International Journal of Scientific and Management Research
Volume 8 Issue 8 (August) 2025
ISSN: 2581-6888
Page: 30-36

Building A Resilient Us Cybersecurity Workforce Through Practical Training

Loveth Odozor, Seth Nti Berko, Augustine Udoka Obu & Kofoworola Idowu
[1]Katz School of Science and Health, Yeshiva University, New York.
[2]Information Security Analyst,SSBiz Solutions, Geogia.
[3]Information Technology (Cyber-security) Strayer University.
[4]Katz School of Science and Health, Yeshiva University, New York.

DOI - http://doi.org/10.37502/IJSMR.2025.8804

Abstract

Cyberattacks aren't just getting more common; they're getting smarter, faster, and harder to detect. This, and many other reasons, is why the United States needs a cybersecurity workforce that's not only large enough but also skilled enough to take on these evolving threats. The problem? The gap between the skills we need and the skills we have keeps getting wider. And too often, cybersecurity training stops at theory, leaving professionals without the real-world experience they need when the pressure is on. Cybersecurity is a cornerstone with regard to the safety of a person, organization, and even a country; hence, the need for skilled persons in this field can never be overemphasized. This article explores why hands-on, scenario-based training is essential for building a truly resilient cyber workforce. We'll look at the problems with the current cyber skillset, the challenges holding us back, suggest programs that are getting it right, and share ideas for how to bridge the gap. The message is clear: book learning isn't enough; we need to be more practical in teaching Cybersecurity, that way, we can build a resilient workforce.

Drawing on examples from government initiatives, private-sector partnerships, and forward-thinking academic programs, we'll show how apprenticeships, simulations, and continuous upskilling can turn theory into action. If we want to stay ahead of the threats, we need to train like the attacks are already here because, in many cases, they are.

Introduction

Protection of sensitive data, information systems, and networks, critical infrastructures, intellectual property, top government secrets, etc., ensuring their availability and restricting unauthorized access, are core elements of cybersecurity. However, Cybersecurity isn't just about protecting computers; it's about safeguarding a nation's security, economy, and the privacy of its people. But as cyber threats evolve faster than ever, from ransomware attacks on critical infrastructure to sophisticated nation-state spying, the need for skilled defenders has reached a critical point, and right now, the U.S. is facing a severe talent shortage. Globally, there are an estimated 3.5 million unfilled cybersecurity jobs (ISC², 2023), and the gap isn’t closing anytime soon. One big reason? Many traditional education programs still depend heavily on theory-based learning while falling short on the kind of hands-on experience that truly prepares professionals for the battlefield of modern cyber defense.

If we want a workforce ready to take on real threats, we have to change how we train. That means prioritizing practical and immersive learning through simulations, cyber ranges, and apprenticeships, which puts people directly in the kinds of situations they’ll face on the job. That way, the gap will be bridged.

In this article, we’ll look at the current state of the cybersecurity workforce and skills gap. We explore where conventional education is lagging, highlight real-world success stories from government, academia, or even industry, and make great recommendations for building a sustainable pipeline of cyber talent. The goal is simple: learning by doing, so we can build a workforce capable of meeting the challenges of an increasingly dangerous digital world.

The Cybersecurity Skills Gap: A Growing Crisis

Organizations are pouring millions into cybersecurity tools, buying the latest SIEM platforms, EDR tools, deploying intrusion detection and prevention systems, rolling out next-gen firewalls, file integrity monitoring, and every antivirus under the sun. On paper, it looks like a fortress. But here’s the catch: even the best tools are only as good as the people behind them. The question is this: “How skilled are those who are behind the screens, monitoring these tools”? And right now, there simply aren’t enough skilled hands to turn all that technology into real protection. According to the ISC² Cybersecurity Workforce Study (2023), 41% of organizations say they can’t find enough qualified professionals to get the job done.

Why? The skills gap isn’t just about not having “enough people”; it’s about not having people with the right skills. From mastering complex detection tools to understanding evolving threat tactics, techniques, and Procedures (TTPs), today’s cybersecurity professionals need a mix of technical skillset, critical thinking, and hands-on experience. And as it is, that mix is in short supply. And here’s where it gets even more concerning: cybercriminals aren’t waiting for us to catch up. They’re innovating faster than we’re training. Every unfilled position becomes an open window for attackers, whether it’s a phishing email that slips through, a vulnerability left unpatched, or an incident that takes hours longer to contain than it should. Without closing this gap, we risk building castles with no one to guard the gates.

Rapidly Evolving Threat Landscape

With the increased evolution of Artificial Intelligence capabilities, attackers are getting smarter, evolving, and moving faster at a pace that it’s difficult to keep up. Threats are getting more difficult to spot. Attackers are now using AI, automation, and zero-day exploits to slip past even the most sophisticated defenses. The rules of the game change daily, and cybersecurity professionals are under constant pressure to master new tools, threats, and techniques just to keep up. The problem? Many academic programs simply can’t move at the same speed. By the time a new curriculum is approved, the threat landscape has shifted greatly. That means too many graduates step into the workforce unprepared for the messy, unpredictable nature of real-world cyber defense.

The Key Challenges and Problems:

- **AI-Powered Attacks**: Hackers are using generative AI to create phishing emails that could fool even seasoned professionals, mimic voices for vishing attacks, create AI-powered videos that look as convincing as possible, and push out automated malware at scale.
- **Supply Chain Attacks:** Breaches like the SolarWinds incident demonstrate how infiltrating a single vendor can compromise thousands of networks, including high-profile organizations and government agencies. This highlights that it is not enough to be secure as an individual entity; third-party risk will always be a factor.
- **Ransomware-as-a-Service:** This is a dangerous business model that allows affiliates to buy ransomware tools and techniques without needing to have the skills to carry out an attack. You no longer have to be a skilled hacker; underground marketplaces now enable anyone to deploy powerful ransomware kits like LockBit or REvil.
- **Overreliance on theory-based learning:** Many universities and other learning centers still lean heavily on theory as a means of learning; they focus on cryptography basics, foundations of cybersecurity, previous cyberwars and crimes, etc. While all these are important for strong cybersecurity knowledge, it is also important to inculcate practical learning in these areas and ensure that important aspects of cybersecurity, such as cloud security, AI-driven threats, practical skills in threat detection, advanced incident response techniques, and penetration testing, are not left out (DHS, 2023).
- Nearly half of cybersecurity professionals (47%, ISC^2 2023) say their formal education didn’t prepare them for actual on-the-job threats. This exposes the lapses in the academic system, requiring urgent remediation.
- **Lack of Adequate Diversity in the Workforce**: Based on recent research (updated on January 29, 2025) from the U.S. Bureau of Labor Statistics (BLS), women and Minorities continue to be underrepresented in the cybersecurity workforce, which limits the talent pool. While this percentage has increased over the years, it can be improved further by encouraging diverse massive participation in cybersecurity through accessible, skills-based training, mentorship programs, and associations. This will ensure that the gap can be closed.
- Some very popular and most required certifications in the industry often test static knowledge instead of training people to adapt in real time.

If the cyber battlefield is evolving by the hour, then our training methods can’t afford to be stuck in last year’s playbook.

The Need for Practical Training

The challenges we’ve discussed so far make one thing crystal clear: cybersecurity training shouldn’t just be carried out with textbooks and PowerPoint slides. We must build a workforce that’s ready for today’s fast-changing threat landscape. We need to train people to be ready to defend critical systems and networks. It is paramount to employ hands-on training. Here’s what that looks like in action:

1. **Cyber Ranges and Simulation Labs**: The use of AI-powered cyber ranges and simulation labs in training the workforce is vital. This involves the use of a virtual battlefield where you can defend against live cyberattacks, without the risk of taking down a real network. It can be compared to testing out a product in a test environment, and not the actual life environment; however, it is the real product being tested. That’s what cyber ranges offer. The Department of Defense uses its Persistent Cyber Training Environment (PCTE) to prepare teams for high-pressure scenarios. Universities like Northeastern and Maryland are also integrating these labs into their programs, so students graduate with more than just theory; they graduate with real-life practical experiences, making them more qualified.
2. **Apprenticeships and On-the-Job Training**: Programs that offer on-the-job training are another resourceful way of equipping the task force. Sometimes the best classroom is a real job. These programs show how apprenticeships can open doors, especially for those without traditional degrees. Technology giants like IBM and Microsoft are proving the model works, offering paid training, certifications, and hands-on experience to help people transition into cybersecurity roles.
3. **Continuous, Adaptive Learning**: Cybersecurity moves too fast for “set it and forget it” training. Short, focused micro-certifications on emerging threats like MITRE ATT&CK tactics or AI security keep skills sharp. Platforms like Cybrary and RangeForce take it further with just-in-time, interactive labs that simulate attacks as they happen. This reinforces what one has learnt and helps keep one updated.
4. **Capture the Flag (CTF) and Bug Bounties:** One of the best ways to learn security is by playing offense and defense. Capture The Flag (CTF) competitions, such as DEF CON and SANS events, force participants to think like attackers while sharpening problem-solving skills. Bug bounty programs like HackerOne and Bugcrowd let you hunt for real vulnerabilities in real systems and get paid for it. This is another way to encourage learning and hard work.
5. Community and Mentorship programs: Cybersecurity can be very complex field, but one does not have to navigate it alone. Groups like BlackGirlsHack, Cyversity, and Women in Cybersecurity (WiCyS) offer mentorship, networking, and hands-on labs that help break down barriers. A good mentor can guide career moves, boost confidence, and help new talent see the bigger picture.

Case Studies: Successful Workforce Development Programs

National Initiative for Cybersecurity Education (NICE): NICE, led by the National Institute of Standards and Technology (NIST), promotes workforce development through frameworks aligning education with industry needs (NIST, 2023).

Cybersecurity Apprenticeship Program by the Department of Labor (DOL): The US Department of Labor promotes and funds cybersecurity apprenticeships, helping individuals transition into the field without traditional degrees (DOL, 2023). The program help people earn while they learn, and it is industry-driven and recognized globally. Generally, the program has significantly increased the number of skilled cybersecurity professionals over the years. This has been achieved through grants, funding, partnerships and campaigns.

Why is a more practical training approach non-negotiable?

Cybersecurity is not a spectator sport, but a full-contact game that demands quick thinking, fast action, sharp instincts, and the ability to adapt under pressure. Those skills cannot be learnt by reading a textbook alone; they're forged through real-world practice. When professionals train in simulations, cyber ranges, or hands-on labs, they're not just memorizing concepts or building vocabularies; they're learning how to spot threats in the wild, respond in real-time, and recover systems under fire. That kind of preparation makes the difference between reacting slowly and detecting an attack and stopping it before it causes serious damage.

Hands-on experience also changes the way people retain and apply knowledge. When you've solved a problem yourself, the lessons stick, long after a lecture would fade from memory. This kind of active learning builds confidence, especially for entry-level people in the field who might otherwise struggle with impostor syndrome. And it builds trust with employers as well. While degrees and certifications open doors, nothing speaks louder than the proven ability to perform under pressure. In a profession where seconds count, that capability is worth more than any line on a résumé.

Recommendations

Building a strong and resilient cybersecurity workforce will take more than good intentions; it requires deliberate investment and partnerships. Policymakers and industry leaders should expand funding for hands-on training programs, from state-of-the-art cyber ranges to apprenticeships and community college partnerships. These initiatives give learners the real-world experience they need to respond to evolving threats, while also opening the door to more diverse candidates.

We also need to rethink how we measure talent. Skills-based hiring should be prioritized over rigid degree requirements, making room for people with practical expertise gained through bootcamps, certifications, or self-directed learning. Cybersecurity curricula in different universities and colleges should be required to inculcate some level of hands-on training into the learning process, to ensure that graduates have the proper skillset required for the field. Stronger public-private partnerships between government agencies, universities, and tech companies can help create standardized training models that keep pace with industry demands. And to truly future-proof the workforce, cybersecurity fundamentals should be introduced in K–12 classrooms, sparking interest early and inspiring the next generation of defenders.

The Role of Academia, Industry, and Government Collaboration

No one sector can solve this alone. The cybersecurity workforce ecosystem should be a collective effort co-built by:

Academia: Developing flexible, hands-on curricula and partnering with employers for internships that will expose students to real-world cases, ensuring students have both skills and degrees.

Industry: Offering real-world challenges and hiring based on skills.

Government: Funding accessible programs and setting national workforce standards.

Conclusion

To reiterate, knowledge alone isn't enough in the fight against cyber threats. One's the ability to act, adapt, and respond under pressure that defines true readiness, and this is the kind of workforce we should be aiming for. Closing the cybersecurity skills gap will require a shift in how we prepare talent, putting real-world practice at the heart of every learning journey. From cyber ranges to apprenticeships, from K–12 programs to public-private partnerships, the path forward is clear: we must invest in people as much as we invest in technology. A fully equipped cybersecurity workforce is a great asset to the industry, but more importantly, it's a cornerstone for national security, economic stability, and public trust. The sooner we commit to building a resilient workforce, the stronger and safer our digital future will be.

References

1) Department of Homeland Security (DHS). (2023). *Building the Cybersecurity Workforce of the Future*. Available at: https://www.dhs.gov/topics/cybersecurity (Accessed August 3rd, 2025) U.S. Department of Homeland Security
2) Department of Homeland Security (DHS). (2023). *Future of Work Strategic Workforce Objectives (HSAC Subcommittee Final Report)*. Available at: https://www.dhs.gov/sites/default/files/2023-09/23_0914_hsac_workforce_subcommittee_final_report.pdf (Accessed August 5th , 2025) U.S. Department of Homeland Security
3) DHS GAO. (2025). *Cybersecurity Workforce: Departments Need to Fully Implement Key Practices*. Available at: https://www.gao.gov/assets/gao-25-106795.pdf (Accessed August 8th, 2025) Government Accountability Office
4) Federal Bureau of Labor Statistics (BLS). (2025). *Labor Force Statistics from the Current Population Survey*. Available at: https://www.bls.gov/cps/cpsaat11.htm (Accessed August 8th, 2025) NIST
5) National Institute of Standards and Technology (NIST). (2022). *Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework*. Available at: https://csrc.nist.gov/csrc/media/Presentations/2023/nice-framework-preparing-a-job-ready-
6) cybersecurity/images-media/NICE_Framework_Preparing_a_Job-
7) Ready_Cybersecurity_Workforce.pdf (Accessed August 10th, 2025) NIST Computer Security Resource Center
8) National Institute of Standards and Technology (NIST). (2025). *NICE Workforce Framework for Cybersecurity (v2.0.0)*. Available at: https://niccs.cisa.gov/tools/nice-

framework (Accessed August 8th, 2025) NICCS

9) National Institute of Standards and Technology (NIST). (2023). *Unlocking Cybersecurity Talent: The Power of Apprenticeships* [Blog]. Available at: https://www.nist.gov/blogs/cybersecurity- insights/unlocking-cybersecurity-talent-power-apprenticeships (Accessed August 8th, 2025) NIST

10) National Initiative for Cybersecurity Careers and Studies (NICCS). (2024). *Federal Virtual Training Environment & Career Pathways Resources*. Available at: https://niccs.cisa.gov/ (Accessed August 8th, 2025) WikipediaCISA

11) (ISC)². (2023). *Cybersecurity Workforce Study*. Available at: https://www.isc2.org/Research/Workforce-Study (Accessed August 8th, 2025) ISC2

12) U.S. Department of Commerce, White House. (2023). *National Cyber Workforce and Education Strategy*. Available at :https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf (Accessed August 10th, 2025) The WhiteHouse