AMERICAN ASSOCIATION OF COMMUNITY COLLEGES

# CYBER SKILLS FOR ALL: COMMUNITY COLLEGES LEAD THE WAY

# Cyber Skills for All: Community Colleges Lead the Way

Strategies and Promising Practices for Bolstering and Expanding Cybersecurity Programming at Community Colleges

## Table of Contents

# Introduction

The American Association of Community Colleges (AACC), in partnership with Microsoft, developed a community of practice for community colleges to expand and bolster their cybersecurity programs and train the next generation of security professionals. From 2021-2024, three cohorts of 14 colleges took part in the Cyber Skills for All: Community Colleges Lead the Way program. AACC is grateful for Microsoft's support of this work and the community college sector.

Cybersecurity is a critical issue facing communities and businesses across the United States. It is in demand both as a stand-alone academic discipline and as a cross-cutting set of skills and competencies needed in other sectors, including manufacturing, agriculture, business, accounting, engineering, criminal justice, healthcare, and many others.

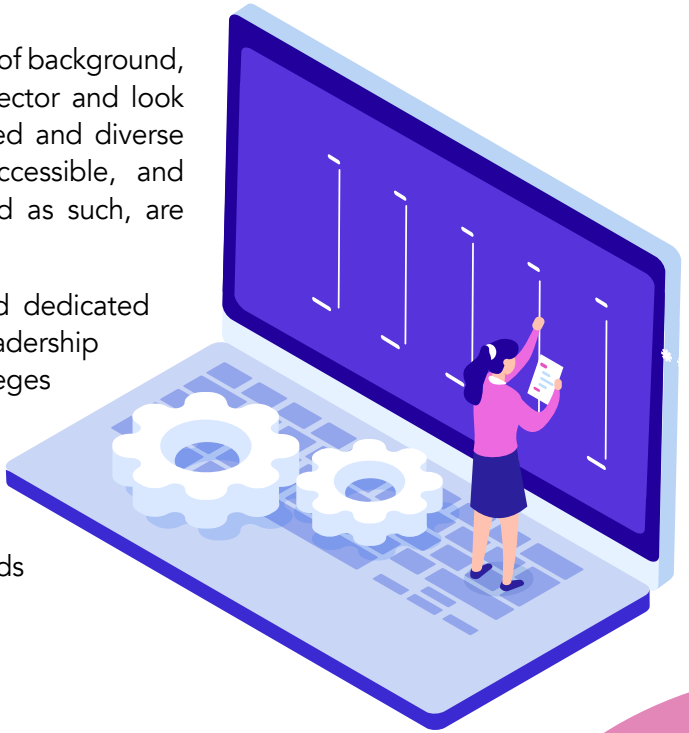
To support Microsoft's goal to develop a pipeline of students from 2-year institutions with cybersecurity skills into a variety of professional opportunities, AACC identified 42 community colleges with leadership and faculty that prioritized this work. Each college received funding to advance projects of importance in their area, including recruiting students, developing hands-on and job experience, and training faculty. Each cohort also met monthly to share best practices with each other and receive technical support as needed. AACC is pleased to present this collection of promising practices to community colleges across the country.

In addition to the Cyber Skills for All initiative, Microsoft has a collection of resources and supports for educators in the cybersecurity, IT, and computer science spaces that include training for educators, and certification and scholarship supports for both students and faculty. You can learn more by visiting the Cybersecurity Skills page at https://aka.ms/Cybersecurity_Skills.

## Why Community Colleges?

Cybersecurity is both a critical workforce skill across all industries and a high-demand profession in the IT sector across the nation. Community colleges are uniquely positioned to address the demand for an estimated 500,000[1] new cyber professionals, and also, as the training ground for professionals across many other sectors, to build cyber awareness and competency for critical sections of the workforce in industries such as healthcare, business administration, and manufacturing, to name a few.

Businesses like Microsoft have seen the need for more diversity of background, thought, experience, race, and ethnicity in the technology sector and look to community colleges as a critical source for a highly trained and diverse workforce. Community colleges are the most diverse, accessible, and affordable post-secondary institutions across the country and as such, are ideally positioned to respond to this demand.



Through the consistent use of program advisory boards and dedicated workforce and economic development staff, as well as leadership with strong connections to the business community, colleges can rapidly respond to changing workforce needs. A diverse portfolio of solutions that include both credit and non-credit programming, highly customized incumbent worker training, asynchronous instruction, as well as in-person, remote, and hybrid teaching allows colleges to meet the needs of their communities.

[1]https://www.nist.gov/speech-testimony/finding-500000-addressing-americas-cybersecurity-workforce-gap

Community colleges that lead this work with AACC on behalf of their communities included:

Alamance Community College, NC
Bellevue College, WA
Bismarck State College, ND
Blue Ridge Community and Technical College, WV
Central Community College, NE
Chippewa Valley Technical College, WI
City Colleges of Chicago, IL
Clover Park Technical College, WA
College of Sothern Idaho, ID
College of Southern Nevada, NV
College of Western Idaho, ID
Community College of Baltimore County, MD
Community College of Beaver County, PA
Community College of Philadelphia, PA
Community College of Vermont, VT
County College of Morris, NJ
Cuyahoga Community College, OH
Fletcher Technical Community College, LA
Glen Oaks Community College, MI
Hawai'i Community College, HI
Hostos Community College, NY
Ivy Tech Community College, IN
Lakeshore Technical College, WI
Laramie County Community College, WY
Miami Dade College, FL
Middlesex Community College, MA
Mississippi Gulf Coast Community College, MS
Moorpark College, CA
Mountwest Community and Technical College, WV
North Hennepin Community College, MN
Northwest-Shoals Community College, AL
Oklahoma City Community College OK
Paradise Valley Community College, AZ
Southern State Community College, OH
Southside Virginia Community College, VA
Southwest Tennessee Community College, TN
Temple College, TX
Tulsa Community College, OK
UA Cossatot, AR
Waubonsee Community College, IL
Wichita State University Campus of Applied Sciences and Technology (WSU Tech), KS
York Technical College, SC

## Faculty Recruitment and Retention

One of the most common challenges faced by community colleges across many departments is the recruitment and retention of highly qualified faculty. Causes of this challenge can vary across college departments, but in cyber and other high-tech fields, highly compensated private sector opportunities are often a factor. Additionally, in the cyber field, rapid industry advances mean that continuous training and industry connection are important to ensure that classroom teaching reflects current industry needs and trends. Colleges continue to strategize around this challenge. Promising practices include:

- Increasing pay rates for open and hard-to-fill positions. Some colleges have a process through which the case for increasing pay for a position that would have a higher private sector pay rate is made. Colleges that went through this process reported that they were able to increase rates above a typical full-time or adjunct instructor, but that often, private sector professional opportunities were still much more lucrative than could be offered by colleges. Additionally, there was the potential for resentment within and between the staff for these exceptions to the traditional funding/salary model. (In states in which faculty pay is collectively bargained, this is typically not possible.) Finally, there have been discussions in multiple state legislatures about allocating, or re-allocating, funding to address this issue.
- Developing co-teaching models. Colleges also are exploring methods of co-teaching wherein industry professionals are engaged as subject matter experts (SMEs) so these individuals can co-teach with qualified instructors. SMEs may be compensated by their employers as part of their job (some companies, recognizing the incredible need for cyber professionals, are willing to work with colleges in this way) or they may be offered a stipend or other contract compensation by the college.

- Sharing faculty. While none of the Cyber Skills for All colleges have actualized this strategy to date, there have been multiple discussions between and among several of them regarding the practicality of remotely sharing a faculty member. The premise is that a course taught at College A could be attended remotely by students at College B, with both colleges sharing in the compensation of the faculty member. This is a more challenging strategy, especially for colleges who are served by different regional accrediting bodies.

## Recruiting Untapped Talent

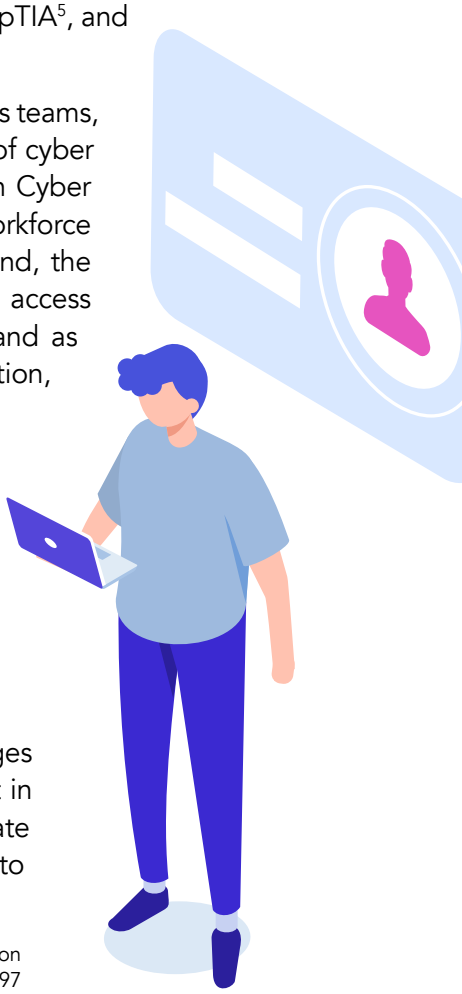
Many colleges have made great progress in fostering diversity within cyber education programs however increasing gender parity and racial diversity continue to be a challenge across the tech sector. Every community has a swath of untapped talent that may thrive in the cyber industry and fostering an environment of inclusion and belonging for students who might not consider the sector is a great step to attracting and retaining students in cyber programs. Some strategies might include:

- Intentional recruitment or training of diverse faculty. This fosters a sense of belonging for diverse students. Education researchers have found, "Overall graduation rates for underrepresented minority students of all races/ethnicities are positively affected by increased diversity of their faculty."[2]

- Increased community engagement with K-12 partners, students, jobseekers, and others to educate community stakeholders about cyber careers. Tools like CyberSeek[3], an interactive cybersecurity jobs heatmap and career pathway tool created in partnership with the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE)[4], CompTIA[5], and Lightcast[6] can be helpful in illustrating the demand in the industry.

- Developing industry relevant extracurricular programs such as cyber clubs, esports teams, robotics teams, and hackathons to elevate community and student awareness of cyber programs and careers. For example, the mission of the organization Women in Cyber Security[7] (WiCyS) is to "help build a strong gender-diverse cybersecurity workforce by facilitating recruitment, retention and advancement in the field." To that end, the organization helps colleges establish campus chapters whose members gain access to training, mentoring, and other professional activities during their studies and as professionals. Colleges with WiCyS chapters report increased interest, participation, and success of female cybersecurity students.

- Deliberately engaging with minority-serving, low-income, and diverse high schools for dual enrollment. This can be an effective method to expose, streamline, and accelerate students who are historically underrepresented in community college cyber programs, and into the industry as a whole. Northwest-Shoals Community College (AL) had success with this strategy, reporting that many local high schools have asked for cybersecurity courses to be taught in a dual-enrollment format on their campuses.



As with multiple markets across the country, AACC has heard from member colleges and industry partners that employers are in dire need of talent now. Their interest in waiting for candidates with doctoral, master's, bachelor's, and even 2-year associate degrees remains limited. More often, they are seeking students with 6-weeks to

[2]Stout, R., Archie, C., Cross, D., & Carman, C. A. (2018). The relationship between faculty diversity and graduation rates in higher education. Intercultural Education, 29(3), 399–417. https://doi.org/10.1080/14675986.2018.1437997
[3]https://www.cyberseek.org/
[4]https://www.nist.gov/itl/applied-cybersecurity/nice
[5]https://www.comptia.org/
[5]https://lightcast.io/
[6]https://www.wicys.org/

6-months of upskilling to fill their labor gaps. This shorter training time frame is also critical for many low-income or non-traditional students who are trying to balance their pursuit of skills training with financial or familial obligations.

The cyber market is no different. Many colleges note the need to consider the time it takes to impart critical information without jeopardizing student opportunities in the local labor market. For example, Laramie County Community College (WY) found that the delivery of cybersecurity instruction in a flexible format has directly led to the continuing education of one recent graduate. Without a program built on stackable credentialling and certificate milestone markers, it was natural to see retention challenges of career-changers who were eager to enter the workforce. The certificate diploma graduate from the spring of 2022 had recently entered a new career as a datacenter technician for a local employer. His work schedule and overall life requirements were forcing him to abandon his goal of an AAS in cybersecurity. With a scholarship to offset some of the tuition costs, as well as a flexible classroom experience, he has been able to continue as a part-time student, with the ability to engage in his class sessions remotely with permission from his employer. This has provided him with an avenue to hone his existing skills in the workplace, while still developing new capabilities and pursuing his AAS degree. This student shifted back to full time in the spring 2023 semester and is planning to graduate this spring with his degree. He has a commitment from his employer to move him into a network security analyst role once he has completed his degree and the associated certifications, which will come with a sizable increase in compensation.

## Integrating Cyber Across Other Industries

As jobs across all sectors increasingly include handling of electronic data and information, digital and phone communications, and other computer use, strong cyber awareness and cyber literacy are considered basic work-readiness skills across all sectors with many industries requiring more advanced cyber competencies across all professionals (not just those in designated IT roles). Some strategies for integrating cyber across curriculum include:

- Requiring all community college students to complete a basic email and phone cyber skills training as part of orientation.
- Meeting with all college advisory boards to discuss cyber skills needs and challenges unique to each industry. This can lead to the development of bootcamps and skills training to meet those immediate needs as well as working with other departments to identify opportunities to infuse relevant skills training into programs and courses.
- Performing outreach and level-appropriate educational opportunities to organizations such as retirement homes, Boys and Girls Clubs, scout groups, faith-based or other community-based organizations.

## Hands-On and Job Experiences Are Critical

Community colleges should position themselves as the premier continuing education center for cyber professionals by hosting cyber ranges, bootcamps, hackathons, and other continuing education and practical training needs for professions at all levels in the cyber industry. Such programs can be revenue neutral and revenue generating.

### Becoming a Center of Academic Excellence

An important partner and resource throughout the Cyber Skills for All initiative has been the National Cybersecurity Training and Education Center (NCyTE). NCyTE is located at Whatcom Community College (WCC) and is an Advanced Technological Education (ATE) National Center, funded through a National Science Foundation (NSF) grant.

NCyTE's Mission[7] states, "The National Cybersecurity Training & Education (NCyTE) Center advances cybersecurity education in the U.S. by investing in technological innovation, resources, professional development and tools to support faculty, community colleges, and the workforce pipeline of tomorrow." NCyTE hosts a wealth of vetted resources for students, faculty, and college administrators for program and curriculum development including professional development. Additionally, NCyTE's Centers of Academic Excellence Candidates Program is designed to guide colleges and universities through the application process for Centers of Academic Excellence[8] (CAE) in Cybersecurity designation. This designation indicates that a college's program meets rigorous requirements to produce cybersecurity professionals essential for our national infrastructure. Many colleges report that the CAE designation is a valuable outreach tool both in the jobs and workforce development space and for student recruitment. Colleges who worked through the CAE application process with NCyTE reported their guidance was invaluable.

## Cyber Ranges

Colleges that are able to provide hands-on learning experiences that mimic what students will experience on the jobsite position their graduates to stand out in a field where many employers are looking for experienced candidates, even for entry-level jobs. With a cyber range, colleges are able to create a virtual environment that replicates an IT environment where students or professionals can practice responses to different types of cyber-attacks in real time. Cyber ranges can vary widely in price and scale and community colleges must consider a wide range of factors such as price, computing power, and technical support needed, as well as local industry capacity and needs when choosing the right design.

Many colleges are able to leverage large blocks of funding to purchase professionally designed and supported ranges from cyber security companies, others are able to join coalitions of state agencies or other educational institutions to share access to large ranges, and others may choose to design and custom build smaller scale ranges. The prices of large "out of the box" ranges can be prohibitive for many colleges, but those who can raise funds or partner with other institutions to cost share may enjoy the benefit of technical support, frequent updates, and provided curriculum. Some colleges report that integrating these types of tools into existing courses can be challenging as they are often designed for professional practice rather than education.

Colleges should also engage with local and state governments to become apprised of agency priorities and opportunities for collaboration, partnership, and funding. For example, Mississippi Gulf Coast Community College is part of the Mississippi Cyber Initiative, a statewide initiative prioritizing cyber education, "created to meet the challenges of the cybersecurity reality in the state and around the nation and position Mississippi as a leader in a field that will be of critical importance in the years and decades ahead. The mission of MCI is to provide statewide leadership that prepares Mississippi's future economy through unparalleled collaboration and innovation in cybersecurity. The MCI will be an economic development catalyst leveraging the collective expertise among academia, the private sector, state, federal and local government, law enforcement, the U.S. Department of Defense, and the Mississippi National Guard."[9]

[7]https://www.ncyte.net/about-ncyte/about-us
[8]https://www.caecommunity.org/
[9]https://mgccc.edu/wp-content/uploads/2022/08/Mississippi-Cyber-Initiative-Brochure.pdf

Colleges with the expertise and capacity to design smaller scale ranges have the potential for significant cost savings and the ability to customize their ranges around course learning objectives. Significant attention must be paid to maintaining and updating these ranges, and colleges that go this route will need to plan for maintenance and updating these systems.

Laramie County Community College[10] (LCCC) hosts an impressive custom cyber range[10] designed and built by faculty and staff to meet course learning objectives and provide hands-on multisensory work experience for students in the classroom as well as remote and distance learning students. LCCC's CyberLab utilizes open-source software and recycled components everywhere possible to be cost conscious. It is comprised of a CyberRange built on a ProxMox virtualization cluster connected to the CyberCity Tactile Learning Environment (CTLE) through a custom pfSense firewall deployment. The CTLE consists of a physical miniature model city on top of a six by twelve foot welded steel platform with an HO-scale model train and city built upon it. All of the items in the city, short of trees and cars, are attackable/controllable endpoints attached to microcontrollers and/or single-board computers such as Raspberry Pis. LCCC links the city to the cyber range through modbus and GPIO controls from a virtualized command and control server. Students executing actions in LCCC's CyberRange can trigger changes to files within the virtualized environments, which then trigger the command/control server to issue the commands to the controllers downstream at the model city. With this model, instructors are able to design custom challenges within the city where students gain practice in threat defense and detection. The model provides an exploratory experience for students that aren't on the guiderails of the lab exercises instructors build. Students are also able to interact with the city remotely, via VPN access and web-camera live-streams. An advantage of this approach is that it provides future IT professionals with a visual experience to contextualize impact of a failure to secure a hospital's critical environment controls when they can see the building without power, or cannot access systems, and there is a display on the building showing the increased emergency service wait times and direct casualties as a result.

Southern State Community College's[11] cyber range was recently custom built (partially with funding provided through the Cyber Skills for All initiative in a similar fashion with the added layer of involving students in the design and building process. In addition to gaining the critical hands-on program elements, the involved students exhibit pride and ownership of the space, creating lasting ambassadors for the college and the cyber program.

## Hosting Hackathons

Typically, a hackathon describes a situation where a group of people come together to solve a problem. In the cybersecurity and education space, a hackathon might be focused on coming up with solutions for a real or potential security challenge faced by a business or other organization or institution. Hackathons can be organized to resemble a workplace project or as a competition between teams of students designing solutions for the same problem.

Colleges wishing to host a hackathon should consider involving participation by departments and businesses from advisory boards in industry clusters outside of IT and cyber programming for input in designing challenges and as potential judges, team participants, or mentors. Colleges can host hackathons for a relatively low monetary investment with potentially very high outcomes. By inviting interdepartmental collaboration on event and problem design, students can gain insight into a variety of industries with critical cyber needs through the lens of real-world problems faced across different industries (for example, small businesses, medical offices, educational institutions, and public utilities all have different vulnerabilities and risks). Hackathon challenges

[10]https://www.lccc.wy.edu/pathways/InformationTechnology/cybersecurityProgram/index.aspx
[11]https://www.sscc.edu/academics/programs/computer-science.shtml

can be presented entirely theoretically to a team, (a group of students, for example, may be presented with a written scenario describing a business with a critical security failure or vulnerability and the group collaborates to design an emergency response and preventative plan for the business). If a cyber range is available, teams can work together to defend simulated attacks. Inclusion of real-world scenarios from local stakeholders serves the dual purpose of contextualizing learning and showing those stakeholders the quality and depth of training students are receiving.

### Internships, Apprenticeships, and Work Experience

Many community colleges report that finding apprenticeship and internship opportunities for cybersecurity students is challenging. Many businesses are hesitant to design internship programs around such critical tasks given the business risks of security breaches, etc. Colleges should consider working with their own IT departments to design work experience and earn-and-learn opportunities for their cyber students. County College of Morris in New Jersey has developed a student helpdesk operated by credit and noncredit students, providing students with the opportunity for resume-worthy experience. Participating students gain increased customer service skills, along with basic help-desk experience.

Similarly, LCCC had addressed the need for experience by placing students in small non-profit organizations to assist with cybersecurity needs, as they often lack the resources to fill such positions on their own. This provides the added cachet of offering a valuable community benefit. Additionally, because cyber professionals need regular training and upskilling as the industry evolves, this type of community engagement can help secure a community college's place as a relevant high-quality continuing education option for businesses and professionals.

## Conclusion

Following AACC's work with Microsoft on Cyber Skills for All: Community Colleges Lead the Way, multiple college members over the last 3 years individually, and through collective technical support, AACC believes that the following considerations are worthy of elevating and discussing in communities across the country seeking to expand their own cyber security efforts:

### Consider Creative Solutions at Every Cost Point

The Cyber Skills for All initiative has shown that colleges can build high-quality programs with budgets of any size. Small and rural colleges and large colleges alike can build robust contextualized and industry relevant learning opportunities for students. Colleges can build programs using components purchased with grant funds, or creatively utilize donated equipment, and can partner with larger institutions and state agencies to gain access to computing power and cyber ranges. Institutions with more purchasing power can build larger scale programs and become resource centers in their communities and regions.

### Build Cross-Industry and Industry-Relevant Programs

By engaging with local businesses, government agencies, college faculty and staff, and even students, colleges have built strong training programs that reflect the needs of their local economy and also meet rigorous standards that are critical to effectiveness in cyber careers. Colleges can work across departments and with advisory boards for non-IT industry clusters such as manufacturing, business administration, and healthcare to integrate critical cyber skills and competencies across existing programs. Equally, the students in cybersecurity programs benefit from industry contextualized learning opportunities to better prepare for their critical professional roles.

## Recruit Untapped Talent

There is a critical need for cyber professionals and workers with strong cyber skills across the country and one way that colleges can expand programming is through engaging with untapped talent. Colleges should examine current cyber programs and identify portions of their local community who may not currently be aware of cybersecurity as a profession and perform outreach to community groups or other agencies working with those populations. For example, local jobs centers, workforce agencies, U.S. Department of Labor Adult or Youth Programs, Girls and Boys Clubs, scouting groups, or other community-based organizations.