

Cybersecurity Workforce Playbook

An employer's guide to creating
entry points to cybersecurity careers



Table of Contents

Overview	2
The Urgent Need for Cybersecurity Workers	2
The Drivers of Cybersecurity Talent Shortages	3
Employer Practices That Create Entry Points to Cybersecurity Careers	4
A Skills-Based Cybersecurity Talent Strategy	4
Partnerships Across Sectors to Equip and Recruit Cybersecurity Talent	5
On-Ramps to Cybersecurity Careers for Existing Employees	10
A Call to Action for Employers	11
Mindset Shifts for Success	12
Conclusion	13
Appendix	14
Additional Resources to Support a Skills-Based Cybersecurity Talent Strategy	14
Appreciation	15
Endnotes	16

Overview

Business Roundtable has developed this playbook based on employer input to provide guidance for cybersecurity and human resources professionals who seek to create more entry points to cybersecurity careers. While this guide does not provide an exhaustive overview of all elements of a cybersecurity workforce strategy, it seeks to provide practical information that leaders can use as they build talent pools.

The Urgent Need for Cybersecurity Workers

The nation's cybersecurity talent shortage presents a risk to national security and economic competitiveness. As of December 2023, there were over 570,000 open cybersecurity roles in the United States¹, and it takes, on average, 20% longer for an employer to fill a cybersecurity role than another technology position.²

Cybersecurity talent shortages can have a real impact on business operations. A recent survey of cybersecurity leaders found that 59% of all respondents would be challenged to respond to a cybersecurity incident due to the shortage of skills within their teams.³ By 2025, it is estimated that a lack of talent or human failure will be responsible for over half of significant cybersecurity incidents.⁴

The risk of a significant cybersecurity incident will only grow as attack surfaces continue to expand, industries face increased cyber threats from nation-state actors and technological advances such as quantum computing push the limits of traditional digital security infrastructure. While generative artificial intelligence may help boost productivity of cybersecurity workers, it also poses new risks when harnessed by bad actors. Nearly 75% of cybersecurity professionals view the threat landscape as of 2023 as the most challenging it has been in the past five years.⁵

Increasing risks and workload, along with chronic staffing shortages, are among the drivers of the retention challenges on cybersecurity teams. One industry survey notes that 60% of companies experienced difficulties retaining qualified cybersecurity professionals,⁶ and another notes that nearly half of cybersecurity leaders will change jobs by 2025.⁷

The Drivers of Cybersecurity Talent Shortages

Increased employer demand is one driver of this worker shortage. Cybersecurity is not only a concern for technology companies but for retail, energy, manufacturing, consumer goods, critical infrastructure, healthcare and other industries. Cybersecurity risk management is also a challenge for small and large enterprises and for the public sector. In the last 10 years, the number of cybersecurity job postings has grown three times faster than the overall technology job market.⁸ These cybersecurity jobs include a range of roles, such as cybersecurity analyst, penetration tester, system administrator, information technology (IT) auditor, digital forensics analyst and chief information security officer, among others.

The cybersecurity talent shortage is not merely a demand challenge. Employer practice can create barriers for talent with interest and aptitude, particularly through the types of requirements often embedded in entry-level cybersecurity job postings:

- **Degrees:** Nearly 88% of cybersecurity job postings specify a bachelor's degree or higher. Yet around 80% of hiring managers no longer believe a bachelor's degree prepares students for cyber jobs.¹⁰
- **Certifications:** Nearly 6 in 10 cyber positions request at least 1 industry-recognized certification, versus 2 in 10 information technology jobs overall.¹¹ However, such certifications are not always synonymous with job readiness, particularly for entry-level roles.
- **Practical experience:** Hands on experience is rated more highly than all other factors in evaluating new hires in cybersecurity.¹² In fact, nearly 90% of all cybersecurity job postings require at least three years of experience.¹³

Together, these practices may exclude qualified talent from the profession. The credential requirements present additional barriers for professionals who are less likely to hold a four-year college degree but may have aptitude and interest in the field.¹⁴ Cybersecurity, like other science, technology, engineering and mathematics (STEM) fields, does not mirror the overall gender, racial and ethnic diversity of the U.S. workforce. For example, around 25% of U.S. cybersecurity employees are female,¹⁵ 9% are Black and 4% are Hispanic or Latino.¹⁶

Bringing more individuals into the cybersecurity talent pipeline will not only solve immediate employer talent needs but also create opportunities for more individuals to access well-paying, in-demand jobs today and in the future.

Employer Practices that Create Entry Points to Cybersecurity Careers

The concept of an entry-level job is often associated with an early career professional or a recent graduate. However, employers increasingly recognize that individuals may enter a cybersecurity career at any stage of professional life, with a range of educational and work

Employers increasingly recognize that individuals may enter a cybersecurity career at any stage of professional life, with a range of educational and work experiences.

experiences. This section is designed to help employers create more clear entry points to cybersecurity for a range of individuals, including those who are in high school, studying at community college, pursuing a four-year degree, transitioning from

U.S. military service or seeking a new role as a mid-career professional. Also, many of the practices in this section help support retention of existing cybersecurity professionals by providing opportunity for career growth and internal mobility.

A Skills-Based Cybersecurity Talent Strategy

Before identifying new recruitment channels or training providers, employers can lay the groundwork for an effective cybersecurity talent strategy through the following activities:

Evaluate credentials and certification requirements across positions.

- **Revise positions** to remove degree requirements that are not linked to core knowledge and skills. One study estimates that removing bachelor's degree requirements in early career cybersecurity job postings can increase the candidate pool by over 60%.¹⁷
- **Revise positions** to remove certification requirements that are not tied to core job needs or are inappropriate for entry level. Industry-recognized certifications (both vendor-neutral and vendor-specific) can demonstrate mastery of a body of knowledge. However, over-indexing on certifications can prevent qualified talent from entering the workforce. For example, a CISSP certification requires five years of experience and a rigorous exam and thus is not an appropriate requirement for an entry-level role. Both credentials and certifications do not necessarily indicate that an individual possesses the problem solving, critical thinking and teamwork skills that are just as valued by cybersecurity leaders.¹⁸

Develop a skills taxonomy and clear career pathways for cybersecurity professionals

- **Build** a skills taxonomy for cybersecurity talent across all roles in an organization, in partnership with cybersecurity leaders. Per LinkedIn, “[s]kills taxonomies ... provide an exhaustive listing of the skill sets relevant to an organization. Skills taxonomies offer a skills-based approach to identifying, acquiring, and managing the core competencies that make your business successful.”¹⁹ Developing a taxonomy allows employers to hire new staff and create development and mobility pathways for existing cybersecurity employees.
- **Leverage** the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity as a basis for a skills taxonomy. The NICE Framework establishes a common language that describes cybersecurity opportunities based on tasks, knowledge and skills and maps them to updatable work roles.²⁰ Increasingly, education institutions are adopting the NICE Framework to help prepare students for cybersecurity roles. Using the common lexicon allows students, jobseekers and incumbent employees to more clearly understand the range of cybersecurity roles and the knowledge and skills they need to obtain those roles. Some certification providers, such as Global Information Assurance Certification (GIAC), have mapped the NICE Framework to industry-recognized courses and certifications, which helps human resources leaders and learners use coursework to address skills gaps.²¹
- **Develop** career pathways that clearly articulate opportunities for new and existing cybersecurity professionals to develop, building on the skills taxonomy. This includes development across cybersecurity sub-disciplines such as engineering, network security, governance, architecture, operations, threat intelligence, etc. Such pathways should also include opportunities to move through individual contributor and management roles, and be clearly linked to the knowledge, skills, certifications and experiences needed to advance.

Partnerships Across Sectors to Equip and Recruit Cybersecurity Talent

Employers need partners to build robust cybersecurity talent pools with industry-relevant skillsets. Partners can support the entire talent lifecycle from sourcing through development and can help employers bring new populations into cybersecurity careers.

Partnerships with education institutions that serve a range of learners.

Partner Institutions:

- Community Colleges
- Four-year Colleges
- Community-based Training
- Career Technical Education (CTE)

Employers should consider creating partnerships with a range of education institutions that cultivate and provide access to new and diverse talent pools, including community colleges, community-based training providers and minority-serving institutions such as Historically Black Colleges and Universities and Hispanic Serving Institutions. Employers should clearly signal to

all education partners what skills are required for current and future cybersecurity roles.

- **Community colleges:** Community colleges provide flexible, work-oriented certificate and associate degree programs in IT and cybersecurity fields. Students of all ages who are seeking to change careers may bring prior relevant experience to their studies at a community college. The National Security Agency designates some community colleges, colleges and universities as a National Center of Academic Excellence in Cybersecurity Education (NCAE-C), indicating a program meets various standards for curriculum, outreach and professional development.²²

Employer action: *Co-create industry-specific coursework that can accompany the standard credential program to equip students with industry-relevant knowledge as they enter the workforce.*

- **Four-year colleges:** While employers have historically looked to computer science or similar degree programs, they are increasingly recognizing that a range of majors can build the creative problem solving and critical thinking that lay the groundwork for success in a cybersecurity role.

Employer action: *Identify for colleges the certificates and/or certifications that students in all majors can pursue alongside their degrees to build technical skills.*

- **Community-based training provider:** Training providers offer short-term courses in IT and cybersecurity that often result in industry-recognized certifications. Some nonprofit providers such as Per Scholas,²³ NPower and Year Up work exclusively with underserved populations and offer their students low- or no-cost training in addition to career

coaching and other wraparound support.^{24, 25}

Employer action: *Provide structured mentorship and coaching for new hires sourced from training providers to support their inclusion and success.*

- **Career technical education (CTE) programs:** Career technical education (CTE) programs: CTE programs provide students with a range of technical and professional skills, experiential learning opportunities, and certifications that prepare them for work. CTE for cybersecurity is offered in different institutions and formats to learners of all ages, including courses of study offered to students in K-12 settings, specialized career academies, adult education programs and dual enrollment programs, among others.²⁶ CTE programs are often overlooked as sourcing partners but may provide employers access to diverse talent

Employer action: *Provide job shadowing, career talks and mentorship opportunities for students in CTE programs to raise awareness of cybersecurity careers.*

Partnerships that provide experiential and work-based learning opportunities.

By investing in experiential and work-based learning opportunities like those identified below, employers can increase student readiness for work, build their own employment brand and identify potential talent.

Learners in all settings mentioned in the above section can benefit from opportunities to gain hands-on, project-based experience in cybersecurity. Employers often note that students leaving cybersecurity education programs, including four-year degree programs, lack some of the key skills required for entry-level roles.²⁷ Experiential

learning opportunities help learners of all ages develop key professional skills such as communication, problem solving, critical thinking and teamwork. By investing in experiential and work-based learning opportunities like those identified below, employers can increase student readiness for work, build their own employment brand and identify potential talent.

- **Cyber ranges** are “interactive, simulated representations of an organization’s local network, system, tools and applications that are connected to a simulated internet level

environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing.”²⁸

Employer action: *Invest in a community-based cyber range that can be used by both students and employees.*

- **Cybersecurity skills competitions** are “interactive, scenario-based exercises” where “individuals or teams engage in cybersecurity activities” such as capture the flag, cyber defense or forensics.²⁹ Competitions mimic real-world situations faced by cybersecurity professionals, such as the configuration of modern solutions and products, and can be conducted on a cyber range. Cybersecurity competitions can be especially effective at reaching students of different learning styles when paired with classroom instruction. Competitions provide an opportunity for talent who may otherwise be overlooked (both students and employees) to demonstrate interest and aptitude.

Employer action: *Provide industry-led and age-specific cybersecurity challenges to enhance student learning experiences and offer cybersecurity employees the chance to participate as competitors, coaches or judges.*

- **Internship or co-op programs** are a proven method of providing students with short-term, paid work opportunities that expose them to technical fundamentals of cybersecurity while building business acumen and professional skills.

Employer action: *Expand internship sourcing to a broader range of education institutions, including community colleges, minority serving institutions and community-based training providers.*

- **Apprenticeships** combine work and learning through structured programs whereby individuals receive paid work experience, classroom instruction and a nationally recognized credential.³⁰ Historically, apprenticeships were considered suitable only for manual labor occupations, but increasingly employers are turning to apprentices for a range of IT and cybersecurity roles. Apprenticeships can be implemented for both entry-level and advanced roles and can provide on-ramps for experienced professionals pursuing a career change into security.

Employer action: *Seek out intermediary organizations to more quickly launch or scale an apprenticeship program in cybersecurity.*

Partnerships that leverage the experience of U.S. military veterans and spouses.

Many U.S. military occupations require technical skills that can translate to civilian roles, and service members often resonate with the mission orientation of cybersecurity work.

While many U.S. military veterans are already working in cybersecurity and other STEM fields, this population is ripe for further development. Many U.S. military occupations require technical skills that can translate to civilian roles, and service members often resonate with the mission orientation of

cybersecurity work. U.S. military veterans often possess security clearances or are able to obtain clearances as needed.

- **Veteran-serving workforce development organizations** provide employers access to talent with a range of skill sets, and several specialize in training veteran talent for cybersecurity and related fields such as NPower, VetsinTech and Onward to Opportunity.^{32, 33}

Employer action: Invest in nonprofit veteran cybersecurity training programs and leverage veteran employee resource groups to support new hires in acclimating to the civilian workplace.

-
- **The U.S. Department of Defense SkillBridge program** is an opportunity for employers to host transitioning service members for short-term work experiences such as internships or apprenticeships at no cost to the employer.

Employer action: Participate in the [SkillBridge](#) program with a focus on placing service members in cybersecurity or related roles.³⁴

-
- **Spouses of active-duty U.S. military** service members are a diverse, skilled group of mission-oriented talent who face barriers to employment due to the structure of military life such as frequent moves and family care responsibilities. In a recent survey, 25 percent of military spouses reported interest in technical roles such as cybersecurity.³⁵

Employer action: Create remote cybersecurity roles and consider participating in the U.S. Department of Defense Military Spouse Employment Partnership or Military Spouse Career Accelerator Pilot.^{36,37}

On-Ramps to Cybersecurity Careers for Existing Employees

Employers who offer clear career development pathways and learning opportunities for existing employees are less likely to report staffing shortages in cybersecurity than those who do not.

While many employers focus on recruiting new talent into cybersecurity roles, they are increasingly realizing the value of tapping into their existing workforce. Employers who offer clear career development pathways and learning opportunities for existing employees are less likely to report

staffing shortages in cybersecurity than those who do not. They are also more likely to realize increased retention of cybersecurity staff.³⁸

Leverage technology and other adjacent roles as a gateway to cybersecurity.

Technology positions are a clear entry point to cybersecurity careers. These roles may include software development, network administrator and IT help desk, among other roles.³⁹ These roles allow individuals to build technical foundations and learn the business. While also in demand, these roles are often easier to fill than pure cybersecurity roles.

- **Use a skills taxonomy** (as defined on page four of this document) to define the knowledge and skills needed to transition from IT to security positions and communicate that pathway to employees.
- **Provide time and training resources** for IT staff to pursue the knowledge or credentials needed to transition to a security-focused role.
- **Structure mentorships or job shadowing** for IT staff interested in exploring cybersecurity opportunities.
- **Intentionally provide opportunities for IT staff to demonstrate their skills** through cybersecurity competitions, assessments, gig assignments and job rotations. solving, critical thinking and teamwork skills that are just as valued by cybersecurity leaders.

Use learning and development activities to upskill and retain cybersecurity professionals.

Traditional learning and development programs are critical for cybersecurity as technology and threat landscapes change rapidly. In addition to supporting the advancement and

retention of existing cybersecurity employees, these programs can build relevant skills for those interested in exploring a transition to security roles.

- **Build internal learning platforms** that allow an employee to gain skills at their own pace and demonstrate competency for new roles.
 - **Create internal gig assignments** that allow individuals to apply knowledge and demonstrate skills while gaining experience that may help them move into security.
 - **Provide educational benefits** such as tuition reimbursement to employees pursuing cybersecurity certifications and college degrees that help them advance their careers.
-

Expose a wide range of employees across the enterprise to cybersecurity jobs.

Many employees are unaware of the breadth of roles in the cybersecurity field and may not see the connection to their current skill set. Employers can help bridge this awareness gap and then offer development activities to transition more employees into cybersecurity roles.

- **Identify and communicate how skills translate to cybersecurity roles** so that individuals working in operations, data analytics, risk management or other functions can see the potential to move into security.
 - **Develop early career rotation programs** for both technical and non-technical staff that include exposure to cybersecurity roles and teams.
 - **Use enterprise-wide cybersecurity awareness programs** to spark interest in and assess aptitude for cybersecurity among a range of employees.
 - **Create communities of practice for cybersecurity** that enable employees from any discipline to network, learn about the field and find mentors.
-

A Call to Action for Employers

Tackling the cybersecurity workforce shortage requires changes in practice as well as in organizational culture and leadership mindset. CEOs recognize the importance of cybersecurity and risk management to their business and can demonstrate further commitment by equipping their senior cybersecurity leaders with resources to build

talent in new ways. Senior cybersecurity leaders can, in turn, demonstrate a long-term commitment to talent development by adopting and sharing the following mindsets with their teams.

Mindset Shifts for Success

Adopt a skills-based orientation to the talent lifecycle. Increasingly, U.S. companies are shifting their hiring and talent management practices to emphasize the value of skills rather than degrees or years of experience alone. This approach is embodied in the Business Roundtable Multiple Pathways Initiative,⁴⁰ wherein companies are implementing new recruitment and assessment strategies to better recognize and evaluate the skills of all job seekers. In addition, employers are identifying upward career paths that employees can navigate by acquiring new and/or different skills along their career journey. Organizations that take a skills-based approach to hiring entry-level cybersecurity workers can expand their skilled candidate pool by over 60%.⁴¹ While cybersecurity employers are utilizing this skills-based approach to talent management today, there is room to grow.

Reset expectations for “entry-level” talent. The perception in cybersecurity is that talent must possess all the skills and knowledge needed to be effective on day one. Yet, this is often not the expectation for other entry-level jobs. Employers can hire for aptitude, interest and willingness to learn and then train new talent in-house to develop their technical skills. Some managers feel that cybersecurity is too important to leave to new entrants, yet these fears are unfounded. Within six to nine months, most cybersecurity professionals in entry-level roles are ready to work independently.⁴² All new employees in cybersecurity roles can benefit from structured mentorship and coaching to accelerate learning and inclusion.

Commit to a portfolio of cybersecurity talent strategies over a longer time horizon.

There is no single solution to the cybersecurity workforce challenge. Employers who have successfully addressed this issue have committed to multiple strategies over several years. It takes time to build new internal processes to recruit, develop and support new hires to be successful. Today, there is significant demand for cyber talent at all levels, and that demand will only continue to grow. In 2023, about 75% of cybersecurity professionals viewed the threat landscape as the most challenging it has been in the past five years.⁴³ Cybersecurity leaders must recognize the need to build a broader entry-level talent pool today to ensure a seasoned, sustainable talent pipeline to deal with the threats of tomorrow.

Conclusion

Employers are adopting the practices and mindsets for successfully developing cybersecurity talent outlined in this paper. For example, almost half of employees under 30 who are entering the cybersecurity profession have a non-technology background.⁴⁴ Employers are increasingly treating certifications as a means of building skills versus a requirement for entry. A recent survey of cybersecurity professionals shows that individuals are less likely to think that an undergraduate degree is the most important qualification for a cyber professional.⁴⁵ However, more opportunity lies ahead for employers seeking to fill critical cybersecurity roles. As technology evolves, so does the threat landscape, and the demand for security professionals will grow with it. Now is the time to build multiple pathways into the cybersecurity workforce and not rely on a single pipeline.

Appendix

Additional Resources to Support a Skills-Based Cybersecurity Talent Strategy

Title & Hyperlink	<i>An Employer's Guide to Writing Effective Cybersecurity Job Descriptions: A Tool for Hiring Managers and Human Resource (HR) Professionals</i>
Author	The Modernize Talent Management (MTM) working group, led by NICE under the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce
Description	Guide to developing an effective job description that aligns role requirements to candidate competencies that includes planning, drafting, revising and creating an assessment rubric for candidates.
Title & Hyperlink	<i>Cyber Resource Kit for Human Resources (HR)</i>
Author	Society for Human Resource Management (SHRM) in partnership with the SANS Institute
Description	Comprehensive toolkit written for HR professionals to hire and retain cybersecurity talent with topics including Understanding Cyber Recruiting 101, Assessing Cyber Talent, How to Build a Cybersecurity Team and Using the NICE Framework for Workforce Planning.
Title & Hyperlink	<i>Skills-Based Hiring Toolkit: Cybersecurity Analyst</i>
Author	Rework America Alliance and JFF
Description	Toolkit to support hiring cybersecurity analysts with customizable resources, including skills-based job posting guidance, a resume screening guide, interview questions and an evaluation rubric, and an onboarding plan, among other resources.
Title & Hyperlink	<i>Tech Job Posting Optimizer Tool</i>
Author	CompTIA
Description	Web-based tool to help employers write cybersecurity job postings with a skills-first mindset, including technical and "soft skills" while avoiding unnecessary credentials.
Title & Hyperlink	<i>NICE Framework Resource Center</i>
Author	NICE under the NIST at the U.S. Department of Commerce
Description	A suite of resources to implement the NICE cybersecurity workforce framework as part of a cybersecurity talent strategy, including example use cases for employers, implementation guides, articles and training material, among other tools.
Title & Hyperlink	<i>Bridging the Gap Between Talent and Opportunity: An Apprenticeship Playbook for Professional Jobs</i>
Author	Chicago Apprenticeship Network
Description	A guide to establishing apprenticeships in cybersecurity and other professional fields, including planning and execution steps, case studies and best practices.

Appreciation

Business Roundtable created this playbook in collaboration with staff from its members' companies, including senior leaders in cybersecurity and human resources.

- Abbott
- Accenture
- Amazon
- American Tower Corporation
- AT&T
- Booz Allen Hamilton
- Cisco
- Dell Technologies
- General Motors
- Guardian Life Insurance Company
- Hewlett Packard Enterprise
- Leidos
- Merck & Co., Inc.
- Palo Alto Networks
- PayPal
- World Wide Technology

Several field leaders have also provided valuable insight, including:

Michael Barnes, Director of Technology Workforce Solutions, CompTIA

Marian Merritt, Deputy Director, NICE at the NIST, U.S. Department of Commerce

Rodney Petersen, Director, NICE at the NIST, U.S. Department of Commerce

Brian Correia, Director of Business Development, GIAC, SANS Institute

Endnotes

1. Cyberseek. Hack The Gap. (n.d.). Retrieved from <https://www.cyberseek.org/index.html>
2. Markow, W., Bittle, S., & Liu, P.-C. (2019, June). *Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring*. Retrieved from Burning Glass Technologies website: https://paper.bobyli.com/Security/Annual_Report/2019/recruiting_watchers_cybersecurity_hiring.pdf
3. Pipikaite, A., Bueermann, G., Joshi, A., Jurgens, J., Bissell, K., Aguirre, C., Browder, T., & Pruitt, J. (2022, January). *Global Cybersecurity Outlook 2022*. Retrieved from World Economic Forum & Accenture website: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
4. Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025. (2023, February 22). Retrieved from Gartner website: <https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025>
5. ISC2. (2023). *Cybersecurity Workforce Study, 2023: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. Retrieved from https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
6. ISACA & LookingGlass. (2022, March 23). *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations*. Retrieved from <https://www.isaca.org/state-of-cybersecurity-2022>
7. (2023, February 22). Gartner.
8. Markow, W., Bittle, S., & Liu, P.-C. (2019, June).
9. Markow, W., Bittle, S., & Liu, P.-C. (2019, June).
10. Crumpler, W., & Lewis, J. A. (2019, January 29). *The Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS). Retrieved from <https://www.csis.org/analysis/cybersecurity-workforce-gap>
11. Markow, W., Bittle, S., & Liu, P.-C. (2019, June).
12. ISACA & LookingGlass. (2022, March 23).
13. Markow, W., Bittle, S., & Liu, P.-C. (2019, June).
14. National Center for Education Statistics (NCES). NCES Fast Facts Tool. (n.d.). Retrieved from <https://nces.ed.gov/FastFacts/display.asp?id=72>
15. (ISC)2. (2018). *Women in Cybersecurity: Young, Educated and Ready to Take Charge*. Retrieved from <https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Women-in-Cybersecurity-Report.pdf>
16. Reed, J., & Acosta-Rubio, J. (2018). *Innovation Through Inclusion: The Multicultural Cybersecurity Workforce*. Frost & Sullivan. Retrieved from <https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/Innovation-Through-Inclusion-Report.pdf>
17. *Growing the National Cybersecurity Talent Pipeline: U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection*. 118th Cong. 14 (2023, June 22). (Testimony of Will Markow). Retrieved from <https://www.congress.gov/event/118th-congress/house-event/115910?s=1&r=7>
18. ISACA & LookingGlass. (2022, March 23).
19. Santa Maria, A. (2023, May 29). What is a Skills Taxonomy and Why Do You Need It? [Blog post]. <https://www.linkedin.com/business/talent/blog/learning-and-development/what-is-a-skills-taxonomy-and-why-do-you-need-it>
20. Petersen, R., Santos, D., Smith, M., Wetzell, K., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181, Rev.1. pp-pp. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-181r1>
21. GIAC Certifications. *NICE Framework*. (n.d.). Retrieved from <https://www.giac.org/workforce-development/government/niceframework/?msc=main-nav>
22. National Security Agency & Central Security Service. *National Centers of Academic Excellence in Cybersecurity*. (n.d.). Retrieved from <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/>
23. Home Page. (n.d.) Retrieved from <https://perscholas.org/>
24. Home Page. (n.d.) Retrieved from <https://www.npower.org/>
25. Home Page. (n.d.) Retrieved from <https://www.yearup.org/>
26. National Initiative for Cybersecurity Education & National Institute of Standards and Technology at the U.S. Department of Commerce. (2023, August 22). *Cybersecurity Career and Technical Education Programs*. Retrieved from https://www.nist.gov/system/files/documents/2023/08/22/nice_cte_6.27.18.pdf

Endnotes

27. Crumpler, W., & Lewis, J. A. (2019, January 29).
28. National Initiative for Cybersecurity Education & National Institute of Standards and Technology at the U.S. Department of Commerce. (2018, February 13). *Cyber Ranges*. Retrieved from https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf
29. National Initiative for Cybersecurity Education & National Institute of Standards and Technology at the U.S. Department of Commerce. (2023, August 21). *Cybersecurity Competitions*. Retrieved from https://www.nist.gov/system/files/documents/2023/08/21/cybersecurity_competitions.pdf
30. Cybersecurity. (n.d.) Retrieved from <https://www.apprenticeship.gov/apprenticeship-industries/cybersecurity>
31. Home Page. (n.d.) Retrieved from <https://www.npower.org/>
32. Home Page. (n.d.) Retrieved from <https://vetsintech.co/>
33. Onward to Opportunity. (n.d.) Retrieved from <https://ivmf.syracuse.edu/programs/career-training/about-o2o/>
34. Home Page. (n.d.) Retrieved from <https://skillbridge.osd.mil/>
35. O’Kane, L., Hanno, E., & Simon, J. (2020). *Military Spouse Career Journeys: Examining Entrepreneurship, Remote Work, and Upskilling as Drivers of Economic Success for Military Spouses*. Retrieved from the Hiring Our Heroes at the U.S. Chamber of Commerce Foundation website: <https://www.hiringourheroes.org/resources/military-spouse-career-journeys/>
36. Home Page. (n.d.) Retrieved from <https://msejobs.militaryonesource.mil/msep/>
37. Home Page. (n.d.) Retrieved from <https://myseco.militaryonesource.mil/portal/article/military-spouse-career-accelerator-pilot>
38. (ISC)2. (2022). *Cybersecurity Workforce Study, 2022: A Critical Need for Cybersecurity Professionals Persists Amidst a Year of Culture and Workplace Evolution*. Retrieved from <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196>
39. CyberSeek. Career Pathway. (n.d.). <https://www.cyberseek.org/pathway.html>
40. Business Roundtable. (n.d.) Retrieved from <https://www.businessroundtable.org/workforceskills>
41. *Growing the National Cybersecurity Talent Pipeline: U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection*. 118th Cong. 14 (2023, June 22).
42. ISC2. (2022). *Cybersecurity Hiring Managers Guide: Best Practices for Hiring and Developing Entry- and Junior-Level Cybersecurity Practitioners*. Retrieved from <https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Hiring-Managers-Guide.pdf>
43. ISC2. (2023). *Cybersecurity Workforce Study, 2023: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. Retrieved from https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
44. ISC2. (2022). *Cybersecurity Workforce Study, 2022: A Critical Need for Cybersecurity Professionals Persists Amidst a Year of Culture and Workplace Evolution*.
45. ISC2. (2022). *Cybersecurity Workforce Study, 2022: A Critical Need for Cybersecurity Professionals Persists Amidst a Year of Culture and Workplace Evolution*.