ISC2 | Chartered Institute of Information Security

Recruitment & Retention

in Cybersecurity

identify hire support

The talent, expertise and resources of your workforce are your business' most valuable assets. Caring for those assets matters across all industries, and even more so where there's a considerable skills gap. The global cybersecurity workforce grew to encompass 5.5 million people in 2023, reaching its highest-ever levels, but demand is growing even faster. The cybersecurity workforce gap has grown more than 12.6% year-over-year, making it a profession in dire need of more people. 4 million more people, if we're being specific.

The Chartered Institute of Information Security (CIISec) has joined forces with ISC2 to increase the number and diversity of professionals that enter, stay, and advance within the cybersecurity profession. This guide is designed to provide tips to organizations looking to increase their diverse hiring by helping them identify, hire and correctly support skilled employees from all backgrounds.

First, Understand the Basics

There are several considerations like compensation and benefits, meaningful work and work life balance that are universal workforce considerations. Consider the following when looking to attract, recruit, onboard and retain professionals in the cybersecurity industry:

- **Offer competitive compensation and benefits:** Cybersecurity professionals are in high demand, and competitive compensation packages can help organizations stand out and attract skilled individuals.

- **Provide tailored professional development opportunities to accommodate different learning and retention styles:** Cybersecurity is a rapidly evolving field, and professionals seek continuous learning and growth. Providing multiple routes to opportunities for professional development, such as training programs, certifications, conferences and workshops, can attract candidates who are eager to enhance their skills and knowledge.

- **Create challenging and/or meaningful work:** Cybersecurity professionals are motivated by the opportunity to work on challenging and impactful projects. Providing meaningful work that allows them to make a difference in protecting organizations from cyber threats can be a strong attraction and retention factor.

- **Build a strong organizational culture that prioritizes cybersecurity:** Promote a sense of teamwork, collaboration and innovation. Fostering an environment that encourages knowledge sharing, creativity and open communication helps cybersecurity professionals find meaning in their work.

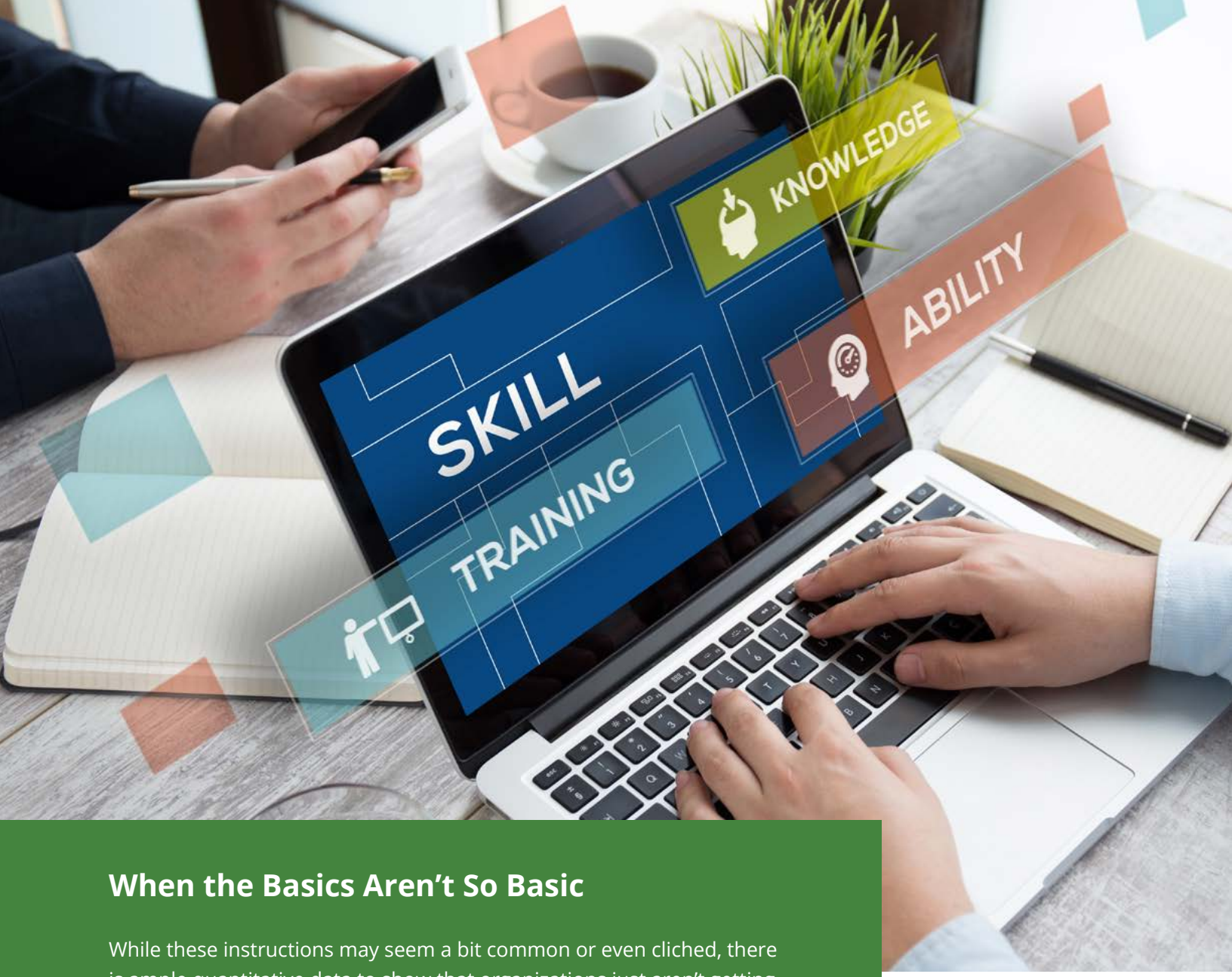
- **Understand what work-life balance means to each employee:** Striking a balance between work and personal life is essential for employee satisfaction and retention. Providing flexible work arrangements, such as remote work options or flexible hours, can be appealing to cybersecurity professionals who often face demanding workloads and irregular hours.

- **Cybersecurity mentorship programs are critical to support the next generation:** Effective leadership and mentorship programs are crucial for new entrants in the cybersecurity industry. Providing guidance, support and opportunities for mentorship from experienced professionals can help accelerate their learning and development and improve retention rates.

- **Provide up-to-date technology and tools:** Cybersecurity professionals rely on advanced tools and technologies to carry out their work effectively. Providing access to up-to-date technology and cybersecurity tools is essential for attracting and retaining talent in the industry. This also includes tools such as screen readers, time management and other inclusion tools that allow ALL employees to thrive.

- **Recognize and reward employees:** Recognizing and rewarding cybersecurity professionals for their contributions and achievements is important for fostering a positive work environment. Acknowledging their efforts through incentives, bonuses, promotions or public recognition can help boost morale and increase job satisfaction.

- **Develop clear career pathways:** Providing clear career progression pathways and growth opportunities is crucial for attracting and retaining professionals. Offering well-defined job roles, advancement opportunities, and offering lateral moves and pathways for specialization within the cybersecurity field can motivate individuals to stay and grow within the organization.



When the Basics Aren't So Basic

While these instructions may seem a bit common or even cliched, there is ample quantitative data to show that organizations just aren't getting it. Only about half of workers in the United States are very satisfied with their jobs, with even smaller numbers expressing satisfaction with training, compensation and advancement opportunities. Worldwide, less than a quarter (23%) of full and part-time employees feel engaged at work. And in the cybersecurity industry itself, stress and overwork can run rampant.

Clearly, there's room for improvement. To break down these basics into more manageable and actionable steps, we separated them into three categories:

- **Attracting and recruiting new candidates to cybersecurity**
- **Onboarding, training and developing new employees**
- **Nurturing and retaining cybersecurity professionals**

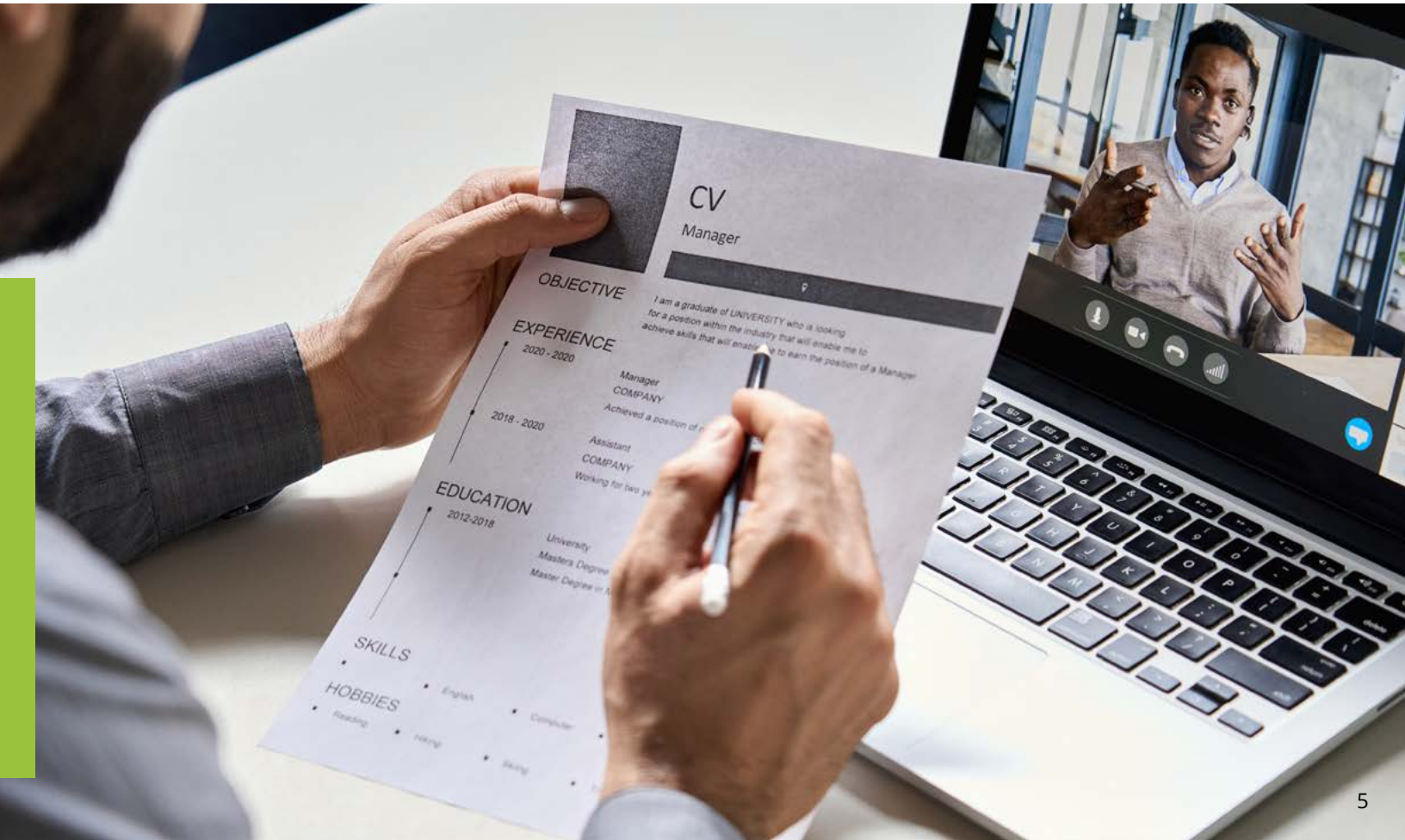
These tips, from industry experts, will help you increase your diverse hiring and create and maintain a truly inclusive working environment where everyone can thrive.

Filling the Roles

Cybersecurity professionals are responsible for protecting data, assets and people so it's important to attract employees that reflect the customer base and communities they protect. People with different backgrounds bring new perspectives to the table, which can help to identify and mitigate security risks that might otherwise be overlooked. This isn't just about recruitment. It's about attracting people to the profession that may not have seen themselves in the role, and it's also about making space for staff with nontraditional career paths who bring a new approach and way of thinking to solving problems. This includes different genders, races, ethnicities, socioeconomic statuses, neurotypes and gender identities, as well as candidates with different physical and psychological needs.

First, consider where jobs are advertised. Along with traditional job portals, include academic campuses, career and skills development centers, diversity-focused member associations and nonprofits, recruitment fairs, and military bases in your outreach. Find young people where they are - social media, tech communities and forums, gaming centers, lobbies or conventions.

Next, look for professionals early in their careers. Cybersecurity is often learned through hands-on experience, which can be limiting for young people. Providing opportunities for practical experience, such as simulations, lab exercises and real-world projects, is crucial to their growth. These professionals may not have experience in a sector where ethical conduct is paramount. Provide ways to emphasize ethics, integrity and the importance of maintaining confidentiality so that they understand how it is vital to their jobs. Early career professionals may also lack some specific technical skills required for cybersecurity positions. These can be learned, but it's important to address any skill and knowledge gaps early on and provide a pathway for how they can be acquired.



Another way organizations can attract employees to cybersecurity is to look at what SKILLS you need to hire for, as opposed to what looks great on paper. Many transferable skills that are valuable in other professions (critical thinking, problem-solving and attention to detail, among others) are needed in cybersecurity. This means that companies can often find qualified cybersecurity staff from other industries without having to train them from scratch.

Career changers can come from any walk of life. For example, a cybersecurity professional with a background in finance may be able to apply their skills in risk management to cybersecurity, while a cybersecurity professional with a background in marketing may be able to apply their skills in communication to the job. Engineers have a strong understanding of how systems work, which can help them identify and mitigate security risks, while lawyers can help them to ensure that organizations are compliant with cybersecurity regulations. Business analysts have a strong understanding of business processes, while teachers have experience in educating and communicating complex concepts. They can also help to raise awareness of cybersecurity issues among students and the public.

Last, understand what unconscious bias is and how it affects the way you attract, recruit and interview both young professionals and candidates looking to make a career change. The best way to demonstrate that you are a multicultural organization that respects diversity is to BE a multicultural organization with multicultural leadership across different levels to drive and support inclusivity.

Preparing Cyber Professionals for Success

Once organizations have hired cybersecurity professionals, they need to put programs in place to ensure that those hires are best positioned for success. An ISC2 report, ***In Their Own Words: Women and People of Colour Detail Experiences Working in Cybersecurity***, found that the lack of diversity in mentors and role models in the cybersecurity industry, along with struggling to feel a sense of belonging and value, is a common experience for diverse cybersecurity professionals. Proper onboarding, along with ongoing training and development, can help address some of these challenges.

Cybersecurity professionals in the early stages of their career don't only need technical skills. They also need to learn how to communicate, problem solve and collaborate. Often referred to as "soft skills," these professionals may need guidance on how to work effectively with different teams and stakeholders. These hires also need to learn the ins and outs of their organizations' cultures. Demonstrating how cybersecurity aligns with the organization's broader business goals and risk appetite will help these young professionals understand where they fit and more importantly, how they can have an impact on overall business operations. They may have imposter syndrome and doubt about their abilities in a competitive and constantly changing field like cybersecurity. Showing them their impact, encouraging them, and listening can go a long way during the onboarding process.

Career changers may have more confidence in their ability to adapt to a challenging and evolving environment, but organizations still need to provide an introductory experience that inspires and ideally excites them. A buddy system can help reduce onboarding time, showing the new worker how to learn the ropes, get familiar with the company's security policies and procedures and get up to speed on company processes. By setting up your new hire with a buddy (ideally one with similar skills and interests) early on, the organization can help identify any challenges or problems that the new worker is facing and provide the support they need to succeed. It also encourages communication and creates a supportive and collaborative work environment.

Both young employees and career changers need ongoing training and development. Cybersecurity is a fast-paced industry, and professionals need to continually update their skills and knowledge. Consistent training and mentoring will also help these hires keep up with the latest trends, tools and best practices. Because the security landscape is constantly changing, organizations need to make sure their employees are motivated and equipped to tackle the challenge. This can take the form of external industry-standard qualifications or training. Along with these tangibles, it's important to create a culture that embodies development. Be patient with new hires as they learn and grow in their new roles and provide them with the support they need to succeed. This includes providing resources, encouragement and opportunities for growth.

Retaining Talent That Excels

Once talent has been recruited, hired and onboarded, organizations need to provide a workplace culture that those hires WANT to stay in. CIISec's 2022/23 ***State of the Profession*** report found that 80% of cybersecurity professionals believe they have good or excellent career opportunities, and more than 84% say the industry is growing. That said, more than 22% work more than 48 hours per week and 8% work more than 55 hours which, according to the World Health Organisation, marks the boundary between safe and unsafe working hours. When asked what keeps them awake at night, the two main sources of stress for cyber professionals are their day-to-day stresses and workloads (50%) and suffering a cyber-attack (32%).

Burnout is real. As is poor management, imposter syndrome, unsatisfying work and bad atmospheres between colleagues. Early career professionals might face burnout and stress as they strive to prove themselves and excel in their roles. Providing a supportive work environment and promoting work-life balance are important in preventing them from losing their spark. For career changers with no prior cybersecurity experience, it's important to have a structured career path in place, and unambiguous examples of "what good looks like" to provide them with the appropriate support to help them succeed.

Because the skills shortage in the security and IT industries is well-advertised and understood, employees have more options to change companies if firms don't offer them the appropriate support. Be prepared to offer significant salary increments in the first few years of employment. It isn't uncommon for new graduates to cycle through two or three jobs within the first few years of their career, gathering significant salary jumps for each one. If you're prepared to invest in training and developing a person new to the industry, be prepared to pay them the going rate – otherwise your competitors will thank you for your training and development efforts. Senior leadership should be approachable and demonstrate, from the top, that their organization is a welcoming environment where individuals can thrive and be productive, innovative and creative in solving problems. Encouraging, developing and supporting a diverse workforce will help individuals grow, but it also helps everyone feel like they belong and shows other individuals from non-traditional backgrounds that this is a truly multicultural organization.

Conclusion

The cybersecurity industry is in desperate need of more people with different and innovative backgrounds that can bring new and inclusive ways of thinking to solving global challenges. Focusing on finding the right people, even if they come from nontraditional backgrounds, and providing them with pathways for advancement and equitable compensation and benefits, will help get us there.

Chartered Institute of Information Security

The Chartered Institute of Information Security (CIISec) is the natural home for the cyber and information security professional community at every career stage. This is achieved through having programmes that support:

Development – CIISec is the place to go for cyber professional development and ethical practice.
Recognition – CIISec provides an authoritative voice for the cyber industry and recognition of excellence in practice.
Success – CIISec helps you and your business succeed securely in the digital world.

CIISec provides a universally accepted focal point for the cyber and information security profession. It is an independent not-for-profit body governed by its members, representing over 35,000 individuals.

For more information visit **www.ciisec.org/** or connect with us on **LinkedIn**.

ISC2

ISC2 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, ISC2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 600,000 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 general public through our charitable foundation – **The Center for Cyber Safety and Education**™. For more information on ISC2, visit **ISC2.org**, follow us on **X** or connect with us on **Facebook**, **LinkedIn** and **Youtube**.

CC SSCP CISSP CCSP CGRC CSSLP ISSAP ISSEP ISSMP