A Window of Opportunity
Ending the Cyberworkforce Shortage Once and for All

Two years ago, the cyberworkforce shortage was the number-one concern for chief information security officers (CISOs), security operations center (SOC) managers and other security leaders. Researchers estimated that there would be 1.8 million unfilled cybersecurity jobs by 2022 and that every third SOC seat was open. Nearly 70 percent of security leaders in North America did not have the security professionals they needed to protect their organizations.¹

In 2020, this challenge was overtaken by a new concern: protecting a newly and predominantly remote workforce in the midst of a global pandemic. Along with the COVID-19 pandemic came some of the highest unemployment rates the world has ever seen. In April 2020, unemployment in the United States hit 14 percent, and a total of 23 million workers were jobless.² Although US 2020 unemployment rates have been the country’s worst since the 1930s, they have created a unique opportunity for security leadership.

Despite what traditional job descriptions and hiring models say, true cybertalent is not defined by the certifications a candidate has or the number of tools and languages they know. Fundamentally, cybertalent is built on problem solving, creativity, an analytical mindset, communication skills and passion. Although the technical skills of the unemployed millions may vary, many of them possess these essential qualities and—with the right training, opportunities and mentorship—can be great candidates for even the most technical cybersecurity jobs.

Simply put, the cybertalent shortage is over. The talent pool is bigger than ever and, with the right training and career development programs in place, CISOs can rapidly build the talent they need to establish a diverse cyberworkforce for the long term.

The Workforce Shortage Is a Problem of Development, Not People

The crux of the cyberworkforce shortage in most western countries has long been people. With unemployment at record lows (pre-pandemic) and cyberskilled resources at negative unemployment, it did not seem as if there was anywhere for employers to find an additional 2 million people to fill the cybergaps. The hand wringing over that issue, at last, should be over.

Newly unemployed people from a variety of professional backgrounds have suddenly hit the job market. The unprecedented economic crash has created a unique pipeline of potential talent that is eager to learn new skills and make a difference.

Philip Casesa
Is the director of product development at Focal Point Data Risk, bringing years of insights from roles in cybersecurity, software development and consulting. Prior to Focal Point, he spent 11 years as the director of IT/service operations for (ISC)², leading and growing a team of enterprise architecture, applications, operations, security and web staff. At Focal Point, he is focused on translating his experience into new offerings from Focal Point Academy, a leading provider of hands-on cybersecurity training, working with its elite team of educators to pioneer new models for building world-class enterprise cybersecurity organizations.
market. They are developers from tech startups, auditors, IT staff, writers from newspapers and magazines, strategy experts from Fortune 500 enterprises, educators from colleges and universities, artists, hospitality professionals, and small business owners.

These potential employees bring with them tremendous diversity of thought, experience and capability—but lack the entry-level technical skills to qualify for a cyberjob under normal circumstances. With the right talent-development programs, these are solvable skills gaps.

For those with a passion to learn and grow, and for those who would hire them, now is the time to act.

Forward-looking security leaders will capitalize on this moment to re-load their teams with fresh talent, building around them a workforce development program that can transition new employees into cyberprofessionals and existing cyberprofessionals into the next generation of security leaders.

**What Is Cybertalent?**

If cybertalent is not measured by one’s knowledge of the history of malware or if they have their Certified Information Systems Security Professional (CISSP) certification, how is it defined? While technical skills, knowledge of cybertool sets and certifications are important, key elements of strong cybertalent are a set of critical soft skills and intangible traits (figure 1).

---

**Figure 1—Elements of Cybertalent**

Cybertalent is problem solving. Problem solving is a good skill to have in any job but especially in cybersecurity. Security professionals are constantly presented with new risk areas, threats and vulnerabilities and often with very little accompanying intel or context. They must come up with solutions to these problems without a complete picture of how the issue evolved or the full extent of its impact. The ability to analyze a problem and propose a solution using limited data is an invaluable quality to cybersecurity leaders.

Resilience is a critical facet of problem solving and an essential trait in the world of cybersecurity. Not every problem has a clear solution, and not every solution solves the problem. Mistakes will be made and sometimes the adversary will win. Talented cyberprofessionals learn from their mistakes and get back in the game to solve new issues.

Outside of the security realm, there are many professions that have helped hone this unique problem-solving skill. For example, healthcare professionals are often required to make life-or-death decisions within a matter of minutes, working with very little information. Recent Gallup research found that 13 percent of healthcare workers were laid off amid the pandemic and another 31 percent received reduced hours. In addition, those with military backgrounds have similar experience making critical in-the-moment decisions with limited intel. People with an analytical mindset sharpened in these careers can translate into effective cyberanalysts, capable of parsing data to identify indicators of compromise, draw conclusions and move issues to triage.

Drawing from first-hand experience, hiring professionals who may not look great on paper but exhibit strong problem-solving skills pays off. Anecdotally, an enterprise once hired someone who was installing cable modems for commercial
clients because the hiring manager sensed the cable modem installer was a prolific problem solver who would not rest until a satisfactory job was done. His passion combined with dogged persistence to identify and solve problems enabled his development as a cyberprofessional, and the team was all the better for it.

**Cybertalent Is Creativity**
Creativity goes hand-in-hand with strong problem-solving skills and is equally critical to cybersuccess. For example, when sifting through threat data, security analysts must think differently about how an intruder might gain access or what a new threat might look like. When faced with a new threat or discovered vulnerability, coming up with the right solution with the tools on hand requires out-of-the-box thinking.

Outside of threat analysis, cybersecurity professionals must try to think like hackers to crack malicious malware. Incident response requires an immense amount of creative thinking, requiring security professionals at every level to think differently about how to address and communicate the impact of a breach or incident.

According to the aforementioned Gallup survey, one in four creative workers (e.g., artists, designers, actors, performers, musicians) has been laid off in 2020, and nearly half of them have seen a reduction in pay. With the right training, these professionals can bring unique perspectives to the world of cybersecurity, helping to break down long-standing issues.

**Cybertalent Is People-Centric**
It is not enough for cybersecurity professionals to be skilled at detecting threats, analyzing malware and addressing vulnerabilities. They must have a deep-seated desire to defend their organizations and the individuals who trust it and the ability to design solutions that accommodate both human and technological needs. Care for the well being of others is a key motivator for many of the best cyberprofessionals.

Employees with this skill set build security solutions with people in mind. Sometimes, security professionals can create tools or design processes to address threats that can make work more difficult for end users, be they employees or customers. This can cause users to circumvent these tools or measures in unpredictable ways, putting the organization at risk. Approaching solution design with a people-first mentality is critical for overcoming this pitfall.

Military veterans and reservists who have dedicated their lives to protecting others often embody this quality. Cybersecurity gives them the opportunity to continue this mission in the civilian world. In addition, those coming from consumer technology backgrounds (i.e., application developers, coders, user interface [UI] designers, product managers) are adept at viewing problems from a nonsecurity perspective and can make valuable contributions to security policies and solutions that interface directly with end users. Of course, educators, public service workers and healthcare professionals have also built careers on their passion for serving and protecting others, and experts from these fields can make their own contributions to a human-centered security team.

**Cybertalent Is Strong Communication**
A security program could boast the best tools, the most skilled professionals and streamlined processes, but security outcomes will still be poor without strong communicators to introduce and apply these processes and policies across the organization.

Communication skills are needed in a number of areas within a security program. For example, strong communicators are needed to raise cyberawareness across the organization. They need to be able to put together effective emails warning of new phishing schemes, announcing new

"**CYBERSECURITY TEAMS NEED TWO-WAY COMMUNICATION—UNDERSTANDING THE NEEDS, GOALS AND OPPORTUNITIES OF THE ORGANIZATION AND TRANSLATING THOSE OBJECTIVES INTO SECURITY PRIORITIES.**"
password policies and alerting users to critical software updates. They must be able to build effective trainings that help employees recognize suspicious activity and report it effectively. Security professionals must be able to clearly communicate findings and trends to team leaders. They must have productive conversations with other business leaders on the value and need for cybersecurity and communicate in a way that their superiors understand and is clear enough to elicit the right decision or action necessary to best protect the organization’s assets.

And they must be able to listen. Cybersecurity teams need two-way communication—understanding the needs, goals and opportunities of the organization and translating those objectives into security priorities. The best security organizations are those that reduce friction, working alongside the business to bring products to market faster, protecting the most important data and deploying secure solutions that enable employees to do their jobs. These goals are all worthwhile, and they all start with listening.

Strong communicators make valuable additions to many security teams. Sales professionals were hit hard by the pandemic, with 18 percent losing their jobs and 46 percent seeing a reduction in pay. Many salespeople are adept in communicating to various audiences (e.g., executive, manager, users) and selling these different groups on a single topic or product. Writers, editors, instructional designers, public relations professionals, auditors and marketers also have a great deal to bring to the table in drafting communications and building effective, clear policies. Strong communicators are the bridge between cybersecurity and the business and a key component of an effective security program.

How Gatekeepers and Bad Job Descriptions Keep People From Cybersecurity

One of the biggest obstacles to attracting diverse cybertalent is the humble job description. An inescapable piece of enterprise paperwork, job postings are often:

- Poorly written
- Overly aspirational
- Unnecessarily restrictive
- Not reflective of the actual work to be performed

A poorly written job description will eliminate many strong candidates and discourage many others from even applying.

Human resources (HR) departments, where rigid adherence to process and standardization rules the day, often place arbitrary requirements on positions to reduce candidate pools. It is not their fault, necessarily, but the effect can be damaging particularly to parts of the organization, such as cybersecurity, that fall well outside the expertise of most HR professionals. Many of the top security professionals in the country do not have a formal degree in cybersecurity or computer science, yet HR and recruiting professionals continue to set that as a requirement. Certifications, likewise, artificially skew candidate pools to reward good test takers, at the expense of people who are equally capable of doing the work but may not have had the time, resources or access to common industry certifications. Often hiring managers add certification requirements that are not even possible, so an entry-level analyst position may end up requiring a CISSP, an achievement that comes with five years of paid work experience.

The issue is that organizations have set foundational job requirements that do not fit the cybersecurity world, keeping potential talent out and leaving critical seats empty. Cybersecurity leaders must advocate for a different approach to cyberhiring.
Certifications and Degrees Are Not Always Indicators of Talent

Cybersecurity degrees have steadily grown in popularity in recent years, with many universities and colleges across the globe offering four-year or master's-level programs in this field. Long before security degrees hit the scene, certifications were the key marker of a real-life, I-know-what-I'm-talking-about security professional. For HR and recruitment professionals without a strong cyberbackground, certifications serve as a shortcut to identifying potential hires with at least the baseline skills required for the job. But are these mainstays of the profession true indicators of cybertalent? If cybertalent is marked by soft skills such as problem-solving ability, creativity and communication as much as it is by technical know-how, do certifications and degrees adequately identify them?

The answer is a simple “no.” Degrees and certifications have their place. They can lay a solid foundation for those passionate about pursuing a career in cybersecurity. They can mark the knowledge a professional possesses about certain areas of the field. But they cannot identify a strong communicator, a passionate defender or a future leader. Most do not test expert skills or hands-on experience. For employers seeking book smarts, certifications and degrees are helpful, but for those looking for true talent, these qualifiers will not provide sufficient insight.

Years-of-Experience Requirements Can Exclude Cybertalent

Years of experience is a standard job requirement, typically designating the incoming professional level (e.g., five years for managers, 10 for directors). However, as in many professions, a rigid adherence to years-of-experience benchmarks will remove potential talent from the hiring pipeline. This is especially detrimental in the cybersecurity field. With the pace of change in the cybersecurity industry, a decade of experience does not hold nearly as much weight. Twitter, a wellspring of cybersecurity pet peeves, is filled with complaints from security professionals about job postings requesting more years of experience in a certain tool than the tool’s lifespan (figure 2).

Shifting hiring priorities from years of experience to skills is critical. The tools a professional knows, the problems they have solved in their careers, the way they keep abreast of change and how they expand their knowledge are important indicators of experience. These skills and experiences indicate someone who truly understands the nature of the work and is prepared to take on the work.

Searching for Purple Unicorns Discourages Cybertalent

HR and recruiting teams struggle with creating cybersecurity job descriptions. Cybersecurity teams
struggle with writing cybersecurity job descriptions. One team does not understand the role and the other cannot communicate the nature of what is needed to do this job well. This struggle often ends up being a copy-and-paste exercise, pulling from competitor postings. The result is a Frankenstein description of a professional that could not possibly exist. They must have 5 or more years of experience in Linux, Windows, Amazon Web Services (AWS), security information and event management (SIEM) configuration, Python, pen testing, and incident response, plus be masters at compliance regulations such as the US Sarbanes-Oxley Act of 2002 (SOX) and the Payment Card Industry Data Security Standard (PCI DSS).\(^7\)

Savvy job seekers will often pass these opportunities by, seeing the poor job description as an indicator that the organization does not have clearly defined roles for its cybersecurity team. Lack of defined roles leads candidates to assume that there is no clear career path, responsibilities will be difficult to manage and expectations will be mismanaged.

Writing job descriptions that include a reasonable set of technical skills and clearly define the responsibilities of that role are better than trying to cover every possible tool available. Job descriptions should be focused on the role, reduce unnecessary roadblocks and allow for unconventional applicants who may bring something unique to the role.

Leadership expands the job description, adding responsibilities, knowledge, skills and abilities, but keeping the same title. Then, when the professional in that role feels overwhelmed or gets a better offer and moves on, a gaping hole is left.

Instead, advancing employees into the next role when new skill sets are achieved and they are ready for new responsibilities makes the cybertalent pipeline much easier to manage. Then the seat that must be filled has a reasonable set of responsibilities and skills. In addition, this model sets up clear roles and career paths for the team, an exciting prospect for those already on board and those looking to join the team.

Cyberworkforce Development Solves Long-Term Talent Challenges

Traditional hiring is not working for cybersecurity leaders (or their team members), and cybertalent is not just about skills or years of experience but also innate personal qualities. The issues have been identified, but what does a CISO or a SOC manager do to find the solution to fixing these issues? Different organizations will take different approaches, but a strong option is formalized “cyberworkforce development,” a concept that has grown in popularity, partially in response to the cyberworkforce shortage.

A cyberworkforce development program is one that defines, measures and builds cybertalent over time, helping organizations build stronger teams and design career paths for each member of their security team. It is deliberate and programmatic, requiring strategic thinking and clear leadership buy-in. It takes an investment of time and energy, a shift in thinking and culture, and a fundamental commitment both to the team and the individuals within it. But the rewards are massive.

A formal cyberworkforce development program improves hiring and retention. It takes professionals from varied backgrounds and gives them the tools they need to build the cybercareer they want. It builds a pipeline of cybertalent, helping security leaders minimize their talent shortage, and although it is an up-front investment, it pays dividends over time as

"A FORMAL CYBERWORKFORCE DEVELOPMENT PROGRAM IMPROVES HIRING AND RETENTION."
employees grow stronger, new talent is nurtured, and the organization is better protected from malicious threats and subsequent fines and damages.

What Is Cyberworkforce Development?

Cyberworkforce development looks different for every organization based on their threat landscape, team models and industry, but there are typically seven key components to this approach (figure 3).

These seven steps result in a program that effectively defines, measures and builds strong cybertalent.

Phase One: Define

Phase one is focused on defining both the current and future team. In this phase, security leaders must analyze current roles, identify new roles that are needed and detail the skill sets the team must have.

Identify Roles

Surprisingly, few security leaders know the specific positions they need on their teams to effectively address the risk their organizations face.

Identifying roles starts with outlining the tasks a team must complete to meet the organization’s acceptable risk level. These tasks should then be grouped into high-level job roles, which should cover existing and near-future roles. Performance levels (e.g., threat analyst I, threat analyst II) should then be assigned to these roles. The US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-01 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework lays out a good list of recommended roles.8

Define Skills

Defining skills is a critical part of cyberworkforce development. Having a set list of skills tied to a job role smooths out the hiring process, sets clear expectations for new hires and sets employees on a clear career path. Without defined skills and responsibilities, roles can become overwhelmed with tasks and become impossible to fill or retain.

Once roles are identified, they should be mapped to a set of knowledge, skills and abilities (KSAs), as defined in the NIST NICE framework. KSAs are not just a list of tasks—they are specific skills and areas of expertise a team member must have to fulfill their roles. This may take some time to map out and it will certainly change over time, but it is an important piece of groundwork before building the team.

Phase Two: Measure

Once needs are established, it is necessary to determine what skills are already on the team. Phase two is dedicated to identifying these skills through a series of assessments.

Assess the Team

An unbiased assessment of a cybersecurity team’s KSAs measures the team’s current capabilities and identifies areas for growth. Some leaders will choose to work with an outside firm for this assessment, benchmarking their programs against their peers and industry standards, while others will use in-house resources.

Through this assessment, most teams will find a competency gap, which is a normal part of the development process. These assessments are not intended to make leaders feel like their program has failed a test but that they are taking steps to advance their capabilities.
Assessments should vary based on role. Analysts should be asked different questions than incident responders, who should not be evaluated by the same standards as threat hunters. These assessments will provide a baseline of their skills and knowledge and help leaders build training plans that put them on a path forward.

Phase Three: Build
Phase three can be the most challenging phase of this approach. First, a strategy for building skills across the team is needed; then, trainings and knowledge sharing methods must be selected; and finally, new skills must be tested.

Build a Plan
Once roles are solidified and the team has been assessed, it is time to develop a strategy that addresses current gaps and plans for the future. Looking forward is key to creating a strong training plan. It is not just about mitigating current gaps but also building a team that can scale with the organization and take on future challenges.

Although much of the plan will focus on training, it should also include mentoring, hands-on experiences, soft skills development, thought leadership and other critical areas of professional development. Some teams may even want to consider role rotations where team members can test different roles and spend time learning about another team member’s responsibilities.

The plan should also map how each role will advance, and this mapping should be shared with team members. They should understand what is expected of them and where their path will take them.

Acquire Skills
Many security leaders will think this is the easy part. Training models are already in place, and skills development is happening. But the truth is, most of these programs are extremely ad hoc, trusting employees to pick and choose the trainings they want to attend, which are often very expensive and too often ineffective. When following a workforce development model, trainings must align with the plan developed in phase two to close the skills gap and push team members forward in their careers.

Skills development should happen continuously throughout the year. Many organizations choose to take a “micro-training” approach, supplementing week-long courses with hour-long or half-day sessions throughout the year. No matter what approach is selected, it is critical that selected trainings are 100 percent applicable to the individual’s job role and happen throughout the year. Continuous training results in a “batter up” approach, which means when attrition happens, another resource with a similar skill set is ready to step into the vacant position.

Validate Skills
Workforce development does not end with training. The only way to determine if the training plan is working is to put the team member’s skills to the test. This is not an exercise to determine who has been paying attention or who is not equipped to be on the team. It is meant to strengthen skills learned in training and identify areas for further improvement.

And, while individual validation is important, team validation is also crucial. Periodically testing the team through various exercises such as red team assessments lets leaders see how the team works as a whole and where gaps may still exist.

Phase Four: Repeat
Phase four is critical to the success of a workforce development program. Workforce development is a never-ending process.

Adapt and Revise the Plan
Organizations, technologies and threats all change
rapidly, and cybersecurity teams must be able to adapt to these changes. Regularly revisiting the roles designed for the team, the skills needed and the plan in place will help the security team adapt to these changes and better protect the organization.

Is Cyberworkforce Development Worth the Investment?

Cyberworkforce development requires significant budget, time and people to be successful. It is not just an investment in cybersecurity—it is an investment in people and the future, and the payoff can be immense.

First, cyberworkforce development is designed for people. Few alternates to this approach can boast the same. Traditional hiring is focused more on organizational needs. Ad hoc training is often driven by the technology trends or the latest certification. But cyberworkforce development evaluates current capabilities and uses that information to design a clear path forward, helping team members build the cybercareers they want that also move an organization forward. It reevaluates their needs, it equips them to do their jobs better and it gives them new opportunities.

For those just joining the cybersecurity field (e.g., writers, veterans, salespeople, healthcare workers), workforce development transforms their careers. It gives them the skills they need to exercise core traits such as problem solving and creativity. Cyberworkforce development works for individuals at every point in their cybercareer—whether on the threshold of their journey or farther down the path.

Second, cyberworkforce development is an investment in an organization’s future. It is not a quick patch job on existing issues or a short-term solution to filling a few empty seats. It builds highly flexible cybersecurity teams that are ready to fight future threats, secure future technologies and adapt to future changes. It enables security leaders to build a pipeline of cybersecurity talent, providing a path into the field for newcomers and a leadership path for today’s cyberworkers.

Cyberworkforce Development and IT and Internal Audit

Cybertalent is founded on a set of key personal traits, and cyberworkforce development is the catalyst for building that talent. With these two ideas in mind, internal and IT auditors can play a key role in minimizing the cybertalent shortage. First, the innate qualities and experience of auditors make them ideal candidates for many cybersecurity job roles. With specialized cybertraining, IT and internal auditors can increase their support of cybersecurity programs and better assess and address enterprise risk.

"CYBERWORKFORCE DEVELOPMENT WORKS FOR INDIVIDUALS AT EVERY POINT IN THEIR CYBERCAREER—WHETHER ON THE THRESHOLD OF THEIR JOURNEY OR FARTHER DOWN THE PATH."

Transitioning From Audit to Cybersecurity

There are a number of reasons why auditors are a good fit for a cybersecurity career. Although they may not have a depth of technical knowledge on cybersecurity topics, their unique experience and expertise equip them for future success in cybersecurity.

Auditors are focused on identifying and mitigating risk to their organizations, making them experienced problem solvers, a valuable quality for cybersecurity professionals. Auditors spend much of their time reviewing policies and procedures and interviewing business leaders, searching for ineffective controls, gaps in compliance and opportunities for improvement. But they do not stop once they have identified issues. They also build plans for addressing risk. They work with stakeholders across the organization to design
improved controls and policies that effectively reduce risk. Leveraging these same skill sets, cybersecurity professionals could better coordinate with other teams to implement security measures and policies, reduce cyberspend, and bring a new perspective to risk mitigation.

Auditors must also have an interest and understanding in today’s business technologies, tasked as they are with evaluating the risk posed by an organization’s systems, tools and custom applications. As part of this process, internal and IT auditors come to understand the critical role these technologies play within an organization and the catastrophic impact on an organization should they be compromised or unavailable. While professionals from a variety of backgrounds are a good fit for cybersecurity work, this understanding of technology and its pivotal role within an organization makes an auditor’s transition to cybersecurity much smoother. In addition, auditors who are making the move from audit to cyber within their own organization already have a strong understanding of the systems and tools in place at the organization, streamlining portions of the training process.

In addition to the technology background, many auditors also possess a finely tuned ability to communicate with the business. Auditors must be adept at writing clear reports on findings, communicating the impact of risk and illustrating solutions. They must be able to work with leaders from various functions across the organization and must be able to advocate for the value of risk management to executive leadership. Applying these communication skills to a cybersecurity team could result in better security policy and process integration across the organization, better reporting on cyberrisk, and increased investments in cybersecurity from senior management.

When enrolled in a strong cyberworkforce development program, internal auditors will find the transition to cybersecurity a little easier than those from other backgrounds.

Supporting Cybersecurity Programs

Even without making a career move to cybersecurity, there is a great deal internal and IT auditors can do to help support cybersecurity teams and lessen the burden of the cyberworkforce shortage. This starts with a desire to partner with security teams and to expand cybersecurity knowledge and skills. Internal audit can provide the macro view of the cybersecurity program's effectiveness, guiding leaders on alignment between organizational priorities and security objectives.

Internal audit leaders should also work with cybersecurity management to understand the unique security challenges of the organization and ensure that the audit team is staffed with the skills (or outsourced experts) necessary to properly evaluate cybersecurity and IT controls. Similar to a workforce development program with the cybersecurity team, internal audit should ensure that all auditors receive regular training, guidance and practice on evaluating key data security concepts.

In partnership, cybersecurity and audit teams better evaluate cyberrisk, build stronger risk management solutions and convey the value of cybersecurity to the rest of the organization.

Conclusion

Cybersecurity leaders are at a unique inflection point in the history of the industry. For more than a decade, leaders have battled a growing gap between open jobs and people to fill them and a lack of skilled professionals, but 2020 turned this issue on its head. As an unfortunate side effect of a global pandemic, the labor market is suddenly awash with smart, creative, hard-working talent ready to be groomed into budding cybersecurity analysts.
At the same time, new and innovative cyberworkforce development models have emerged that solve the skills gap challenge—giving security leaders a framework for training new security employees and advancing existing ones.

Increasing sophistication within internal audit and more pervasive training of auditors in cybersecurity concepts has created a powerful ally for the cybersecurity organization. Internal audit is now better equipped than ever to contribute to the overall cybersecurity strategy, helping security leaders take a risk-based approach to identifying security goals and objectives, which in turn guides staffing and training decisions.

The cybersecurity industry has been stuck in a rut of its own making for years, but now is the time to tear down the barriers that created the cyberworkforce shortage and let in the talent. It is time to work together, develop skilled people and bring fresh ideas into the industry. It is time to shift the mindset from a workforce shortage to a development shortage—a problem with an achievable, sustainable solution.

Endnotes
4 Ibid.
5 Ibid.