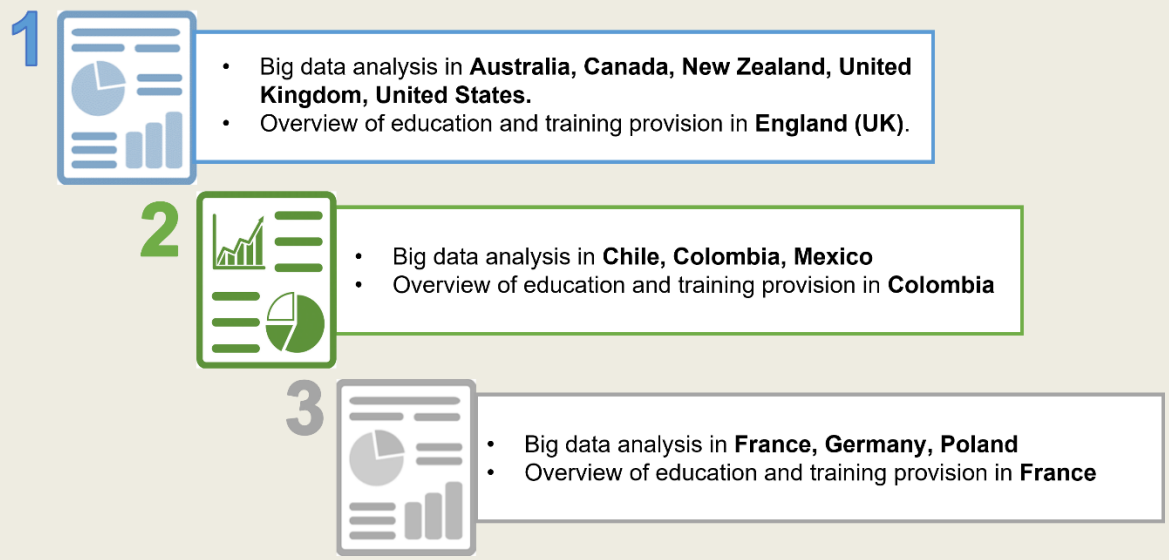
Given the substantial costs associated with cyber threats, it is crucial for policy makers and businesses to gain detailed insights into their vulnerabilities and identify areas needing more resources. Understanding the supply and demand dynamics of the cyber security labour market, including the skills required, is essential in addressing these skill shortages.

The OECD's "Building a Skilled Cyber Security Workforce" project is a key initiative in this context. The project analyses the global demand for various cyber security roles and identifies the corresponding educational and skill requirements. The project also evaluates how different countries' education and training systems are preparing individuals with these technical skills. Furthermore, it facilitates an informal forum for dialogue and discussion on best practices and future requirements in cyber security skills. This synthesis note summarises the main findings from three reports covering three different regions. The first one focuses on Australia, Canada, New Zealand, the United Kingdom and the United States (henceforth referred to as the countries of the Five Eyes alliance). The second and third reports cover Latin America (i.e. Chile, Colombia and Mexico) and Europe (i.e. France, Germany and Poland), respectively. Each report dives into the case studies to analyse the landscape of cyber security education and training provision in England (United Kingdom), Colombia and France (see Box 1).

Box 1. The "Building a Skilled Cyber Security Workforce" project

The project is segmented into three components that blend big data intelligence with policy analysis to examine the demand and supply of cyber security skills, as well as the policies and strategies in place to grow and diversify the cyber security workforce, thereby addressing cyber security skill deficits. Each of these three parts zooms in on different geographical areas (see Figure 1), investigating three to five countries for the demand-side analysis and a single country for an in-depth case study on the supply side. The first report was published in March 2023, the second in September 2023 and the third in February 2024 (OECD, 2023[1]) (OECD, 2023[2]) (OECD, 2024[3]).

Figure 1. Outputs of the cyber security project



Understanding the growing demand for cyber security professionals

The demand for cyber security professionals has seen a significant surge in the Five Eyes, Latin American, and European countries, driven largely by the rapid digital transformation that has increased the connectivity and digital reliance of businesses and governments. This transformation, coupled with the COVID-19 pandemic's push towards remote work, has heightened vulnerabilities to cyber threats leading to an acceleration in the demand for cyber security experts.

This rising demand has outstripped the growth in other occupations in most of the countries analysed in the project (see Box 2). Specifically, Canada, Chile, Mexico, New Zealand and Poland experienced notable increases in the demand for cyber security professionals. This growth is partly a response to enhanced national strategies focusing on cyber security and the efforts to develop a safe cyberspace environment. Interestingly, some countries like Chile and Mexico, initially lagging in the volume of new cyber security job vacancies published on line, have begun catching up with more mature and larger cyber security markets like the United States and Germany.

The increasing demand encompasses a range of different roles in the cyber security profession, with cyber security architects, engineers, and analysts being at the core of this demand. Results for Canada and Colombia, in particular, indicate a notable demand for cyber security analysts, who play a crucial role in

system security planning, operations, and maintenance. In Australia and New Zealand, managers are among the most demanded roles, indicating strong employers' interest in those positions involved in decision-making tasks within the cyber security team structure. Results for Germany show a high demand for auditors and advisors. This role encompasses professionals dedicated to providing both internal and external guidance on the efficiency and compliance of security solutions.

Geographically, the demand for cyber security professionals is concentrated in major urban areas, where large enterprises and government entities are usually located. However, results show that in some of the countries from the Five Eyes alliance, there is a trend towards geographic diversification as the need for cyber security expertise spreads across various economic sectors and regions. This is the case of the United Kingdom, where the geographical concentration of cyber security online job postings (OJPs) in London decreased by 10 percentage points in between 2012 and 2021. A more geographically widespread demand for cyber security professionals highlights the growing recognition of cyber security as a vital element of digital resilience in our interconnected world.

Box 2. Tracking the demand data for cyber security professionals through the lens of big data intelligence

The analysis of big data, and in particular the study of the information contained in online job postings (OJPs) has been instrumental in tracking labour market developments in the three reports of the project "Building a Skilled Cyber Security Workforce", (see (OECD, 2022[4]; OECD, 2023[5]; OECD, 2024[3])). Data on OJPs have been collected by Lightcast.[1] The data contain a variety of information including the geographical location of the new job posting (i.e. region and city), the occupation and industry identifiers (i.e. job title, enterprise, occupational codes from national and Lightcast taxonomies, etc.), and the job requirements (i.e. education, experience, skills, among other characteristics).

- The report "Building a Skilled Cyber Security Workforce in Five Countries" uses data from January 2012 to June 2022. In total, more than 400 milllion job postings are used, coming from Australia, Canada, New Zealand, the United Kingdom and the United States.
- The report "Building a Skilled Cyber Security Workforce in Latin America" looks at Chile, Colombia, and Mexico in 2021 and 2022, using data from nearly 14 million OJPs over a two-year period.
- The report "Building a Skilled Cyber Security Workforce in Europe" utilises data extracted from nearly 82 million OJPs sourced from France, Germany and Poland in between January 2018 and June 2023.

Delving deeper into skills requirements in the cyber security profession

The adoption of digital technologies and the emergence of cyber threats have transformed the cyber security job market. Such a fast and dynamic market comes with challenges both for employers, in identifying the skills and experience requirements that meet their needs, and for workers, who may face difficulties entering in the cyber security labour market and deciding what skills to develop in their professional career.

Qualifications, certifications and experience are key factors in candidate selection globally. Education requirements in the cyber security profession vary, but often include tertiary education, particularly bachelor's or master's degrees. The job market shows, instead, limited opportunities for less experienced or lower educated individuals.

Specifically, in the Five Eyes countries, a bachelor's degree is a frequent requirement, while in the three countries from Latin America, familiarity with cyber security frameworks and certifications, which are mostly offered through non-formal training, are emphasised. Technical knowledge in computing systems and IT networks is essential, with skills in programming, scripting, ethical hacking, and specific software applications varying by country. Knowledge of network protocols and frameworks is also crucial, with regional variations in areas of specialisation. For instance, the ISO 27 000 standard, a very well-known guideline for IT security, is frequently required in the Latin American countries covered in the project, while its relevance is lower in the European countries.

Professional skills encompass broader skills not limited to a particular job or discipline, but applicable in various situations or work environments. In the cyber security profession, analytical, problem-solving and strategic thinking abilities, are highly valued. Communication and persuasion skills are particularly important in the countries from the Five Eyes alliance and Poland, signaling the need for cyber security teams to interact and communicate effectively. Insights from the project also show that European cyber security professionals are expected to understand business processes and strategies. This result can be influenced by the share of OJPs seeking managers or auditors/advisors in France and Germany, roles that are more specialised in the strategic management of cyber security teams. In Latin America, proficiency in English is a notable requirement due to the dominance of English-language training resources and standards. Overall, results indicate that the cyber security job market demands a combination of technical expertise and professional skills, with variations across countries which depends on the maturity of the market, technological adoption and specific characteristics of the region under consideration.

Establishing a framework for dynamic skills development in cyber security

A better understanding of the cyber security profession and the skill requirements needed to deal with cyberattacks globally requires multilevel international stakeholder co-ordination. This demands co-ordinated efforts from international bodies (e.g. European Network and Information Security Agency, ENISA; Organisation of American States, OAS) governments, businesses, civil society, and individuals for establishing dynamic skills frameworks and occupational standards in this field. National cyber security strategies play a pivotal role by uniting stakeholders, allocating resources and emphasising education, training, research, public-private partnerships, regulatory frameworks and international co-operation. Skills frameworks can contribute in aligning the demand for skills with the offerings of educational and training institutions, bringing consistency, relevance and standardisation to the field.

Globally, joint initiatives in public and private sectors devise cyber security skills strategies. Many countries participating in the "Building a Skilled Cyber Security Workforce" project have national strategies or policies. The United Kingdom and the United States, for instance, have established comprehensive national strategies to address cyber security challenges, including skill gaps. Policies in Latin American countries covered in this project focused on risk management and combating cyber threats but, more recently, they have shifted towards enhancing citizens' cyber competence and developing the cyber security industry. France's "France 2030" strategy includes a significant investment in the cyber security sector to stimulate economically the cyber security sector, strengthen the cyber security workforce, increase the development of cyber security solutions within the country and strengthen the government's resilience against cyber threats. Germany and Poland have integrated cyber security into broader national security strategies. The Polish strategy objective is to enhance resilience against cyber threats, strengthen defensive capabilities and improve information. The German strategy actively modernises the government's cyber security infrastructure and enhance its cyber defence capabilities.

The adoption of cyber security skills frameworks is key to defining relevant skills for various roles and experience levels. In the countries from the Five Eyes alliance, the National Institute of Standards and Technology (NIST) Cybersecurity Framework from the United States, developed collaboratively with

industry, sets standards and best practices for managing cyber risks and aids in communication among stakeholders. Though US-centric, it is influential internationally. The National Initiative for Cybersecurity Education (NICE) Framework, another US initiative, concentrates on workforce aspects, offering a universal language for categorising and understanding cyber security roles. Countries like Australia, and Canada have adapted it for their own programmes, underscoring its value in building a skilled workforce. Latin American countries, though not formally adopting these frameworks, could benefit from such unified approaches. In Europe, the European Cybersecurity Skills Framework (ECSF) helps articulate tasks, competencies and skills for European cyber security professionals.

Providing education and training in cyber security

Education and training to develop the right cyber security skills are crucial for tackling shortages and avoiding cyber security risks. Various education and training pathways lead into cyber security roles, offering opportunities for progression. In the three countries selected for the case studies – England (United Kingdom), Colombia, and France – both formal and non-formal education and training opportunities are available in the cyber security field. These opportunities vary in difficulty level and come in a wide range of formats to meet learners' skills needs and employers' requirements. Depending on the education system's structure (see Box 3), cyber security education and training programmes are available at an early stage, embedded in vocational upper secondary education, or later through more specialised higher education programmes. Non-formal training offerings also vary in levels of difficulty, content, duration and types of certification awarded.

Box 3. Understanding formal education provision in cyber security, in selected OECD countries

Cyber security education programmes take many forms within the formal education systems of the countries analysed in this project. In most cases, foundational cyber security programmes are covered through upper secondary vocational education (equivalent to ISCED 3) and postsecondary and short tertiary cycle programmes (ISCED 4 and 5, respectively). In some cases, specific initial technical training in cyber security starts at the higher education level, including bachelor's or even master's programmes. To understand and compare the different degrees offered, their levels of difficulty and the learning pathways discussed in this sythnesis note for England (United Kingdom), Colombia, and France, Table 1 presents a summary of the relevant levels of education and programmes offered in each country, placing them in terms of their respective ISCED levels.

Table 1. Formal degrees and qualifications available in the field of cyber security in England (United Kingdom), Colombia and France

ISCED level equivalent	England (United Kingdom)	Colombia	France
ISCED 3	T-levels, Level A and Level 3 qualifications	Technical upper secondary education	Vocational and Technological Baccalaureate
ISCED 4	Not available	Not available	University Techology Diploma, DUT (available until 2021)*
ISCED 5	Higher technical qualifications	Professional technical and technologist programmes	Brevet de Technicien Superieur, BTS
ISCED 6	Bachelor's programme	Undergraduate programme	Professional, Academic and Technology (BUT) Bachelors
ISCED 7 and 8	Master's and doctoral programmes	Specialisation, Master's and doctoral programmes	Engineering, master's, specialised masters and doctoral programmes.

Note: The “Diplôme Universitaire de Technologie” (DUT) in France was undergoing a transition in the academic year 2021-22. The DUT was being replaced by the “Bachelor Universitaire de Technologie” (BUT), a new three-year degree programme introduced to align with the European Higher Education Area’s Bologna Process.

In England (United Kingdom), Colombia, and France, the provision of cyber security education within formal education systems exhibits common characteristics as well as distinct approaches. Common across these three countries is the emphasis on diverse educational and training pathways leading to cyber security roles, reflecting the growing demand for such skills in the global labour market. Each country offers opportunities for progression in this field, integrating cyber security modules at various educational levels. Additionally, all three countries have reported increasing enrollment in cyber security programmes, indicative of rising awareness and interest in this field.

However, there are notable differences in their approaches. England’s education system provides a wide range of classroom-based programmes and apprenticeships in cyber security at intermediate, advanced and degree levels (e.g. cyber security technologist qualification), enabling learners to develop skills on the job. Colombia’s approach emphasises foundational information and communication technology (ICT) education at an early stage in upper secondary education and more specialised technical cyber security skills through undergraduate programmes in higher education (e.g. technological programmes). France, meanwhile, integrates basic technical cyber security skills and concepts into vocational upper secondary education (e.g. Vocational Baccalaureate in cyber security, IT and networks, and electronics, CIEL), facilitating transitions to more specialised and advanced training in the field. These variations reflect each country’s unique educational philosophy and labour market requirements, shaping how cyber security education is delivered and experienced by learners.

Young people and adults can also engage with cyber security non-formal training courses which tend to be shorter, and more flexible than formal education programmes. In England (United Kingdom), non-formal training includes government-funded Skills Bootcamps and a wide array of online courses, focusing on providing sector-specific skills and initial steps into cyber security for those with varying levels of experience. Colombia’s approach involves diploma certificates offered by higher education institutions, blending practical training with case studies and group discussions and varying in difficulty and specialisation. France also offers non-formal training, including professional certificates and specialised training modules through continuing education, as well as a plethora of online courses, all contributing to the rapidly expanding landscape of cyber security education.

In the cyber security sector, a common challenge remains regarding the provision of education and training in the three countries: educational pathways lack alignment with the predominant skill and qualification requirements widening the skills shortages in the field. The analysis of online job postings (OJPs) highlights the necessity for specialised non-formal training, particularly in Colombia, where certifications and technical skills like ISO/IEC 27 001 and Security Information and Event Management (SIEM) are in high demand. However, this training requires experience and advanced prior qualifications such as post-secondary and higher education degrees. In England (United Kingdom) and France, a substantial number of cyber security job postings requires at least one year of experience, indicating a preference for candidates with higher education and substantial experience. This emphasis on advanced qualifications and experience creates a challenge for new entrants to the field, contributing to the creation of barriers to entry which, in turn, reinforce the existing shortage of skilled cyber security professionals. The complexity and advanced nature of tasks in cyber security roles, underscored by the focus on specific certifications and technical expertise, indicate the necessity for more sophisticated educational backgrounds. This trend implies that in environments where higher degrees are in high demand, cyber security jobs are likely more intricate, necessitating enhancements in the provision of cyber security education and training programmes to keep pace with the demand for a highly skilled cyber security workforce.

Making cyber security education and training more inclusive and flexible

Efforts to increase the accessibility and diversity of cyber security education have been a focal point in various countries, with specific initiatives targeting disadvantaged groups and women. Gender stereotypes, along with multiple barriers to enrollment in cyber security programmes (e.g. digital literacy, financial constraints), are faced by students, especially among the most disadvantaged or minority groups, leading to their under-representation in the cyber security sector. Addressing these issues to ensure that the cyber security profession is more representative of the population it serves is crucial. This is not only beneficial for gaining diverse perspectives and ideas that an inclusive workforce can bring, but also essential for expanding the cyber security workforce, which is facing a shortage of highly skilled professionals.

The strategies implemented in England (United Kingdom), Colombia, and France offer valuable insights into diversifying and making the cyber security workforce more inclusive. Expanding access to education and training in cyber security across different demographic groups is key. England's approach, which includes providing clear career information, financial incentives and targeted initiatives for under-represented groups such as women, highlights the need for tailored strategies to engage diverse populations. Colombia's focus on developing basic digital skills among the wider population and removing barriers to entry, like financial constraints, underlines the importance of building awareness and interest in cyber security. France's use of quotas in higher education programmes illustrates an approach to promote pathways in an inclusive manner and address the lack of socio-economic diversity. Collectively, these strategies underscore the need for a multifaceted approach that combines educational opportunities, policy interventions and industry partnerships to create a more diverse and inclusive cyber security workforce.

Enhancing the employer's role in the design and delivery of learning opportunities in cyber security

Involving employers in the design of cyber security education and training programmes is imperative to understand and develop the knowledge and skills that learners need, especially in such a fast-changing sector. Employers play a key role in providing work-based learning opportunities in cyber security, given the high levels of skill shortages. Similarly, they often remain unaware of the relevance of certifications. This requires raising awareness about the varied training ecosystem in the field of cyber security and the advantages of certifications in signaling skills and competencies.

Initiatives in England (United Kingdom), Colombia and France exemplify the importance of employer involvement in cyber security training programmes. It is imperative to establish a close collaboration between educational institutions and industry to ensure that learning programmes are tailored to the actual needs of the labour market. England's emphasis on engaging employers in the design of cyber security programmes and apprenticeships highlights the value of aligning education with diverse industry requirements. Colombia's approach, focusing on partnerships for custom training programmes and addressing teacher shortages, demonstrates the importance of industry involvement in both content and delivery. France's model of integrating industry professionals directly into the teaching workforce through flexible regulations points to innovative solutions for keeping educational programmes abreast of recent developments in the field. Collectively, these strategies reveal that effective cyber security education hinges on a symbiotic relationship between training providers and industry, ensuring that learning opportunities are current, practical and directly relevant to the evolving demands of the cyber security sector.

References

OECD (2024), *Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/3673cd60-en. [3]

OECD (2023), *Big Data Intelligence on Skills Demand and Training in Umbria*, OECD Publishing, Paris, https://doi.org/10.1787/4bbbbfd6-en. [5]

OECD (2023), *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, the United Kingdom, and the United States*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. [1]

OECD (2023), *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/9400ab5c-en. [2]

OECD (2022), *Skills for the Digital Transition: Assessing Recent Trends Using Big Data*, OECD Publishing, Paris, https://doi.org/10.1787/38c36777-en. [4]

Note

[1] See https://lightcast.io

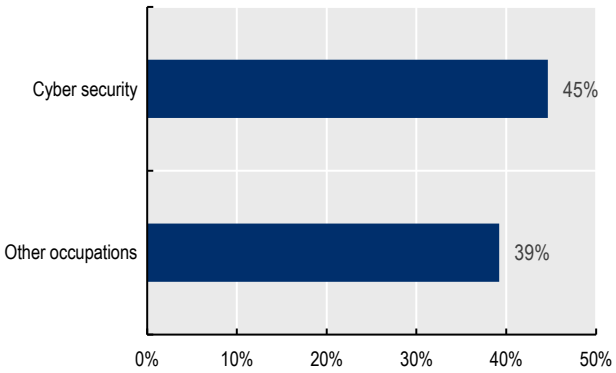
AUSTRALIA

The demand for cyber security professionals in Australia, measured by the number of job postings advertised online, has shown **a steady upward trend since 2017**. After the 2020 pandemic, the number of job postings experienced rapid growth which **peaked at the end of 2021**.

Recent growth

2019H1 vs 2022H1

- The demand for cyber security professionals grew 45% between the first half of 2019 and 2022. This growth is slightly above the average of the rest of the professions suggesting that the cyber security profession has followed the overall trends of the Australian labour market demand.

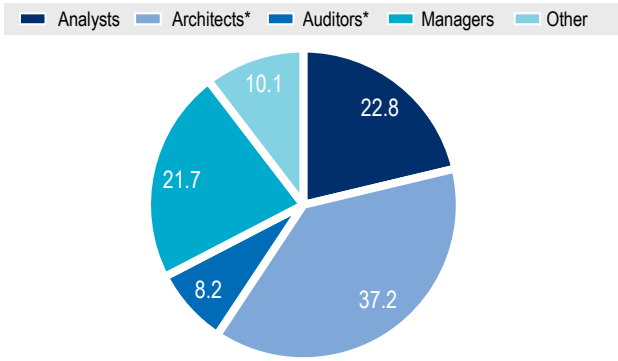


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

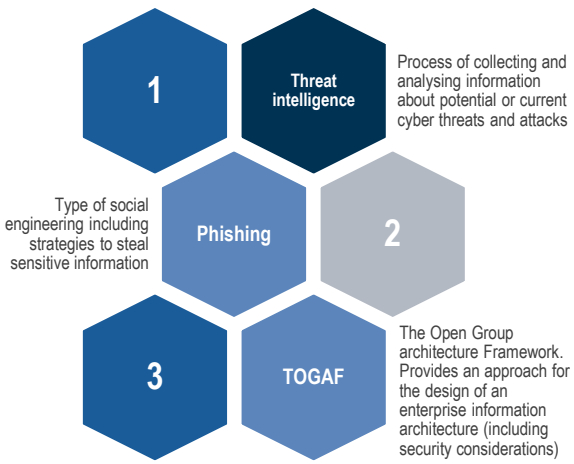
Average share 2019 - 2022H1

- Highly technical roles, such as architects and analysts represent nearly 60% of the demand for cyber security professionals. Some positions in these roles are, for instance, network security engineers and information security analysts. Managers represent an additional 22% of the cyber security online demand.

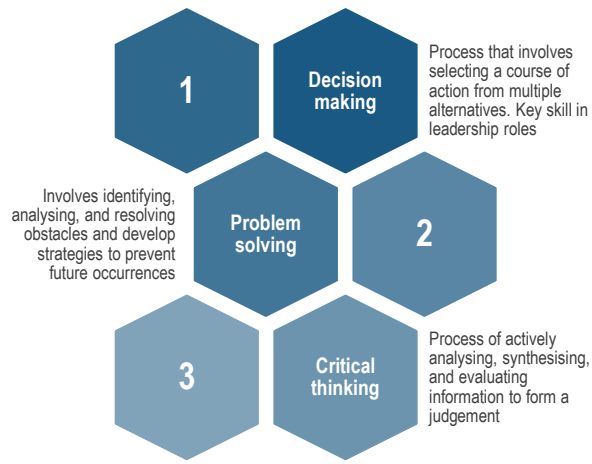


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2021)



Professional skills and abilities (2021)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

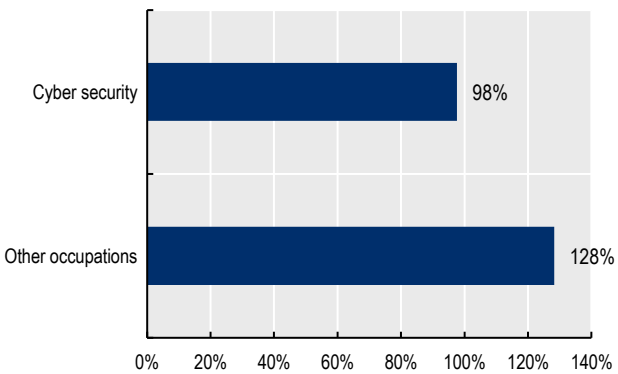
CANADA

The demand for cyber security professionals in Canada, measured by the number of job postings advertised online, has shown a **steady upward trend after the 2020 pandemic**. This is in line with the increasing trend in overall demand in the Canadian labour market.

Recent growth

2019H1 vs 2022H1

- Labour market demand in Canada, as measured by the number of job postings advertised, has shown a significant expansion after the 2020 pandemic. The cyber security profession has been part of this trend with a growth of 98% in between the first half of 2019 and 2022.

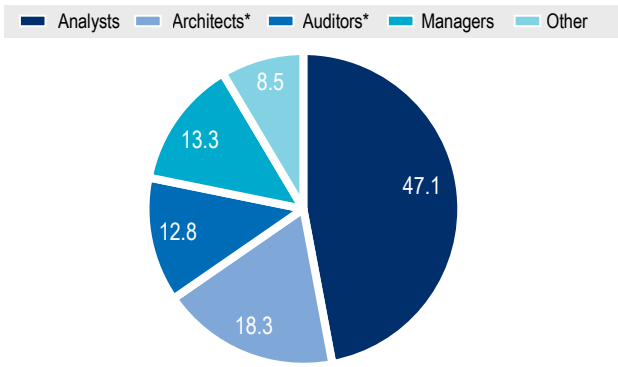


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

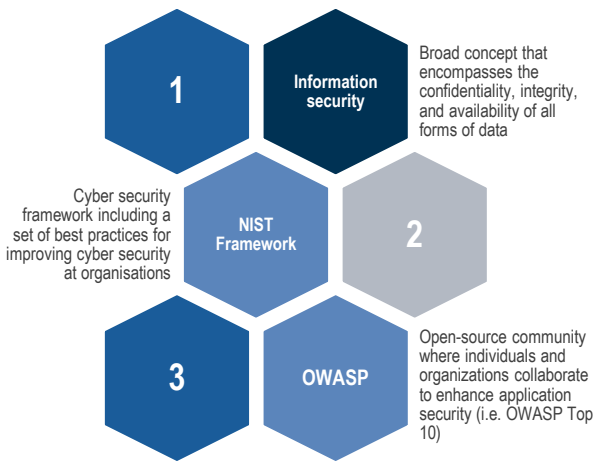
Average share 2019 - 2022H1

- In contrast with most of the countries analysed in this project, Canada exhibits a high demand for cyber security analysts, representing nearly 50% of the demand in recent years. Examples of positions included in this role are security analysts and cyber security specialists.

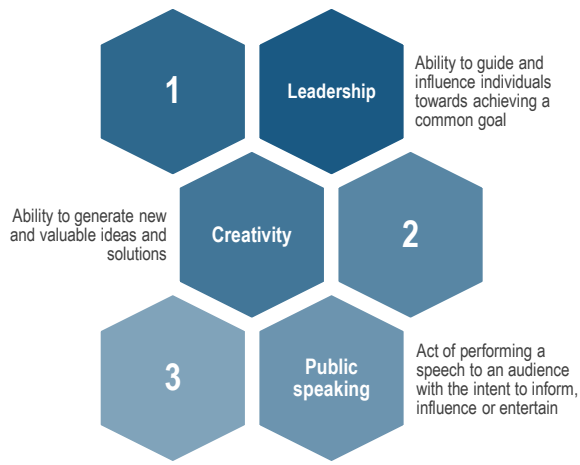


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2021)



Professional skills and abilities (2021)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

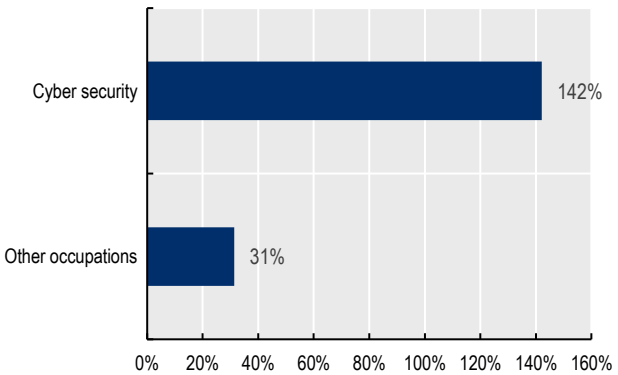
NEW ZEALAND

The demand for cyber security professionals in New Zealand, measured by the number of job postings advertised online, has **steadily increased since 2019**. In consequence, the annual share of cyber security job postings over the total has doubled in between 2019 and 2022.

Recent growth

2019H1 vs 2022H1

- Cyber security job postings have significantly grown in recent years. The share of cyber security job postings over the total nearly doubled in between the first half of 2019 (0.08%) and 2022 (0.15%). This share is still below that for other countries (UK or USA), suggesting there is still potential to grow.

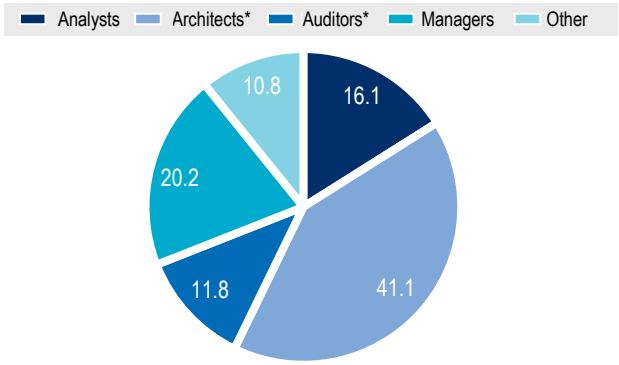


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

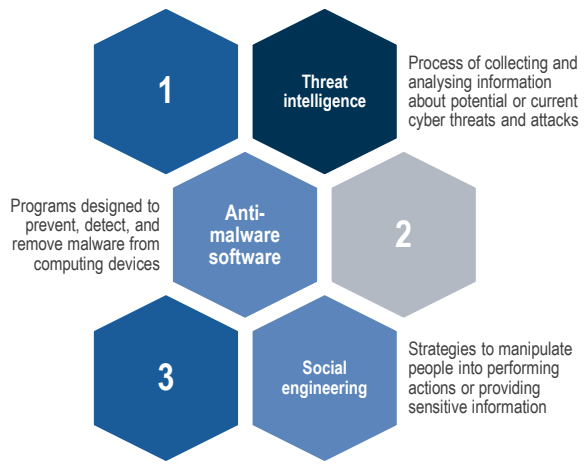
Average share 2019 - 2022H1

- Architects and managers represent more than 60% of the demand for cyber security positions. Specifically, the demand for managers in New Zealand is higher than in most of the countries analysed in this project. Some examples of management positions are information security manager and IT security lead.



Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2021)



Professional skills and abilities (2021)

Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

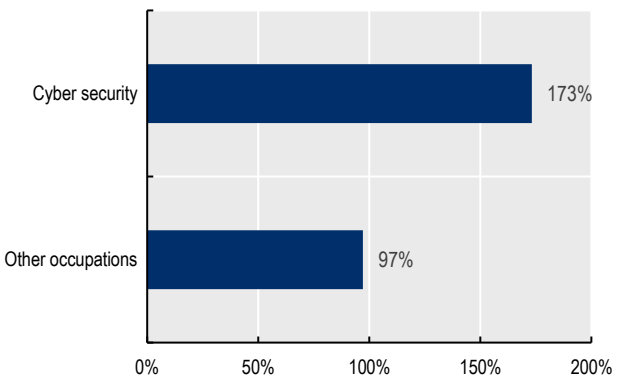
UNITED KINGDOM

The demand for cyber security professionals in the United Kingdom, measured by the number of job postings advertised online, has shown a **strong growth after 2019**, following the decreasing trend that characterised the 2017-2019 period.

Recent growth

2019H1 vs 2022H1

- Cyber security job postings have grown well above the rest of occupations in between the first half of 2019 and 2022. Even though the overall labour market demand has also experienced substantial growth, the demand for cyber security professional significantly accelerated after the 2020 pandemic.

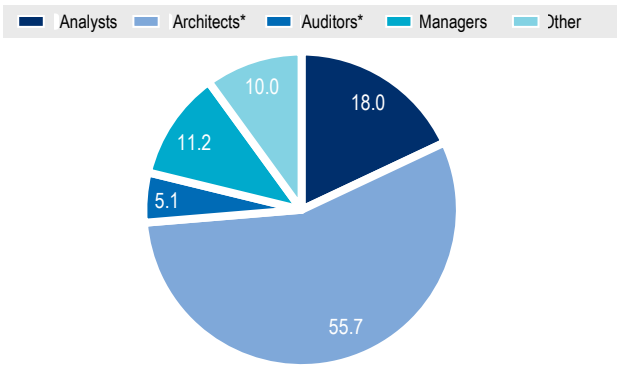


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

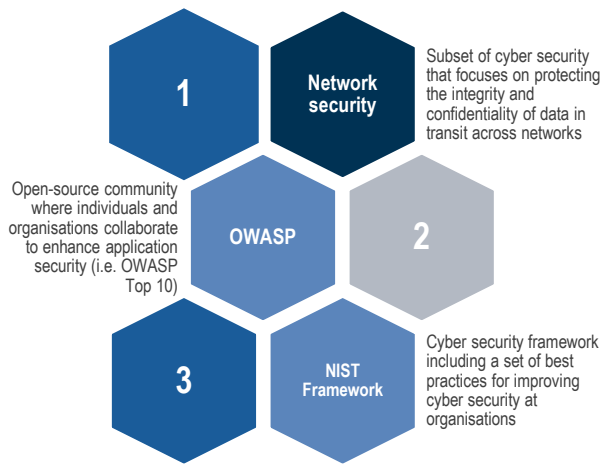
Average share 2019 - 2022H1

- Architects and engineers represents nearly 60% of the demand for cyber security professionals. This result is well above of the average share for this role in the countries analysed in this project (38%). Some positions advertised in this role are cloud security architects and information security engineers.

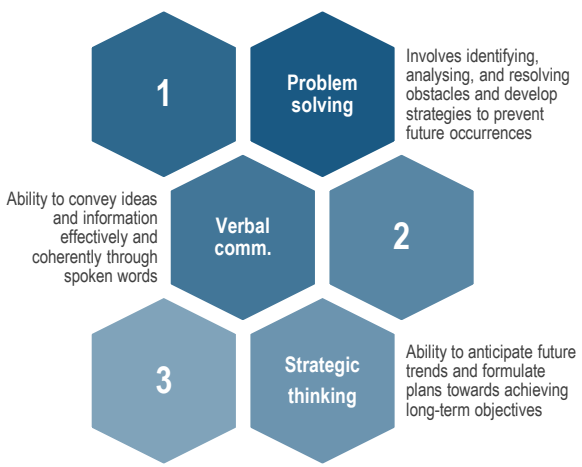


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2021)



Professional skills and abilities (2021)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

ENGLAND (UNITED KINGDOM)

Insights on education and training provision

- England offers various pathways into cyber security roles, including formal education leading to qualifications like bachelor's degrees from Further Education (FE) and Higher Education (HE) institutions, and non-formal training like bootcamps.
- There has been an increase in enrolment for cyber security programmes in further and higher education, though numbers remain relatively limited. This includes basic cyber security skills at lower education levels and apprenticeship opportunities for on-the-job skill development.
- Non-formal training such as Skills Bootcamps, which are flexible and can last up to 16 weeks, are provided by the Department for Education and private providers. These are aimed at building sector-specific skills and are often fully government-funded.
- The cyber security workforce in England lacks diversity, with only 22% women, and even fewer in senior roles. Factors contributing to this include a lack of female role models, unconscious bias in recruitment, and a general unawareness of available opportunities.
- The government has implemented multiple policies and strategies to expand and diversify the cyber security workforce. These include providing clear information about careers, financial incentives, and subsidies, especially targeting disadvantaged groups and women, to increase participation in cyber security education and training.

Interesting practices from England

- **Apprenticeships in the cyber security field** combine practical training on the job with off-the job training, allowing apprentices to gain job-specific skills while working alongside experienced staff from the sector in addition to the more theoretical aspects of cyber security. They are available at different levels of qualification. Enrolment in cyber security apprenticeships increased strongly in the last five years.
- **CyberFirst** is a programme led by the National Cyber Security Centre (NCSC) which aims to develop the United Kingdom's next generation of cyber security professionals through bursaries, free courses for 11 17 year olds and competitions. The programme provides opportunities for young people to explore their passion for tech applied to the fast-paced cyber security sector.
- **CyberFirst Girls** is a complementary programme to CyberFirst focused on demystifying the idea that only boys can succeed in IT, especially in the cyber security sector. The programme includes a CyberFirst Girls competition which aims to support girls interested in a career in cyber security. Additionally, NCSC offers the CyberFirst girls' development day, where girls can have interactive learning experiences and witness inspirational speeches from women leaders in the cyber industry. This event helps girls to have a better understanding of the learning and aspirational possibilities.
- **Department for Education Skills Bootcamps** are free, flexible courses of up to 16 weeks at various levels, available in England, allowing people to build up sector-specific skills and fast-track to a job interview with a local employer once the training is completed. The courses are open to adults aged 19+.
- **Cyber security career route map** is a website developed by the UK Cyber Security Council that provides detailed information about the different areas of specialisation in cyber security. It also suggests learning pathways for individuals interested in a specific field. The information shown for each area of specialisation includes characteristics of the role, skills and knowledge required and helpful information to enter the specialisation.
- **NCSC certification** is a certification of cyber security apprenticeships, bachelor's, master's and integrated master's degrees with well-defined and relevant content delivered to an appropriate standard. Working in partnership with the DCMS, Cabinet Office, and UK Research and Innovation, the NCSC certifies programmes across higher education institutions that better respond to cyber security standards established by CyBOK and the national cyber security priorities. This certification should help students differentiate between the many cyber security degrees on offer and employers distinguish between applicants' qualifications.

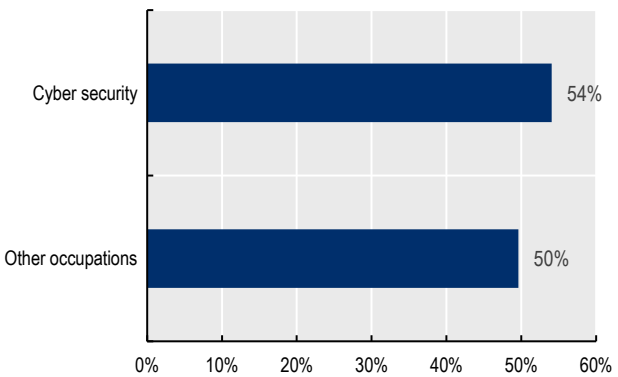
UNITED STATES

The demand for cyber security professionals in the United States, measured by the number of job postings advertised online, has shown **an upward trend in line with the overall expansion of the demand in the US labour market**.

Recent growth

2019H1 vs 2022H1

- The demand for cyber security professionals follows similar trends than that for the rest of occupations, growing 54% in between the 2019H1 and 2022H1. As USA is one of the most established cyber security markets in the world, its expansion may be more aligned with overall labour market trends.

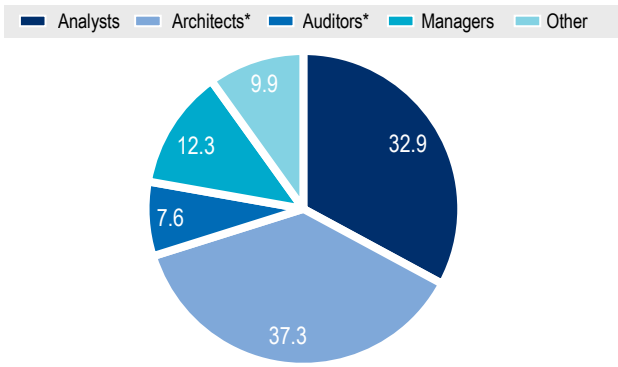


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

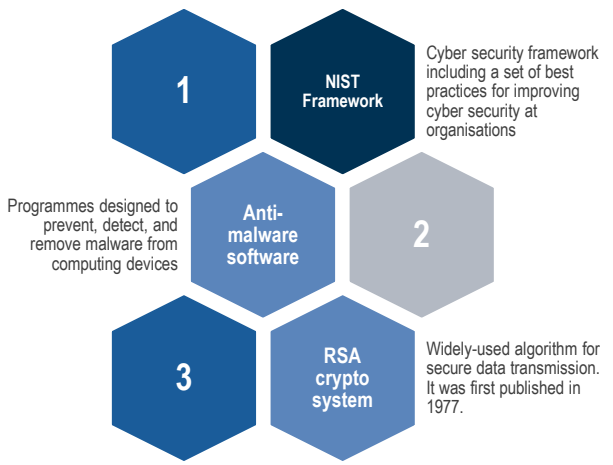
Average share 2019 - 2022H1

- Cyber security architects/engineers and analysts represent nearly 70% of the demand for cyber security professionals in the United States. These roles include positions such as Information security specialists and network security engineers.



Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2021)



Professional skills and abilities (2021)

Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

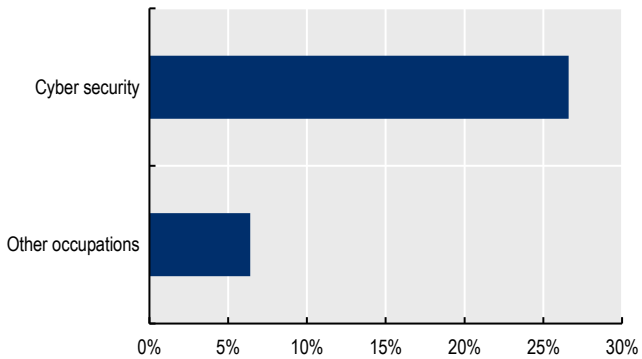
CHILE

In total, the analysis uses 2.9 million online job postings across all jobs to investigate the demand for cyber security professionals in Chile between January 2021 and December 2022.

Recent growth

2021H1 vs 2022H1

- The demand for cyber security professionals in Chile grew by 28.7%, a substantially higher growth rate than for other professions (2.9%). There is an increasing emphasis in Chile on developing its cyber ecosystem in recent years. The National Cyber Security Policy 2017-2022 identified concrete goals of promoting a free, open, safe and resilient cyberspace

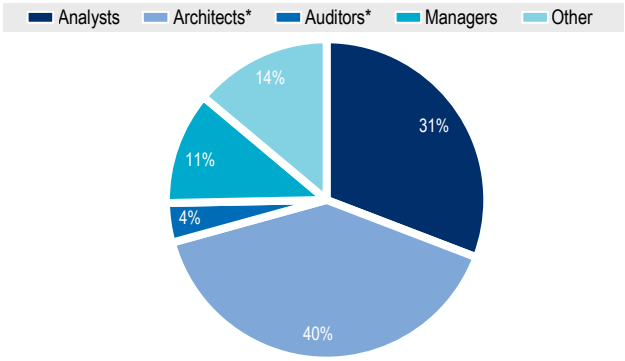


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

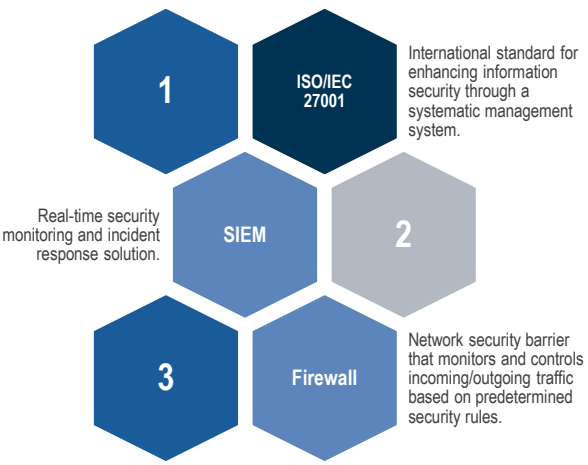
Average share 2021 - 2022

- The demand for cyber security architects/engineers is particularly strong in Chile where they represent 40% of the total number of OJPs advertised during 2021 and 2022. This group also had a strong growth of 38% in between those two years. The role of auditors and advisors by contrast, was the only role to see a significant decrease in 2022 compared to 2021.

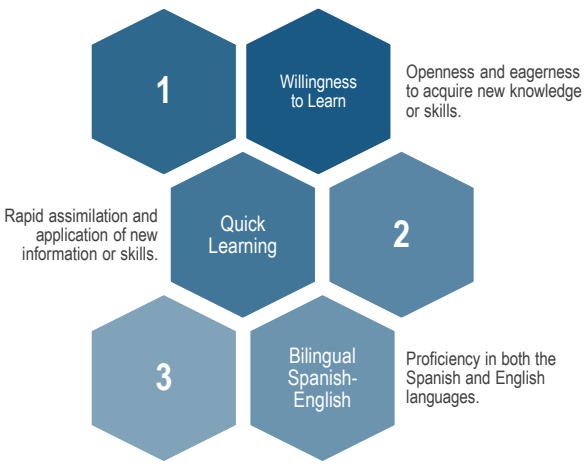


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2022)



Professional skills and abilities (2022)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

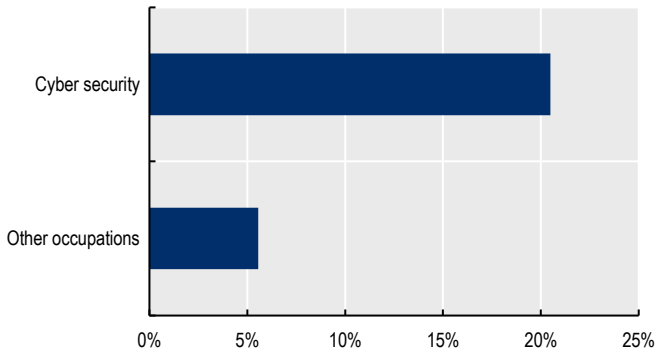
COLOMBIA

In total, the analysis uses 3.6 million online job postings across all jobs to investigate the demand for cyber security professionals in Colombia between January 2021 and December 2022.

Recent growth

2021H1 vs 2022H1

- Between 2021 and 2022 the number of cyber security Online Job postings (OJPs) grew at a significant rate of 21%, similar to the growth rate of non-cyber security roles. This can be linked to the improvements in the cyber security regulatory framework that have been ongoing for more than a decade.

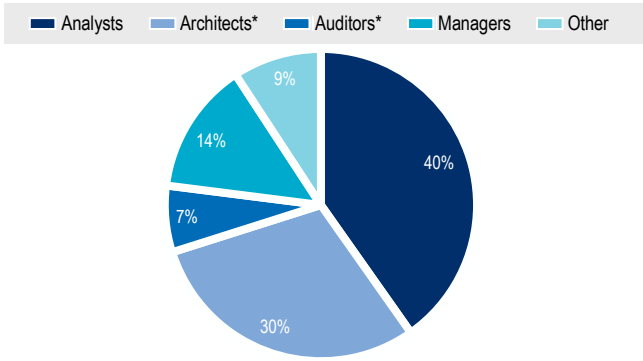


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

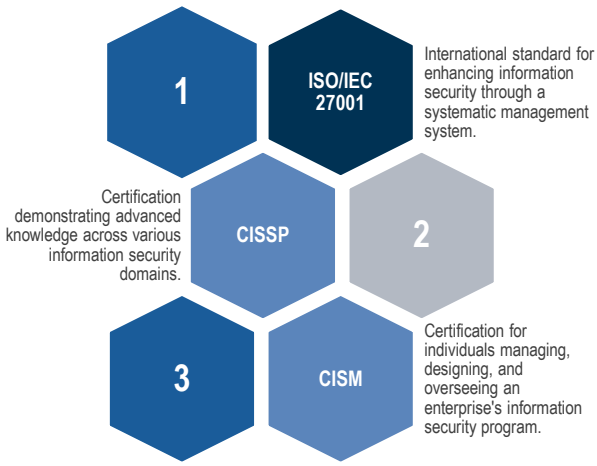
Average share 2021 - 2022

- Cyber security analysts, which provide insights to support planning, operations and maintenance of systems security, represent the largest share of OJPs. However, this role experienced a decrease in new OJPs by 4% between 2021 and 2022.



Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2022)



Professional skills and abilities (2022)

Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

COLOMBIA

Insights on education and training provision

- Colombia offers various educational and training pathways into cyber security roles, including both vocational and undergraduate programmes recognised by the National Ministry of Education (MEN). These range from practice-oriented technical courses to more theoretical undergraduate programmes.
- Vocational programmes focus on practical training for cyber security operations and management, taking 2-3 years to complete. Undergraduate programmes, on the other hand, delve into theoretical foundations, emphasising research, innovation, and critical thinking.
- In addition to formal education, Colombia provides non-formal training opportunities, often in the form of diploma certificates. These courses, offered by both public and private institutions, range from basic cyber security concepts to advanced topics aligned with industry standards.
- Colombia has developed national strategies to strengthen responses to cyber threats and enhance capabilities in the sector. This includes increasing flexibility in higher education and innovative strategies to address teacher shortages in ICT, aiming to cater to a diverse group of learners.
- The country focuses on developing basic digital skills across the population, fostering interest in cyber security training. Policies to eliminate barriers for interested individuals, such as financial support for basic technical training, are also in place to diversify the cyber security workforce.

Interesting practices from Colombia

- **Policy frameworks in cyber security**, such as the most recent document of National Council for Economic and Social Policy (Consejo Nacional de Política Económica Social, CONPES) 3995 on National policy of trust and digital security (DNP, 2020[20]) have been crucial to enhance the digital skills of the workforce, including the introduction of incentives to boost ICT training participation among various target groups (e.g. financial support for disadvantaged individuals to engage with non-formal and formal education) and promoting cyber security education in higher education institutions.
- **Diploma certificates** are offered by higher education institutions, professional associations, and private organisations. Some educational institutions form partnerships with private sector companies or specialised international providers to deliver these certificates. In cyber security, for instance, SENA developed the 'Technological centre of excellence and simulation in cyber security' jointly with MNEMO (an IT and cyber security services company) to deliver diploma certificates in information security and courses related to the field
- **Universities and employers designing short training programmes in cyber security** has become a common practice (for diploma certificates and other non-formal programmes). These short trainings include modules for developing basic technical ICT skills. In some cases, the courses contain modules fully customised by employers to meet their specific needs. These programmes also tend to be flexible and adaptable to students' learning needs, with some including mentoring, tutoring and other types of individual support.
- **Cyber security skills programmes for managers** fund training for employees in enterprises to raise awareness of cyber security issues, covering 100% of training expenses. The programmes include two diploma certificate courses for directors and high-level managers and IT managers to promote a culture of cyber security and improve the ability of companies to protect themselves against digital risks and threats.
- **The National school of instructors** (ENI) delivers targeted training for the teaching of ICT, including cyber security programmes. This process includes selecting qualified individuals from industry and developing their pedagogical abilities. Technical training in cyber security is also provided to ensure up-to-date knowledge among ICT teachers.
- **Hacker girls** is a national programme that aims at promoting women's participation in technology and cyber security. The programme provides opportunities for women of all ages to develop knowledge and skills in these fields and to encourage more women to pursue careers in technology and cyber security (e.g. hackathons and competitions).
- The **"Por TIC Mujer"** programme is an initiative in Colombia launched by the Ministry of Information and Communication Technology (Ministerio de las Tecnologias de la Información y las Comunicaciones, MinTIC) to enhance women's access to and usage of ICTs. The programme aims at overcoming digital illiteracy, improving women's access to technology, and supporting women's use of ICTs for entrepreneurship.

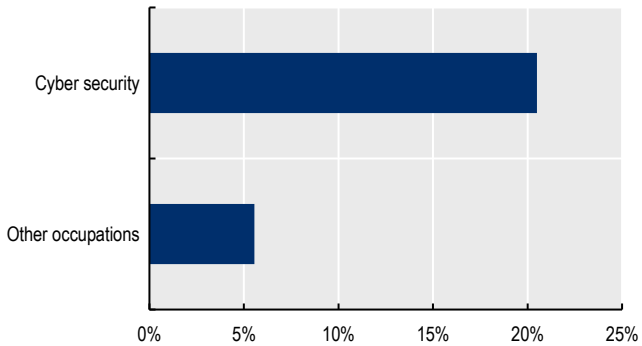
MEXICO

In total, the analysis uses 7.5 million online job postings across all jobs to investigate the demand for cyber security professionals in Mexico between January 2021 and December 2022.

Recent growth

2021H1 vs 2022H1

- Cyber security Online Job Postings (OJPs) grew at a rate that is 2.4 times higher than the overall growth rate. The number of cyber security OJPs increased by 65% in 2022 compared to 2021. To combat threats, Mexico implemented a national cybersecurity strategy in 2017 and has proposed a new federal law on cybersecurity in 2023.

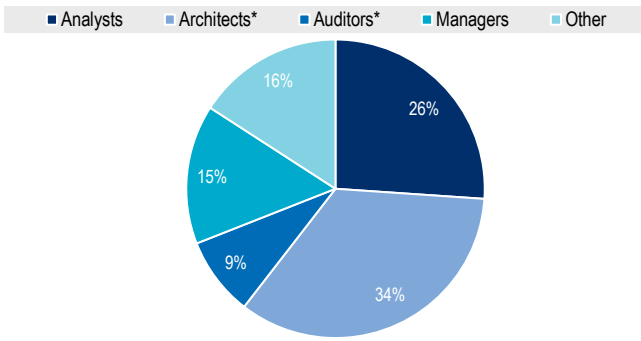


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

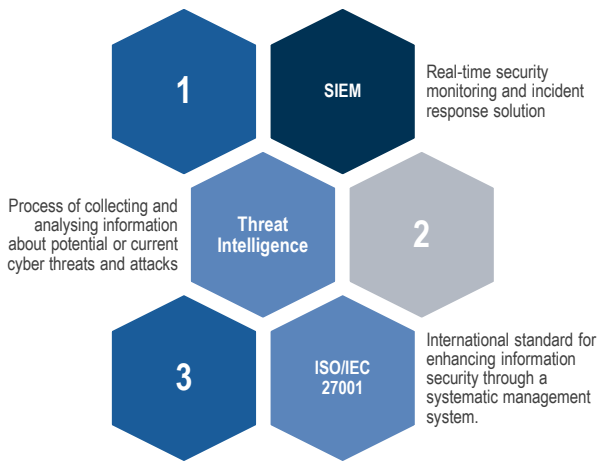
Average share 2021 - 2022

- Mexico experienced positive growth in all cybersecurity roles between 2021 and 2022, indicating a thriving cyber security labour market. Cyber security analysts and managers saw the strongest growth in OJPs, as demand has expanded by 80% and 53%, respectively, between 2021 and 2022.



Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2022)



Professional skills and abilities (2022)

Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

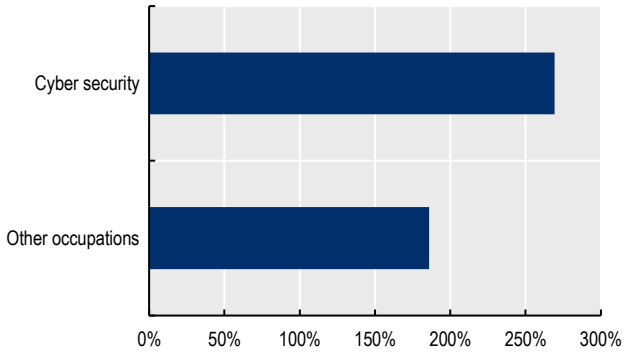
FRANCE

In total, the analysis uses 32.7 million online job postings (OJPs) across all jobs to investigate the demand for cyber security professionals in France between January 2018 and June 2023.

Recent growth

2019H1 vs 2022H1

- Between 2019H1 and 2022H1 the number of cyber security OJPs grew at a significant rate of 269%, 1.4 times faster than non-cyber security roles. The demand for cyber security professionals increased rapidly during and after the COVID-19 pandemic, due to amongst other increased teleworking.

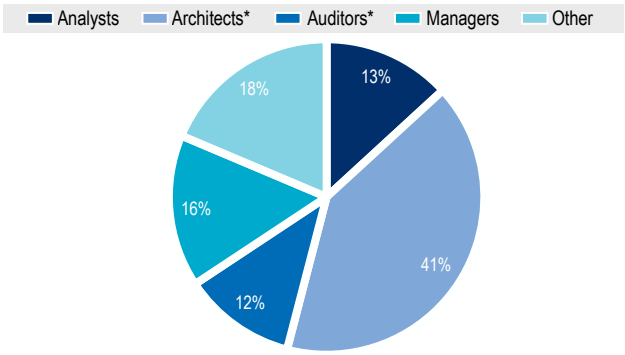


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

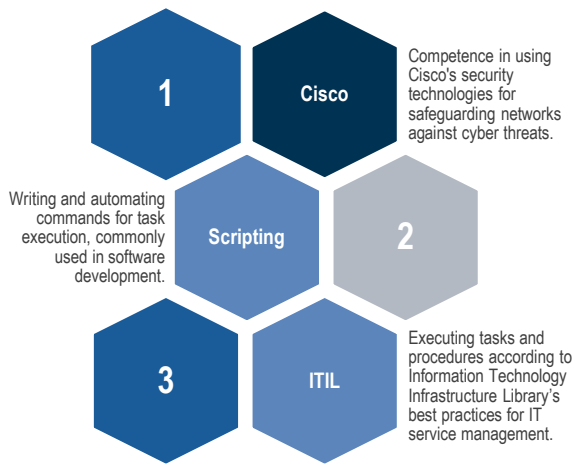
Average share 2018 – 2023H1

- Demand for architects constitutes 41% of online job postings (OJPs) for cyber security roles in France, indicating a high need for technical roles in security solutions design and implementation, and a shifting landscape with increased demand for managers.

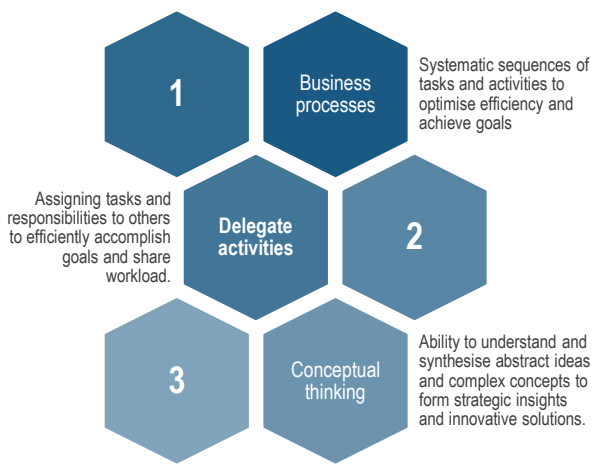


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2022)



Professional skills and abilities (2022)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

FRANCE

Insights on education and training provision

- France offers diverse pathways in cyber security education, ranging from upper secondary education to higher education, including short-cycle tertiary programmes. Enrolment in these programmes, particularly at the Bachelor's level, has been increasing, reflecting labor market demands.
- Basic cyber security skills are integrated into upper secondary education, including in Vocational and Technological Baccalaureate courses. Additionally, work-based learning programmes like apprenticeships allow learners to develop practical skills on the job.
- In addition to formal qualifications, France offers non-formal training that is usually shorter and more flexible, leading to certificates but not formal qualifications. The rise in demand for specialised ICT skills has resulted in a significant expansion of short courses and certificate training programmes.
- Industry involvement in programme delivery provides work-based learning opportunities, enhancing graduates' employability. France has also implemented policies allowing cyber security professionals to enter the teaching workforce, addressing teacher shortages and demand fluctuations.
- France focuses on diversifying enrolment in cyber security programmes, particularly by increasing female participation and socio-economic diversity. This includes national campaigns to break down role stereotypes and quotas in higher education programmes to facilitate the transition of graduates from diverse backgrounds into cyber security fields.

Interesting practices from France

- **Les cadettes de la cyber** Launched by the Cyber Excellence Centre, this programme fosters young women's careers in cyber security through mentorship, training in cyber geopolitics, managerial skills, and public speaking. It facilitates job transitions with internships, job dating sessions, and personalized coaching, and empowers cadettes to be ambassadors at events and on social media.
- **Campus Cyber**, a national initiative serving as a hub for cyber security expertise, it brings together businesses, government, academia, and research to address cyber security challenges. It focuses on fostering innovation, knowledge exchange, and addressing the shortage of qualified educators through partnerships and scalable training solutions.
- The **French National Acceleration Strategy** for Cyber security, supported by significant investment, this strategy aims to enhance cyber defenses and digital security. Goals include increasing the cyber sector's turnover, doubling jobs, supporting cyber security unicorns, and promoting cyber security culture and research. Educational integration at all levels and public awareness campaigns are central to this strategy.
- Higher education institutions have expanded **apprenticeship opportunities in cyber security**, offering practical experience alongside academic learning. Businesses value apprentices for fresh perspectives and building a tailored talent pipeline, with varied candidate profiles influenced by educational backgrounds and recruitment cycles.
- The **SecNumedu label**, awarded by the **French National Agency for the Security of Information Systems** (ANSSI), identifies high-quality specialized programmes in cyber security, meeting rigorous training standards. It enhances the prestige of educational institutions and guarantees students a quality education, improving employment prospects. The label concerns engineering and master's programmes and some professional bachelor's degrees.
- **"TomorrowCyberSpecialist" (DemainSpécialisteCyber)**, launched in 2023 by ANSSI, MENJ, and Campus Cyber, is a French national campaign to address the cyber security skill gap. Aimed at middle, high school, and post-secondary students, it seeks to raise cybersecurity awareness and highlight career diversity in the field, encouraging interest among young girls and boys. This initiative is part of a broader effort to familiarize students with various professions.
- The **CyberEdu label**, established by ANSSI, marks education programmes in France that integrate cyber security. This initiative, following the 2013 Defense and National Security White Paper, aims to weave cyber security awareness into all digital-related training. CyberEdu certifies various programmes, from vocational baccalaureates to short-cycle tertiary qualifications, focusing on cyber security competencies.

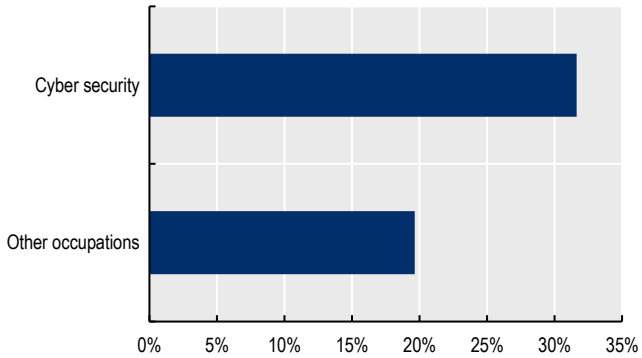
GERMANY

In total, the analysis uses 41.5 million online job postings across all jobs to investigate the demand for cyber security professionals in Germany between January 2018 and June 2023.

Recent growth

2019H1 vs 2022H1

- The cyber security labour market in Germany captured 0.33% of all OJPs at the start of 2019, showing greater maturity than in either France or Poland. In addition, the growth in demand for cyber security professionals significantly outpaced that of other occupations in between 2019H1 and 2022H1.

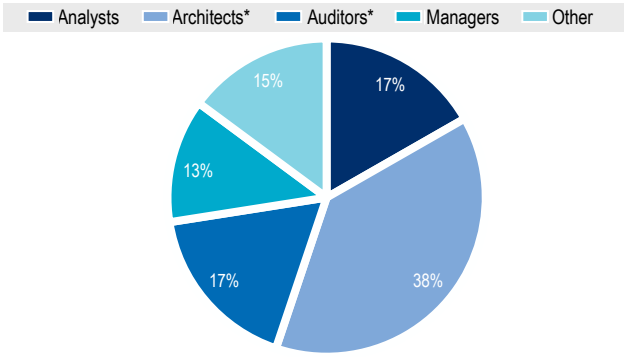


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

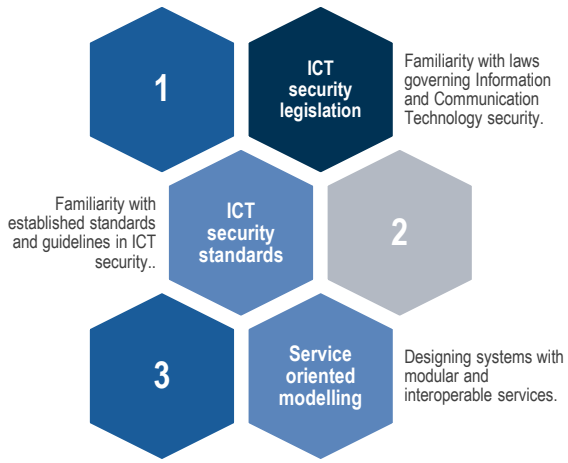
Average share 2018 – 2022H1

- Demand for the highly technical jobs of architects and engineers represents the largest share of OJPs in Germany, as in both France and Poland (38%). Notably, there is a heightened demand for auditors and advisors in Germany, reflecting organisations' recognition that cyber security involves ongoing evaluation, verification, and integration with legal frameworks alongside technical implementation.

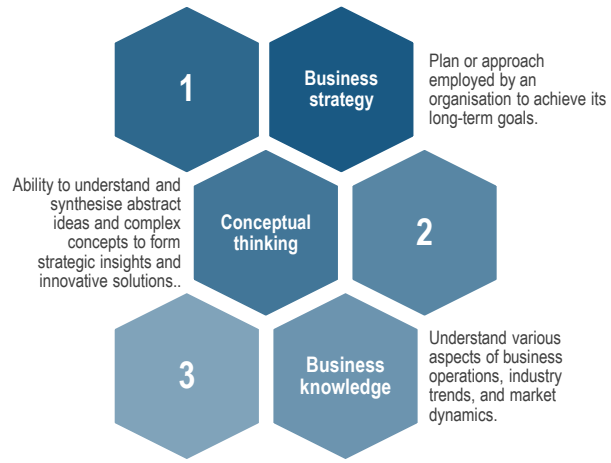


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2022)



Professional skills and abilities (2022)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

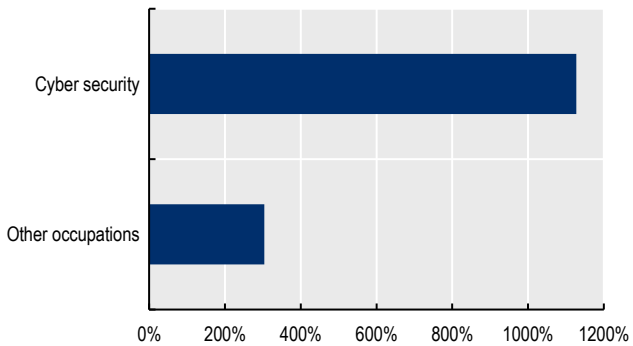
POLAND

In total, the analysis uses 4.9 million online job postings across all jobs to investigate the demand for cyber security professionals in Poland between January 2018 and June 2023.

Recent growth

2019H1 vs 2022H1

- Cyber security job postings have significantly grown in recent years, partially because of better coverage in the data. The share of cyber security job postings over the total collected more than tripled in between the first half of 2019 (0.11%) and 2022 (0.34%). This share is now in between that of France and Germany.

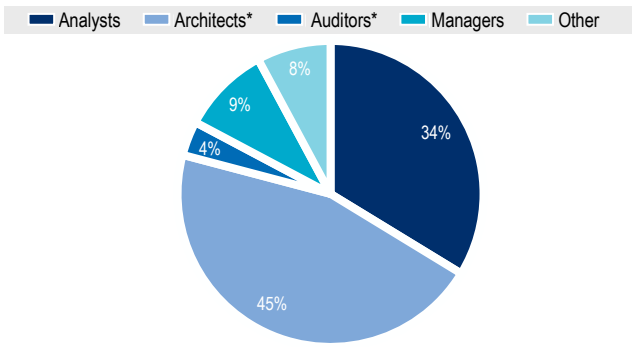


Note: Growth is measured by comparing the average monthly number of job postings between both periods.

Roles

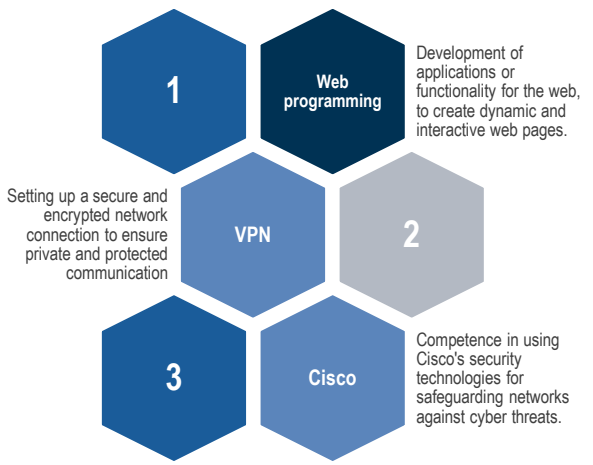
Average share 2018 – 2023H1

- Demand for architects represents 45% of the total of OJPs for cyber security roles. The second largest demand is that for analysts at 34%, a significantly larger share than in France and Germany. Cyber security analysts play a pivotal role in the protection of digital assets and sensitive information.

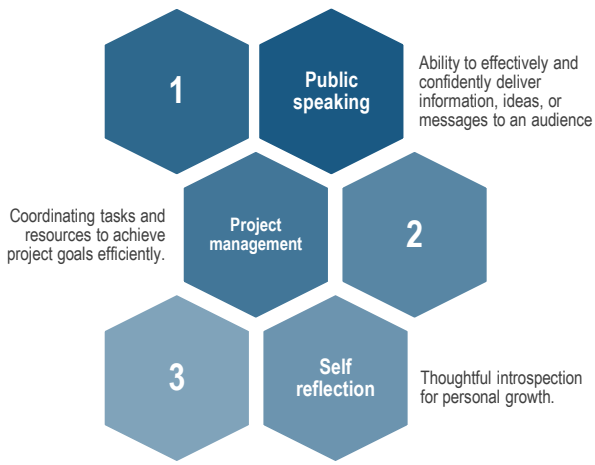


Note: * Architects/engineers and Auditors/advisors

Technical skills and knowledge (2022)



Professional skills and abilities (2022)



Note: The figure presents a selection of the most relevant technical and professional skills. Skills relevance is the result of analysing the skills mentions in job postings by applying Natural Language Processing (NLP) techniques.

Source: OECD based on Lightcast

Building a Skilled Cyber Security Workforce
INSIGHTS FROM OECD COUNTRIES

SYNTHESIS NOTE

For more information on the project go to: oe.cd/cyber-security-skills-project

Microsoft