“HACKING” THE CYBERSECURITY SKILLS GAP IN DEVELOPING COUNTRIES
Acknowledgements

This practitioner note was written by Ghislain de Salins and benefited from the inputs and reviews of Anat Lewin, Samia Melhem, Hyea Won Lee and Casey Torgusson from the World Bank’s Digital Development Global Practice. The note also benefited from the inputs of Diego Angel-Urdinola (World Bank’s Education Global Practice), Kerry-Ann Barrett and Mariana Cardona Clavijo (Organization of American States, OAS), Orhan Osmani and Caroline Troein (International Telecommunications Union, ITU), Matthew Griffin (consultant for the ITU), Natasa Perucica (World Economic Forum), Tatyana Bolton (Google) and Lucas Hernandez (Microsoft).

The development of this note was funded by the World Bank Cybersecurity Multi-Donor Trust Fund.
# Table of Contents

- **Executive summary** .................................................................................................................. 5
- **Introduction** ............................................................................................................................... 6
- **Adopting a holistic and strategic approach to cybersecurity skills development** .................... 7
  1. Assessing current and future needs and gaps ........................................................................... 7
  2. Implementing a comprehensive action plan .............................................................................. 8
  3. Building partnerships and incentives ....................................................................................... 11
  4. Monitoring and reviewing progress .......................................................................................... 13
- **Thinking outside the box: promoting inclusion, gender diversity, and ethical hacking** ............ 14
- **Conclusion** .................................................................................................................................. 16
- **Highlighted partners’ initiatives** ............................................................................................... 16
- **References** .................................................................................................................................. 17
“HACKING”
THE CYBERSECURITY SKILLS GAP
IN DEVELOPING COUNTRIES

This practitioner note discusses emerging best-practices to accelerate cybersecurity skills development in low- and middle-income countries. It focuses on specialist cybersecurity skills, i.e., the human capital needed to fill advanced professional roles such as, inter alia, chief information security officer (CISO), cyber threat intelligence analyst, penetration tester, or cybersecurity architect. The note is intended for policy makers in developing countries and for the development community more broadly.

In Nigeria, the CyberGirls Fellowship equips girls and women from across Africa with the skills they need to launch successful cybersecurity careers. Credit: CyberSafe Foundation.

Executive summary

Key findings

Investing in cybersecurity skills development is a major opportunity to enhance overall cyber resilience and build a pipeline of high-quality jobs in developing countries.

Access to skilled cybersecurity professionals is a major hurdle for developing countries on their journey towards cyber resilience. The global workforce currently lacks more than 4 million cybersecurity professionals, with developing countries particularly exposed.

This shortage of skilled labor is expected to grow significantly in the coming years, as the gap between supply and demand of cybersecurity talent grew by 26 percent in 2022.

Gender biases are still significant in the cybersecurity industry, with women representing less than 25 percent of cybersecurity professionals worldwide.

Promising initiatives driven by local communities, often focusing on women and youth, are already delivering results and could be replicated and scaled up at the country- and regional-level.

Early cybersecurity education, from primary school to high school, can help scout and nurture talent more effectively.

Policy recommendations

A holistic and strategic approach is needed to accelerate cybersecurity skills development. It should leverage both formal education (e.g., university) and lifelong learning – i.e., reskilling and upskilling the current workforce, including through Technical and Vocational Education and Training (TVET).

To implement this approach, governments in developing countries can follow a four-step process: 1) assess current and future needs and gaps; 2) implement a comprehensive action plan; 3) build partnerships and incentives; and 4) monitor and review progress.

Multi-stakeholder partnerships stand out as a best practice for developing human capital in cybersecurity. They often leverage private sector expertise and online training platforms to reduce costs and maximize reach. They include public-private partnership (PPPs), cybersecurity skills academies, cybersecurity clinics, and “train the trainer” initiatives.

Governments should incentivize both demand and supply for cybersecurity skills. For instance, they can mandate cybersecurity roles for operators of critical infrastructure, provide scholarships for cybersecurity trainings, and support the pipeline of cybersecurity careers through internships and apprenticeships.

Addressing societal gender biases and promoting women in cybersecurity should be a key pillar of any action plan aiming to accelerate cybersecurity skills development.

---

2 Cyber resilience is the ability of a country or an organization to prepare for, adapt to, withstand and recover from cybersecurity incidents. The cybersecurity community increasingly focuses on the notion of “resilience,” recognizing risk management as the most effective conceptual framework to enhance cybersecurity and acknowledging that “100% security” is not achievable as neither vulnerabilities nor threats can be entirely eliminated.

3 Human capital consists of the knowledge and skills that individuals accumulate throughout their lives, enabling them to realize their potential as productive members of society. Investing in human capital is key to end extreme poverty and drive shared prosperity.
Introduction

The need to invest in cybersecurity skills development grows ever more pressing as the societal impact of cybersecurity incidents continuously increases. Today, their annual costs to society represent between 6 and 8 percent of global GDP.\(^1\)

The global shortage of skilled cybersecurity professionals is widely recognized as one of the key impediments to achieving cyber resilience.\(^i\) Whether at the country-level or within an organization, the ability to access, nurture, and retain talent is at the core of any successful strategy to manage cybersecurity risks. However, the global workforce currently lacks around 4 million cybersecurity professionals\(^i\) - and the shortage is expected to increase significantly in the years to come. In 2022, the pool of cybersecurity talent grew by 11.1 percent, yet the gap between workforce supply and demand grew by 26.2% - more than twice as much.\(^iv\)

Developing countries are particularly at risk and struggle even more to keep pace with the increasing demand for cybersecurity professionals. Recent research suggests that in India, the cybersecurity skills gap grew by a staggering 630 percent in 2022.\(^v\) LinkedIn data\(^vi\) confirm that the cybersecurity workforce gap in developing countries is growing much faster than in more developed countries. In 2022, the number of job postings for cybersecurity professionals increased by 76 percent in Brazil and by 55 percent in Indonesia, against an average of 35 percent in the 28 sampled countries.

Several factors contribute to the widening cybersecurity skills gap. The increasing speed, scale, and scope of digital transformation – and of associated risks – result in a soaring demand for cybersecurity talent. Despite such demand, the workforce supply is struggling to adjust. Just 15 years ago, cybersecurity was considered a niche market. Today, however, widespread demand for cybersecurity talent is growing exponentially across nearly all sectors of the economy. A recent survey indicates that the cybersecurity skills gap is most prominent in critical sectors such as energy, banking, and government.\(^vii\)

In parallel, current academic offerings often fail to keep pace with quickly evolving technological trends and industry best-practices (e.g., zero-trust architectures and automatic incident detection based on artificial intelligence and machine learning or AI/ML), particularly in low- and middle-income countries. Many cybersecurity training programs, from university degrees to professional certifications, are unaffordable for the average income-level in developing countries. Widespread misconceptions and societal biases also tend to limit the demand for education and training in cybersecurity. For instance, IT degrees are still perceived by many as a pre-requisite for a career in cybersecurity,\(^4\) and women represent less than 25 percent of cybersecurity professionals worldwide.\(^viii\) Beyond the challenge of growing local talent, governments in developing countries also face the risk of “brain drain” as they struggle to retain skilled cybersecurity professionals, who often find attractive job opportunities in the private sector or in more developed countries.

---

4 Recent research suggests that almost 50 percent of cybersecurity professionals under 30 years old come to the profession with a background outside of the IT industry (https://www.isc2.org/research).
Adopting a holistic and strategic approach to cybersecurity skills development

To effectively reduce the cybersecurity talent gap, developing countries can adopt a holistic and strategic approach to skills development. Implementing this approach will require a paradigm change, as many initiatives still tend to be built in silos. For instance, some initiatives are driven exclusively by the ministry of education without involving the ministry in charge of digital transformation. Other initiatives strictly rely on government input, neglecting to engage the private sector, academia, and civil society.

In practice, developing countries can follow a 4-step skills development lifecycle process (see Figure 1):

1) assess current and future demand for cybersecurity skills;
2) implement a skills development action plan, with clear milestones and quantifiable objectives;
3) build multi-stakeholder partnerships and develop incentives to achieve shared objectives; and
4) monitor effectiveness and review progress on a regular basis.

Figure 1 – The cybersecurity skills development lifecycle

1. Assessment
2. Action plan
3. Partnerships and incentives
4. Monitoring and review

Feedback loop

1. Assessing current and future needs and gaps

Developing countries must first conduct a quantified assessment of cybersecurity workforce needs and gaps based on a shared understanding and analysis across stakeholders. Frameworks for the definition, identification, and mapping of key cybersecurity roles and associated skills are essential to enable the assessment of current and future gaps in the national workforce. Developing countries can leverage the existing cybersecurity skills frameworks developed in high-income countries, for instance in the United States and the European Union.

The National Initiative for Cybersecurity Education (NICE) framework\(^\text{ix}\) provides a common language and structure for employers, educators, and individuals to identify, define, and evaluate cybersecurity-related tasks, knowledge, and abilities. The NICE framework, developed by the United States’ National Institute of Standards and Technology (NIST), comprises 7 categories (e.g., “operate and maintain”), 33 specialty areas (e.g., “digital forensics”) and 52 work roles (e.g., “incident responder”).

Similarly, the European Cybersecurity Skills Competence Framework (ECSF)\(^\text{x}\) supports the identification of tasks, skills, and knowledge associated with the roles of cybersecurity professionals. The ECSF, developed by the European Union Agency for Cybersecurity (ENISA), summarizes cybersecurity-related roles into 12 profiles (see Figure 2), each of which are associated with specific responsibilities, skills, and interdependencies. By providing a common understanding, the ECSF enables the design of cybersecurity training programs.
In Singapore, the Cyber Security Agency (CSA) published a cybersecurity competency framework dedicated to the specific challenges of operational technology (OT). In France, the national cybersecurity agency (ANSSI) maintains an observatory of cybersecurity jobs, which provides an operational framework for positions and skills as well as a repository of certified formal education processes.

Governments in developing countries can use these frameworks to start a dialogue with the key stakeholders that drive the demand for cybersecurity skills (e.g., operators of critical activities) and quantify the current and future gaps in the national cybersecurity workforce. Such an assessment should consider the specific challenges arising from a low- and middle-income context and prioritize the roles and tasks that are most needed for the early stage of building a cybersecurity workforce.

2. Implementing a comprehensive action plan

As a second step, developing countries can adopt a comprehensive action plan to develop cybersecurity skills. A successful action plan must leverage both formal education, from primary school to university, and lifelong learning – reskilling and upskilling the current workforce. Too often, skills development initiatives focus solely on formal education, neglecting the importance of on-the-job training. Likewise, other initiatives only target university-level degrees, failing to implement vocational programs at the primary and secondary education levels. Furthermore, certain initiatives focus on supporting the supply-side of the skills market - e.g., universities and training providers - without also engaging the demand-side - e.g., public and private organizations in need of recruiting cybersecurity specialists. Involving the demand-side in the design of a cybersecurity skills development action plan is paramount to ensure that cybersecurity training programs and curricula match the needs of the cybersecurity market and to maximize successful job placements upon graduation. Figure 3 lists key areas of focus and provides concrete examples of successful country initiatives.
## Designing a comprehensive cybersecurity skills development action plan

<table>
<thead>
<tr>
<th>Key areas</th>
<th>Good practice examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Formal education</strong></td>
<td></td>
</tr>
<tr>
<td>Primary</td>
<td>In the United Kingdom, the CyberFirst program. xxix</td>
</tr>
<tr>
<td>Secondary</td>
<td>In Israel, the Magshimim initiative. xxi</td>
</tr>
<tr>
<td>University</td>
<td>In Ghana, the Cyber Security Authority’s partnership with the Elizabeth Sloane Institute of Technology (ESIT). xxii</td>
</tr>
<tr>
<td><strong>Lifelong learning</strong></td>
<td></td>
</tr>
<tr>
<td>From engineering and IT to cybersecurity: channeling technical talent towards a career in cybersecurity.</td>
<td>In India, the CyberShiksha program. xxiii</td>
</tr>
<tr>
<td>From anything to cybersecurity: coaching women and youth to choose a career in cybersecurity.</td>
<td>In Nigeria, the Cyber Safe Foundation. xxiv</td>
</tr>
<tr>
<td>Leveraging international and regional cooperation: bringing together North-South and South-South capacity building.</td>
<td>In Senegal, the Regionally Oriented National School of Cybersecurity - RONSC (École nationale de cybersécurité à vocation régionale, ENCVR). xxv</td>
</tr>
</tbody>
</table>


### Providing opportunities throughout the entire education journey

Countries leading in cybersecurity skills development understand the need to scout and nurture talent as early as possible. An emerging good practice, increasingly common in developed countries, is to introduce cyber literacy classes in primary schools and offer advanced cybersecurity classes in high schools.

For instance, in the **United Kingdom**, the National Cyber Security Centre (NCSC) launched CyberFirst, a program of opportunities to help young people (aged 10 to 17) explore their potential for cybersecurity through dedicated competitions, classes, and trainings. CyberFirst is a public-private partnership that brings together schools, various parts of the UK government, from NCSC to the Department for Education, and the private sector to identify and nurture a diverse range of talented students, encouraging them to pursue cybersecurity careers.

In **Israel**, the government co-sponsors Magshimim, a diversity-focused cybersecurity talent program for high-schools. In 2013, the program started with around 500 students. Today, it attracts more than 5,000 participants every year. It is specifically designed to scout and nurture cybersecurity talent from underrepresented groups more likely to be excluded from the Israeli workforce. Such groups include girls, recent immigrants, Haredi (Ultra-Orthodox), Arabs, and people living in rural areas. Prospective high-school students are screened through a series of tests and interviews focusing on dedication and sociability — but prior computing experience is not needed. Magshimim accepts roughly 30 percent of applicants.
Universities in developing countries can also incorporate innovative models to develop capacity for local companies, civil society, and underserved communities that are unable to invest in cybersecurity. The establishment of cybersecurity clinics is an emerging good practice in this area. Cybersecurity clinics are agile hubs that bring together university professors and students to assist external stakeholders in enhancing their cybersecurity knowledge and posture. These clinics typically offer their services to organizations with lower cybersecurity maturity such as hospitals, municipalities, small businesses, and non-profits. The clinics offer regular hands-on workshops where professors and students work on building capacity along specific themes (e.g., responding to an incident, vulnerability management, etc.). In 2023, the Consortium of Cybersecurity Clinics published a Clinic Development Toolkit, an accessible guide on how to start and operate a cybersecurity clinic.

Beyond the supply-side aspect of education, policy initiatives supporting the demand-side are increasingly recognized as essential to cybersecurity skills development action plans. Awareness-raising campaigns can demystify cybersecurity and promote cybersecurity careers, especially for women and girls. Such campaigns are typically organized through multi-stakeholder initiatives (e.g., bringing together high-schools, cybersecurity companies, telecom operators, and social networks), often with the support of the national cybersecurity agency, and can significantly stimulate demand for cybersecurity education. Other important demand-side policy tools address the affordability of cybersecurity education, which often stands out as a key obstacle in developing countries. Scholarship grants are an important policy tool to increase affordability. Such assistance often proves instrumental in supporting local demand for cybersecurity education. Furthermore, the allocation of grants could also be contingent on graduates’ commitment to serve a number of years within the government as a cybersecurity specialist. Such a measure would help avoid a loss of cybersecurity talent by mitigating the risk of “brain drain.” Additionally, governments in developing countries could also work directly with universities to provide cybersecurity students with apprenticeships in the public sector.

Maximizing the opportunities of lifelong learning

Providing lifelong learning, i.e., programs designed to re-skill and up-skill the current workforce, is vital to building and maintaining the cybersecurity talent pool. Too often, governments tend to focus on traditional education pathways (e.g., universities) while overlooking the many benefits of investing in non-traditional training opportunities for the current workforce. Lifelong learning initiatives provided to cybersecurity professionals and prospective candidates are typically agile, short, and intense training programs (e.g., from 3 to 12 months) that rely on online learning platforms. These platforms are often operated by leading technology companies (e.g., Google’s Cybersecurity Certificate) and offer cutting-edge cybersecurity training resources for free or for a low fee. These initiatives may target a wide audience, from recent graduates to experienced professionals seeking a career change (including existing IT specialists, such as network engineers or cloud architects). Compared to traditional education pathways, lifelong learning initiatives are usually more cost-effective, more agile (e.g., online training materials can be updated quickly, whereas traditional curricula updates take more time), and deliver faster results. These initiatives may be bundled with specific credentials or certifications that can attest to the level of cybersecurity proficiency of candidates (see Box 1 for a detailed discussion on the benefits and challenges of certifications).
The following section discusses in more detail various initiatives that leverage lifelong learning opportunities to accelerate cybersecurity skills development.

3. Building partnerships and incentives

Multi-stakeholder partnerships enable governments to leverage the resources of the private sector, civil society, and academia to achieve public policy objectives. The main benefits of this model are to enable cost-sharing between stakeholders (including for capital expenditure and operational expenditure), enhance the business model and financial viability of the project, facilitate access to private sector expertise, boost scalability, and ensure the adoption of a holistic approach. Beyond promoting interdependent operational arrangements, a multi-stakeholder partnership reaches success by fostering a common determination to solve a particular development challenge and committing resources to achieving ambitious results. Such commitment can relate to inputs – financial (e.g., US$10 million dedicated by the private sector to building a cybersecurity campus) or non-financial (provision of human resources, hardware, software, online platforms, offices) – or outputs (e.g., training 5,000 cybersecurity professionals in three years).

---

5 Beyond the topic of skills development, cybersecurity certifications may also relate to products, services, or organizations for which they can provide assurance that they reach a certain level of cybersecurity. Those certifications are typically based on national or international standards – e.g., NIST CSF, ISO:27001 or ETSI EN 303 645.

In the context of cybersecurity skills development, multi-stakeholder partnerships yield other significant benefits. They can facilitate knowledge transfer – in particular, through “train-the-trainer” initiatives – and bring down the costs associated with trainings and certification, while also ensuring that curricula correspond to market demand. Such initiatives typically focus on Technical and Vocational Education and Training (TVET) tracks, which go beyond formal education systems and universities and integrate other tools such as online courses, apprenticeships, and internship placements.

In India, for instance, Microsoft partnered with the Data Security Council of India (DSCI) to launch CyberShikshaa, a free program for skilling female engineering graduates from small towns in the field of cybersecurity through four-month intensive trainings. Since 2018, CyberShikshaa enabled the training of more than 1,000 women in cybersecurity. In 2022, the program was updated to include “CyberShikshaa for Educators,” which provides cybersecurity training to 400 faculty members across 100 rural institutions.

In April 2023, the Cyber Security Authority (CSA) in Ghana launched a partnership with the Elizabeth Sloane Institute of Technology (ESIT), a higher education provider that offers online self-paced cybersecurity certificates in collaboration with the International Information Systems Security Certification Consortium (ISC2). The partnership aims to build the capacity of Ghanaian Cybersecurity Professionals through the allocation of grants that may cover up to 60 percent of the training and certification costs associated with selected professional certification programs, including the CISSP, CompTIA Security+, and CompTIA PenTest+.

In Senegal, the Dakar Cybersecurity School, launched in 2021, is an innovative model of combined North-South and South-South development cooperation. It was created as a joint venture between the governments of France and Senegal aiming to develop cybersecurity skills across the entire African continent. It provides 29 international training courses to around 700 auditors each year, mostly from francophone countries. The training programs range from a few days to a few weeks, and focus on four main areas: network security, tools for law enforcement, gathering digital intelligence and the governance of cybersecurity. These training courses are intended for a wide range of professionals, such as senior officials and decision-makers, ICT specialists, police officers, as well as judges and prosecutors. In 2022, a similar regional school was launched in Podgorica, as a joint venture between France, Montenegro, and Slovenia, aiming to develop cybersecurity skills across the entire Western Balkans region.

These initiatives model the Cybersecurity Academies that have recently gained traction in many countries, including in the European Union (EU). In 2023, the EU launched the Cyber Skills Academy, an initiative that brings together EU governments, the private sector (e.g., Cisco and Microsoft), as well as organizations specialized in cybersecurity training (e.g., ISC2) around shared quantified objectives of trained cybersecurity professionals. Private sector participants have pledged to train a specific number of students over the course of a few years and provide practical training programs through an online platform. In developing countries, the companies that are spearheading digital transformation (e.g., internet service providers, mobile operators, and banks) are also increasingly investing in re-skilling and up-skilling the workforce through dedicated cybersecurity training. In South Africa, Absa Bank launched a Cybersecurity Academy in 2019, in partnership with the Maharishi Institute. Their Cybersecurity Academy now trains up to 300 students each year.

More broadly, multi-stakeholder partnerships in other cybersecurity domains – e.g., incident response – can play a key role in accelerating skills development, in particular, through knowledge transfer. In 2021, the government in Togo established the national Cybersecurity Incident Response Team (CIRT) as a public-private partnership (PPP). The national CIRT is operated by Cyber Defense Africa (CDA), a joint venture between the Togolese government and Polish IT company, Asseco. The PPP model enabled the Togolese government to significantly lower barriers to entering
the cybersecurity profession, by reducing financial costs\(^9\) and increasing access to skills. The latter was a key obstacle for establishing a national CIRT, as the Togolese workforce had very few cybersecurity professionals experienced in the operation and management of a CIRT. The partnership with Asseco enabled CDA to accelerate cybersecurity skills development through knowledge transfer – experts from Asseco headquarters provided a robust training program to the staff of CDA (the technical team being composed almost exclusively of Togolese nationals). In just a few months, the caliber and expertise of the CIRT staff grew significantly, and enabled the Togolese CIRT to join the Forum of Incident Response and Security Teams (FIRST)\(^{10}\), the international community of incident response teams. Togo hence became the first - and so far, the only - low-income country in Western and Central Africa represented by an incident response team in FIRST.

Effective incentives for stakeholders and cybersecurity professionals are key to ensure the effectiveness and sustainability of a skills development action plan. For stakeholders, incentives can include government subsidies that fund part of the tuition or certification fees. For cybersecurity professionals, incentives typically include globally competitive financial compensation (e.g., above the local market rate for civil servants) as well as non-financial aspects such as flexible work options (e.g., in terms of leave or remote working) and formal recognition within the organization. These incentives are a must-have for governments in developing countries in order to mitigate the risk of a “brain drain” of cybersecurity talent.

More broadly, governments should use policy tools to stimulate demand for cybersecurity talent. For instance, regulations that incentivize or mandate operators of critical activities to hire cybersecurity roles (e.g., a CISO at minimum) can be helpful in supporting the demand-side of the cybersecurity job market. Governments can also play a more direct role by offering cybersecurity apprenticeships and clear career pathways for cybersecurity professionals within the public sector.

4. Monitoring and reviewing progress

Finally, developing countries should monitor and review the implementation of the action plan for cybersecurity skills development. This includes assessing effectiveness, identifying shortcomings, and implementing course corrections and adjustments. By regularly evaluating the implemented initiatives, stakeholders can measure the success of various training programs and capacity-building efforts.

---

9 The capital expenditure (capex) for establishing the national CIRT required a much lower public investment, while the operational expenditure (opex) is financed by the joint venture. In fact, Cyber Defense Africa (CDA) provides CIRT services to Togolese organizations for free, but also offers Security Operations Center (SOC) services (e.g., incident detection tools) for a fee. This model has enabled the government of Togo to significantly reduce the public investments needed for operational expenditures (opex) as well.

10 FIRST is the global platform that gathers CIRTs from around the world. Countries with advanced cybersecurity capacity typically have several national and sectoral teams that are members of FIRST. In contrast, countries with lower cybersecurity capacity typically have no teams participating in FIRST.
Thinking outside the box: promoting inclusion, gender diversity, and ethical hacking

Beyond implementing the holistic and strategic approach to cybersecurity skills development outlined above, developing countries can gain additional benefit by thinking outside the box and leveraging more innovative tools.

**Promoting inclusion and gender diversity in the cybersecurity talent pool is the first innovative way to further reduce the skills gap.** Underrepresented or vulnerable groups, such as women and LGBTQ+ people, are often discouraged from cybersecurity careers because of societal biases and misperceptions of cybersecurity work culture. Consequently, as referenced above, women represent less than 25 percent of cybersecurity professionals worldwide.\(^\text{v}\) However, countries currently leading the way in bringing more diversity and inclusion to the cybersecurity workforce are nearly all developing. As shown in Figure 4, four out of the five leading countries for promoting gender-diversity in the cybersecurity workforce are middle-income. For instance, Nigeria and Mexico both rank 1st with 34 percent of women in their cybersecurity workforce. These examples confirm strong interest and potential amongst developing countries for championing gender-diversity in the cybersecurity workforce.

**Figure 4 – Top 5 countries with the most gender diverse cybersecurity workforce**

<table>
<thead>
<tr>
<th>Country</th>
<th>Women</th>
<th>Men</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nigeria</td>
<td>34%</td>
<td>66%</td>
</tr>
<tr>
<td>Mexico</td>
<td>34%</td>
<td>66%</td>
</tr>
<tr>
<td>Ireland</td>
<td>33%</td>
<td>67%</td>
</tr>
<tr>
<td>Brazil</td>
<td>31%</td>
<td>69%</td>
</tr>
<tr>
<td>India</td>
<td>30%</td>
<td>70%</td>
</tr>
</tbody>
</table>

Source: ISC2, global survey of 11,155 cybersecurity professionals\(^\text{v}\), 2022.
To address the lack of diversity, governments and stakeholders need to reframe the overall narrative around cybersecurity, for example, through awareness raising campaigns and material promoting inclusive and diverse role models and success stories in cybersecurity careers. To this end, in 2021, the International Telecommunications Union (ITU) launched the Women in Cyber initiative, a mentorship program aimed at tackling the cultural and systemic barriers preventing women’s inclusion in cybersecurity. The program broke the barriers through community building, guidance, and senior-junior solidarity among women in the sector. Since its inception, the program has coached 300 women from more than 73 developing countries into cybersecurity careers, including several leadership positions. Such initiatives could be replicated and scaled up at the country- and regional-level.

In Nigeria, the CyberSafe Foundation launched the CyberGirls Fellowship, an ambitious program that offers young women, aged 18 to 28, an intensive seven-month training in cybersecurity. The program, which spans across 22 African countries, focuses on equipping young women from underprivileged regions with critical cybersecurity skills. Each year, the program receives more than 20,000 applications, from which a cohort of 500 girls is selected — a figure that is projected to reach 1,000 students in 2024. Through a structured regimen of technical training, mentorship, and entrepreneurial skills development, followed by internship placements, the fellowship is enabling young African women to build rewarding careers in cybersecurity – on average, program graduates benefit from a 400 percent increase in their income after graduation. The CyberGirls Fellowship is financed by donations that cover the tuition fees for all students, and heavily relies on partnerships with the private sector, including IS2C, ISACA, Microsoft, InfoSec institute, EC Council, Practical DevSecOps, AWS, Security Blue Team, and Cisco.

Another innovative way to further reduce the cybersecurity skills gap is to leverage the untapped potential of ethical hackers. Ethical hackers are informal groups of talented individuals, who often learned cybersecurity in their spare time outside of formal education systems. Policy initiatives that aim to better recognize their talent and connect them to the job market (e.g., through hackathons, national competitions, bug bounties, or formal certification processes) could prove helpful in reducing the cybersecurity workforce gap. Integrating these experts, who were previously disconnected from the job market, into the cybersecurity workforce will expand the talent pool and help build a community of practice that can participate in cybersecurity education (e.g., ethical hackers can be recruited to teach cybersecurity classes in schools and training programs). Recent research showed that the community of ethical hackers is very present in some developing countries. For instance, India ranks 1st – above the United States – in terms of number of HackerOne platform participants. According to the research paper, 58 percent of ethical hackers are self-taught, and less than 5 percent learned hacking skills in a classroom. In Togo, the national agency for cybersecurity (ANCy, Agence Nationale de Cybersécurité) launched “capture the flag” in 2022, an annual hacking competition. Open to all, the competition aims at scouting cybersecurity talent in Togolese youth and awards top candidates with a variety of awards – including internships at ANCy.

These research results and real-world examples confirm the importance of adopting a holistic approach to cybersecurity skills development. As such, governments and stakeholders must go beyond formal education systems and aim to build a community of practice at the national and international levels.

---

11 Bug bounty program (BBPs, or “bug bounties”) are crowdsourcing initiatives that reward individuals for discovering and reporting vulnerabilities.
Conclusion

Supporting and accelerating the development of cybersecurity skills should be a key component of any national cybersecurity strategy. The lack of cybersecurity professionals continues to be a major impediment to achieving cyber resilience, particularly in developing countries. Without a skilled cybersecurity workforce, the return on investments in other domains (e.g., incident response, critical infrastructure protection, or legal frameworks) is likely to be significantly hampered. As the impact of cybersecurity incidents increases – with annual costs to society currently representing between 6 and 8 percent of GDP – the need to further invest in cybersecurity skills development is even more pressing.

Investment in cybersecurity skills development also presents a major opportunity for low- and middle-income countries to create high quality jobs locally. The demand for cybersecurity roles is growing significantly faster (26 percent in 2022) than the current supply of cybersecurity professionals. Such demand means that investments aiming to grow the cybersecurity talent pool in developing countries are likely to result in the creation of a pipeline of higher-income jobs, which can, in turn, drive economic growth and support broader poverty reduction policies.

Governments in developing countries can leverage supply-side and demand-side policy tools that effectively address existing barriers in the job market. For instance, governments can provide grants and scholarships to support demand for cybersecurity education and trainings, and bundle them with requirements to work for the public sector for a limited number of years. Such initiatives can boost the talent pipeline and help limit the risk of a “brain drain” in the cybersecurity workforce.

International and multi-stakeholder cooperation stands out as a key success factor for effectively reducing the cybersecurity skills gap. In particular, governments in developing countries can promote public-private partnerships and action plans with concrete milestones and quantified objectives for cybersecurity skills development. As shown in this note, many inspiring initiatives, often driven by local communities and centered around women and youth, are already delivering promising results. Replicating them and scaling them up through capacity-building initiatives, including World Bank operations, offers significant potential for boosting cybersecurity human capital in a sustainable manner.

Highlighted partners’ initiatives

Beyond the World Bank, other international partners are rising to the challenge of accelerating cybersecurity skills development in developing countries.

The International Telecommunication Union (ITU) and the Organization of American (OAS) are working on a joint-initiative to provide support and guidance for low-and-middle income countries to develop contextualized approaches to national cybersecurity education capacity. This includes the development of a research paper that takes a systems approach to understanding national cybersecurity education capacity and shares concepts and leading-practice recommendations to support policy makers and practitioners in their efforts to build secure and resilient digital societies. This forthcoming paper will be complemented by a workshop-series and an online education course that will continue institutionalizing an approach to a structured process for a sustainable cybersecurity workforce.

The World Economic Forum's Centre for Cybersecurity recently launched the “Bridging the Cyber Skills Gap” initiative to accelerate public-private responses to address the global cybersecurity skills and talent gap. The initiative brings together a multi-stakeholder group comprising industry leaders, government agencies, civil society, and academia to create a strategic cybersecurity talent framework and devise actions to help individuals enter and thrive in the cybersecurity workforce.
References


iv ISC2, 2022, https://www.isc2.org/Research/Workforce-Study

v Ibid.


xii ANSSI, https://www.ssi.gouv.fr/entreprise/formations/observatoire-des-metiers-de-la-cybersecurite/


xv ISC2, 2022, https://www.isc2.org/Research/Workforce-Study


xix Ibid.

xx NCSC, https://www.ncsc.gov.uk/cyberfirst/overview


xxiv CyberSafe Foundation, https://cybersafefoundation.org/