The Path to Expertise:
A Competitive Cybersecurity Team in Every School by 2027

Authors: Dennis Devey,

Abstract:

The shortfall in cyber talent the United States faces is a lack of expertise rather than a lack of applicants, caused by educational pipelines which fail to teach students the skills they need in the workforce. Cyber security Capture the Flag competitions are an effective, inexpensive, and quantifiable way to train and assess students in real-world skills. A national effort to create a competitive Capture the Flag team in every middle school, high school, and college in the country by 2027 would immediately and permanently increase the diversity and expertise of our cyber workforce.

Introduction

Over the past decade, the “Learn to Code” initiatives spearheaded by Code.org and AP Computer Science knocked down many of the barriers to building a technical and diverse American workforce. The next step in this progression is building expertise in specific fields: for the purpose of this paper, cybersecurity.

There is no lack of people who use computers and technology every day, and— thanks to a wide range of training pipelines to teach computer and programming fundamentals—there is no lack of people applying for entry-level cyber jobs. The issue stems from a fundamental mismatch between the vast majority of applicants’ skill levels and experience required by the companies to which they are applying. The Cyberseek data [1] shows that of the ~210,000 unfilled jobs categorized by experience level, only 30,000 of the openings are defined as entry-level. Companies are generally unwilling to hire someone into a higher level role who will require a significant amount of training to contribute. While the Cybersecurity Apprenticeship Sprint [2] will alleviate some of those problems at the entry-level, there is no substitute to the skills and knowledge gained over years of experience. The talent deficit stems from a shortage of experts, not a shortage of applicants, which means that increasing the accessibility of entry-level training will not solve the problem.

[1] *Cybersecurity Career Pathway.* Cyberseek. https://www.cyberseek.org/pathway.html
[2] *Cybersecurity Apprenticeship Sprint*. Apprenticeship.Gov. https://www.apprenticeship.gov/cybersecurity-apprenticeship-sprint

The educational approaches for building a cybersecurity workforce up to this point have been well-intentioned, but ineffective in building expertise. While many colleges and universities have rolled out new cyber security degrees in recent years, these programs intentionally focus on providing a well-rounded education, vice developing any specific expertise. Many cyber-focused bootcamps and similar programs focus their classroom time teaching students introductory vocabulary and trivia so that they can pass entry-level certifications, primarily Comptia Security+. Degrees and certifications can lead to jobs if a company is willing to take a chance on a new graduate, but either way, these graduates now have to fight to get themselves on the path to expertise, rather than being guided in the right direction during their education. Education pipelines must focus on problem-solving that mirrors what a future employer will expect them to be capable of and teach students to embrace the complexity inherent in the domain.

The most effective education pipelines are prohibitively expensive, which excludes many applicants from historically under-represented groups. Providing the appropriate number of scholarships for these groups requires a massive amount of funding and cannot scale far enough at the national level. Profit-driven training organizations have found a gold mine in the Government's willingness to subsidize entry-level education, and there is no indication this gold rush is going to end. The most likely outcome of this current effort to refine our nation's cybersecurity workforce strategy is the creation of another pot of money for funding scholarships to education pipelines that do not have any interest in quantifying outcomes or guaranteeing the expertise of the students they produce.

On the opposite side of this conversation is the Capture the Flag (CTF) community, which with nearly zero funding, fanfare, or other support has been quietly producing a significant portion of the cybersecurity expertise entering the workforce over the past decade.

Capture the Flag competitions are events that require participants to solve challenges to acquire a 'flag' across a variety of technical categories. The points awarded for solving these challenges are weighted differently based on difficulty and are designed to require the use of a wide range of tools, techniques, and technologies to solve. Challenges run the entire range of the NICE Framework Competencies [3], teaching offensive, defensive, investigative and system administrator skills. These competitions can be for individuals, but are primarily team-based and rely on communication and teamwork. The results of a time-constrained competition are an easily quantifiable snapshot of a student or team's ability to solve problems across these categories. This makes CTF a powerful tool to distinguish educational organizations and teachers who effectively build expertise.

CTF is a scalable approach to this problem because the community is extremely open and has no commercial interests. Registration for events is free, and detailed explanations of challenges from competitions are released the following week for training purposes– meaning that free training material to improve at CTF is massive and continually growing. The majority of CTF

[3] *NICE Framework Resource Center.* NIST.gov. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

competitions are held independent of a specific level of education, but there are some organizations like picoCTF[4], which prioritize reaching Middle and High School students, and CSAW[5], which runs competitions for college students. The CTF community has invested in America, and it is time for America to invest in CTF.

While the CTF community is not currently a model of diversity, with participants typically originating from more privileged communities, CTF is inherently an accessible program. There is a negligible cost for a school to start a CTF team, since participation requires no new equipment or training, and there are no fees for competition entry or travel. A national lack of awareness of CTF is the primary barrier preventing CTF events from being as diverse as the schools that make up this country. The secondary obstacle is ensuring that all potential participants feel welcome and supported, no matter what background they come from.

A nationwide effort to encourage all middle schools, high schools, and colleges to establish CTF teams would lead to a massive and lasting increase in the quantity and quality of security experts our country will create. A minimal investment would be required to approve a national CTF curriculum and support recurring competitions for Middle School and High School students. This process is slowly happening organically, but with support from the White House, we can build a culture of expertise in our schools that will have an enduring effect on the workforce.

Defining Expertise

Excellence in security requires personnel who fundamentally understand the technology. In order to develop true experts in cyber security, practitioners must truly understand how computers and the programs that run on them work. Without that understanding, there are constant breakdowns at every level of communication and at every step of implementation as people with broken mental models attempt to fix problems they can't grasp. There is no substitute or shortcut to expertise; in order to be a useful member of the workforce there must be a foundational understanding of these systems. Computers, the networks they run in, and the programs that run on them, operate within a set of pre-determined and finite rules that can only be learned by putting the time in and then staying on top of changes in technology.

Fields like cyber security are too complex to rely on practitioners with perfect recall and complete understanding of the infinite unique problems a practitioner will encounter in their career. Quick recall of best practices, a solid understanding of underlying principles and problem-solving skills are the key hallmarks of an expert-- not the rote repetition of port numbers, vocabulary, or arcane commands. Creating a workforce of cyber security experts requires introducing students to the belief that they can solve any problem they come across. The expert knows the general search path to take and adapts their hypothesis as more

[4] *picoCTF Home*. picoCTF. https://www.picoctf.org/
[5] *CSAW Home*. CSAW. https://www.csaw.io/

information is learned or possibilities are eliminated. They rely on documentation and existing resources. If they don't know which resource contains the answers, they do the research required to find the resource. If they don't know enough to find a resource, they find another expert to point them in the right direction. If that resource doesn't exist, they create it and share it.

In short, experts don't view their skillset in terms of certifications they have, or tools and programming languages they use, but in problems they can solve. Expertise in cybersecurity is being excellent at the technology and the systems built around it by being able to find answers to layered problems. Ensuring students embrace that "hacker" mentality is essential to building an expert workforce.

Capturing Expertise

Skill in a field is based on the number of iterations of the problem-solving cycle someone has done in the problem space they are working in. Employers struggle with entry-level applicants because normal education pipelines have minimal focus on solving realistic problems, so applicants come in with few of the mental models or skills required to fend for themselves outside the structure, and stricture, of a classroom.

Capture the Flags, in comparison, are entirely focused on providing participants with deliberate opportunities to practice problem-solving skills. With a new competition occurring nearly every weekend, the most dedicated of CTF players wind up with thousands of hours more "reps and sets", and unsurprisingly, develop the base and depth of knowledge required to achieve "expertise" long before they enter the workforce. By introducing CTFs and other quantifiable challenges to the rest of the future workforce, educators can expose students to problems that teach crucial problem-solving skills and allow them to gain confidence and experience as they participate in additional challenges.

There is plenty written about the value CTFs provide to students, with statistics and discussions about gamification, creativity, and teamwork, but it is more important from a workforce development standpoint that we talk about how we can measure the success of a national CTF initiative. As described before, competitions provide a discrete snapshot into a student's ability at the time of assessment. This quantitative measure of an individual's ability to solve a wide range of problems can be used to assess the student's progress, their ranking among other students, and the efficacy of pedagogy. Breaking problem types into categories enables even greater fidelity, enabling specific comparisons across general competencies like systems administration and networking, or more specialized skills like binary exploitation and threat detection.

The challenges in each category are given different weights, with more difficult challenges being worth more in the final rankings. There are also mechanisms built in to identify when challenges'

weights do not equate to students' ability to solve them– whether they are too hard or too easy– allowing an updating of weights and even more accurate measurements.

A student who plays in their first CTF, regardless of their level of technical experience, will be able to find problems they can solve and learn from, enabling an enjoyable experience due to the low-weighted challenges meant for beginners like them. With an intentional approach to challenge writing, organizers can ensure that every student's first event is fun and educational. A student with more technical experience will be able to attempt more difficult challenges, and if they solve them, will receive an appropriately higher score.

When a student sees their initial results, broken down across categories, they can be given a learning plan to guide them towards precisely what they need to get to the next level. With no two challenges being exactly alike, each practice problem helps a student understand another possible approach to take to similar problems. Tracking progress through these practice problems has value, but the ultimate measure of progress is how they perform on their next assessment. A student's next CTF event can be used to get another snapshot of a student's ability, giving instructors a clear look into the progress of their students. These assessments can be repeated at any periodicity and provide a clear idea of a student's progression.

A cybersecurity professional does not stop learning once they leave school and enter the workforce. It is a profession distinctive for the requirements to stay on top of the changing threat landscape and technology. CTF is the base for life-long learning and remains available for even veterans of the workforce to refresh their skills on a category of problems. Regular participation in competitions will keep a player on the cutting edge of the industry and keep them sharp across a wide range of general skills, even if their current role is more specialized.

But aiming far beyond measuring individuals, we can measure the efficacy of classrooms, grades, schools, states, and even whole countries. This puts significant pressure on school administrations and local governments to make policy decisions that improve their outcomes. While adding yet another standardized test might be a bridge too far, simply comparing participation levels and scores in voluntary events allow us to get deep insight into the state of workforce development.

As a final note, CTF teams provide an opportunity for teammates, camaraderie, and competition outside typical athletic teams. Existing options for technically minded team activities are Math Olympiad and extremely expensive robotics teams. A CTF team has zero startup costs because of the ability to use already existing or free resources. Students do not need new computers to compete: standard school-issued laptops are more than enough to access web-hosted virtual machines that give them all the resources they need to learn. Students can represent the school in regional and national competitions without leaving the school grounds, and no events require entry fees or expensive uniforms. Teams can even train themselves without the need for a dedicated teacher by leveraging the huge amount of free curriculum material found on the internet and dedicated support forums for technical questions, though of course, a teacher who could help coach and answer questions would be an incredible benefit for students.

CTF, a free game played from behind a computer screen, is an inherently neutral activity that should not favor any race, ethnicity, gender, or class. This has not been historically true, as a massive percentage of participants are white and Asian males coming from affluent schools with existing CTF programs. A coordinated effort for every school in the country to start and maintain gender-neutral CTF teams would permanently shift this balance to reflect the talent and diversity that comprises the entire country, not just the narrow slice who has benefited from a CTF-backed education up to this point. Everyone belongs in CTF, and so far that has not been the case.

Getting a CTF team into every middle school, high school, and college in America is something that could be accomplished by 2027 with no cost to the government outside of helping spread awareness. White House support for Code.org and Hour of Code was a watershed moment in opening up Computer Science, that same high-profile support of CTF would permanently solve many of the existing issues in the cybersecurity workforce.

Implementing Expertise

Creating a national strategy to prioritize CTF participation requires five things to succeed:

1) Recurring CTF Competitions
2) An approved standardized curriculum
3) A CTF and security community willing to share their knowledge
4) Support from the gov. to incentivize schools to create and support CTF teams
5) Support from the gov. to increase the visibility of underrepresented groups

Item 1, recurring CTF competitions, is the easiest to implement because it is already happening. The exemplary organization in this space is picoCTF, which runs the world's largest high school cybersecurity CTF competition. The organization has been hosting the event since 2013 and is widely regarded as the pre-eminent CTF education organization because of its focus on supporting beginners. In the 2022 edition, 6,000 middle school and high school students participated over two weeks[6]. Pico also runs a year-round training gym which provides access to all challenges they have released over the past few years, as well as online virtual machines that students can use to solve challenges[7]. Pico is far from alone in hosting recurring CTFs, but the professional example they set for the rest of the community is why they are the best choice to introduce the country to CTFs. While there are many annual collegiate events, the premier organization is CSAW, which hosts a range of seven competitions from standard CTFs and technical research presentations, to policy and journalism events. These competitions are open

[6] Tkacik, Daniel. *picoCTF 2022 Review*. CMU Cylab. https://www.cylab.cmu.edu/news/2022/04/14-picoCTF.html
[7] Owens, Kentrell and Alex Fulton. "pico-Boo!: How to avoid scaring students away in a CTF competition." https://picoctf.org/pdfs/FINAL_CISSE_paper.pdf

to all colleges, but the same schools are there every year. An increased focus on getting CTF teams to new schools, especially to community colleges and Historically Black Colleges and Universities will change the landscape. Pico and CSAW will continue doing great things for the students who play in their events but with White House support, we can get thousands more students to participate.

Item 2, a standardized curriculum, is slightly more difficult, if only because there is no clear consensus on what is the most effective curriculum to teach Capture the Flag fundamentals. There is a wide range of free computing, networking, and security fundamentals available online, so choosing a specific one to direct students toward would require some level of work. No matter which curriculum is chosen as the initial national standard, it must have no commercial motivations and be open source to avoid the vendor lock-in that commercial training organizations are desperate to create. One of the only existing curriculums to teach students the skills needed to participate in CTF is the Fundamentals Track produced by Roppers Academy[8]. This material is released under a Creative Commons Attribution-NonCommercial- ShareAlike license, meaning that anyone can share, remix, or build upon the material and release it in any form. This free and open-source nature allows the entire curriculum to be subsumed into any larger organization that wants to share the material with their students, while still benefiting from any changes made to the original material. A shining example of a technical open-source curriculum for high schoolers is David Malan's CS50 AP Introduction to Computer Science[9]. This Massively Open Online Course (MOOC) is delivered remotely to thousands of high schoolers and gives teachers in the classroom all the tools they need to automatically grade assignments and get students the support required without having to be experts themselves.

Item 3, the community's willingness to teach, is an imperfectly solved problem. The CTF community is constantly creating free educational material and generally producing engaging content to share their knowledge. A broad group of hackers and creators are continually working to create an environment where any student can be pointed to find what interests them and follow tutorials, watch entertaining videos, and spend more time immersed in the field they want to work on when they enter the workforce. The downside is that despite the huge amount of content being created, it does not reflect the diversity of our country. It is likely that potential new entrants to the CTF community and security field as a whole will have difficulty finding someone who looks like them to learn from.

Item 4, support and incentivization is a public policy problem best suited for another paper, but the White House's 'Commitments to Support Computer Science Education' initiated in 2013[10] is an excellent framework to follow.

---

[8] *Ropper CTF Bootcamp*. Roppers.org. https://www.roppers.org/courses/ctf
[9] Malan, David. *CS50 AP*. Harvard. https://cs50.harvard.edu/ap/2023/
[10] *Commitments to Support Computer Science Education*, White House Archives: Obama. https://obamawhitehouse.archives.gov/the-press-office/2014/12/08/fact-sheet-new-commitments-support-computer-science-education

1) Seek commitments by school districts to create and support CTF teams for their students
2) Serious work must be done to build and approve an AP Cybersecurity course, in a similar model to AP Computer Science
3) Provide funding for training middle school and high school teachers to be able to teach a CTF curriculum in the style of CS50 AP
4) Take steps to increase the participation of women and underrepresented backgrounds in CTF competitions

Number 4 in the list of White House commitments rolls neatly into Item 5 on the initial list: support to increase the visibility of under-represented groups in the CTF community and the broader cybersecurity field. As long as it is not immediately obvious to new students that they belong and are welcome in the security field from their first introduction to it, we will be losing out on talent. There are plenty of extraordinary men and women from underrepresented backgrounds who have put themselves out into the public space, built courses, and done incredible amounts of unpaid work to help open up the industry. Going forward, the government must support grants to pay these volunteer teachers, mentors, and coaches. Teachers who double as coaches after school need to be paid for their time like coaches of other athletic teams. Without supporting these efforts financially, we take advantage of their willingness to make the world a better place than when they entered the field.

The initial work to build a computer science workforce has been set in motion-- now it is time to build cybersecurity expertise that reflects the diversity of our country.

Moving Forward

No matter the pipeline a student takes to enter the cybersecurity field, whether formal education, self-study, or a re-skilling boot camp, Capture the Flag has a critical role to play in quantifying ability and incentivizing improvement. A national effort to bring Capture the Flag teams onto every middle school, high school, and college campus will create a culture of excellence driven by friendly competition. Making CTF participation a default for all students regardless of school or background will raise the standard for all educational pipelines.

All the technical requirements to put a CTF team in every school by 2027 have been met, leaving only a coordinated awareness push and alignment of incentives driven by the White House and other organizations who share our mission.