Empowering Women to Work in Cybersecurity Is a Win-Win

September 2022
By David Panhans, Leila Hoteit, Shoaib Yousuf, Theo Breward, Caroline Wong, Alaa M. AlFaadhel, and Basma H. AlShaalan

BCG × Global Cybersecurity Forum

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

The Global Cybersecurity Forum (GCF) was founded in early 2020 by the National Cybersecurity Authority (NCA) as an action and initiative-oriented global platform for policymakers, governments, business, cybersecurity leaders, academia, and NGOs to integrate the global cybersecurity community and drive forward the agenda on cyberspace. Designed to promote collaboration and to share best practice from across the value chain on tackling current and emerging global cyber threats, GCF leverages multidisciplinary thinking to promote and achieve enhanced global cyber resilience. Through the annual events, continuous research, design and launch of new initiatives, and more, the GCF aims to catalyze socioeconomic change, push the knowledge boundaries on core cybersecurity topics, and build the foundations for global cooperation on key challenges and opportunities in cyberspace.

Empowering Women to Work in Cybersecurity Is a Win-Win

The world is increasingly turning to digital, but there's a twist: a significant escalation of digital threats. Cybercrime inflicted a trillion-dollar global business loss in 2020 alone. Compounding the danger: 57% of organizations report unfilled cybersecurity positions. The weaker a company's line of defense, the more vulnerable it is to major damages.

At the same time, we note, some 75% of today's cybersecurity workers are men.

There's a huge opportunity to expand the numbers and capabilities of the cybersecurity workforce by attracting women to the field. Why hasn't this happened? The apparent stumbling block is well known: long-standing obstacles have kept many women from entering and pursuing careers in science, technology, engineering, and math (STEM) disciplines, including cybersecurity.

Solving both of these cybersecurity challenges—the staffing shortfall and the gender-based inequity—begins with opening STEM doors to women and girls. But the effort can't stop at early-stage access. It must gain breadth and depth as women advance in the field so that they can fully participate in cybersecurity throughout a career trajectory.

The findings of our research—including a worldwide survey of 2,000 women studying STEM subjects—underscore the hurdles to expanding the cybersecurity workforce and making cybersecurity a viable career focus for women. (See the sidebar "About the Survey.") Importantly, our findings also reveal some surprising opportunities for significant progress.

The Dual Challenges

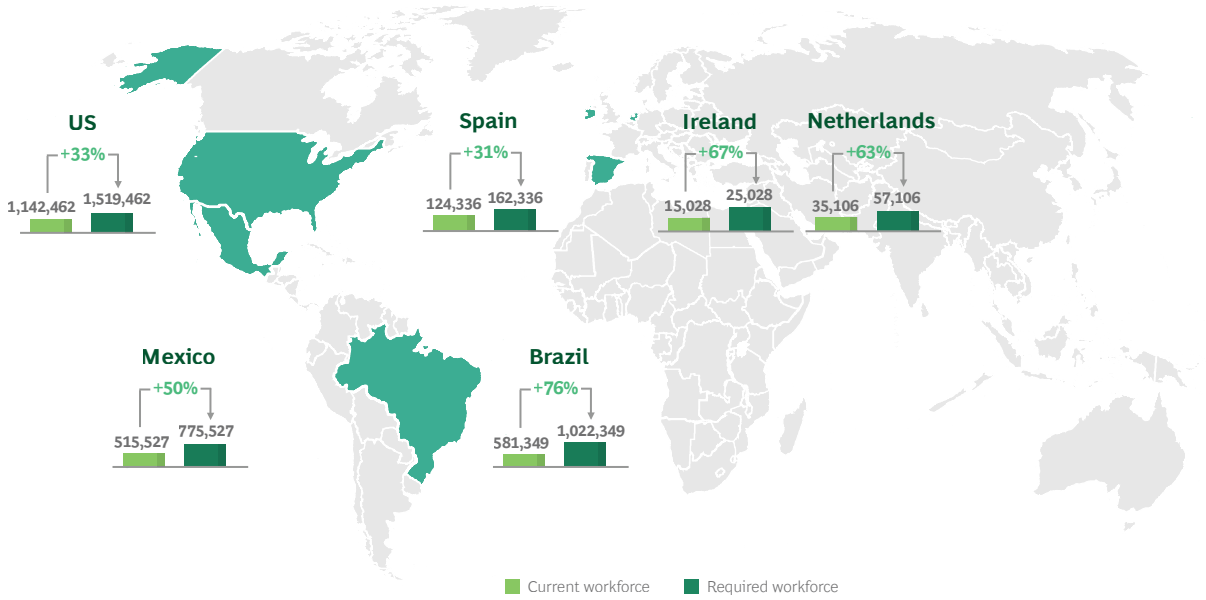
The global cybersecurity workforce was short some 3.5 million workers in 2021, according to Cybersecurity Ventures; by that count, the workforce of 4.4 million was 80% shy of the demand. (See Exhibit 1.) Concern over the dearth of tech talent in general has been growing for years, but it's coming to a head as organizations increasingly rely on digital. With cybercrime on the rise, the shortfall in cybersecurity is particularly urgent.

How did this immense talent gap emerge?

Partly from a mismatch of supply and demand. This is a fast-growing but nascent and dynamic field. It takes time and money to acquire the specialized education, certification, and experience required to gain expertise. As demand continues to outstrip supply, the talent gap expands. Between 2020 and 2021, it grew by 13%.

But the extreme gender differential among the cybersecurity employee base indicates that other forces are at work. Women make up 39% of the overall workforce. They account for 38% of workers in STEM jobs but only about 25% of the cybersecurity workforce, according to Cybersecurity Ventures.

Exhibit 1 - Where the Cybersecurity Talent Gap Is Most Acute



Sources: (ISC)² Cybersecurity Workforce Study 2021; BCG analysis.

Note: The workforce gap is calculated as the number of hiring organizations multiplied by the expected head count per organization minus the supply of cybersecurity professionals. The calculation of supply includes estimates for new entrants to the workforce and estimates of professionals currently in other fields who are pivoting to cybersecurity.

Attracting women to cybersecurity would do more than fill the empty chairs. It would:

- **Broaden and strengthen cybersecurity capabilities** by bringing diverse perspectives to problem solving and innovation.
- **Improve business performance.** Diversity pays dividends; companies with a gender-diverse board typically have higher returns on assets, and companies with a gender-diverse employee base tend to have financial returns that top national industry averages.
- **Strengthen and diversify national economies** by encouraging women to pursue careers in cybersecurity, which is a well-paying, highly productive, and future-proof industry.

But various barriers keep women out of cybersecurity.

According to research from (ISC)², a nonprofit that focuses on cybersecurity training and certification, the majority of women who have worked in the field report gender-based discrimination. Nearly all women (87%) reported having experienced unconscious discrimination, while 19% said they had been subjected to overt discrimination. Women also cited unexplained delays in career advancement (53%) and exaggerated responses to errors (29%).

Discrimination also manifests in a compensation gap. (ISC)² research shows that 32% of men working in cybersecurity earn an average of $50,000 to $100,000 annually, while just 18% of women in cybersecurity occupy the same income bracket. And 25% of men versus 20% of women earn $100,000 to $500,000 annually.

But women's low rate of participation in cybersecurity, and STEM fields in general, has traditionally been attributed to a narrow talent pipeline, itself a consequence of women's low participation in tertiary STEM education. In fact, that's a major theme that emerged from our review of more than a hundred reports, studies, indices, articles, and relevant global initiatives as well as our interviews with some 20 international experts from the public and private sectors, not-for-profits, academia, think tanks, and international NGOs.

This research informed our global survey of 2,000 women undergraduate STEM students in 26 countries spanning six regions—one of just a few studies on this topic to include a global sample.

New Insights from BCG's Global Survey

Because sources pointed to early-stage STEM access as the primary stumbling block to women's participation in cybersecurity, we focused our global survey on women undergrads in STEM-related programs. Specifically, we regarded our survey as an opportunity to test the conventional wisdom about women in STEM and cybersecurity.

Confirming and Refuting Notions of Gender Disparity. Our survey corroborated some traditional thinking—but refuted other key, long-held hypotheses. (See Exhibit 2.) Here's what we found:

- **It's important to engage girls in STEM early.** Our research confirmed this hypothesis. A majority—78%—of our respondents said that they had first developed an interest in STEM in middle school or high school. This is critical. "If you don't engage girls before high school, you have already lost them," said Jay Koehler, a former diversity, inclusion, and equity manager at Cisco Systems and a member of the board of Women in Cybersecurity, an organization dedicated to recruiting, retaining, and advancing women in the field.

- **Women *are* aware of cybersecurity.** There's a perception that awareness of cybersecurity is low among women. We found the opposite to be true: 82% of survey respondents said they had some or a lot of knowledge of cybersecurity.[1]

- **Women *do* have access to cybersecurity education.** Another perception: women do not participate in cybersecurity because they lack access to cybersecurity education. Our survey indicated otherwise: 58% of respondents said they had access to cybersecurity education and 68% had already taken a cybersecurity-related course.

- **Role models and senior encouragement are critical.** That's what anecdotal evidence suggested, and our survey validated the hypothesis. Of our survey respondents, 70% of those who have some or a lot of knowledge of cybersecurity said that they had a role model who encouraged them to learn more about the field.

- **Some women have negative perceptions of cybersecurity as a career choice.** The top three priorities for women in choosing a job are contributing to society, earning a high salary (another reason to address the compensation gap in cybersecurity), and having a good work-life balance, our survey showed. However, 37% of respondents regard cybersecurity as a field where achieving that balance is difficult.

- **Women with low awareness of cybersecurity have negative perceptions of people who work in the field.** We found that women with little knowledge of cybersecurity regard those working in the field as "nerds" or "hackers." Conversely, women who have greater awareness of cybersecurity have a more positive perception of such workers, thinking of them as "cool coders." These characterizations of cybersecurity professionals are extensions of broader perceptions of the field itself. Some people associate it with the military and intelligence operations that were historical entry points into cybersecurity. And it's often regarded as a "boys' club." Betsy Bevilacqua, a former head of information security programs and operations at Facebook, told us, "When people think of cybersecurity, they imagine a guy in a hoodie sitting in front of a computer in his parent's basement breaking into systems." Debunking stereotypes and negative perceptions of cybersecurity workers will be necessary to attract more women to the field.

Our survey also explored the reasons why some women said they did not want to pursue a career in cybersecurity. (See Exhibit 3.) A subset of these respondents (22%) cited a lack of information about cybersecurity as a career path or a lack of technical knowledge, suggesting that there is an opportunity to attract a greater proportion of women to cybersecurity by making information and technical capabilities more widely available. Also, 47% of women simply said they were not interested in a career in cybersecurity—but when we asked them to elaborate, some also cited insufficient information, telling us, among other things, "I hadn't thought of it" and "I have never been exposed to this field," meaning that opportunities to engage in cybersecurity projects, internships, and other experiences were lacking. This suggests that there's an even larger opportunity to attract women to the field through outreach efforts.

1. Our survey involved STEM undergraduate students, who might be more aware of cybersecurity and might have more access to cybersecurity education than undergraduate students in general.

Exhibit 2 - What We Learned from Our Survey

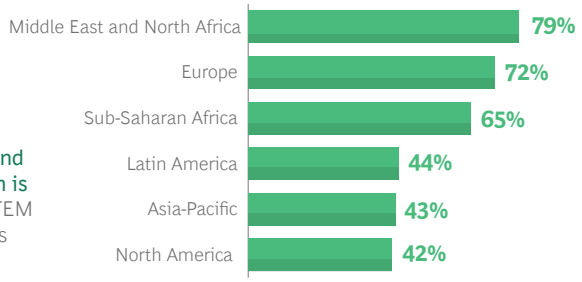
Sparking girls' interest in STEM at an early age is critical

54%
Participated in **targeted programming** for girls in STEM

78%
First developed an interest in STEM in **middle or high school**

The **Middle East and North Africa region is a leader** in K–12 STEM programs for girls

Share of respondents who participated in K–12 STEM programming for girls, by region



Women's access to cybersecurity education is high, and role models drive cybersecurity awareness

58%
Have **access to** cybersecurity **education**

68%
Have **already taken a course** related to cybersecurity

82%
Have some or a lot of **knowledge of cybersecurity**

70%
Had a **role model who encouraged them** to learn more about cybersecurity

Raising awareness would encourage more women to enter cybersecurity

Those who have **a lot of knowledge of cybersecurity** tend to perceive women in cybersecurity as **"cool coders"**

Those who have **no knowledge of cybersecurity** tend to perceive women in cybersecurity as **"nerds" or "hackers"**

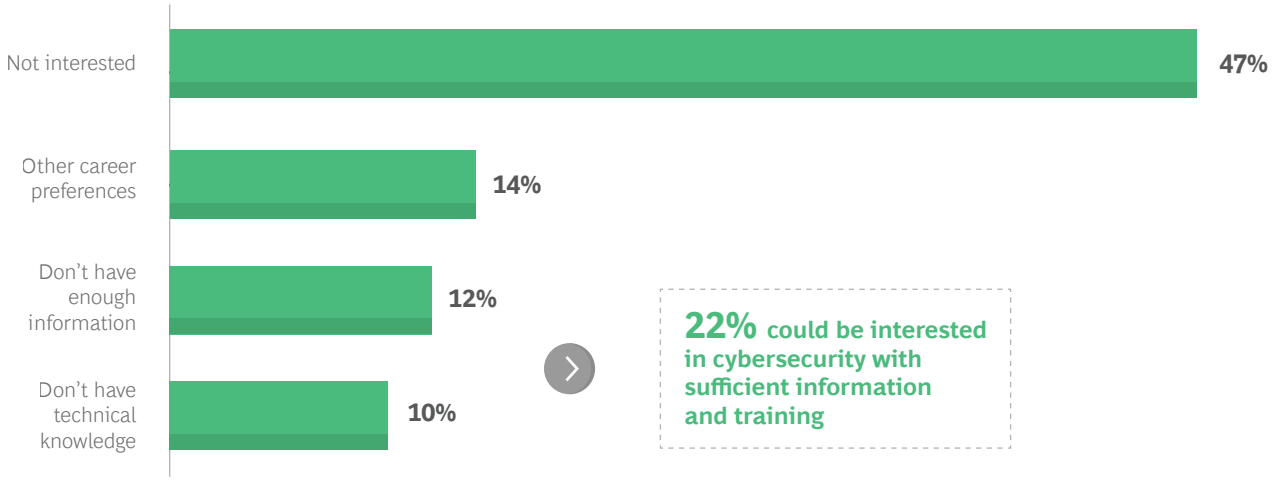
In choosing a job, women prioritize three factors

1. Contributing to society
2. Earning a high salary
3. Balancing family and work needs

But a **large minority perceive cybersecurity** as a career where achieving a good **work-life balance is difficult** for women who want a family or home life

Source: BCG research.

Exhibit 3 - Top Reasons Why Women Do Not Wish to Pursue a Career in Cybersecurity



Source: BCG research.

Our international survey revealed interesting differences across regions as well. For details, see the sidebar "Survey Results by Region."

Access Versus Agency. Our survey results suggest that access—such as greater awareness of cybersecurity and increased access to higher education in the field—is not the stumbling block that keeps girls and women from participating in cybersecurity. But sizable gender gaps persist in the field, which means increased access is not generating increased participation. How to explain this paradox?

The true difficulty lies in agency. The problem is not primarily a lack of access to necessary resources or opportunities, such as the option to pursue a cybersecurity degree or apply for cybersecurity jobs. Rather, the problem is a lack of capacity to control resources and make decisions about their use: in many circumstances, social or cultural norms constrain a woman's choice of what she can study, and unpaid home and care responsibilities limit a woman's ability to enter or succeed in a career in cybersecurity.

Both dimensions—access and agency—need to be addressed to empower women to achieve their full potential. Certainly, both are necessary to advance women's participation in a STEM field like cybersecurity.

The push for access in general has gained ground in recent years, thanks to the work of organizations worldwide dedicated to establishing gender equity. Today, an unprecedented number of women have access to education, health care, and political commitment to gender equality. Nonetheless, women's participation in the labor force still falls short; in fact, it is declining and on target to reach what would be a 40-year low of 46% by the end of the decade, whereas the participation rate for men is projected to be 72% in 2030.

Many initiatives consider access primarily; they don't address agency challenges. Women continue to carry the burden of unpaid household and care work—by a factor of three. They spend half as much time as men doing paid work. The result: they work more hours than men overall but receive less remuneration for their time.

Further limiting agency, women working in fields that predominantly employ men can suffer from a low sense of belonging and from impostor syndrome—a pattern of doubting one's abilities and feeling like a fraud despite possessing the requisite capabilities and having a track record of accomplishments. In sum, systemic cultural, social, and legal barriers continue to constrain women's agency to participate in STEM fields, including cybersecurity.

The pace of progress has been slow. At this rate, it will take more than 130 years to close the global gender gap. We propose that the urgent need to fill cybersecurity positions should be regarded as impetus to accelerate the effort.

Survey Results by Region

Our survey found differences among respondents from different regions.

North America. Among respondents in North America, 61% expressed interest in pursuing a cybersecurity degree, but significantly larger shares in other regions—the Middle East and North Africa (MENA, 94%), Europe (89%), sub-Saharan Africa (84%), Asia-Pacific (82%), and Latin America (77%)—said they were interested. Only 45% of North American women were aware of cybersecurity programs at their institutions, whereas 88% of those in MENA and 73% of those in Europe said they were aware of such programs. Women in North America were also less likely to participate in targeted STEM programming in their K–12 education (45%) relative to women in Europe (72%) and MENA (79%). And while 50% of women in North America took cybersecurity-related courses, 91% of women living in MENA and 82% of European women did. Our respondents from North America were the most likely to report having no knowledge of cybersecurity, at 32%.

Europe. The results here show some dichotomies. Our respondents in Europe reported the highest participation in targeted K–12 STEM education (72%) and a cybersecurity course (82%). They had the greatest interest in pursuing a cybersecurity degree (89%). They were also the regional group that reported the highest degree of mentorship in the form of role models (82%). At the same time, our European respondents ranked highest in terms of regarding STEM to be male dominated (77%), regarding women in cybersecurity as "nerds" or "techies" (28%), and regarding the field as a difficult area for women to achieve a work-life balance (48%).

Middle East and North Africa (MENA). This region is a standout on several measures. Respondents reported the highest interest in cybersecurity education (94%) and the highest awareness of these programs (88%). They are the most likely, relative to those in other regions, to take part in targeted STEM (79%) and cybersecurity (91%) programs. Only 3% of MENA respondents report having no knowledge of cybersecurity. However, they are particularly likely to hold negative perceptions of cybersecurity workers, to regard cybersecurity as a field affiliated with the military or intelligence fields, and to anticipate difficulties in achieving a good work-life balance if pursuing a career in the field.

Asia-Pacific. Our respondents from Asia-Pacific were the least likely to regard cybersecurity as a male-dominated field—35%, versus 76% to 77% of women in Europe and MENA. They were also less likely than those in most other regions to perceive women working in the field as nerds or hackers—11% versus a range of 16% to 30% in sub-Saharan Africa, North America, Europe, and MENA. It follows that they were more likely than many others to regard women working in cybersecurity as "cool coders"—41% of respondents from Asia-Pacific reported this perception, exceeded only by those in MENA (46%) and Europe (50%).

Latin America. Women in Latin America appear to hold less negative perceptions of cybersecurity workers compared with the rest of the world. But only 9% of Latin American respondents reported having a lot of cybersecurity knowledge—the lowest percentage on that measure in our study. Latin American respondents rank highest, though, in terms of having ***some*** knowledge of cybersecurity—70% versus 54% to 56% of women in Europe, MENA, sub-Saharan Africa, and North America.

Sub-Saharan Africa. Fewer respondents from sub-Saharan Africa than anywhere else developed an interest in STEM in elementary school (7% versus a high of 27% in North America). But 73% of sub-Saharan Africans said they had developed an interest in high school—more than in other regions. Ultimately, the percentage of respondents developing an interest only once they had entered university was lower, at 21%, than in Asia-Pacific (23%) and MENA (33%). Sub-Saharan Africans were also fairly likely (76%) to report having had a role model to encourage them to learn more about cybersecurity.

A Framework for Change

In creating a framework to guide women's empowerment in cybersecurity, we did not start from scratch. We built upon lessons learned from the significant accomplishments of initiatives that are seeking to establish women's empowerment across industries and regions. These resources showed that the main constraints are adverse social norms, lack of legal protection for women, a failure to recognize and redistribute household and care work, and women's lack of access to financial, digital, and property assets.

BCG's approach to women's economic empowerment recognizes the need to address the issues of access and agency that women will confront across the four major stages of the employee journey: pipeline, recruitment, retention, and advancement. (See Exhibit 4.)

In our framework, the stages are cyclical, not linear, recognizing the value that women at each stage hold for women at the other stages. Primarily, women who are leaders in cybersecurity (who have reached the advancement stage of the journey) will bolster women who are newcomers to the field, inspiring those at the pipeline and recruitment stages and mentoring women at the retention stage. As Betsy Bevilacqua, from Facebook, told us: "Compared with careers in tech, the path of a security engineer is not clear. There are many directions you can take. Women in cybersecurity need more support navigating different career levels as we don't have a playbook."

Pipeline. At this stage, the issue is having a sufficient pool of talent with the requisite skills and interest to enter a field.

Giving women greater access to pursue cybersecurity education would broaden the talent pipeline. Targeted STEM engagement of girls and gender mainstreaming of cybersecurity before high school are essential steps for building the pipeline. Role models and senior encouragement will support this effort.

Exhibit 4 - Key Barriers to Women's Empowerment in Cybersecurity

Source: BCG research.

To spark girls' interest in cybersecurity in middle school and high school and sustain that interest over time, it's also necessary to address agency-related perceptions of cybersecurity as a boys-only or technologically elitist career. "We need to reframe cybersecurity as much more than a solely technical field," said Nadya Bartol, a managing director at Platinion, a digitally focused BCG specialty business. "Women have a lot to offer in a field that requires a combination of people, process, and technology skills to succeed."

Recruitment. The recruitment stage involves applying and interviewing for jobs and the screening and hiring process. The recruitment challenge related to cybersecurity is ensuring that women are included and treated equitably.

One key barrier to access that emerges in this stage is the tendency to want to recruit the "perfect candidate"—a tendency that kills diversity. Recruiters seek candidates who look like current employees, with the right tenure, education, and technical expertise; given the urgent need in the workplace, they are reluctant to consider candidates who will require training. This thinking can exclude women, particularly young women who are new to the field—and it doesn't help close the workforce gap. Access could be improved here by expanding the lens to include nontraditional candidates, sometimes hiring based on aptitude and being prepared to train or reskill for specific cybersecurity roles. Targeting women for internships is another way to address the issue.

Retention. Retention is a broad stage, encompassing many years of an employee's career. A focus on retaining women in cybersecurity must address compensation, gender biases, and more. Fostering a gender-inclusive workplace culture and implementing diversity, equity, and inclusion policies are key drivers for retaining women employees.

Efforts to date are not serving to keep women in cybersecurity jobs, though. What explains the leaky retention pipeline?

- Some women leave or suspend their careers because of expectations that they will take on unpaid household and care work—an agency challenge that we've previously discussed. Among the measures that companies can use to address this issue are "returnship" programs (a corollary of internship programs), gender- and family-friendly policies, equal and paid parental leave, and onsite childcare. Society at large must address the larger, and stickier, issue of redistributing unpaid care and household work.
- Women in Cybersecurity board member Jay Koehler provided another insight: "Women drop out because it's a 'boys' club,' and there is a low sense of belonging." Leaders can address this challenge—for example, through commitment and accountability to foster psychological safety and a gender-friendly workplace and by creating women's networks.
- Leaders should also take note of the fact that a good work-life balance is important to women—it is, in fact, a top-three career consideration—and that cybersecurity is perceived as a career where work-life balance is a challenge. (See Exhibit 5 for a look at women's career considerations by region.) This drawback can be addressed. Angela Bray Heise, a former vice president at Lockheed Martin, told us, "I pushed against the 24-7 culture in security operation centers and showed that it's not necessary for cybersecurity resilience."

Advancement. Advancement means moving people into leadership roles—and doing so equitably. Mentors and sponsors are crucial to advancing women to senior leadership roles in cybersecurity and to helping them navigate the industry overall and build business acumen, but it's hard to find women who can serve as mentors and sponsors at this senior stage.

Women's networks are crucial as well. Heise attested to the value of such networks in the cybersecurity field: "I had a strong women's network at Lockheed Martin. It was a key resource to share information and guidance for career advancement and find mentors." But it can be difficult for women in prominent positions in cybersecurity to find resources like this.

A Call to Action

We screened more than 120 public- and private-sector organizations around the world with a stake in women's empowerment in general and women in cybersecurity in particular to assess existing efforts. The progress made by such initiatives is clear—but so are the limitations.

Most of these stakeholders have a national or regional scope. Most are nonprofits. And most are concentrated in the US and Europe; data on women in cybersecurity in non-Western countries is lacking. The numerous initiatives are siloed and redundant. And stakeholders tend to focus on only one or two stages of the career lifecycle—the early stages of building a pipeline of qualified candidates through education and connecting candidates with employers for entry into the job market—rather than taking the holistic view that characterizes our cyclical pipeline.

Exhibit 5 - Women's Top Three Career Priorities by Region

	Having flexibility to balance work and family needs	Having a high-paying job	Making a meaningful contribution to society	Having opportunities for promotion and advancement	Being in a workplace that is welcoming to people like me	Having a job that others respect and value
Asia-Pacific	1	2	3			
Latin America		1	2	3		
Europe	2		3		1	
Middle East and North Africa				1	3	2
North America	1	3	2			
Sub-Saharan Africa			1	2		3

Source: BCG research.

There's a clear opportunity for an inaugural international initiative on women's empowerment in cybersecurity that covers the entire career lifecycle holistically and connects existing stakeholders and activities to share best practices and pool resources.

What can those with an interest in women's empowerment in cybersecurity do? National governments, companies, schools and universities, NGOs, and individuals can all play a role. For each of these stakeholders, it's important to consider agency- and access-related barriers across an entire career lifecycle. This could result in a broad range of constructive changes: at one end of the spectrum, planning and implementing policies; at the other, resolving with a partner to redistribute household and care work.

The challenges are great but the progress is encouraging, as indicated by our survey results—demonstrating higher-than-expected access to information, for instance—and by the women who talked to us about their successful careers in cybersecurity. Other promising trends: More women are entering cybersecurity; their participation doubled from 2017 to 2020, according to (ISC)² research. Women working in cybersecurity tend to have advanced education, which strongly positions them for leadership positions. And the cybersecurity compensation gap is narrowing among younger generations.

Continued efforts to empower women to participate in cybersecurity will bolster gender equality, broaden horizons for women, and strengthen cyber resilience.

About the Survey

In partnership with Ipsos, BCG conducted an online survey of 2,000 women undergraduate students in STEM (science, technology, engineering, and math) fields in six regions and 26 countries between February and March 2021. This survey was launched to provide insights into women's potential challenges entering STEM studies and their interest in and perceptions of cybersecurity careers. Survey questions addressed the significant global data gaps identified after a thorough global baseline assessment of women's empowerment in cybersecurity.

The regional breakdown of survey respondents was as follows: Asia-Pacific (500), Middle East and North Africa (287), Latin America (250), Europe (375), North America (500), and sub-Saharan Africa (88). In terms of age groups, 12% of respondents were aged 16 to 18, 63% were aged 19 to 23, and 25% were aged 24 to 30.

About the Authors

David Panhans
Managing Director & Senior Partner
Boston Consulting Group
panhans.david@bcg.com

Shoaib Yousuf
Managing Director & Partner
Boston Consulting Group
yousuf.shoaib@bcg.com

Caroline Wong
Consultant
Boston Consulting Group
wong.caroline@bcg.com

Ms. Basma H. AlShaalan
Global Cybersecurity Forum (GCF)
bshaalan@globalcybersecurityforum.com

Leila Hoteit
Managing Director & Senior Partner
Boston Consulting Group
hoteit.leila@bcg.com

Theo Breward
Project Leader
Boston Consulting Group
breward.theo@bcg.com

Ms. Alaa M. AlFaadhel
Global Cybersecurity Forum (GCF)
afaadhel@globalcybersecurityforum.com

Acknowledgments

The authors thank the participants from around the world who completed the survey. We extend our thanks to our colleagues from the BCG network for their insights, research, coordination, and analysis. We thank Angela Heise, Betsy Bevilacqua, Jay Koehler, and Nadya Bartol for their contributions as interviewees.

For Further Contact

If you would like to discuss this report, please contact the authors.


BCG
Global
Cybersecurity
Forum