MARKET RESEARCH

In Their Own Words

Women and People of Color Detail Experiences Working in Cybersecurity

(ISC)² Inspiring a Safe and Secure Cyber World

INTRODUCTION

Take a look around the table the next time you're in a security team meeting. Chances are, most everyone looks alike and comes from similar backgrounds. Diversity in all its forms (gender, age, ethnicity, skill set, etc.) is a rarity in the cybersecurity industry and has been for decades. This study looks at the contributing factors behind why the status quo has remained virtually unchanged for so long.

The current cybersecurity workforce gap stands at more than 3.1 million trained professionals worldwide, according to the 2020 (ISC)² Cybersecurity Workforce Study. While the number of professionals in the industry grew by more than 700,000 in 2020, women still only represent approximately 25% of the cybersecurity workforce compared to at least 40% of the global workforce, according to the Pew Research Center.

While organizations like (ISC)² have been studying the makeup of the workforce since 2004, and looking more deeply at gender, ethnic and cultural representation in recent years, numbers alone don't tell the full story of just how much of a challenge is before us to bring balance to organizational diversity practices.

This lack of diversity is amplified by a seeming inability to make meaningful progress over time, at least up until now. In the following study, (ISC)² wanted to move beyond quantitative findings to examine personal accounts of those who face the everyday challenges and dynamics associated with being a minority in the cybersecurity industry. This type of feedback can help us to better understand which practices, initiatives and efforts may help us create a more diverse cybersecurity workforce and foster more rapid progress toward greater inclusion and equity.

(ISC)² commissioned Synergia Multicultural Research and Strategy (Synergia) to conduct a global qualitative study in May 2021 that would help define where the cybersecurity profession stands today on the diversity spectrum.

Respondents were cybersecurity professionals from nine different countries who participated in 90-minute focus groups conducted by seasoned moderators from Synergia. The participants were asked about their perceptions of diversity in the cybersecurity sector, their unique challenges and experiences, as well as questions about how they see their organizations' commitment to diversity, equity and inclusion (DEI) programs. They also were asked to discuss what policies and initiatives they believe help contribute to entry and advancement in the industry in general, as well as those that led to their own personal successes.

While we have captured and summarized the key findings in the report that follows, our goal is for the words of our participants to speak for themselves.

These are their stories.

WHAT IS DEI? DEPENDS ON WHO YOU ASK

For many younger workers, DEI has always been a part of workplace training and development programs. And while many organizations, at least in theory, understand that highly diverse teams can directly contribute to greater profitability — meaningful progress to diversify the profession has been slow. If we are to address the workforce gap, we must look to both non-traditional areas to find qualified candidates and at the existing barriers to entry and advancement within the industry.

> "I'm typically the only woman in the room, no matter what country I'm working in, what conference I'm attending. That's the reality, the Cybersecurity profession today is still a white, middle-aged man profession."

When asked to define diversity, equity and inclusion, the good news for the cybersecurity industry is that professionals from around the world have similar views on the definitions of DEI.

Respondents define diversity, in the context of increasing diversity within the cybersecurity profession, as increasing "awareness and acceptance of the differences between individuals." These differences can be biological, demographic or cultural, but also refer to differences in thought, experience, ability or leadership style.

Equity seeks to ensure an equal outcome for each person despite different circumstances by allocating the exact resources and opportunities tailored to their specific needs.

Inclusion refers to "creating an environment where diversity is accepted and celebrated, and all people are able to fully share their ideas, collaborate and work in harmony." In other words, participants define inclusion as an environment where everyone feels they belong.

Geography and history obviously shape individuals' perceptions of diversity, and some countries weighted aspects of diversity differently. For example, respondents from the United States spoke about race, ethnicity and ability impacting their definitions, while respondents from Malaysia and Singapore cited region of origin. South Africans highlighted race, gender and socio-economic level, while the United Kingdom pointed to gender, ethnicity and caste, and Germans cited gender and German-language fluency.

Regardless of these weightings, many of the perceptions of DEI in the cybersecurity industry are shared globally. The most common diversity issue around the globe is gender diversity, with women still very underrepresented in the cybersecurity industry across all countries.

There is an overarching perception that professionals in the cybersecurity industry have a very homogeneous profile: white, middle-aged males, who have more than eight years of experience in an IT or Computer Science related field. Professionals surveyed believe that this lack of diversity is particularly significant in leadership positions, and that the pipeline of younger women coming into the profession is also very narrow, causing a systemic problem.

"Women are often set up to a higher bar," said one respondent. **"They get evaluated based on their proven experience, whereas guys get selected based on their potential."**

"I'm a woman, and then I'm Black, and I'm young. So I constantly feel out of place," added another respondent. **"I constantly need to prove myself so that the teams I'm working with respect me."**

Lack of diversity related to experience and skills is another prominent issue in the cybersecurity industry that many respondents discussed. There is a general perception that the bar for entry into the cybersecurity profession is set at such a high standard of educational background and professional certifications that it perpetuates and rewards the same candidate profile as those already in the field. Often, younger, entry-level professionals, who can perform a variety of technical tasks that don't necessarily require professional certification, are overlooked in favor of individuals who hold certifications. This is a missed opportunity as these individuals frequently possess skills in areas such as risk management, analytics or communications that can be just as important to a security team.

One respondent called out the lack of inclusion as a significant issue within the profession.

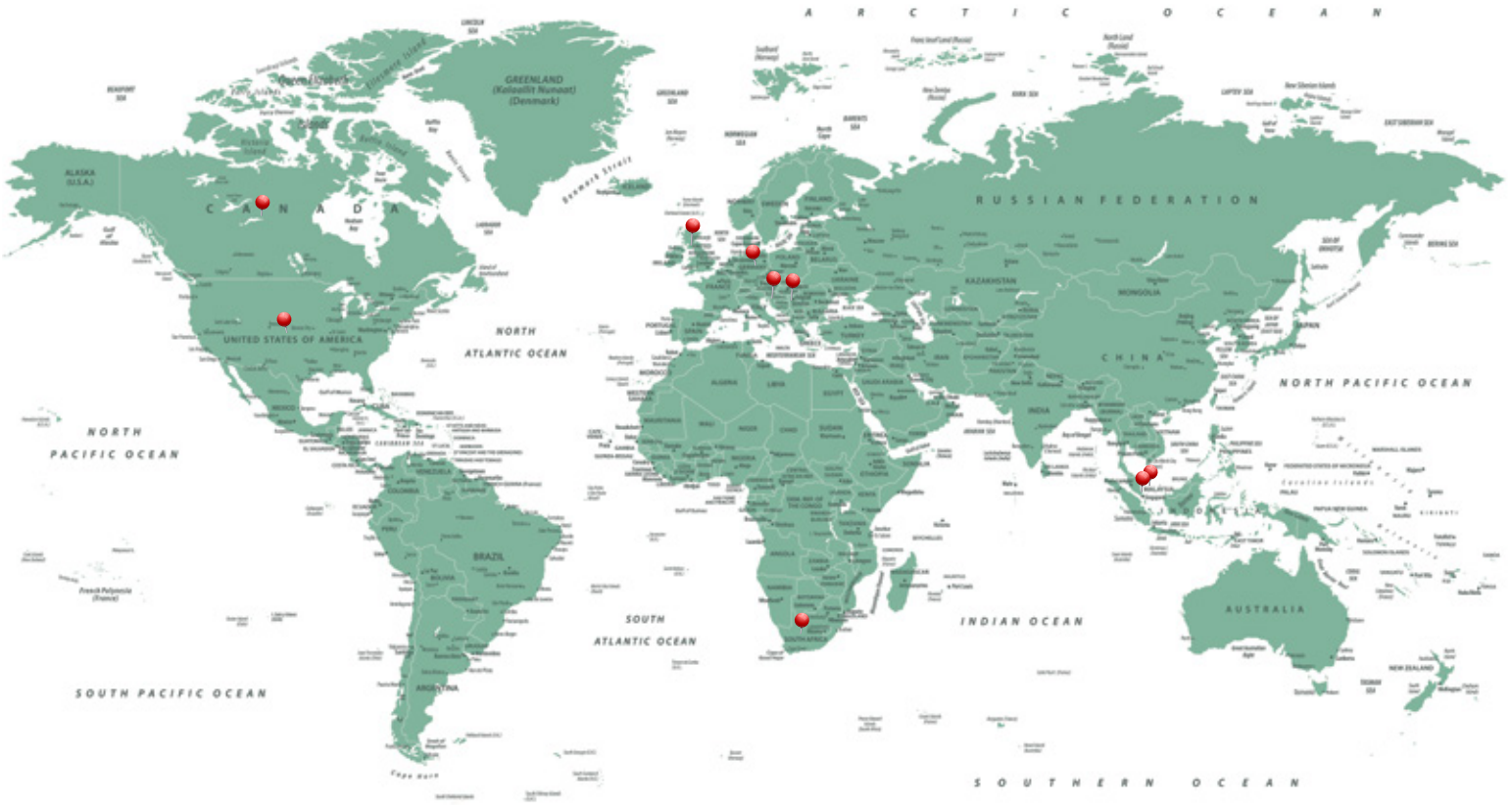
> "Job descriptions and hiring managers still operate within a box. A box designed by non-diverse individuals who set the bar too high and want to hire people who look different to them, but who they expect to think and act the same way as them."

Said another respondent, **"I think there is a global cultural issue. I know there are a lot of women and minorities that are well qualified and get passed over. Maybe because they're not articulating their skills in the right way or they're not even applying for the jobs because the organizations are being unrealistic about the requirements they put on the job description."**

"The cybersecurity profession needs critical thinkers, and critical thinkers can be mathematicians or lawyers," another added. **"They can be all kinds of things that I am not. I think we're heavily lacking from an experience and ability perspective when we talk about diversity."**

Again, regional perceptions shaped by history, culture, socioeconomic conditions and geography factor into assessments of DEI in the cybersecurity industry. In the United States, United Kingdom, and South Africa, ethnic and racial diversity are a prominent issue. In the United States, Blacks and Hispanics still have marginal representation in cybersecurity positions despite representing over 30% of the total population according to recent U.S. Census data. In South Africa, organizations are struggling to achieve equal representation of all the different ethnicities immigrating from across the African continent.

Research participants are located in nine countries including the United States, Canada, the United Kingdom, South Africa, Malaysia, Singapore, Germany, Serbia and Croatia



> "As we always say, representation matters, so I speak from my experience. If we don't see people that look like us in a certain field, half the time we won't pursue it."

In the United Kingdom, Asian-British (Indian, Pakistani) and Black British (African) are still highly underrepresented as well. In Serbia and Croatia, respondents noted a lack of representation of immigrants from neighboring regions, while professionals in France and Germany noted that leadership teams in global cybersecurity companies still lack representation of professionals who are not country natives or fluent in the local language.

There are areas where a "satisfactory" level of diversity in the profession was achieved in the eyes of the participants. In Singapore and Malaysia, for instance, diversity is perceived to be an intrinsic aspect of the culture with professional advancement mainly based in meritocracy. Women also now represent more than half of students enrolled in technology-related careers in these regions. It should be noted, however, that not all cultures treat diverse individuals fairly or respect their rights, and that discrimination can still exist even in places where diversity is perceived to be highest.

Starting Your Own DEI Program?

The (ISC)² DEI Resource Center hosts a number of useful guides that can help you start your own DEI journey, either as an organization or a professional. Examples include:

- Key Terms and Definitions
- How to Develop a Strategic DEI Plan
- Defining the Business Case

For more resources, visit www.isc2.org/dei

WHAT'S HOLDING YOU BACK?

When diverse professionals were asked to talk specifically about the unique challenges and experiences they've had, several common themes emerged: the glass ceiling is still very real; unrecognized or stolen contributions lead to feelings of exclusion; and there is a lack of diverse mentors and role models in the cybersecurity industry.

Several women, and men from minority groups, said they have been bypassed for advancement opportunities, particularly into leadership positions, even when their experience is comparable to that of a white male in the same position. Respondents also noted that the salaries for white men are higher than those for women and minority ethnic professionals, even when the title and responsibilities are the same. Quantitative data backs that up, especially on the gender divide. According to the 2020 Cybersecurity Workforce Study, women of all experience levels earn significantly less than their male counterparts globally in cybersecurity roles. In some cases, such as those women with between one and three years of experience in the field, the delta is stark. Men with the same years of experience earned $26,836 more in 2020. And those shortfalls don't disappear further into a career. At the C-level, the differential between women's and men's salaries was $42,890 last year.

The "maternal wall" is also a common issue for women, with many companies and professional organizations not allowing accommodations for women needing to take time off after they give birth.

One woman in the U.K. said, "a lot of women, when they get pregnant, go away and they don't come back to that job for one reason or another, even if it is protected under law. They get pushed out, they get treated oddly. Most leave the profession altogether or move into academia, where they typically find more accommodations."

Women and men from minority groups also struggle to feel a sense of belonging and value within traditional cybersecurity organizational settings. Not being heard, not having their opinions validated by others, and even having their contributions or ideas stolen by others, are common experiences for diverse cybersecurity professionals.

"I've been in meetings where people have used my words. They've used my strategies. They have taken my work, and they presented it as their own," said one respondent. "They get the credit for my talent. It would burn me so bad but, yet, I didn't really have anyone to lean on."

"I've seen really experienced professional women, and I asked them why don't you express your opinion? Why don't you speak up? They feel afraid that their male colleagues will start asking uncomfortable questions or have uncomfortable comments, which is something that we really should stand against," said another respondent.

This "I didn't have anyone to lean on" concept was highlighted by many respondents when talking about both the lack of mentors and role models for diverse individuals in the industry. It's a case of "you can't be what you can't see." Individuals report having a hard time finding mentors to guide them in their professional advancement, and the limited representation of diverse individuals in leadership

> "We see a lot of diverse professionals in entry-level positions. But they don't stay long enough to advance into higher positions. Exit surveys report they leave because the culture doesn't support them. They feel lost."

roles across the cybersecurity industry causes many women, and members from minority ethnic groups, to perceive it as an industry where they are not welcome.

The absence of diverse role models that aspiring professionals can identify with, and find inspiration from, is a major barrier for awareness and consideration of a cybersecurity career. For the respondents, this, along with historical, social and cultural stereotypes in many countries exacerbates the perception that technology and security careers are for males only.

One woman noted, **"for a very long time, I was the only CISSP-certified woman in my country. And we have 4.1 million people. Now it's getting better, but still not a lot of women are aware this is a career for them. There is no one to look up to, to be inspired by."**

Another added, **"As the only woman in my team, I always had a hard time finding a mentor I could relate to or who gave honest advice. I often felt lonely and had to learn a lot of things through trial and error."**

Burnout for those who do stay in the industry is real, according to participants. A great majority of diverse professionals who start their career in cybersecurity (as entry level technicians or interns) leave the profession because companies don't have a clear succession plan to make them feel like they belong in the organization. Diverse individuals in the profession often must carve their own paths. They spend a great deal of energy figuring things out on their own, learning through unpleasant experiences and continuously inspecting their own behaviors and how they could be perceived. All these factors typically lead to career abandonment.

WHY IS IT SO DIFFICULT TO SUSTAIN EXCITEMENT AND SUPPORT FOR DEI PROGRAMS?

One of the biggest challenges to making progress with DEI programs is unconscious bias, or social stereotypes about certain groups of people that individuals form outside their own conscious awareness. We all hold unconscious beliefs about social or identity groups, rooted in our tendency to organize and categorize information. Because these biases are implicit, they can be hard to acknowledge and address and they show up in the workplace in practices ranging from recruitment and retention to merit increases, career progression opportunities and who gets invited to meetings — or lunch.

> "It is human nature to like and be attracted to others who share similar interests, experiences and even appearances to our own."

While unconscious bias is difficult to spot, understand and tackle, it provides a powerful catalyst for discussion.

"I've witnessed how unconscious bias is a huge factor impeding the consideration of diverse professionals for leadership positions."

"If you actually historically doubt the intelligence level of many minorities and women, if you have those thoughts as a hiring manager and don't think a diverse candidate is even smart enough, just because of some type of discriminatory belief that you have, then you are not going to give them that opportunity," another added.

Unconscious bias applies to everyone, even those in the minority within an organization. Shining light on bias and making room for workplace conversations has been shown to be highly effective in sparking change – as long as it's not treated as a check-the-box activity by management.

In addition, transformative change takes time, and many current business practices are not built to encourage patience. DEI initiatives can suffer from some of the same problems that any large business initiative faces. Without clear goals, expectations and investment from the organization's leadership, these initiatives become generic and are doomed to fail, according to respondents.

> "Convincing the majority of cybersecurity professionals (white, middle-aged men) that diversity and inclusion is not a threat to their jobs or their companies, but an asset, is not going to be easy. There are many unconscious biases that are deeply ingrained in our system."

"It's easy to start an initiative when the global temperature on diversity is so high. However, DEI initiatives typically don't get fast results," said one respondent. "**They are a slow, tedious process that requires ongoing commitment and dedication from the whole organization, along with designated performance metrics that help to track success and keep stakeholders' motivation up."**

Another added, **"Many companies are still seeing DEI practices as an extracurricular/voluntary activity, something that is optional, therefore not a lot of people make it a priority. Whenever there is a DEI meeting or workshop in my company it's only us (the Black and Hispanic folks) who show up. It's like preaching to the choir."**

And yet these programs are sorely needed and valuable in making individuals feel seen, according to one respondent. **"As a Black woman in cybersecurity, I need to have a formal avenue to talk to other folks that are not diverse, to tell my story, to share my successes and challenges."**

FRAMING THE OBJECTIVES AROUND DEI GROWTH

Successful DEI programs require embracing change, discomfort and commitment. While lasting change takes time, there are three key areas where individuals and organizations can strive to make progress toward creating a diverse, more equitable and inclusive cybersecurity profession. These include creating awareness about and access to cybersecurity careers, fostering inclusivity and purposeful advancement, and laying a programmatic foundation for diverse professionals.

Create Awareness and Access

The cybersecurity industry suffers from an overarching lack of awareness about the breadth of opportunities and flexibility that the profession offers. It's critical that DEI initiatives are not viewed as an add-on or "nice to have," according to respondents. Organizations should review marketing and education materials to reflect diversity and portray the cybersecurity profession as inclusive for minority groups.

Leaders should celebrate diverse individuals who have become trailblazers in the cybersecurity industry and ensure that these successes are communicated in places that reach minorities at crucial stages of their career selection process.

"We need more Black women and Latinas in cybersecurity, speaking, showcasing their talent, being the trailblazers and paving the path for others knowing that these cybersecurity careers exist, and that it's personal," said one respondent. When asked specifically about personal factors that led to their success in the industry, respondents highlighted supportive supervisors and mentors who valued diversity of thought, recognized their talent and were eager to give them an opportunity to shine. Working in organizations where DEI practices are ingrained in the culture, and where diverse individuals are treated with dignity and respect were also called out.

"I'm a Black guy from a small rural town. So, I'm miles away from where you think I'd end up. But I had the luck to be in the right place at the right time, and a boss who gave me the chance to take care of an issue no one seemed to be able to fix," said one respondent. **"I was able to succeed at it and that opened a big door for me. That motivated me to get a CISSP certification. The rest is history."**

Foster Inclusivity and Purposeful Advancement

To encourage long-term career success, organizations should create formal mentorship programs for professionals from diverse backgrounds. These programs should match up employees new to the industry with an experienced cybersecurity professional they can trust and rely on, and who can help them navigate and grow into their roles.

Just as important, and arguably even more so, organizations should foster a culture and environment that's conducive to informal mentorship as well. That kind of buy in from individuals can support a culture of inclusivity and permeate an organization from within.

The great news is that organizations do not need to recreate the wheel. There are already a number of established organizations that support diverse groups in cybersecurity like **Blacks in Cybersecurity Association**, **ICMCP** (International Consortium of Minority Cybersecurity Professionals), **WICyS** (Women in Cybersecurity), **(ISC)²** and **Black Girls Hack** that offer formal training and scholarships to help make cybersecurity more accessible. Organizations can partner with them and leverage their expertise to build successful programs. The (ISC)² DEI Resource Center hosts a broad range of free, downloadable content that can help organizations and individuals audit, build and measure DEI initiatives of their own.

Lay a Programmatic Foundation

Many respondents cited their early exposure to STEM as a personal factor that led to their success in the cybersecurity industry.

"Although I knew nothing about it, when I was in college, I volunteered at a STEM event for young girls … They actually had to decode a message, find some evidence within the hard drives, and I said 'this looks interesting'." shared one respondent. **"So, I did some research, attended the University of Maryland [Global Campus] and realized that there's a non-technical side of cybersecurity as well, and the skills I had in engineering could transfer into cyber. That's how I ended up getting into cybersecurity."**

Developing programs to make cybersecurity an integral part of early education will help ensure diverse representation in the future. Exposure to cybersecurity and the profession from an early age, at a global level, through classes, STEM-related workshops or conferences hosted at colleges and universities is one way to address this.

"Ever since I was a girl I loved mathematics and playing with my brother's Meccanos. Instead of having me play with dolls, my parents always supported me and signed me up for STEM summer programs," said one respondent. **"When it came to selecting a career, computer science was a natural fit. Because I was great at math, I started to be invited by the cybersecurity guys to help them break codes, and eventually I became a full-time member of their team."**

> "Cybersecurity today should be a topic as important as fire safety or health education. We need to start building awareness earlier on so children start embracing it from a young age, dreaming about becoming a cybersecurity officer just as they dream of becoming a fireman or a doctor."

As educational systems increasingly weave STEM and STEAM concepts into curriculum, organizations in a position to do so should build programs that increase curiosity among young women and people of color in the different cyber-related careers that exist and demonstrate how science, technology, engineering, arts and mathematics can help to develop marketable skills that can aid entry into such a career. Individuals in the field can also get involved by volunteering in such programs and providing mentorship to students.

WHERE TO START: RECOMMENDED ACTIONS FOR IMPROVING DEI IN CYBERSECURITY

DEI is never going to be a "set it and forget it" proposition, so organizations need to commit for the long-term as well as be flexible and adaptable. Achieving DEI "success" is doable with the right best practices. Several respondents noted that their private and public organizations are taking slow but steady steps toward embracing DEI practices, with the most effective ones being:

- **Diverse Leadership.** Maintain a balance of men and women in leadership roles, both on executive teams and on boards of directors, as well as representation of people from different ethnicities across all levels of the organization. Leaders should encourage global representation and collaboration by giving team members in international regions stronger roles on teams.

- **Cultural Sensitivity Training.** Hold dedicated and mandatory training focused on raising cultural awareness, educating staff on the nuances of cross-culture communication, recognizing common workplace biases and highlighting the value of diversity. We all have unconscious bias, and the only way to combat it is to actively address it through mindfulness exercises and consistent training.

  "My organization has made DEI training mandatory and not voluntary like it used to be. They have also hired several women for key leadership positions. I've witnessed a change in the past year with more people sharing their ideas and collaborating, rather than everyone trying to protect their territory," said one respondent.

- **Purposeful Inclusion.** Ensure conscious leadership and give everyone a voice. Actively engage diverse professionals to collaborate on key projects and in meetings.

"Recruiting for diverse talents is a bit of a challenge and our organization really is trying to get more women involved in cybersecurity," said another respondent. **"They have monthly brown bags that they promote in order to have women tell their story of their pathway into a cybersecurity field. I think sharing that story of how you got there kind of does help attract women and minorities, so they can feel a sense of not being the only one trying to pursue this."**

» **Diverse Working Groups and Committees.** Actively ensure that working groups have a mix of individuals from different gender, ethnic background, age and experience levels, among other diversity characteristics.

"Our organization has introduced diverse hiring panels for recruiting for both technical and non-technical roles," added another respondent. **"Diversity includes men, women and others that are there to just be engaged in the conversation, to learn how we are recruiting. Working in teams and embracing remote hiring practices is helping to identify diverse candidates to join the cybersecurity division."**

» **Hiring and Recruitment Targets.** Establish targets to help organizations grow a workforce that closely reflects the diversity of the specific region's population.

"In the public sector in the U.S., there has been a lot of focus on getting more women, getting more minorities and getting everyone to share their story. Hiring diverse professionals, with less solid skill sets and putting together work teams with an experienced leader that helps everyone get to a similar level of skill set. Having diverse teams to promote different ideas and perspectives, not only their cybersecurity-related skills."

- **Advancement.** Document clear advancement practices that create transparent paths to leadership positions for diverse professionals, and provide the necessary resources for advancement, including technical training, language tutors, opportunities to pursue certifications, etc. Organizations need to develop guidelines for such programs including standardized parameters and metrics. These should be focused on helping organizations develop competencies among diverse employees, through targeted learning, job rotation and training, to fill key positions and ensure diverse leadership.

  "One of the things that we are looking to do is to create more formalized succession planning that is really targeted toward what we call URGs: underrepresented groups," said one respondent. **"That includes women and other underrepresented groups. We have drafted career plans and identified the key resources needed to achieve those career goals."**

- **Pay Equity.** Actively monitor pay equity for all roles within an organization and ensure that salary and benefits are aligned based on role requirements and experience.

- **Success Stories.** Like any other skill, some people will need to learn how to be more inclusive. Organizations should implement formal training and skills development programs focused on creating awareness and fostering effective DEI practices across the company, across all departments and management levels. It's also important to share wins, highlighting successful DEI best practices and programs from organizations around the world.

HOW DO WE MAINTAIN AND GROW OUR COMMITMENT TO DEI?

DEI is crucial to the future success of cybersecurity. Set goals and objectives that are measurable and where progress can be tracked over time. Be transparent on your progress toward achieving KPIs —share the good, and the bad. When employees see that DEI initiatives have practical impact and drive results, they be more likely to embrace new practices. Progress gets people excited.

Work with your human resources team and recruiters to clearly articulate the skills needed for cybersecurity roles so that job descriptions clearly reflect not only the required technical skills, but also the diversity of thought, experience and non-technical skill sets you seek.

When entire organizations from the C-Suite down to entry-level employees invest time and energy to create an inclusive and equitable culture for all employees, change happens.

> "The diversity of thought is a global crisis. I mean, it needs to be in the cybersecurity workforce or else nothing's going to be secure in this world."

To find more actionable content that can guide you and your organization along the DEI journey, please visit the (ISC)² DEI Resource Center at www.isc2.org/DEI

About This Research

(ISC)² commissioned Synergia Multicultural Research and Strategy (Synergia) to conduct a global qualitative study that would help the organization define where the cybersecurity profession stands today on the diversity spectrum.

- A total of 22 respondents participated in the research.
- Seven 90-minute focus groups and one individual interview were conducted from May 18 to May 26, 2021. Groups were conducted in English by a seasoned moderator from Synergia Multicultural Research and Strategy.
- Countries represented in this research included: United States, United Kingdom, Germany, Croatia, Serbia, Singapore, Malaysia, South Africa and Canada.

About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 160,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education™. For more information about (ISC)² visit our website, follow us on Twitter or connect with us on Facebook.