WORLD ECONOMIC FORUM

Strategic Cybersecurity Talent Framework

WHITE PAPER

APRIL 2024

Images: Getty Images, Midjourney

Contents

Executive summary

The strategic Cybersecurity Talent Framework should guide public- and private-sector decision-makers in building and sustaining a skilled cybersecurity workforce.

In today's hyperconnected digital landscape, the cybersecurity industry faces a critical global shortage of nearly 4 million professionals. With a consistent year-on-year increase in demand for qualified practitioners, the deficit shows no sign of abating.

At a time when cyberthreats are increasing in sophistication and frequency, the cybersecurity workforce, as the backbone of organizational security, plays a key role in securing the benefits of the Fourth Industrial Revolution. Failure to ensure a steady supply of cybersecurity professionals may have far-reaching consequences, with organizations worldwide finding themselves vulnerable and understaffed in the face of emerging threats. It is, therefore, imperative for decision-makers to prioritize cybersecurity talent management as a strategic necessity.

Recognizing that a single actor alone cannot effectively tackle the cybersecurity workforce shortage, the World Economic Forum established the Bridging the Cyber Skills Gap initiative. Bringing together more than 50 public and private organizations, the initiative developed a strategic Cybersecurity Talent Framework (CTF) featuring actionable approaches to help organizations build sustainable talent pipelines.

More specifically, the CTF is structured around four key priority areas intended to provide a holistic approach to talent management in cybersecurity.

Among other things, the priority areas explore how:

- **More talent could be attracted** into cybersecurity by improving the understanding of what cybersecurity professionals do, removing barriers to entry and improving diversity in the workforce
- **Cybersecurity education and training could be improved** to effectively equip students and professionals with essential skills for a career in the field
- **Recruitment practices could be rethought** by addressing challenges such as unrealistic and demanding requirements in job descriptions and misalignment between hiring managers and human resources (HR) departments
- **Retention of cybersecurity professionals could be improved** by tackling issues such as the lack of appreciation and recognition for the field as well as the high stress levels

As a universally applicable framework, the CTF is intended to serve as a source of reference for industry leaders, government agencies, civil society and academia – that is, all stakeholders concerned by the cybersecurity workforce shortage and committed to developing and nurturing robust cybersecurity talent across their respective sectors.

Introduction

The cybersecurity industry is affected by the global shortage of workers and urgently needs to take actionable approaches to attract and retain skilled staff.

The workforce shortage is a global concern that spans nation states and industries. Estimates suggest that by 2030 there could be a global talent shortage of more than 85 million workers, leading to an estimated loss of $8.5 trillion in unrealized annual revenue.[1]

The cybersecurity industry is also affected by this pervasive challenge. While the cybersecurity workforce grew by 12.6% between 2022 and 2023, there is a shortage of nearly 4 million cybersecurity professionals worldwide.[2] With a consistent year-on-year increase in demand for qualified practitioners, there is little optimism that the supply will catch up. In fact, only 15% of all organizations are optimistic that cyber skills and education will significantly improve the situation over the next two years.[3]

From a regional perspective, the shortage is most pronounced in Asia-Pacific, which lacks more than 2.5 million cybersecurity workers, followed by North America, which faces a workforce gap of almost 522,000 people.[4] In Africa, with a total population of more than 1.4 billion, the number of certified security professionals is estimated to be only around 20,000.[5] At a country level, the talent shortage is particularly pronounced in China, India, the US and Brazil. India, despite boasting one of the world's largest youth populations and 31.7% of science, technology, engineering and mathematics (STEM) graduates worldwide,[6, 7] had an estimated 40,000 job openings for cybersecurity professionals in May 2023.[8] Due to talent shortages, 30% of these vacancies could not be filled.[9] Similarly, as of January 2024 the US has an estimated 448,000 cybersecurity job vacancies across the private and public sectors.[10]

The cybersecurity workforce shortage is especially apparent in the education, government and healthcare sectors.[11] In fact, the Global Cybersecurity Outlook 2024 found that the lack of resources and skills is the biggest challenge when designing for cyber resilience for 52% of public organizations.[12] Similarly, small and medium-sized enterprises (SMEs) struggle to digitalize due to a lack of cyber skills. Research shows that 43% of UK SMEs have been unable to hire cybersecurity support due to the shortage of specialists or challenges in attracting, recruiting and retaining cybersecurity practitioners.[13] When it comes to specific cybersecurity roles, the workforce shortage is acute in domains such as cloud security, cyberthreat intelligence and malware analysis.[14]

As organizations confront the complexities of escalating cyberthreats – ranging from sophisticated ransomware attacks to insidious data breaches – the scarcity of qualified cybersecurity practitioners is reaching alarming proportions, and it comes as no surprise that more than two-thirds of organizations face additional risks because of cybersecurity skills shortages.[15]

The root causes of the cybersecurity workforce shortage are many. One key factor is the rapid evolution of the cybersecurity landscape, which outpaces the development of a commensurate workforce. As threat actors continue to refine and innovate their methods of attack, the demand for professionals with both a diverse and specialized skill set outstrips the supply. However, the shortage of skilled professionals capable of defending against increasing cyber risks extends beyond the immediate challenges faced by organizations. As a systemic risk, there is growing concern about the potential impact of the cybersecurity workforce deficit on national security, critical infrastructure and the overall resilience and security of economies and societies. Moreover, the proliferation of cutting-edge technologies – such as generative artificial intelligence (AI), quantum computing and internet of things – introduces new risks, expanding the attack surface and, therefore, further amplifying the need for a cybersecurity workforce equipped with evolving know-how. The cybersecurity sector also has a pronounced lack of diversity – including the representation of women, migrants, ethnic minorities and neurodiverse employees – so it should come as no surprise that 91% of organizations believe that there is a need to push for a more diverse range of people in the cybersecurity field.[16]

Other factors contributing to the workforce shortage include issues such as the inability of certain employers, primarily from the public sector, to compete with the salaries offered by other organizations; misalignment among educational programmes; the evolving needs of the cybersecurity industry; and the lack of clarity about career opportunities in the field.

To address the cybersecurity workforce gap, the following strategic Cybersecurity Talent Framework (CTF) aims to present actionable approaches and best practices to public and private decision-makers worldwide on how to cultivate and sustain a pipeline of skilled professionals.

> The cybersecurity workforce landscape is multifaceted and involves a diverse array of actors forming a dynamic and interconnected network dedicated to securing an increasingly digitalized world.

Finding a common language

When discussing the cybersecurity workforce deficit, terms such as “skills shortage”, “talent shortage”, “capacity shortage” and “experience shortage” are often used interchangeably despite their distinct nuances. This inaccuracy leads to confusion and misunderstanding regarding the specific type of scarcity that the industry faces.

Taking a closer look at the different types of deficits, a “skills shortage” typically refers to a dearth of specific technical and soft competencies or abilities required for particular roles within the cybersecurity field. In this context, organizations may struggle to find an individual proficient in a specific programming or foreign language. On the other hand, a “talent shortage” suggests a lack of individuals possessing the broader set of skills, knowledge and attributes needed to excel in diverse cybersecurity roles. The term “capacity shortage” extends beyond cybersecurity staff and encompasses aspects such as the digital infrastructure and regulatory frameworks needed to establish and maintain robust security measures in the digital landscape. Finally, “experience shortage” refers to a lack of practical and hands-on expertise in dealing with real-world cybersecurity problems. In addition to these types of scarcities, organizations are increasingly struggling to find individuals with the right drive and motivation.

To devise efficient and effective solutions to the problems at hand, there is a need to identify the precise nature of the shortage that a given geography, industry or organization is encountering. It is important to note that in cybersecurity multiple shortages can manifest simultaneously and in an interconnected manner. For instance, recent graduates may possess the right skills but lack real-life experience. On the other hand, experienced professionals may lack skills because many organizations struggle to invest in upskilling initiatives. Finally, qualified professionals with the right skills and experience tend to seek higher salaries, and organizations may find themselves experiencing a workforce shortage simply because they cannot afford to hire the talent.

Adopters and enablers

The cybersecurity workforce landscape is multifaceted and involves a diverse array of actors forming a dynamic and interconnected network dedicated to securing an increasingly digitalized world.

At the forefront are adopters of the CTF. In essence, any public or private organization facing a shortage of cybersecurity talent can be an adopter of the CTF. More specifically, adopters acknowledge that attracting, educating, recruiting and retaining talent is a strategic imperative that demands actionable approaches.

In parallel, certain adopters may also choose to play the role of an enabler, acting as catalysts for the successful implementation and continuous improvement of the CTF. Enablers possess specialized knowledge, resources and tools that can help navigate the complexities of cybersecurity talent management to yield tangible results. Enablers include:

Government entities: Responsible for defining and setting policies and regulations in cybersecurity workforce development according to supply and demand, government entities may also provide funding, grants and resources for cybersecurity training programmes and initiatives. Relevant examples of government entities include national cybersecurity bodies, ministries of education, ministries of information and technology and ministries of labour and employment.

Private sector: The private sector, which is usually the biggest employer of cybersecurity professionals, plays a critical role in enabling cyber talent development by supporting and promoting training programmes and offering a diverse range of avenues for practical development of competencies through internships and apprenticeships.

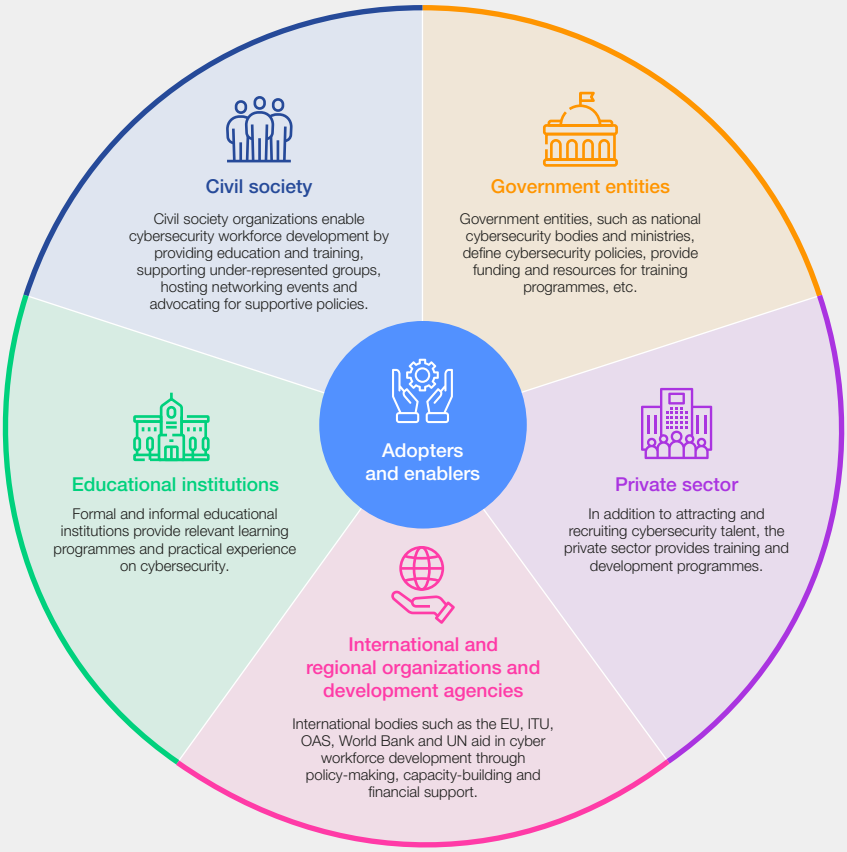
International/regional organizations and development agencies: Organizations such as the European Union, the International Telecommunication Union, the Organization of American States, the World Bank and the United Nations help build a cyber-savvy workforce through a number of activities, including shaping policies, facilitating capacity-building programmes and providing technical and financial assistance.

Educational institutions: Formal education on cybersecurity occurs in a systematic, structured environment and comprises primary, secondary and tertiary levels. Non-formal training consists of programmes and courses designed to provide learners with cybersecurity skills, knowledge and competencies outside the formal education system, including community education, boot camps and hands-on competitions as well as professional development courses.

Civil society: Civil society organizations enable the development of a cybersecurity workforce by providing affordable and accessible education and training, supporting under-represented groups such as women and youth through mentorship opportunities, hosting networking events and advocating for supportive policies.

The synergy between adopters and enablers of the CTF forms the cornerstone of a comprehensive approach to cybersecurity workforce development.

FIGURE 1 | **Enablers of the Cybersecurity Talent Framework**



Four priority areas

To address the different types of shortages comprehensively and to build sustainable cybersecurity talent pipelines, it is imperative to identify and address the underlying reasons contributing to the broader cybersecurity workforce gap.

The World Economic Forum's Bridging the Cyber Skills Gap initiative brings together more than 50 global public and private organizations committed to building sustainable cybersecurity talent pipelines. Complementary to and in alignment with existing World Economic Forum efforts on skills, including the Reskilling Revolution and Skills-First,[17] the initiative has identified the following four priority areas central to the CTF:

- Attracting talent into cybersecurity
- Educating and training cybersecurity professionals
- Recruiting the right cybersecurity talent
- Retaining cybersecurity professionals

It is important to note that the four priority areas should not be viewed in isolation but as interconnected components of a comprehensive cybersecurity talent-management approach.

FIGURE 2 | **Visual representation of the Cybersecurity Talent Framework**

The four priority areas should not be viewed in isolation but as interconnected components of a comprehensive cybersecurity talent-management approach.

Attracting talent into cybersecurity

Despite the fact that cybersecurity careers tend to be well paid, purposeful and offer opportunities for career development, the industry struggles to attract talent. A lack of understanding of what cybersecurity professionals do in their daily work, coupled with insufficient awareness of how to enter the cybersecurity sector and what career opportunities may be available, discourages individuals from pursuing a career in cybersecurity. Moreover, a lack of diversity (which makes the talent pool of available workers smaller than it need be), fierce competition for niche talent and the evolving job demands exacerbate organizations' difficulties in attracting skilled talent.

What measures could be taken to attract cybersecurity talent?

Educating and training cybersecurity professionals

Irrespective of whether they are intended for primary- or secondary-school students, university students or professionals, educational programmes on cybersecurity face numerous challenges, including outdated and misaligned curricula, a shortage of qualified instructors and a lack of structured mentorship programmes. Such setbacks are exacerbated even further by the frequent demand for expensive cybersecurity degrees and certifications with varying levels of recognition and relevance. The limited supply of training that recognizes the diversity of learners' needs, backgrounds and learning preferences also hinders the effectiveness of cybersecurity education.

How can cybersecurity education be improved to equip students and professionals effectively with essential skills?

Recruiting the right cybersecurity talent

While many cyber skills are transferable, employers' demand for formal cybersecurity education creates a barrier to entry. In addition, many potential (entry-level) candidates are discouraged from applying for cybersecurity roles due to the extensive requirements listed in job descriptions, including certifications and several years of experience. One of the underlying reasons for such unrealistic and demanding requirements is because HR departments often do not understand the jobs for which they are recruiting and do not speak the language of cybersecurity.

How can organizations rethink recruitment and talent-sourcing practices?

Retaining cybersecurity professionals

Continued stress, fatigue and pressure experienced by cyber professionals result in high employee attrition rates. Another factor that leads to short tenures within cybersecurity is a lack of appreciation of and recognition for cybersecurity staff. Sometimes individuals leave their cybersecurity roles for other internal opportunities, seeking a change in responsibilities, while others quit the organization altogether. The departure of cybersecurity experts not only has financial implications for organizations as they try to replace talent but also contributes to the loss of invaluable institutional knowledge and can have implications for the security posture of affected organizations.

How can organizations create incentives for talent and retain their staff?

1 Attracting talent into cybersecurity

Cybersecurity professionals have a meaningful impact on the digital world, protecting it from cyberthreats. Yet despite the fact that this is valuable work with major benefits for wider society, the industry struggles to attract talent.

A number of reasons contribute to this difficulty, including the flawed perception that cybersecurity roles are highly technical. Moreover, about 85% of cybersecurity professionals believe that individuals are often discouraged from pursuing a career in the sector because they lack insights into the field's variety of potential roles and opportunities for upward mobility.[18]

The challenge is also visible at an organizational level. With an estimated 78% of organizations reporting that they do not have the in-house skills to fully achieve their cybersecurity objectives,[19] talent attraction becomes increasingly difficult, with organizations – irrespective of their size, industry or geography – competing for mission-driven professionals who care about creating better outcomes for their organizations and broader communities.

1.1 Key challenges that organizations face when attracting cyber talent

The increasingly complex cybersecurity landscape demands both individuals with highly technical skills to navigate intricate systems and networks and others with non-technical skills such as risk management and policy development to address strategic cybersecurity challenges.

Many organizations seeking to attract cybersecurity talent struggle to:

- Compete with other organizations in terms of proposed salaries and benefits, especially in the age of remote working, which gives them wider options. This challenge may be experienced particularly by SMEs, public organizations in the Global South and highly regulated industries such as finance and healthcare.
- Evaluate the educational qualifications of applicants due to a lack of standardized education pathways.
- Craft precise job descriptions as HR teams may have limited abilities to translate technical requirements into appealing narratives. Moreover, hiring managers within cybersecurity departments often struggle to communicate desired skills and competencies in non-technical language.
- Manage the expectations of early-career talent in terms of promotions, work location and so forth.
- Find highly experienced cybersecurity professionals and specialized talent in emerging technologies.
- Recognize the need for a broader spectrum of cybersecurity talent, beyond highly specialized experts, by acknowledging the critical role of technicians who perform essential operational and intermediate tasks.
- Integrate diversity and inclusion due to insufficient outreach efforts targeting under-represented groups (e.g. lack of gender-sensitive language in job descriptions), inadequate representation of diversity in leadership positions, insufficient support for work–life balance, language barriers and so forth.

1.2 Consequences of failing to attract talent

The World Economic Forum's *Future of Jobs Report 2023* found that in the next five years the inability to attract talent will constitute one of the most important barriers to industry transformation.[20] In cybersecurity, failure to attract talent can result in several consequences for organizations, including:

- Overstretched staff who are unable to focus on their respective roles and professional growth. This, in turn, can decrease an individual's ability to perform and meet goals and objectives. In the long run, overstretched staff can lead to reduced innovation and delays in development, production and launch of products and services.
- Difficulty in implementing cybersecurity regulations and meeting compliance requirements.
- Inadequate prioritization and diversion of attention away from essential cybersecurity measures and investments.
- Financial losses due to a lack of sufficient cybersecurity personnel available for monitoring, responding to and mitigating the consequences of cybersecurity incidents.
- Reputational damage for organizations unable to hire the right talent to respond to emerging cybersecurity threats.

1.3 Approaches to attracting talent

To tackle the previously mentioned challenges and mitigate the negative effects of the failure to attract talent, organizations need to think carefully about how to equip themselves with the right cybersecurity workforce. Broadly speaking, every approach to attracting cybersecurity talent should seek to market cybersecurity as value-based work that helps protect sensitive data, intellectual property and digital infrastructure, emphasizing its profound impact on wider society. Moreover, it should promote the multidisciplinary nature of cybersecurity and the ability to pursue a career in cybersecurity across different industries and contexts.

While there is no "one-size-fits-all" solution, a robust approach to attracting talent should incorporate practices that help organizations identify and engage individuals who would not only fill a role but who would also stay with the organization.

BOX 1 Characteristics of attracting talent

Approaches to attracting talent should:

- Be flexible and adaptable to reflect the rapidly evolving landscape of threats, technologies and skill requirements.
- Make the most of the corporate brand and reputation based on values and commitment to cybersecurity excellence.
- Prioritize diversity and inclusion by setting diversity goals as well as demonstrating and highlighting commitment to inclusion at all levels of the organization.
- Incorporate partnerships with groups or institutions working with under-represented stakeholder groups in cybersecurity, such as women in cyber, refugees and military veterans. By broadening outreach efforts and promoting inclusive practices, organizations can tap into a more diverse talent pool through recruiting outside of traditional computer science graduate cohorts, enhancing innovation and problem-solving capabilities within their cybersecurity teams.
- Offer competitive salaries and comprehensive benefits packages – including healthcare cover, onsite childcare and hybrid working options – to access a wider talent pool and promote work–life balance.
- Highlight learning and career-development opportunities within the organization. By offering professional development programmes, mentorship initiatives and opportunities for advancement, organizations can demonstrate their commitment to nurturing talent and developing long-term career growth in cybersecurity.
- Focus on developing in-house talent by investing in training, upskilling and promotion from within to cultivate a strong pipeline of cybersecurity professionals who are already familiar with the company's culture, processes and systems. This not only enhances employee loyalty and engagement but also ensures continuity and stability within the cybersecurity workforce.

1.4 Implementing actionable approaches to attract talent

Defining actionable approaches to attracting talent is just the tip of the iceberg. For long-term wins in cybersecurity workforce growth, predefined approaches need to be paired with an implementation plan.

BOX 2

Features of an implementation plan

An implementation plan should:

- Ensure that executive leadership recognizes the critical importance of cybersecurity and is fully committed to addressing cybersecurity workforce needs. According to Fortinet research from 2023, more than 90% of boards of surveyed organizations across North America, Latin America, Europe, Middle East and Africa and Asia-Pacific were inclined to push for adding cybersecurity headcount.[21] Leadership can show commitment by prioritizing cybersecurity, providing the necessary resources and tools to cybersecurity professionals and by actively supporting efforts to attract talent within the organization.
- Allocate sufficient budget to the recruitment of cybersecurity professionals. To that end, organizations should research market rates to offer competitive compensation, account for recruitment costs, allocate resources for training and development programmes to upskill or reskill existing talent and collaborate with finance and HR teams to align the budget with organizational constraints and strategic priorities.
- Use a common-language framework to enhance the precision of job descriptions and relevant required competencies for each job role to facilitate effective communication among recruiters, hiring managers and candidates. This framework should standardize terminology and qualifications related to cybersecurity roles, ensuring that job descriptions accurately reflect the skills and experience required for each position.
- Foster collaboration with academic institutions to promote cybersecurity career opportunities and attract qualified candidates. Organizations can reach out to primary and secondary schools, universities and vocational schools to communicate the demand for cybersecurity professionals, participate in career fairs and industry events, offer internships and apprenticeships and provide guest lectures or workshops to educate students about career paths in cybersecurity.
- Ensure HR and recruitment teams are equipped with the necessary skills and training to execute the strategy effectively.

2 Educating and training cybersecurity professionals

Cybersecurity education is a very broad discipline that encompasses a wide range of actors contributing to the skilling and training of the cybersecurity workforce.

Training in cybersecurity may begin in primary and secondary schools and continues in universities, vocational schools, online learning platforms, cybersecurity academies established by the public or private sector, on-the job training and other formal and informal educational settings.

2.1 Identifying the gaps in current cybersecurity education and training programmes

At the primary- and secondary-school level, cybersecurity education is increasingly being recognized as essential in equipping students with the knowledge and skills to navigate the digital landscape safely. While some schools may offer basic courses on digital safety and security – including best practices for creating strong passwords, recognizing phishing scams and protecting personal data – technical knowledge such as malware analysis and encryption often remains overlooked. A survey conducted in the US and the UK in 2023 revealed that 62% of respondents agreed that if they or their child had had a more comprehensive cybersecurity education in school they would have considered pursuing a career in the field.[22] The same survey also found that 90% of respondents believed that insufficient efforts are being made to educate students on the opportunities that exist in cybersecurity.

While cybersecurity may be more integrated into university-level curricula, challenges related to the practical application of knowledge persist. To illustrate, at the European Union level, only 34% of cybersecurity programmes feature a compulsory internship for students.[23] This lack of practical experience can make it more difficult for graduates to land a job in cybersecurity. Higher education also performs rather poorly on professional certification, with only 23% of EU programmes preparing students for specific professional certifications.[24] What is more, cybersecurity education can be unaffordable for many. Research shows that EU citizens have to pay for 71% of cybersecurity programmes at bachelor, master and postgraduate levels in order to enrol.[25]

Despite the fact that the informal cybersecurity education landscape is characterized by greater accessibility and flexibility, it also faces challenges of its own. With a plethora of curricula and programmes, choosing the most relevant becomes a daunting task.

A closer look at cybersecurity education reveals the following:

- An absence of comprehensive cybersecurity curricula at primary- and secondary-school and university levels results in cybersecurity talent lacking either technical or soft skills. This ultimately results in failure to adequately prepare students for the task of securing digital systems and a lack of leadership buy-in to positioning cybersecurity as a strategic imperative.
- Limited commitment to and funding for cybersecurity education and training hinders the development of robust programmes and limits the resources available for educators and students.
- A lack of practical learning opportunities limits exposure to the challenges and complexities of cybersecurity and hands-on experiences that allow the application of knowledge in real-world scenarios.

– A shortage of qualified professionals who can effectively teach cybersecurity concepts and technologies to students in primary and secondary schools, universities and vocational schools. This lack is primarily due to the fact that cybersecurity is still a relatively nascent field. Addressing this gap is key to empowering the next generation with the necessary critical thinking and technical proficiency.

– Insufficient guidance about which training courses and mechanisms are best suited for different cybersecurity roles can lead to confusion and ineffective training programmes.

– The absence of a standardized approach to cybersecurity education across institutions worldwide contributes to inconsistent learning outcomes and accreditation criteria as well as industry misalignment. This, in turn, impedes efforts to produce a cohesive workforce equipped to address the diverse and evolving challenges posed by cyberthreats.

It is important to note that the question of whether cybersecurity curricula and education programmes should be standardized is a topic of debate within the industry. While some argue that a certain degree of customization is needed to reflect a given organization's culture and meet the specific needs of the target group, others believe that standardization is necessary to ensure consistency and alignment with industry requirements.

2.2 What should the future of cybersecurity education and training look like?

The lack of adequate education and training programmes on cybersecurity can have far-reaching impacts on organizations in diverse industries and geographies. To illustrate, a study by the Organization of American States revealed that in Latin America the lack of availability of cyber-specific educational opportunities, together with high employee attrition rates, affect the region's ability to execute other strategic goals such as economic growth, national security and infrastructure modernization.[26]

BOX 3 **Acting on cybersecurity education and training**

Public and private organizations responsible in one way or another for cybersecurity education should therefore take actions to:

– Integrate cybersecurity education across different disciplines (e.g. healthcare, law, political science and so forth).

– Incorporate industry-recognized international professional certifications into training programmes, culminating in certification exams that learners can take upon completion.

– Mobilize greater efforts to incorporate cybersecurity education in primary and secondary schools. Training on cybersecurity should be provided to all students engaging with digital technologies.

– Ensure cybersecurity curricula are flexible and adaptable to the changing cyber landscape. For example, they should include materials on emerging technologies such as AI.

– Provide continuous education opportunities for experienced professionals to stay updated on the latest trends and best practices.

– Aggregate freely accessible cybersecurity training resources into a structured one-stop shop where individuals interested in pursuing cybersecurity careers or cybersecurity professionals can conveniently access them.

– Make use of gamification and immersive learning (e.g. incorporating virtual reality and augmented reality tools) in education programmes to stimulate motivation and engagement among learners.

– Provide specialized training on advanced technical skills, strategic thinking, risk management and leadership abilities for individuals aspiring to become future security leaders.

– Be cognisant of different learning styles and offer personalized learning experiences through adaptive learning platforms that tailor content and delivery methods based on the learner's preferences and progress.

To ensure that individuals are equipped with the right skill set and that cybersecurity education is current and innovative, organizations must work to proactively identify emerging technologies and cybersecurity trends.

BOX 4 **Identifying emerging technologies and trends**

To make sure they spot key technologies and trends, organizations should:

- Develop and maintain a national or global repository with insights on emerging technologies and associated cybersecurity issues. This repository can serve as a centralized knowledge hub, providing up-to-date information on the latest threats and vulnerabilities. Such a repository could help ensure better alignment between education programmes and the demands of the industry.
- Invite guest speakers from the industry to share the latest cybersecurity insights. Academic organizations should also explore partnerships with the private sector to develop cybersecurity curricula that align with industry requirements.
- Break down training materials into smaller modules, to easily revise and update specific components as new threats emerge.
- Seek learner feedback to understand the scope of competencies and gain valuable insights into the effectiveness of current training programmes.
- Develop strong public–private partnerships and focus on practical, hands-on training. Opportunities for in-person or virtual internships or apprenticeships allow learners to tackle work challenges in a managed environment.
- Implement a 70:20:10 learning model where 70% of the skills are gained through job projects, 20% through interactions with others and 10% through formal training.

2.3 Assessing the effectiveness of cybersecurity education and ensuring better alignment with industry demands

With an estimated 91% of organizations willing to pay for the training and certification of their employees,[27] cybersecurity education is a priority for many organizations. That said, cybersecurity talent prefers to have a certain degree of autonomy when it comes to selecting cybersecurity training. In fact, 80% of cybersecurity professionals would prefer to choose their own training programmes.[28]

To evaluate the effectiveness of cybersecurity education and training programmes and identify areas for improvement, organizations should:

- Establish clear and measurable learning targets for cybersecurity education and training programmes.
- Implement pre- and post-education/training assessments, such as open-book practical lab-based exams or projects and hackathons, to measure individual progress and identify knowledge gaps. Specific role-based assessments could be used (e.g. targeting penetration testers or incident responders) to determine competency levels and identify skill shortages. On the back of such assessments, tailored education and training could be crafted.
- Track the number of individuals educated and successfully employed in the cybersecurity industry. This can be accomplished through the use of tools such as centralized databases and job-placement statistics as well as check-ins with students to determine how prepared they feel for their roles.
- Establish a “Cyber Industry Review Board” to review and evaluate cybersecurity courses offered by universities and award a badge to ensure alignment with industry needs and standards.
- Conduct short-term and long-term evaluations to track the number of participants who transition to full-time employment following completion of cybersecurity education or training or to monitor the performance of employees based on the type of education they receive.

3 Recruiting the right cybersecurity talent

Recruitment is essential for building a competent and skilled workforce that can contribute to the overall growth, success and sustainability of an organization.

The stages of the recruitment process – candidate sourcing, applicant evaluation, interviewing and assessments, background checks, final selection and onboarding – must be carried out thoroughly to recruit candidates with the right skill set and experience who demonstrate alignment with organizational culture and values. However, many employers tend to expedite recruitment processes in order to deploy new hires as soon as possible. Rushed recruitment may result in hasty decisions and, ultimately, wrong hires.

In cybersecurity, recruitment is often perceived as a challenge. Research from 2023 shows that 56% of organizations struggle to recruit cybersecurity professionals,[29] and the underlying reasons for this include:

- The shortage of qualified candidates in the job market protracts the recruitment process, creating a competitive hiring landscape where organizations need to invest additional time to identify, attract and engage cybersecurity professionals. On average, 67% of cyber leaders state that their organizations take at least three months to fill non-entry-level positions.[30]
- Miscommunications and misunderstanding between cybersecurity hiring managers and HR teams is a problem. Data shows that only 25% of cyber leaders feel that their HR teams understand cybersecurity hiring needs sufficiently to properly prescreen candidates.[31]
- The lack of diversity and inclusion exacerbates challenges for organizations in recruiting talent by narrowing the field of potential candidates. To illustrate, in the under-30 age group, women represent 26% of the cybersecurity workforce. This number is lower for age groups 30–38 and 39–49, where women account for only 22% and 14% of cybersecurity professionals respectively.[32] The inclusion of ethnic minorities in cybersecurity is also a concern, with the industry struggling to ensure representation of individuals from diverse backgrounds.
- Strict organizational policies impede the hiring of cybersecurity professionals. About 45% of hiring managers state that their organizations are too reluctant to hire entry-level employees or that they rely too heavily on education/degrees when looking for cybersecurity applicants.[33]
- The rigorous security clearances required for some cybersecurity roles due to the sensitive nature of the work are a problem.

As the cybersecurity job market becomes increasingly competitive, organizations need to ensure that they have comprehensive recruitment approaches in place to help ensure better preparedness and minimize rushed hiring processes that can result in hiring mismatches. Actionable approaches on recruitment should define who, why, how and where organizations should hire. Approaches should also outline a clear career path for hired individuals.

3.1 The search for cybersecurity professionals

With the cybersecurity landscape evolving rapidly, organizations face difficulty not only in finding and employing the right talent but also in foreseeing future trends and shifts that may affect demand for organizational talent.

Before embarking on the quest for cybersecurity talent, organizations should:

- Identify which technical and soft skills and experience are essential for their respective contexts and based on the current cybersecurity landscape.

> When identifying skills, attention should be paid to those that are must-have and those that are simply nice-to-have.

– Anticipate which skills and experience will be needed in the future as the cybersecurity landscape evolves. Organizations can make use of industry assessments and reports that track the evolution of the cybersecurity landscape to do this.

When identifying skills, attention should be paid to those that are must-have and those that are simply nice-to-have. In general, organizations should avoid demanding skills unrelated to the role, which can lead them to recruit candidates who are not the best fit for the job. Similarly, organizations should refrain from requiring credentials, including degrees or certifications, that do not match the experience and hiring level of the role for which they are recruiting, as doing so can limit the pool of qualified candidates and may result in them overlooking highly skilled individuals.

These considerations can help in crafting more realistic job descriptions, ultimately ensuring that there is a common language when discussing the requirements for the role.

Once they have mapped the needed skills and experience, organizations should:

– Assess their current cybersecurity workforce and evaluate the skills and capabilities of existing employees to identify any gaps or areas for improvement. HR and the cybersecurity team should work together to determine the top skills in which they should invest.

– Make use of cybersecurity skills frameworks – the Workforce Framework for Cybersecurity (NICE Framework), the European Cybersecurity Skills Framework (ECSF), the SFIA Framework for Cybersecurity Skills, the Operational Technology Cybersecurity Competency Framework (OTCCF), for example – to pinpoint the specific skills, competencies and knowledge needed for prioritized cybersecurity jobs and roles.

To optimize the recruitment process further, organizations should also assess which specific skills and competencies can be acquired in-house and which cybersecurity roles require external hiring.

Organizations can often hire internally for non-technical roles such as governance, risk and compliance, as well as cybersecurity awareness and training specialists. These roles can be filled by individuals within the organization who have a good existing knowledge of company policies, procedures and culture. On the other hand, for technical and specialized roles, it may be more appropriate to hire externals who have experience in dealing with complex cybersecurity incidents and can provide valuable insights and support to the organization.

Even though finding external hires can be advantageous for introducing new perspectives and diversifying the available skill set across the organization, knowing where and how to look for talent can be an overwhelming task.

There are several avenues that organizations can pursue to source candidates:

– Online employment platforms can be used to find a broad range of candidates for cybersecurity roles and positions.

– Head-hunters and recruitment agencies can help identify passive candidates – those who aren't actively looking for a new job – and help organizations hire high-quality candidates.

– Cybersecurity conferences and events allow organizations to recruit professionals already engaged in the field.

– Hackathons and capture-the-flag events (cybersecurity competitions that challenge participants to find and exploit vulnerabilities) can be used by recruiters to identify and potentially hire individuals with the right skill set.

– Referral programmes enable organizations to capitalize on the professional network of their employees and hire qualified like-minded candidates seeking opportunities in cybersecurity.

– Networking groups dedicated to specific communities (women or military veterans, for example) can provide access to skilled candidates with non-traditional profiles.

To build a sustainable cybersecurity talent pipeline, organizations should seek out candidates who have the potential to learn quickly and demonstrate a growth mindset. Moreover, when searching for talent, organizations should consider diversity and inclusion (for gender, race and neurodiversity among others) and integrate them into their recruitment efforts.

By embracing diversity, whether through the use of inclusive language in job advertisements, practising blind hiring or ensuring that hiring managers are reflective of diversity and trained in unconscious bias, organizations can tap into a broader talent pool. EU-based research also shows that employing women in STEM roles could improve the EU's GDP per capita by between 2.2% and 3% by 2050.[34]

“ Cybersecurity is often misunderstood as a discipline, and many tend to regard it solely as a technical field.

Cybersecurity is often misunderstood as a discipline, and many tend to regard it solely as a technical field. From the recruitment perspective, this misperception can result in inaccurate assessments of the required skills and experience. According to a 2021 survey,[35] 29% of cyber leaders noted that HR departments at their organizations likely do not understand the skills necessary to work in cybersecurity and consequently exclude strong job candidates. Moreover, 25% of surveyed cyber leaders also find that job postings at their organization tend to be unrealistic and demand too much in the way of experience, certifications and specific technical skills.

BOX 5 **Addressing misperceptions**

To tackle misperceptions, organizations should:

- Create a recruiter toolkit with key messages and an employee value proposition (EVP). Such toolkits can provide guidance (for screening and interviewing, for example) on how to find the right people for cybersecurity roles.
- Build relationships and direct communication channels between recruiters and hiring managers to ensure a better understanding of the role.
- Involve cybersecurity and HR teams in the development of job descriptions, skills specifications and qualification/certification requirements to ensure that the job prerequisites and expectations are accurately represented.
- Provide foundational cybersecurity training (e.g. workshops) for HR professionals involved in the hiring of cybersecurity professionals. Learning opportunities can help HR understand the industry better as well as the skills and qualifications required for different roles. Ultimately, greater awareness of cybersecurity can allow HR teams to find candidates who match the requirements.
- Update traditional HR processes and requirements that may not be necessary or relevant in the cybersecurity field – for example, by opening up internship opportunities for high-school students rather than just university graduates.
- Develop a cybersecurity culture across the organization by building awareness about the potential threats and highlighting the importance of cybersecurity in all aspects of the business. This will help HR teams understand the significance of cybersecurity roles and the need to prioritize them in recruitment efforts.

3.2 Actionable approaches for evaluation and validation

Evaluation of know-how is a critical aspect that involves a thorough assessment of practical skills, hands-on experience and the ability to apply knowledge in the real world. In cybersecurity, a great deal of attention is paid to technical skills – such as network security, penetration testing, encryption, incident response and so forth – that allow cybersecurity professionals to defend against cyberthreats and secure digital assets.

BOX 6 **Technical and non-technical skills**

To evaluate **technical skills**, recruiters and hiring managers can:

- Make use of scenarios, cyber ranges and other immersive simulations. For candidates who may not have sufficient experience in a specific domain (IT graduates, for example), case studies or scenarios can be a good way of assessing technical abilities. These scenarios can be completed by candidates in their own time before an interview and can help candidates demonstrate their thought processes as well as practical skills while solving real-world cybersecurity problems.
- Request evidence of participation in technical competitions or challenges related to the field. Such evidence can help gauge candidates’ levels of knowledge and expertise.
- Ask technical questions in interviews to determine whether candidates have the

necessary expertise or simply an interest in cybersecurity**.** Technical questions should be asked in the context of previous experience and responsibilities.

– Look for or request industry certifications that can demonstrate proficiency in specific areas of cybersecurity.

While technical skills are important in cybersecurity, it is also crucial to consider other non-technical skills, such as communication skills, problem-solving abilities and teamwork. Hiring candidates solely based on their technical skills may overlook individuals who possess strong soft skills. Combined with technical skills, non-technical competencies contribute to a well-rounded cybersecurity workforce.

To assess **non-technical skills**, recruiters and hiring managers can:

– Conduct psychological assessments to evaluate candidates' personality traits and leadership skills. While these assessments are commonly used for candidates filling managerial positions, they can also provide valuable insights into a candidate's suitability for other cybersecurity roles. This is because such assessments can help determine if a candidate has the necessary qualities, such as self-management and adaptability, to thrive in the field.

– Ask competency-based interview questions about previous projects and how their behaviour and actions contributed to the success (or not) of the projects. Such questions allow recruiters to assess problem-solving abilities, decision-making skills and the ability to work effectively in a team. Moreover, by delving into past experiences, employers can gain insights into candidates' critical thinking, communication and collaboration skills.

– Request writing samples to evaluate written communication skills, attention to detail and ability to articulate complex ideas. These are crucial for cybersecurity roles in which strong communication skills are desired.

– Make use of scenarios to also assess candidates' critical-thinking skills, decision-making abilities and problem-solving approaches in real-world situations. By evaluating responses, recruiters can gauge their ability to analyse risks, make sound judgements and handle challenging situations.

– Have candidates deliver short presentations to showcase their research skills and ability to answer unexpected questions as well as their confidence in presenting information.

3.3 Is the skills-first approach applicable to cybersecurity?

Today, many cybersecurity jobs still require a university degree. A survey from 2022 found that 71% of respondents from Africa required a university degree to obtain a job in cybersecurity.[36] In Asia and Latin America, 68% and 61% of respondents confirmed the same requirement.[37]

The situation is somewhat different in other regions of the world. For example, in Europe and North America, 45% and 49% of surveyed individuals respectively noted that a university degree was a prerequisite for a placement in cybersecurity.[38] The demand for a university degree was the lowest in Oceania, where only 27% of respondents stated that a university degree was required by the employer to obtain a job in the cybersecurity sector.[39] Such a trend could be explained by increasing recognition that cybersecurity professionals must continuously adapt to emerging risks and acquire hands-on knowledge that extends beyond the confines of a formal degree in computer science, software engineering or information technology.

> Cybersecurity professionals must continuously adapt to emerging risks and acquire hands-on knowledge that extends beyond the confines of a formal degree in computer science, software engineering or information technology.

Put differently, practitioners in the field can emerge from unconventional paths, including non-academic courses, self-teaching and certifications that take a fraction of the time and financial investment to complete compared to a formal degree. Some 56% of cybersecurity professionals believe that a degree is not needed for a successful career in cybersecurity.[40]

The World Economic Forum report *Putting Skills First: A Framework for Action* asserts that by focusing directly on skills that individuals actually have – rather than on how they were acquired – organizations can improve economic opportunities and pathways to good jobs for many more people than traditional approaches have done.[41] The study concludes that by prioritizing a skills-first approach, more than 100 million people across 18 different countries could be added to the global talent pool spanning businesses and industries.

In cybersecurity, the skills-first approach emerges as a compelling solution to the shortage of available talent. Organizations can implement this approach by:

- Accepting certifications, microcredentials and other evidence of knowledge (such as participation in capture-the-flag competitions) that can showcase a candidate's skills and identify areas where they need further development.
- Encouraging job rotation for employees with a passion for technical domains in order to increase exposure and facilitate the development of expertise.
- Decentralizing security responsibilities and involving employees from different backgrounds and departments. Introducing competitions and challenges, such as hackathons, helps in identifying and nurturing talent from within the organization. It also allows organizations to bridge the gap between employees who may not traditionally work together, developing a culture of teamwork and shared responsibility.

4 Retaining cybersecurity professionals

From the perspective of cybersecurity, employee retention is an issue across most roles.

Employee retention refers to an organization's ability to keep productive and talented workers engaged and motivated to stay. This often involves efforts to reduce turnover by creating a positive work environment, offering opportunities for growth and addressing factors that make employees seek better opportunities elsewhere.

In cybersecurity, some research shows that the average tenure of the chief information security officer (CISO) is 18 months, which is short compared to that of other executives.[42] Similarly, 56% of cybersecurity leaders have difficulty retaining qualified cybersecurity professionals,[43] and nearly half of cybersecurity leaders are expected to change jobs by 2025.[44]

Cybersecurity workforce retention is particularly challenging for organizations in developing and emerging regions such as Africa, the Western Balkans and Latin America.[45, 46, 47] Motivated by higher incomes and better job opportunities, many skilled professionals transition from cybersecurity careers in the public sector to similar roles in private industry or decide to migrate to other countries, resulting in the cybersecurity brain drain. This not only decreases the talent pool but also contributes to a decline in domestic innovation and economic contribution.

4.1 The causes of cybersecurity employee turnover

In an increasingly competitive and fast-moving cybersecurity labour market, it is critical for organizations to understand why some employees go and others stay. While individual motivations for departure may differ, some of the main causes for attrition among cybersecurity professionals include:

- Insufficient appreciation of and recognition for cybersecurity professionals, which, in turn, contributes to a decreased sense of achievement and demotivation.
- An unhealthy and unsupportive working culture characterized by unrealistic expectations and poor work–life balance. A study found that 99% of CISOs work extra hours every week and about one in 10 CISOs work an extra 20–24 hours per week.[48]
- Poor leadership and management, which results in disengagement, lack of connection and dissatisfaction among cybersecurity employees who seek more positive and supportive work environments.
- Limited organizational budgets, resulting in salary constraints in a competitive cybersecurity marketplace, which can prompt staff to seek alternative employment options that are more attractive financially.
- Prolonged exposure to stress, which not only results in a decline in individual performance and overall workplace happiness but can also have serious implications for employees' physical and mental health, in the form of burnout. Such a demanding work environment affects the productivity of 64% of cybersecurity professionals and is also said to be responsible for nearly 30% of security breaches in organizations across the Asia-Pacific region.[49, 50]

4.2 Understanding the impact of employee attrition

In general, high levels of employee turnover can affect organizations in various ways, including the loss of institutional knowledge, high replacement costs associated with recruiting new employees and rushed hiring processes. In the context of cybersecurity, employee attrition can:

- Delay the development and implementation of projects and stall innovation across the organization.
- Contribute to the loss of intellectual property and confidential information, especially in organizations dealing with proprietary technologies and equipment.
- Increase the risk of security breaches and compliance violations, ultimately affecting the corporate brand and client trust.
- Affect team morale and performance by increasing workloads and imposing more stress and pressure on remaining cybersecurity professionals.
- Contribute to gaps in expertise and loss of niche skills that are not easily replaceable. This can have implications for an organization's ability to perform its operations and may affect the delivery of products or services.
- Increase the pressure on hiring managers and HR to rush recruitment processes in order to fill vacant positions quickly and prevent any workflow disruptions. This can result in the recruitment of less qualified candidates who may not be the best fit for roles.

That said, it is worth highlighting that employee turnover is not always a negative occurrence and can also have a healthy impact on organizational dynamics. It can bring new talent with a different skill set, which, in turn, can provide new momentum and help promote innovation. Moreover, it can create growth opportunities for remaining professionals, who may get a chance of promotion in order to fill existing vacancies.

4.3 Actionable approaches to boost employee retention

To increase employee retention, organizations should cultivate a culture that inspires and motivates employees. While such a culture should encourage high performance by setting clear expectations for staff and rewarding achievement, it should go beyond simply driving productivity.

A culture that inspires and motivates people should also create an environment in which employees feel empowered and have the opportunity to nurture a sense of purpose and belonging.

BOX 7 **Boosting employee retention**

To boost employee retention, organizations, together with their leadership and executives, should:

- Assess employee skills to ensure people are placed in the job that will best maximize their skill set. This exercise can also be used to determine what additional training an employee may need to thrive in their current position.
- Provide individual development plans rather than predefined career paths that do not account for enough flexibility and adaptability to address the different needs and aspirations of employees. Organizations should ensure clarity in terms of promotion and empower employees to craft their own job roles.
- Understand generational diversity and how having a wide age range might affect expectations in the workplace. Generational diversity and individuals' unique perspectives, experiences and ways of working should be acknowledged in the working culture.
- Listen to employees and action the ask. Organizations should take employees' concerns and ideas seriously and demonstrate how decisions are being made to address them (for example, making it clear that the workload is decreasing, stress is being reduced and so forth).
- Ensure managers are equipped with soft skills on how to manage a team. Leaders should be trained to build trust, drive engagement with teams and provide psychological safety for their employees. Moreover, leadership should prioritize mindfulness and employee well-being through leading by example.
- Be transparent about the corporate strategy. To have a sense of purpose and belonging, people need to have insights on the direction in which the organization is moving.
- Create enough resilience across different organizational teams on cybersecurity matters to reduce over-reliance on a few individuals within the cybersecurity team.
- Make cybersecurity jobs more compelling and challenging, rather than repetitive, by allowing employees to tackle more demanding tasks and showcasing their skills and know-how. This can help boost employees' sense of accomplishment and ability to make more meaningful contributions to the organization.
- Provide the right resources and tools to employees for their jobs. That said, while technology can help decrease the workload, it can also be a stress factor for individuals who may struggle to adopt it.
- Motivate and engage cybersecurity employees by giving them visibility and recognition (perhaps through acknowledgement programmes and/or awards or similar) for their efforts.
- Create an engaging workplace with learning opportunities on cybersecurity – including networking events and gatherings – to develop a sense of community.

4.4 Prioritizing mental health in cybersecurity

While working in cybersecurity provides numerous exciting opportunities, a survey found that 67% of cybersecurity professionals would not recommend a career in the industry.[51] Long working hours are often cited as the main cause for employee dissatisfaction. In addition, the high-stress environment and constant demand for vigilance can take a toll on the mental health of cybersecurity professionals. Data shows that two-thirds of cybersecurity professionals experience significant levels of stress at work, and more than half have been prescribed medication for their mental health.[52]

To address mental health concerns in the workplace, executives are increasingly prioritizing the issue. A report by Deloitte found that 76% of executives agree that workforce well-being should be measured and monitored, and 83% say it should be discussed at board level.[53]

BOX 8 **Looking after mental health**

There are a number of actions that organizations can take to promote mental health and the well-being of cybersecurity professionals in the workplace:

- Use a dedicated wellness app that can provide a wide range of resources – such as tips for managing stress, personal resiliency strategies, wellness workshops and so forth – to support employees' welfare.
- Offer mindfulness or mindfulness-based stress reduction training (MBSR) sessions to employees to help them focus and centre. To make these accessible to all staff, various interventions and options for personalization should be provided.
- Create mentoring programmes for junior members of staff, with senior leadership to provide guidance on how to navigate professional responsibilities and ensure a work–life balance.
- Encourage individuals to take regular leave and create a supportive environment that values time off.
- Ensure leadership leads by example and prioritizes taking regular leave themselves and openly communicates about it.
- Offer flexible working arrangements – including remote work options, flexible working hours, quiet workspaces, employee resources groups and so forth – to individuals with family responsibilities, neurodiverse employees, etc., to accommodate different needs and create an environment in which professionals can thrive. Sensory assessments can help identify sensory tolerance levels and individual preferences in teams. These insights could be used to adjust working spaces and models.
- Open additional cybersecurity hubs to cover cybersecurity incidents occurring out of normal working hours. The hubs should be based on the "follow-the-sun model", which allows tasks to be handled by and passed among cyber teams in different time zones.

4.5 Tactics for talent retention

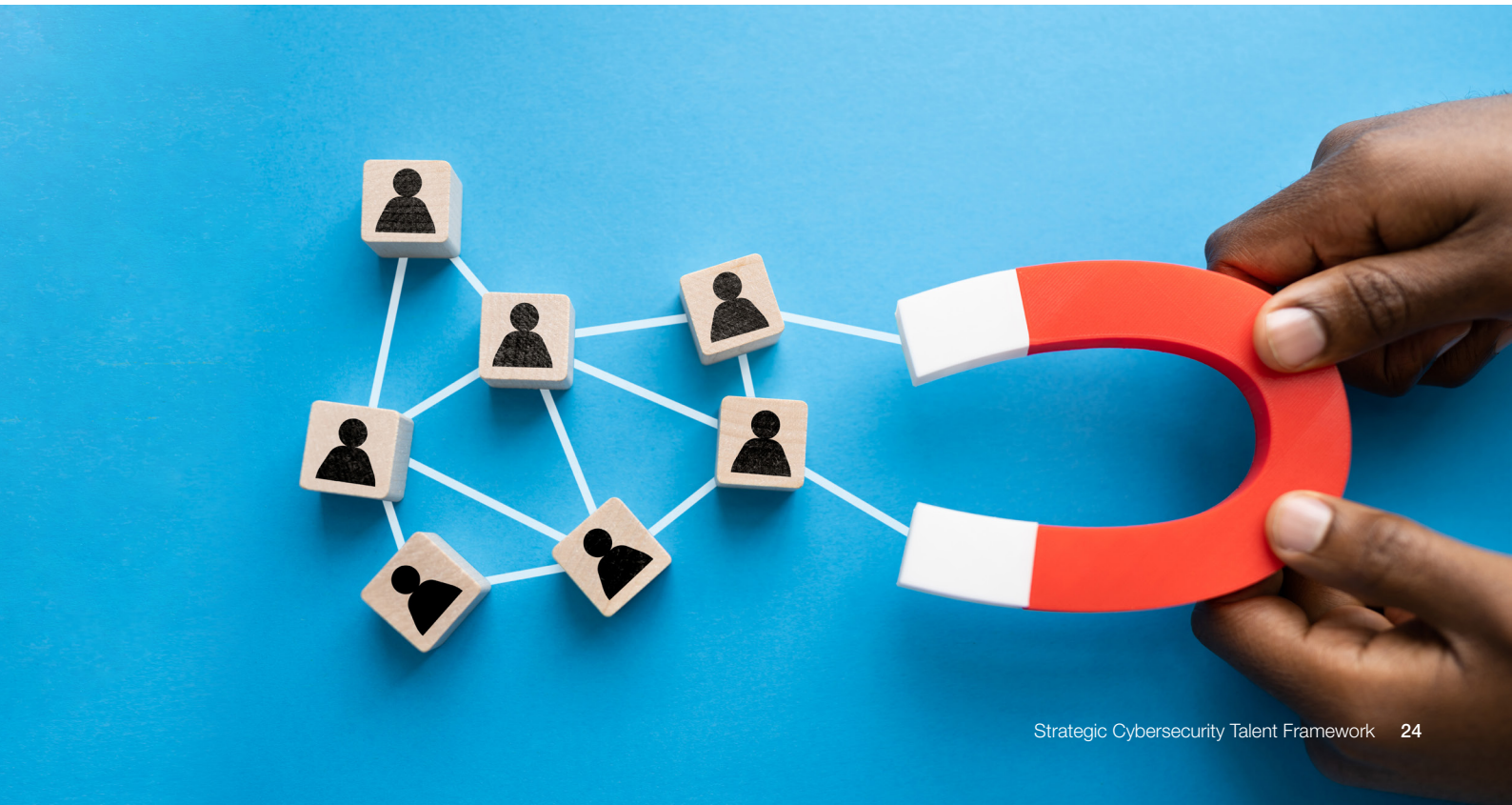
It is important to note that talent retention is not the sole responsibility of HR departments, but is a collective effort of various stakeholders from within the organization, including employees, managers and executive leadership. While approaches to talent retention may need to be tailored to the specific needs and circumstances of organizations (e.g. multinational corporations, SMEs), they should incorporate features that can help organizations build a loyal and committed workforce motivated to contribute to the delivery of organizational goals and objectives.

BOX 9

Features of talent retention

Actionable approaches on talent retention should encompass:

- A people-development toolbox that can support people on their individual development journey inside the organization. The toolbox should provide individuals with information about the best-suited jobs, most appropriate working environment, their strengths, what is needed for which jobs, training programmes, mentorship availabilities and so forth.
- A well-designed onboarding process that provides employees with the right information and tools to navigate the first few days and months in the new role.
- Opportunities for employees to change roles within cybersecurity, for example, from incident response to threat intelligence.
- Internal internship opportunities that enable employees to explore new roles and develop skills and experience without leaving the organization. Such opportunities can facilitate knowledge transfer but also help preserve institutional know-how and ensure a smooth transition of responsibilities when employees retire or move on to other roles.
- Executive commitment to well-being to set the tone from the top that the organization cares about its employees as individuals and not just as workers. This, in turn, can help develop a sense of trust and loyalty among employees, as they feel valued and supported by the leadership.
- Opportunities for employees to engage in fun activities, such as social gatherings and team-building events, to strengthen relationships among team members and improve engagement but also allow employees to unwind and recharge, ultimately improving team dynamics and reducing stress.
- Mechanisms to monitor progress and make adjustments to address any gaps or challenges. Organizations should make use of employee feedback mechanisms – including pulse surveys, town hall meetings, one-on-one discussions – to gather insights into the effectiveness of retention efforts.



Finally, the approaches should be flexible enough to adapt to changing workforce dynamics and employee feedback.

BOX 10

Driving action

Once approaches on talent retention have been defined, it is important to devise actions for their implementation. For example:

- Conduct regular happiness surveys. These can provide indications of employee satisfaction and engagement, helping organizations to track trends over time and make informed decisions accordingly. Organizations should use such surveys to understand why talent is staying and how individuals are evolving in their roles. Allowing cybersecurity professionals to voice their opinions and share ideas about new product ideas also helps develop an open and collaborative environment.
- Gather and analyse data from exit interviews. These give organizations an opportunity to identify reasons why individuals have chosen to leave as well as areas for improvement.
- Communicate the importance of talent retention as well as its potential impact on organizational success. In the development phase, organizations should solicit feedback and input from employees to ensure the approach is aligned with their needs and preferences. Talent-retention strategies should be communicated to all employees to ensure clear understanding and buy-in across all levels of the organization, including the executive leadership.
- Develop and roll out related talent-retention initiatives, such as employee wellness programmes, team-building activities and performance bonuses. That said, such initiatives cannot be delivered without the right resources and budget in place.
- Stay informed about industry best practices and emerging trends in talent retention, which can then be incorporated into the approach.

Conclusion

Left untackled, the cybersecurity workforce shortage could have cascading implications for global security, economic stability and technological innovation.

It is imperative that decision-makers in public and private organizations collaborate in efforts to inspire the next generation of cyber defenders and remove entry barriers for individuals aspiring to pursue a career in the field. While striving to create a positive work environment, organizations should invest in education and training programmes, promote diversity in the cybersecurity workforce and provide professional development opportunities for existing staff. Moreover, as the digital landscape continues to evolve, mapping the Cybersecurity Talent Framework (CTF) against emerging technologies, such as generative AI, becomes essential in ensuring its relevance and adaptability.

That said, this is just the beginning of the journey towards addressing the cybersecurity workforce shortage. While noting that contexts, needs and possibilities may vary across geographies and industries, organizations must take action to translate approaches defined in this CTF into practice.

Appendix: Case studies

Attracting talent into cybersecurity

Data Security Council of India: CyberShikshaa

The Data Security Council of India (DSCI), which was set up by the National Association of Software and Service Companies (NASSCOM), launched CyberShikshaa in 2018 in partnership with Microsoft to equip young female engineers across India with essential cybersecurity skills.[54] Operating through classroom, blended and fully virtual modes in multiple cities and states, CyberShikshaa not only facilitates successful job placements but also narrows the diversity gap in the cybersecurity workforce.

During the COVID-19 pandemic, CyberShikshaa seamlessly transitioned to an online format, expanding its reach to aspiring cybersecurity professionals even in smaller cities. Moreover, the programme has evolved to cater to diverse needs, introducing initiatives such as the "Women on Break" programme, providing training to women professionals re-entering the data-privacy workforce after career breaks.

Additionally, CyberShikshaa has extended its impact through specialized modules such as CyberShikshaa for BFSI (banking, financial services and insurance) and CyberShikshaa for AI/ML (artificial intelligence/machine learning), catering to different segments of learners and addressing the specific cybersecurity challenges faced by particular sectors.

Dubai Electronic Security Center: Dubai Cyber Innovation Park

Dubai Cyber Innovation Park (DCIPark),[55] as the research and knowledge division of the Dubai Electronic Security Center (DESC), aims to create a world-class integrated cybersecurity ecosystem, empowering the next generation of experts in cybersecurity from the public and private sectors along with academic institutions.

To that end, it runs projects such as the Cyber Security Competency Framework (Qudraat), which, among other things, maps all cybersecurity employees in the city to the framework, linking employee assessment and evaluation with training and development. Qudraat also ensures that capacity-building extends to academic institutions and maintains a balance between the city's demand and the supply of skills. The training and upskilling initiatives are delivered through the CyberNode programme, a partnership between the government, private sector and academia, to empower cybersecurity capabilities in the city and beyond. Another DCIPark project is Emirati Capture The Flag, which aims to promote cybersecurity skills among Emirati students and youth as well as invest in their cybersecurity innovations. DCIPark also runs 100-day cybersecurity challenges during which participants are required to address a given challenge by developing a working solution. At the end of the period, contestants submit their solutions to DESC.

DESC has achieved a 50% reduction in time-to-fill critical cybersecurity roles and recorded a 95% increase in employee satisfaction and retention, attributed to ongoing learning opportunities.

Through practical skills development, the nurturing of cybersecurity talent and the creation of a pipeline for future experts, the initiatives align seamlessly with DCIPark as a scalable model, collectively contributing to the cultivation of a skilled and resilient cybersecurity workforce for Dubai's digital future through internal training, external partnerships and a robust competency framework.

Girls Who Code: Work Prep

To close the gender gap in technology, Girls Who Code is leading a movement to inspire, educate and equip students who identify as girls or non-binary individuals with the computing skills needed to pursue 21st-century opportunities. Since launching in 2012, Girls Who Code has reached 580,000 students.

In 2021, Girls Who Code piloted Work Prep,[56] an experiential, virtual programme for college students designed to build career skills and confidence and expose students to partner company culture, opportunities and role models. The three-week programme is designed to be flexible for busy college students, featuring a combination of asynchronous activities (i.e. students working independently according to their own schedule) and synchronous work (i.e. students engaging simultaneously in real-time work). As part of the cybersecurity Work Prep, students are introduced to multiple cybersecurity roles and work together to complete the mitigation, response and recovery phases of an incident-response plan framework while also meeting cyber leaders at the partner company.

As a result of the programme, the overwhelming majority of students said they were more likely to pursue a career in technology and that they felt more prepared to apply for and be interviewed for technical internships and jobs.

Inclusive Cyber: Jumpstarting interest and careers in cyber

Inclusive Cyber,[57] an initiative of the World Economic Forum Global Shapers Community,[58] aims to build a cyber talent pipeline as diverse as the challenges that will be faced. The initiative spans Montreal, Kigali and London and mobilizes atypical and under-represented non-STEM talent to jumpstart their cyber interest and careers. Inclusive Cyber

does this through: 1) leading skills workshops and using a transferable skills toolkit built on the National Institute of Standards and Technology (NIST)'s National Initiative for Cyber Education (NICE) framework; and 2) representing the youth voice on cyber capacity-building and with leading policy-makers, such as the UK Cyber Security Council and Quebec's CyberEco.

At the heart of the initiative is the transferable skills toolkit, which helps individuals from disciplines including literature, fine arts and political sciences reframe and translate the value of their existing skills to best-match cybersecurity roles. Over five years, Inclusive Cyber has run 27 workshops and directly coached some 1,315 students on breaking into cybersecurity. These workshops took place in non-STEM faculties across leading universities, including McGill University, University of Toronto, London School of Economics, Queen Mary University of London, Royal Holloway and University College London. In Kigali, Inclusive Cyber built a new curriculum to equip young underprivileged professionals with competitive cybersecurity and transferable skills.

Institute for Security and Safety: eurobits women academy

In collaboration with the eurobits women academy (ewa),[59] the Institute for Security and Safety aims to inspire women to pursue a career in cybersecurity. At 11%, the proportion of women in cybersecurity in Germany is far below the international average.

As part of a three-year project, the objective is to create a platform for female career changers to:

- Provide orientation and guidance on the career opportunities available in cybersecurity using their existing strengths.
- Offer an in-service, modular training programme that can run alongside their current job to help them acquire the most important knowledge in the field of cybersecurity over several months and give insights into various areas of expertise.
- Facilitate access to a cybersecurity network with contacts in the industry for internship placements and job offers.

The aim is to make it easier for women to enter cybersecurity and support them in achieving their career goals.

Ministry of Transport and Communications of Finland: The Cyber Citizen Project

To develop a common, shared model for learning cyber citizen skills across the European Union, the Finnish Ministry of Transport and Communications, with the financial support of the EU, is leading the Cyber Citizen project.[60]

The project features a Cyber Citizen hub, comprising a dynamic web portal with online tutorials, a cybersecurity game, quick guides and instructions, to raise awareness about the constantly evolving cyberthreat landscape. In addition to the resources, the Cyber Citizen project forges a community dedicated to cybersecurity training and awareness across all EU countries. Governments, NGOs, businesses and individuals, including researchers, are all invited to contribute.

Siemens: CyberMinds Academy

In response to the high demand for cybersecurity talent, Siemens has created the CyberMinds Academy to attract and nurture new talent with no prior experience in cybersecurity into cybersecurity specialist roles.[61]

Running in two locations, in Portugal and Spain, the academy delivers a one-year training programme combining learning and practical on-the-job training. Participants also have the opportunity to work closely with cybersecurity experts and participate in a diverse cultural environment. The CyberMinds Academy not only contributes to the development and training of professionals who can bring fresh perspectives and ideas to cybersecurity but also promotes diversity and inclusion in the workforce.

So far, the two CyberMinds Academies have trained 26 participants from different backgrounds. Eight of those individuals have been hired to work in cybersecurity for Siemens.

Trellix: Soulful Work

As a cybersecurity company, Trellix aims to bring awareness to the purposeful work of cybersecurity and create pathways for under-represented groups to fill the talent gap. Spearheading Soulful Work, Trellix fosters diversity and inclusion through partnerships and initiatives aimed at combating unconscious bias and expanding opportunities for all.[62]

In collaboration with Gotara, Trellix launched a programme focused on empowering women to navigate and advance their careers, addressing the challenges of gender inequality in the industry. Trellix joined forces with the Hispanic Alliance for Career Enhancement (HACE) to create a cybersecurity accelerator programme that includes a mentorship and development initiative tailored specifically to Latinos, equipping them with the necessary skills to thrive in cybersecurity roles. Trellix also collaborated with the National Cybersecurity Alliance to create the Historically Black Colleges and Universities (HBCU) Cybersecurity Career Program, which actively engages in mentoring projects with the aim of raising awareness of cybersecurity careers among students and providing them with the support needed to successfully navigate the job search process. Through these efforts, Trellix is working towards creating a more diverse and inclusive cybersecurity workforce.

Women4Cyber: Supporting the participation of women in cybersecurity

Women4Cyber,[63] a non-profit European private foundation, aims to promote, encourage and support the participation of women in cybersecurity. It currently represents a community of 28 national chapters and over 60,000 followers from across Europe.

To attract women to a career in cybersecurity and address the expected skills shortage in technical, operational, managerial and leadership positions, Women4Cyber focuses primarily on facilitating access to education, providing discounts and scholarships, supporting job seekers and HR departments to increase the number of women in cybersecurity, and uses local experts to amplify its reach and develop on-the-ground activities through the national chapters.

Its successful mentorship programme has helped more than 400 women so far, while scholarships and strategic partnerships are facilitating women's access to cybersecurity education and certification, and the Women4Cyber job corner and network is increasing the number of female applicants for open positions across Europe.

Educating and training cybersecurity professionals

Absa Cybersecurity Academy

Absa in South Africa established a cybersecurity academy in 2019 to address the cybersecurity skills shortage while creating job opportunities for previously disadvantaged and visually impaired learners.[64]

To address the high youth unemployment rate in South Africa, Absa partnered with the Maharishi Invincibility Institute and the Hein Wagner Academy for the Visually Impaired to develop cybersecurity skills for the academy's students. Completion of the three-year programmes accredits these students with 17 international certificates, equipping them for employment in the cybersecurity job market.

So far, through collaboration with the Maharishi Invincibility Institute, 19 students, who also completed a one-year internship, have been given permanent positions at Absa. A second cohort of 20 students is currently enrolled in the year-long internship in Absa's Information and Technology Office.

In 2024, the first cohort of students will graduate from the Hein Wagner Academy for the Visually Impaired. The graduation will be a first of its kind for the industry, proving that visually impaired people are well suited for the technology and cybersecurity job market and charting a course for others to follow.

Cisco Networking Academy

The Cisco Networking Academy equips students with essential and in-demand cybersecurity, networking and digital skills.[65] Since its establishment in 1997, it has trained more than 20.5 million individuals across 190 countries and continues to build on its impact with courses ranging from an introduction to cybersecurity and ethical hacking to professional skills, which are designed to meet industry demands.

The Cisco Networking Academy aims to train an additional 25 million people by the end of 2032 through its new Skills for All platform,[66] featuring mobile-first gamified learning experiences and an unmatched network of 11,700 educational institutions and organizations offering its courses.

The Cisco Networking Academy also collaborates with governments worldwide to develop cybersecurity skills and talent. In alignment with the efforts of the US White House and the European Commission to increase the size of the cyber workforce, Cisco aims to train 200,000 people in cybersecurity skills in the US and 250,000 individuals in the EU by 2025. In the first year following the announcement, Cisco has trained 51,000 individuals in the US and 87,000 individuals in the EU. Remarkably, 95% of students who have completed certification-aligned courses attribute new job and/or educational opportunities to their participation in the programme.

Cyber Security Agency of Singapore: SG Cyber Talent

In 2020, the Cyber Security Agency of Singapore (CSA) established the SG Cyber Talent initiative to nurture cybersecurity enthusiasts from a young age and help professionals deepen their skills.[67] Since its inception, the initiative has helped more than 22,000 individuals through cybersecurity bootcamps, mentoring, career conversion programmes and leadership education. The main programmes under SG Cyber Talent include SG Cyber Leaders, SG Cyber Women, SG Cyber Youth and SG Cyber Olympians.

To illustrate the impact, as part of SG Cyber Youth, the Youth Cyber Exploration Programme (YCEP) was started in 2018 and has since trained more than 1,500 secondary-school students in basic cybersecurity knowledge through a series of bootcamps and capture-the-flag competitions organized by CSA and the five local polytechnics, in collaboration with industry partners. As a step-up, the advanced YCEP is also available to students with some existing cybersecurity knowledge.

The Cybersecurity Strategic Leadership Programme (CSLP), organized by CSA, in collaboration with academic partners, as part of SG Cyber Leaders, aims to equip current and future generations of local cybersecurity leaders with a deep level of understanding on the key global drivers shaping cybersecurity strategies and innovation and to lead their organizations' cybersecurity functions effectively. About 50 senior cybersecurity leaders participated in the first two runs of the CSLP in 2022 and 2023, covering themes such as growing a C-suite Mindset, leading the organization and leading the ecosystem.

The participants also embarked on an overseas immersion trip to the US and the UK to engage in deeper discussions with local cybersecurity leaders and organizations.

Cybersecurity Learning Hub

The Cybersecurity Learning Hub[68] is an initiative designed to tackle the globally cybersecurity skills shortage and democratize access to cybersecurity career paths.

Led by Salesforce with support from Fortinet, the Global Cyber Alliance and the World Economic Forum, the Cybersecurity Learning Hub features training modules on numerous topics such as cyber resilience, artificial intelligence (AI) cybersecurity and cybersecurity table-top exercises.

In addition to the training modules, it also includes a growing library of career-oriented information and expert interviews intended to help learners map their own career path through a variety of in-demand cybersecurity roles.

Since its launch in 2019, the Cybersecurity Learning Hub has trained more than 290,000 individuals spread across all continents.

EDP – Energias de Portugal: Global Black Belt Program

To improve the architecture and security of systems within the organization, EDP has launched the Global Black Belt Program. The programme aims to enhance employees' technical skills and knowledge, enabling them to design and implement secure and robust systems. To meet its objectives, the programme covers topics such as security best practices, threat modelling and secure coding techniques.

To participate in the programme, employees are asked to fill out a questionnaire to assess their level of expertise and provide suggestions for further development. The programme offers various expertise paths, such as Azure Cloud Architect Expert, AWS Cloud Architect Expert, Google Cloud Architect Expert, Human Behaviour Expert, Security Architect Expert, Governance, Risk and Compliance Expert and more.

Each path is structured around three levels of expertise: Global White Belt, Global Green Belt and Global Black Belt. Every level has specific requirements regarding skills, experience, certifications and recommended conferences and learning paths to help participants advance their knowledge and skills.

Fortinet: Security Awareness and Training Service

To educate schools on how to navigate the digital landscape securely, Fortinet has extended its commercial security awareness and training service at no cost to schools in countries around the world.[69] Recognizing the unique educational context, the company tailored staff training to the academic sector and hired teachers to develop a security awareness curriculum that addressed the learning needs of all students aged four to 18. The education edition was initially developed in alignment with the US's White House Cyber Education and Workforce Initiatives in 2022. The following year, the initiative expanded to include Canada, the UK, Australia and Brazil and is now available to 11.8 million education staff and 64 million students, with further plans for global outreach.

In addition to its collaboration with educational institutions worldwide, in 2020, at the outset of the COVID-19 pandemic, Fortinet amplified its existing efforts by offering all self-paced technical certification training at no cost, in response to the escalating threat landscape. The response was staggering, with course registrations peaking at one every seven seconds during the initial weeks.

KnowBe4, MiDO Technologies and the UK Foreign, Commonwealth and Development Office: MiDO Cyber Academy

To reduce poverty and stimulate inclusive economic growth in South Africa, in March 2023 the UK Foreign, Commonwealth and Development Office (FCDO), in partnership with KnowBe4 and MiDO Technologies, established the MiDO Cyber Academy.[70]

Partly inspired by the Absa Security Academy in South Africa and aimed at underserved communities within the Western Cape, the MiDO Cyber Academy focuses on cybersecurity, critical thinking, soft skills, innovation, collaboration and personal resilience. The academy aims to bridge the digital and cyber skills divide that exists between job seekers and internships or junior positions available in the IT and cybersecurity market.

The academy offers a blended-learning approach, combining e-learning with in-person facilitation, personal-resilience training, life skills, industry exposure and mentorship. The programme lasts 10 months, targeting youths aged 18 to 24 and facilitating cohorts of up to 21 candidates, emphasizing real-world projects, candidate placement and integration into the workforce.

Through industry involvement and support, such as masterclasses and hands-on project work, students are exposed to real-life challenges faced by security-industry professionals with the extra benefit of building up a network of senior members in the community and potential future employers.

Metabase Q: Council of Experts in Regulation and Cybersecurity

Metabase Q established the Council of Experts in Regulation and Cybersecurity (CERC),[71] a pioneering, multidisciplinary council comprising cybersecurity practitioners with a recognized trajectory from the private sector, academia and civil society.

The CERC serves as a catalyst to position Mexico as a leader and benchmark in Latin America in the development of cybersecurity.

Within the CERC, the education committee specifically targets United Nations Sustainable Development Goal 4, ensuring inclusive access to education and promoting learning opportunities in cybersecurity for all. For example, the Digital Distance Education programme is designed to provide educational resources for children and young adults. The Digital Cyber Academy (DCA) aims to both attract skilled individuals and bridge the expertise gap in Latin America. The DCA allows students to enrol at no cost and serves as a hub for acquiring technical knowledge and practical skills. The DCA has graduated five generations of students, marking a crucial milestone in preparing the next generation of cybersecurity professionals.

Organization of American States: Creating a Career Path in Cybersecurity

Between 2017 and 2023, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) – with the financial support of Citi Foundation – implemented a multiphased project entitled Creating a Career Path in Cybersecurity with the purpose of addressing the shortage of skilled cybersecurity professionals.[72] The main goal was to equip young people with essential skills to access entry-level positions in cybersecurity, offering technical training, soft skills development and professional growth opportunities.

Over six years, the project successfully trained more than 1,200 individuals across a number of countries, including Argentina, Brazil, Colombia, Costa Rica, Guatemala, Mexico, Panama, Peru, Dominican Republic and Trinidad and Tobago. Its beneficiaries not only acquired technical expertise and certification but also developed crucial soft skills and secured initial job placements in both public and private institutions.

Building on the lessons learned from the implementation of this programme and considering the persistent shortage of professionals in this field, the Cybersecurity Program plans to launch a new workforce development programme in one OAS member state in 2024. This project aims to provide a systemic approach to cyber education, with the long-term goal of increasing the supply of qualified cybersecurity professionals, offering training and employment opportunities while assisting the beneficiary country in developing a national cybersecurity education framework. The goal is to create a sustainable and robust pipeline of skilled professionals, contributing to the country's cyber resilience.

Saudi Arabia National Cybersecurity Authority: Saudi Cybersecurity Higher Education Framework

Saudi Arabia's Vision 2030 emphasizes human capital development, including in cybersecurity, as a core pillar of its coherent development strategy. Central to these efforts, the Saudi Arabia National Cybersecurity Authority (NCA) has introduced the Saudi Cybersecurity Higher Education Framework (SCyber-Edu).[73] This framework aims to elevate cybersecurity education, aligning it with market demands and the objectives of Vision 2030. SCyber-Edu sets standards for cybersecurity education across Saudi universities, ensuring courses meet market-relevant skills and knowledge domains.

The framework involves several critical components, including developing a recognition process for cybersecurity degree programmes, creating incentives for universities to align their courses with SCyber-Edu standards, and establishing a database of recognized degrees to guide student selection.

In 2023, SCyber-Edu had a significant impact on Saudi Arabia's educational landscape. It has been adopted by 45 prestigious institutes, influencing 82 cybersecurity higher education programmes nationwide. The NCA has observed a significant increase in use of the framework by these institutions, further enhancing the quality and relevance of cybersecurity education in the country.

Recruiting the right cybersecurity talent

Cybersafe Foundation: CyberGirls Fellowship

The CyberGirls Fellowship,[74] an initiative by Cybersafe Foundation, confronts Africa's cybersecurity gender disparity. While women represent half of Africa's population, they account for a mere 9% of its cybersecurity workforce. The fellowship aims to change this by empowering young African women aged 18–28 with cybersecurity skills and thereby promote socioeconomic growth.

The fellowship programme is built on three pillars – training, mentorship and placement – and provides a cutting-edge training curriculum that is updated annually to meet industry demands. This curriculum offers free, high-quality cybersecurity education that combines technical and soft skills over an eight-month period. Additionally, a global mentorship pillar features a five-to-one ratio of female mentors to fellows, enhancing support and representation. The initiative's placement arm then assists fellows in securing their first cybersecurity roles, ensuring a smooth transition from learning to employment.

Beyond technical training, the programme employs mindset-shifting tools, such as the CyberGirls mantra consisting of affirmations and positive self-talk, to overcome stereotypes and boost confidence among fellows.

CyberGirls alumni, spread across 22 countries, often see their income increase by more than 400% within six months of landing a cybersecurity role after completing the programme.

Hewlett Packard Enterprise: Cybersecurity Career Reboot Program

The Hewlett Packard Enterprise (HPE) Cybersecurity Career Reboot Program,[75] launched in 2022, is rooted in the belief that the greatest gift is to give someone an opportunity. The programme recognizes that talent can come from non-traditional paths, and that formal degrees or prior cybersecurity experience are not always prerequisites.

The programme is an immersive nine-month experience that offers a blend of mentorship, hands-on experience and formal training to equip participants with the skills required in the cybersecurity domain. Participants are placed in a team aligned with their interests and aspirations and with the business needs of HPE. They are dedicated to specific projects but also spend time attaining cybersecurity certifications and building their network both inside and outside of the company.

HPE's Cybersecurity Career Reboot Program seeks to create new cybersecurity talent rather than taking it from other organizations. Those who have passed through the programme include a school bus driver, a restaurant owner, a respiratory therapist and a nurse. While there are inherent challenges in career transitions, HPE has found many parallels between the skills acquired in candidates' former careers and the ones essential for success in cybersecurity.

Some 93% of graduates have secured full-time positions at HPE or other companies.

NICE Workforce Framework for Cybersecurity

NIST published the NICE Workforce Framework for Cybersecurity (NICE Framework) to aid the development, recruitment and retention of the cybersecurity workforce.

The NICE Framework provides a standard approach for describing the tasks, knowledge and skills needed to perform cybersecurity work, enabling a better understanding of talent needs and expectations. Jobseekers use the NICE Framework through tools, such as those provided by CyberSeek.org,[76] to chart pathways for future learning and career advancement. Educators and trainers, in courses offered by, for instance, Temple University,[77] use it to describe and map the curriculum to current marketplace demand, while employers use it to conduct workforce assessments and identify staffing gaps or to craft more accurate position descriptions and improve recruitment. For example, the NICE Framework Mapping Tool from the Cybersecurity and Infrastructure Security Agency (CISA) measures alignment of job descriptions.[78]

The use of common terms and language helps to organize and communicate cybersecurity work. In this way, the NICE Framework has helped to simplify communications and provide improved clarity and consistency at all organizational levels – from an individual to a programme, organization and more.

Schneider Electric: Cybersecurity Talent Development

Schneider Electric (SE) sees employees as vital to the safe and secure delivery of its products and services, strengthening critical global infrastructure and fuelling the digital economy. SE's Cybersecurity Talent Development initiative is a comprehensive programme that defines the cybersecurity talent needs of the company, then identifies, attracts and upskills cybersecurity talent in an inclusive way.

In preparation for the future, SE implemented a people-centric approach and completed the following milestones:

- **Community identification:** Through careful assessment and mapping, SE has successfully identified cyber employees within the organization.
- **Key roles definition:** SE outlined the current and future top cybersecurity mandates and domains from digital practices and functions to business and operational units. Following this exercise, SE completed career path mapping to common roles.
- **Career path development:** To support the growth of cyber roles, SE established individual role descriptions and recommended training programmes and certifications to facilitate professional development. Learning and rotation are central to developing the company's talent pool.
- **Community meetings:** These monthly calls are designed to create synergies and networking opportunities by sharing initiatives from different teams.

The benefits for employees have been equal career development opportunities and diversity of career paths. The SE benefits are a stronger pipeline of cyber talent and a future-ready cybersecurity community.

Siemens Energy: Cybersecurity and Industrial Infrastructure Security Apprenticeship Program

As an energy organization, Siemens Energy has identified a need to grow the pool of workers who can understand both the physical and cyber aspects of operational technologies.

With fewer than 10 colleges in the United States offering cybersecurity classes focused on operational technologies in 2020, Siemens Energy partnered with ICS Village, the Regional Economic Development

for Eastern Idaho (REDI), MISI Academy, Capitol Technology University, SANS Technology Institute and Idaho State University (ISU) to design and implement the Industrial Cybersecurity Apprenticeship Program (CIISAp).[79] CIISAp is an academically rigorous programme that places apprentices in real-world job rotations designed to immediately apply their skills as they learn. It enables people with moderate computer skills to gain the hands-on experience and knowledge needed to competently fill cybersecurity vacancies that currently pay above $90,000 per year.

Telefónica: Campus 42

Telefónica's Campus 42 is dedicated to attracting, educating and recruiting skilled cybersecurity professionals and experts.[80] Campus 42 – characterized by free access to education with no classes or textbooks, available 24/7 and focusing on practical, project-based learning in a collaborative environment – aims to develop highly skilled technology experts in disciplines such as cybersecurity. The programme emphasizes the development of industry-relevant skills, and admission is based on logical thinking and problem-solving abilities rather than academic prerequisites.

Telefónica, a key partner of Campus 42, provides essential support, including financial assistance and resources such as Telefónica office space. The company extends further support by offering employment opportunities and internships to Campus 42 students, enabling them to gain valuable work experience in the telecommunications and technology sectors. This collaboration has helped create a talent pool of highly skilled professionals available for recruitment, and Telefónica's internal cybersecurity unit actively filters and collaborates with these individuals on internal projects, thereby promoting and refreshing internal cyber skills.

The UK Cyber Security Council

The UK government recognizes that there need to be clear pathways into and through the cybersecurity profession. Knowledge, skills and experience in cybersecurity should be defined and acknowledged in a way that is similar to more established professions, such as law and engineering.

To do this, the UK Cyber Security Council was launched in March 2021 and represents a world first for the cybersecurity profession.[81] Its mission is to be the voice of the profession, bringing clarity and structure to the growing cyber workforce and the range of qualifications, certifications and degrees that exist across the field. It was awarded a royal charter, which enables it to bestow chartership on individuals – a national recognition of excellence and expertise – as is done in the engineering profession. This is a vital step towards bringing cohesion and consistency to the cyber workforce and, through the development of professional standards across numerous specialisms, practitioners are being recognized for their abilities as well as engaging in a more defined career pathway.

The council has now awarded more than 100 cyber professionals with this accreditation across four specialist areas, including Cyber Security Governance and Risk, Secure Systems Architecture, Cyber Security Audit and Assurance and Security Testing (Penetration Testing).

Retaining cybersecurity professionals

European Investment Bank: Job Shadowing Programme in Cybersecurity

The European Investment Bank (EIB), in efforts to enhance its professional development, implemented a job shadowing programme in cybersecurity. This initiative, aimed at employees with a keen interest in cybersecurity, provides a unique opportunity for cross-departmental collaboration and skills enhancement. The programme serves as a platform for mutual learning where cybersecurity experts share their expertise while gaining insights into the operational challenges faced by other departments.

Programme participants, upon agreement with their respective managers and the CISO, are allocated one day per week throughout a quarter to work alongside the information security team. This immersive experience enables participating employees to gain first-hand experience in cybersecurity and equips them with the skills required to perform work functions in cybersecurity such as risk assessment, audit exercises, information security alignment with other international financial institutions and so forth. Ultimately, the programme allows for the creation of an internal talent pool.

Repsol: Strengthening its cybersecurity team

Talent features prominently in Repsol's 2024–2026 cybersecurity strategy. The strategy recognizes that the risk of data breaches and deployment of new technologies, including AI, as well as the evolution of operational technology (OT) security, cannot be successfully managed without strengthening the cybersecurity team. To that end, Repsol aims to:

1. Gain support from the board to strengthen the team and achieve the defined strategy.

2. Enhance talent across key areas, including incident response, identity management, the operational technology security operations centre, network security and cloud security.

3. Draft hiring proposals with the necessary technical and soft skills while promoting diversity, especially female talent.

4. Retain hired talent with an interesting long-term value proposition focused on the physical and mental health of teams, including the possibility of fully remote working and monetary incentives.

Contributors

Lead authors

Marie Laure Esi Alorvor
Project Fellow, Bridging the Cyber Skills Gap, Centre for Cybersecurity

Natasa Perucica
Lead, Capacity Building, Centre for Cybersecurity

World Economic Forum

Sean Doyle
Lead, Cybercrime Atlas Initiative, Centre for Cybersecurity

Tal Goldstein
Head of Strategy and Policy, Centre for Cybersecurity

Akshay Joshi
Head of Industry and Partnerships, Centre for Cybersecurity

Acknowledgements

The World Economic Forum would like to thank the members of the Bridging the Cyber Skills Gap initiative without whose valuable insights, expertise and commitments this report would not have been possible. Our special thanks also go to the Cyber Security Authority of Ghana for their dedicated involvement in this effort. In addition, we would like to extend a warm thank you to: Yevgeny Dibrov, Co-Founder and Chief Executive Officer, Armis; Dorit Dor, Chief Technology Officer, Check Point Software Technologies; Paula Ingabire, Minister of Information Communication Technology and Innovation, Ministry of Information Communication Technology and Innovation of Rwanda; Doreen Bogdan-Martin, Secretary-General, International Telecommunication Union; Cheri McGuire, Chief Technology Officer, SWIFT; Bryan Palma, Chief Executive Officer, Trellix; Vikram Rao, Chief Trust Officer, Atlassian; Ken Xie, Founder, Chairman of the Board and Chief Executive Officer, Fortinet; and to others for their thought leadership, which helped set in motion this initiative.

Bridging the Cyber Skills Gap initiative

Mansur Abilkasimov
Schneider Electric, France

Abdullah M. Albaiz
National Cybersecurity Authority of Saudi Arabia, Saudi Arabia

Bushra AlBlooshi
Dubai Electronic Security Center, United Arab Emirates

Liliana Jiménez Alcocer
Metabase Q, Mexico

Hussain Aldawood
Neom Company, Saudi Arabia

Hussain Alebnalshaikh
Neom Company, Saudi Arabia

Alaa Alfaadhel
National Cybersecurity Authority of Saudi Arabia, Saudi Arabia

Aiman Aljumoay
sirar by STC, Saudi Arabia

Ayad A. AlKhoneen
sirar by STC, Saudi Arabia

Zeyad A. Alkhoneen
Saudi Telecom Company (STC), Saudi Arabia

Yasser N. Alswailem
Saudi Telecom Company (STC), Saudi Arabia

Eric Kafui Bansah
Cyber Security Authority of Ghana, Ghana

Liza Belozerova
Google.org, USA

Sharifa Bernard,
Amazon, USA

Laura Allen Bernstein
Deloitte, USA

Hamad Binsalleeh
Saudi Information Technology Company (SITE), Saudi Arabia

Wong Choon Bong
Cyber Security Agency of Singapore, Singapore

Ivan Bornacelly
Organisation for Economic Co-operation and Development, France

Carla Bouca
EDP – Energias de Portugal, Portugal

Grant Bourzikas
Cloudflare, USA

Jenny Brinkley
Amazon, USA

Nicole Cader
Absa Group, South Africa

Denise Cassidy
Accenture, Ireland

Koh Chia Chee
Cyber Security Agency of Singapore, Singapore

Giuseppe Cinque
Cisco Systems, Italy

Mariana Cardona Clavijo
Organization of American States, USA

Anna Maria Collard
KnowBe4, South Africa

Melonia Da Gama
Fortinet, USA

Arnaud de Vibraye
European Cyber Security Organisation, Belgium

Liat Doron
Check Point Software Technologies, Israel

Bobby Ford
Hewlett Packard Enterprise, USA

Cian Galvin
Department for Science, Innovation and Technology of the United Kingdom, United Kingdom

Debjani Ghosh
National Association of Software and Services Companies (NASSCOM), India

Öykü Işık
IMD Business School, Switzerland

Mercy Araba Kertson
Cyber Security Authority of Ghana, Ghana

Maitha Khalid
Dubai Electronic Security Center, United Arab Emirates

Atul Kumar
Data Security Council of India, India

Felix del Hierro Lapuente
Telefónica, Spain

Stefan Lee
Ministry of Transport and Communications of Finland, Finland

Anat Lewin
The World Bank, USA

Kathy Liu
World Economic Forum Global Shaper, London I Hub, United Kingdom

Moaza Majed
Dubai Electronic Security Center, United Arab Emirates

Paulo Moniz
EDP – Energias de Portugal, Portugal

Anna Moran
Department for Science, Innovation and Technology of the United Kingdom, United Kingdom

Joanne O'Connor
Hewlett Packard Enterprise, USA

Nina Olesen
European Cyber Security Organisation, Belgium

Jakub Olszewski
Standard Chartered Bank, Poland

Barbara O'Neill
EY, USA

Christopher Painter
Global Forum on Cyber Expertise Foundation, Netherlands

Inger Paus
Google, Germany

Chris Perna
Fortinet, USA

Alvin Piket
Trellix, USA

Manoj Puri
Absa Group, South Africa

Rahayu Ramli
PETRONAS, Malaysia

Rob Rashotte
Fortinet, Canada

Maria Teresa Verdú Sánchez
Repsol, Spain

Danielle Santos
National Institute of Standards and Technology (NIST), USA

Birgit Schimmel
Siemens, Germany

Joseph Schiro
At-Bay, USA

Leo Simonovich
Siemens Energy, USA

Lynn Simons
Salesforce, USA

Daniel Soo
Deloitte, USA

Colin Soutar
Deloitte, USA

Confidence Staveley
Cybersafe Foundation, Nigeria

Ina Steyn
Absa Group, South Africa

Santha Subramoni
Tata Consultancy Services, India

Caroline Troein
International Telecommunication Union, Switzerland

Paul Trueman
MasterCard International, United Kingdom

Marieke Vandeweyer
Organisation for Economic Co-operation and Development, France

Salvador E. Venegas-Andraca
Tecnológico de Monterrey, Mexico

Daniel Voloch
Girls Who Code, USA

Leonardo Von Prellwitz
Calypso AI, USA

Annika Wägenbauer
Institute for Security and Safety (ISS), Germany

Tilo Weigandt
Vaultree, Ireland

Elisabeth Williamson
Schneider Electric, France

Swantje Westpfahl
Institute for Security and Safety (ISS), Germany

Jelena Zelenovic Matone
European Investment Bank (EIB), Luxembourg

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Alison Moore
Editor, Astra Content

Endnotes

1. Franzino, Michael, Guraino, Alan and Laouchez, Jean-Marc, "The $8.5 Trillion Talent Shortage", Korn Ferry, 2018: https://www.kornferry.com/insights/this-week-in-leadership/talent-crunch-future-of-work.
2. ISC2, *ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce*, 2023: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.
3. World Economic Forum, *Global Cybersecurity Outlook 2024*, 16 January 2024: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.
4. ISC2, *ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce*, 2023: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.
5. Serianu, ACIC, *Africa Cybersecurity Report Kenya: Reimagining the African Cybersecurity Landscape*, 2023: https://www.serianu.com/downloads/KenyaCyberSecurityReport2023.pdf.
6. International Labour Organization, "Decent Work for Youth in India": https://www.ilo.org/newdelhi/info/WCMS_175936/lang--en/index.htm.
7. Kishore, Anita, "Democratising STEM Skills Is Crucial to Creating a Future Ready India", *The Hindu BusinessLine*, 28 February 2022: https://www.thehindubusinessline.com/opinion/democratising-stem-skills-is-crucial-to-creating-a-future-ready-india/article65094871.ece.
8. Lele, Sourabh, "India Suffering High Cybersecurity Skill Gap, 40K Open Positions: Report" *Business Standard*, 21 June 2023: https://www.business-standard.com/technology/tech-news/india-suffering-high-cybersecurity-skill-gap-40k-open-positions-report-123062100397_1.html.
9. *The Hindu*, "India Unable to Fill 30% of Cybersecurity Jobs Due to Skill Gap: Report", 21 June 2023: https://www.thehindu.com/business/Industry/india-facing-huge-shortage-of-cybersecurity-professionals-teamlease/article66994515.ece.
10. CyberSeek, "Cybersecurity Supply/Demand Heat Map": https://www.cyberseek.org/heatmap.html.
11. ISC2, *ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce*, 2023: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.
12. World Economic Forum, *Global Cybersecurity Outlook 2024*, 16 January 2024: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.
13. Weinstein, Debbi, "Meeting UK Businesses' Calls for Cyber Talent and Support", *Google*, 7 June 2023: https://blog.google/around-the-globe/google-europe/meeting-uk-businesses-calls-for-cyber-talent-and-support/.
14. Fortinet, *2023 Cybersecurity Skills Gap: Global Research Report*, March 2023: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/2023-cybersecurity_skills_gap_report_final.pdf?utm_source=blog&utm_medium=blog&utm_campaign=cybersecurity-skills-gap-2023?utm_source=blog&utm_medium=blog&utm_campaign=cybersecurity-skills-gap-report-2023.
15. Ibid.
16. Lockett, Brett, "Cybersecurity Hiring in 2023: Challenges and Demand for Skilled Professionals", LinkedIn, 6 March 2023: https://www.linkedin.com/pulse/cybersecurity-hiring-2023-challenges-demand-skilled-brett-lockett/.
17. World Economic Forum, "Reskilling Revolution: Insights and Tools": https://initiatives.weforum.org/reskilling-revolution/insights-tools.
18. Trellix, "Trellix Finds Workforce Shortage Impacts 85% of Organizations' Cybersecurity Posture", 1 June 2022: https://www.trellix.com/news/press-releases/trellix-finds-workforce-shortage-impacts-85-of-organizations-cybersecurity-posture/.
19. World Economic Forum, *Global Cybersecurity Outlook 2024*, 16 January 2024: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
20. World Economic Forum, *Future of Jobs Report*, June 2023: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf.
21. Fortinet, *2023 Cybersecurity Skills Gap: Global Research Report*, March 2023: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/2023-cybersecurity_skills_gap_report_final.pdf?utm_source=blog&utm_medium=blog&utm_campaign=cybersecurity-skills-gap-2023?utm_source=blog&utm_medium=blog&utm_campaign=cybersecurity-skills-gap-report-2023.
22. *Security*, "US and UK Express Interest in Cybersecurity Education for Children", 22 August 2023: https://www.securitymagazine.com/articles/99795-us-and-uk-express-interest-in-cybersecurity-education-for-children.
23. ENISA, *Addressing Skills Shortage and Gap Through Higher Education*, 24 November 2021: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education.
24. Ibid.

25. Ibid.
26. Organization of American States, *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions*, June 2022: https://www.gp-digital.org/wp-content/uploads/2021/06/National-Cybersecurity-Strategies.-Lessons-learned-and-reflections-ENG.pdf.
27. Fortinet, *2022 Cybersecurity Skills Gap: Global Research Report*, 2022: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf.
28. Capgemini, *Cybersecurity Talent: Eight Recommendations for How Organizations Can Bridge the Cybersecurity Talent Gap*, February 2018: https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf.
29. Fortinet, *2023 Cybersecurity Skills Gap: Global Research Report*, March 2023: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/2023-cybersecurity_skills_gap_report_final.pdf?utm_source=blog&utm_medium=blog&utm_campaign=cybersecurity-skills-gap-2023?utm_source=blog&utm_medium=blog&utm_campaign=cybersecurity-skills-gap-report-2023.
30. ISACA, *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations*, 2 October 2022: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023.
31. Ibid.
32. ISC2, *ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*, 2023: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.
33. ISACA, *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations*, 2 October 2022: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023.
34. European Institute for Gender Inequality, "Economic Benefits of Gender Equality in the EU": https://eige.europa.eu/newsroom/economic-benefits-gender-equality?language_content_entity=en#:~:text=Improvements%20in%20gender%20equality%20would,80%25%20employment%20rate%20by%202050.
35. Lundell, Bill and Oltsik, Jon, *The Life and Times of Cybersecurity Professionals 2021*, ESG and ISSA, July 2021: https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf.
36. Statista, "Requirement of University Degree for Cyber Security Jobs Worldwide from 2021 to 2022, by Region", 2022: https://www.statista.com/statistics/1322395/cybersecurity-university-requirement-worldwide/.
37. Ibid.
38. Ibid.
39. Ibid.
40. Trellix, "Trellix Finds Workforce Shortage Impacts 85% of Organizations' Cybersecurity Posture", 1 June 2022: https://www.trellix.com/news/press-releases/trellix-finds-workforce-shortage-impacts-85-of-organizations-cybersecurity-posture/.
41. World Economic Forum, *Putting Skills First: A Framework for Action*, May 2023: https://www3.weforum.org/docs/WEF_CNES_Putting_Skills_First_2023.pdf.
42. Cunningham, J.R., "CISO: A Day in the Life", *The Enterprisers Project*, 13 October 2022: https://enterprisersproject.com/article/2022/10/ciso-day-life.
43. ISACA, *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations*, 2 October 2022: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023.
44. Gartner, "Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025", 22 February 2023: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025#:~:text=By%202025%2C%20nearly%20half%20of,Gopal%2C%20Director%20Analyst%2C%20Gartner.
45. Verd, Nicky, "Africa's Brain Drain – the Exodus of the Continent's Potential", *Medium*, 25 January 2024: https://medium.com/@nickyverd/africas-brain-drain-the-emigration-of-africa-s-economic-potential-1b666f09751e.
46. USAID, "Critical Infrastructure Digitalization and Resilience", 31 March 2023: https://www.usaid.gov/north-macedonia/fact-sheets/mar-31-2023-critical-infrastructure-digitalization-and-resilience.
47. France 24, "Latin America's IT Brain Drain a Regional Challenge", 23 March 2022: https://www.france24.com/en/live-news/20220323-latin-america-s-it-brain-drain-a-regional-challenge.
48. Virkkula, Jani, "The Biggest Cyber Threat to Your Organization: Your CISO's Burnout", SSH, 17 August 2022: https://www.ssh.com/blog/ciso-burnout.
49. Forrester, "We Need to Talk More About Burnout In Cybersecurity", 14 February 2023: https://www.forrester.com/blogs/we-need-to-talk-more-about-burnout-in-cybersecurity/.
50. Sophos, *The Future of Cybersecurity in Asia Pacific and Japan*, 5 February 2024: https://mysecuritymarketplace.com/reports/the-future-of-cybersecurity-in-asia-pacific-and-japan-2/.
51. Miller, Emily, "5 Ways to Beat Burnout In Cybersecurity", *BitLyft*, 29 July 2022: https://www.bitlyft.com/resources/5-ways-to-beat-burnout-in-cybersecurity.

52. Forrester, “We Need to Talk More About Burnout in Cybersecurity”, 14 February 2023: https://www.forrester.com/blogs/we-need-to-talk-more-about-burnout-in-cybersecurity/.
53. Deloitte, “As Workforce Well-Being Dips, Leaders Ask: What Will It Take to Move the Needle?”, 20 June 2023: https://www2.deloitte.com/uk/en/insights/topics/talent/workplace-well-being-research.html.
54. CyberShikshaa: https://www.dsci.in/cyber-shikshaa/.
55. Dubai Cyber Innovation Park: https://dcipark.gov.ae; Dubai Cyber Innovation Park, “Emirati CTF”: https://dcipark.gov.ae/courses/capture-the-flag/.
56. Girls Who Code: https://girlswhocode.com/programs/college-and-career.
57. World Economic Forum, “Inclusive Cyber”: https://www.weforum.org/projects/inclusive-cyber-talent/.
58. Global Shapers Community, “The Power of Youth in Action”: https://www.globalshapers.org/.
59. eurobits women academy: https://www.ewa-eurobits.de/.
60. Cyber Citizen: https://cyber-citizen.eu/en/cyber-citizen-initiative/.
61. Siemens, “CyberMinds Academy”: https://www.siemens.com/global/en/company/jobs/growth-careers/cyberminds.html.
62. Soulful Work, “Find Your Home in Cybersecurity”: https://www.soulfulwork.com/.
63. Women4Cyber: https://women4cyber.eu/.
64. Absa, “Cybersecurity Academy”: https://www.absa.africa/a-force-for-good/cybersecurity-academy/.
65. Cisco Networking Academy: https://www.netacad.com/.
66. Cisco Networking Academy, “Skills for All with Cisco”: https://skillsforall.com/.
67. CSA Singapore, “SG Cyber Talent”: https://www.csa.gov.sg/our-programmes/talents-skills-development/sg-cyber-talent.
68. World Economic Forum, “Cybersecurity Learning Hub”: https://www.weforum.org/projects/cybersecurity-learning-hub/.
69. Fortinet, “Security Awareness Training”: https://www.fortinet.com/training/security-awareness-training.
70. MiDO Technologies: https://mido.co.za/overview-2/.
71. Metabase Q, “CERC”: https://www.metabaseq.com/es/area/cerc/.
72. OAS, “Press Release: OAS, MinTIC of Colombia and Citi Foundation Train 52 Students in Cybersecurity”, 28 June 2021: https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-067/21.
73. National Cybersecurity Authority, “The Saudi Cybersecurity Higher Education Framework (SCyber-Edu)”: https://www.nca.gov.sa/legislation?item=199&slug=frameworks-and-standard-list.
74. Cybersafe Foundation, “CyberGirls”: https://cybersafefoundation.org/cybergirls/.
75. Hewlett Packard Enterprises, “Cybersecurity Career Reboot Program”: https://careers.hpe.com/us/en/career-reboot.
76. CyberSeek, “Hack the Gap”: https://www.cyberseek.org/.
77. Temple University, “Course Projects”: https://sites.temple.edu/care/social-engineering/course-projects/.
78. NICCS, “NICE Framework Mapping Tool”: https://niccs.cisa.gov/workforce-development/nice-framework-mapping-tool.
79. Siemens Energy, “Industrial Cybersecurity Apprenticeship Program (CIISAp)”: https://www.siemens-energy.com/us/en/home/careers/industrial-cybersecurity-apprenticeship-program-ciisap.html.
80. Telefónica, “Campus 42”: https://en.fundaciontelefonica.com/employability/campus-42/.
81. UK Cyber Security Council: https://www.ukcybersecuritycouncil.org.uk/.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org