Building the Cybersecurity Pipeline: A Community Based Lifecycle Approach

Lonnie G. Decker, Ph.D.
Lonnie.decker@davenport.edu

Davenport University
6191 Kraft Ave SE
Grand Rapids, MI 49512

Deanne Wesley, Ph.D.
dwesley@forsythtech.edu

Forsyth Technical Community College
2100 Silas Creek Parkway
Winston-Salem. NC 27103

Abstract - The need for cybersecurity workers is clear. With a documented current shortage of cybersecurity workers in the U.S. identified as over 300,000 openings, the need to attract, and retain more future cybersecurity workers could not be more clear. Many efforts have been created to address this need and have had clear positive results. These include the use of summer camps & competitions to increase interest in the field, reaching out to underrepresented populations to help fill the need, and providing scholarships and using shared curriculum to help students through their educational pathway.

This paper proposes the implementation of a Community Based Life Cycle (CBLC) approach to help address this need. With the development of a Cyber Education Task Force (CETF), the ability to use a systems development *approach to identify and align the efforts that already have been developed to help retain students' interest in cybersecurity as a career. Through the use of professional and peer mentoring in a Cascade Advising approach, the professional mentors (and members of the CETF) would identify communities (summer camps, competitions, etc.), where peer mentors can be effective in helping newer and future students be successful.*

Keywords

Cybersecurity Pathways, Summer camps, Competitions, Scholarships, Life Cycle Approach, Mentoring

1. GENERAL PROBLEM

The increasing need for more workers in the cybersecurity workforce has been documented for some time, even if not thoroughly researched and understood. As of July 2018 there was a projected 301,873 total job openings in the U.S. (Cyberseek, 2018). Globally, projections suggest a shortage of 1.8 million cybersecurity workers by 2022 (Department of Commerce & Department of Homeland Security (2017). The report from the Department of Commerce & Department of Homeland Security (2017) include some further key findings, which include:

- The United States needs immediate and sustained improvements in its cybersecurity workforce situation.
- Expanding the pool of cybersecurity candidates by retraining those employed in non-cybersecurity fields and by increasing the participation of women, minorities, and veterans as well as students in primary through secondary school is needed and represents significant opportunities.
- Comprehensive and reliable data about cybersecurity workforce position needs and education and training programs is lacking - even though the general context and urgency of the situation are obvious.

The shortages of workers in the cybersecurity field has led to the discussion of "Building a Cybersecurity Pipeline" (Gonzalez, 2015) to increase the supply of workers in the cybersecurity workforce. Research often methods of addressing the shortage of workers in the cybersecurity pipeline, without specifically identifying the components of this pipeline. For instance, InfoSecurity Magazine identifies one of the solutions to the demand for highly trained security professionals as a need for colleges and universities to address within their curriculum. "Given the situation just described, what can institutions of higher learning do today to increase their contribution to the cybersecurity pipeline? They can begin by recognizing there is a major need for cybersecurity expertise today and that they play a vital role in filling this need" (Infosecurity Magazine, 2013). As for suggested solutions, there are several identified in this article, including the need for technical training at all levels, incorporating cybersecurity with a multidisciplinary approach, and partnering with both K-12 schools to foster interest in cybersecurity careers, and also with industry. "Colleges and universities must collaborate with professional associations, industry, and government agencies to offer their students access to mentoring, internship, and job placement programs and to secure guest lecturers with expertise that will pique the interest of their students. These relationships will prove invaluable for both academia and industry" (Infosecurity Magazine, 2013).

Other research seeks to increase participation in cybersecurity careers by recruiting populations that are underrepresented. "The lack of women is especially troubling with a low percentage in the educational pipeline and a higher than normal dropout rate once employed in technology. The best ways to bring women into cybersecurity and other technology fields is through role modeling" (Gonzalez, 2015). To this end, Recommendation 1.5 of the Report to the President challenges the federal government to "launch a vigorous effort to recruit cybersecurity workers from large and diverse pools of candidates who are underutilized or underrepresented in the cybersecurity workforce. This includes veterans, women, and minorities" (Department of Commerce & Department of Homeland Security (2017). Further recommendations describe other initiatives that would be identified as methods for increasing the potential supply produced by the Cybersecurity Pipeline (Department of Commerce & Department of Homeland Security (2017):

- Recommendation 1.4 (Action 1.4.1) - Federal agencies must also better coordinate recruitment outreach across the government … and make better use of cybersecurity camps, competitions and challenges, games, contests, and other interactive opportunities.
- Recommendation 2.7 - Expand government and private sector support for high-quality cybersecurity camps, boot camps, and similar programs designed to educate and train teachers or students.

- Recommendation 3.2 - Develop model career pathways for cybersecurity-related positions that can be used in the private and public sectors. These pathways should spell out education, training, and other experiences that align with employers' skill needs and prepare an individual to be successful in entering or advancing a cybersecurity career.

2. CYBERSECURITY PIPELINE EFFORTS

In alignment with these recommendations, there are a number of efforts to increase the number of students selecting cybersecurity careers - to increase the number of individuals in various stages of the cybersecurity pipeline. These efforts can be summarized as follows:

- Summer camps
- Competitions
- Shared curriculum (Dual enrollment, Articulation)
- Underrepresented populations
- Scholarships
- Mentoring

2.1 Summer Camps

While there are a variety of summer camps offered at different grade levels, those offered through the GenCyber program are probably the most common and best known. Funded by the National Security Agency and the National Science Foundation, participation in a GenCyber camp is free for participants. The vision for the program is to "to be part of the solution to the Nation's shortfall of skilled cybersecurity professionals. Ensuring that enough young people are inspired to direct their talents in this area is critical to the future of our country's national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives" (Gencyber.com).

As an example of the outreach provided through the GenCyber summer camps, there were two summer camps for students hosted at Forsyth Technical Community College in 2018 - (an additional two camps covered similar topic areas for teachers):

- GenCyber Girls Camp - The Girl's Camp will teach students to program Apple Swift Playgrounds on an iPad, using Apple's proprietary code. Students will also learn to build a Kamigami using robotics technology.
- GenCyber Raspberry Pi Camp - The Raspberry Pi will teach participants how to program Raspberry Pi. Participants will also learn Drone exploration and how privacy rules applies to drones. (https://crrc.forsythtech.edu/gencyber-camps-2018/)

"There is very strong demand for GenCyber programs. For 2018, we have 149 camps in 43 states plus Washington, D.C. and Puerto Rico. Our goal is to sponsor 300 camps by the year 2020, or perhaps even sooner, with camps in all 50 states" (Gen-cyber.com).

2.2 Competitions

The use of competitions to engage potential cybersecurity students has shown increased interest. This includes the ideas of gamification through summer camps, and Capture-The-Flag (CTF) events as methods to entice potential students to learn more about cybersecurity and other topics. "A cyber security CTF is a competition between security professionals and/or students learning about cyber security. This competition is used as a learning tool for everyone that is interested in cyber security and it can help sharpen the tools they have learned during their training" (Harmon, 2016).

Of particular interest are the Collegiate Cyber Defense Competition (CCDC) and CyberPatriot, which focus on college level and high-school level competition respectively. Started in 2004, among the goals of CCDC is to help motivate "more educational institutions to offer students an opportunity to gain practical experience in information assurance" (nationalccdc.org), aligning with Action 1.4.1 above.

Possibly even more illustrative is the increasing demand for CyberPatriot. "CyberPatriot the National Youth Cyber Education Program created by the Air Force Association (AFA) to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future" (uscyberpatriot.org). With registration complete for the 2018-19 competition year, the number of high school teams across the United States has increased to over 6,000, an increase of more than 1,000 teams from 2017-18 (Air Force Association, 2018). Recent additions to the program included starting a Middle School Division, and in 2015 the launch of an Elementary School Cyber Education Initiative "designed to help young students understand the importance of cybersecurity in their everyday lives, equip them with the skills to better protect themselves online, encourage them to behave ethically online, and excite them toward opportunities in STEM" (uscyberpatriot.org). While the competition is focused on activities in which the teams must maintain system functionality while defending against vulnerabilities, the design of the competition also includes the use of volunteers and mentors within the program. "By participating in CyberPatriot, students are introduced to an exciting and lucrative career path. In addition to learning teamwork and organizational skills that set them apart in the STEM job market, Competitors benefit from direct tutelage by industry professionals that volunteer through the CyberPatriot Mentor Program" (uscyberpatriot.org).

The program has demonstrated positive results. In a survey of 2016 participants, 89% indicated that they planned to enroll in a 4-year higher education program, compared to BLS results that only 45.7% of high school graduates in 2015 entered a 4-year program. "Additionally, 78 percent of the respondents indicated they will pursue a 2-year or 4-year education program plan to study cybersecurity, computer science, or another STEM field, whereas the national average is only 14 percent" (Air Force Association, 2016).

2.3 Shared Curriculum

The idea of shared curriculum between high school and colleges/universities can fall under several categories, including dual-enrollment, articulation of credit, and middle-college programs. The overall intention of each category is similar: to entice more students to further their education, and to shorten the time needed to do so. "The number of high school students taking college courses at community colleges has grown dramatically since the early 2000s. To the extent that dual enrollment enables students to 'get a head start' on college, it holds great potential for improving college access and completion rates and lowering the cost of degrees for students and their families" (Fink, et. al. 2017).

While the results demonstrated in Fink (2017) are not without difficulties, the overall results show that implementation of dual-enrollment (and by extension, similar programs) have the potential to increase the number of students seeking higher education, and completing 2-year and 4-year programs in a more timely fashion. Where there were challenges demonstrated, these were most clearly delineated based on differences among the implementation in various states, and variations in success based on the income levels of the students' families. Further, the report indicated varying measures of dual-enrolled students who continued their education, suggesting that some students enrolled in college who were previously dual-enrolled may not be reported as such. "Thus, it appears that community colleges may be "capturing" substantially more dual enrollment students immediately after high school than many seem to think. We suspect that if colleges were more proactive in working with their high school partners to reach out to their dual enrollment students and advise them on the educational opportunities and potential cost savings that community colleges afford, they would thereby be able to increase the yield of their dual enrollment students who go on to enroll at their institutions after high school" (Fink, et. al. 2017).

2.4 Underrepresented Populations

This is an area that has, perhaps, been of the most intense focus. As previously discussed, Recommendation 1.5 of the Report to the President addressed the need to recruit candidates who are underutilized or underrepresented in the cybersecurity workforce, including “veterans, women, and minorities” (Department of Commerce & Department of Homeland Security (2017).

Among the examples of how this area has been addressed, the Women in CyberSecurity (WiCyS) organization was formed in 2013 through Tennessee Tech University, with the mission “to broaden participation in cyber by recruiting, retaining and advancing women in the field of cybersecurity, and improve on the very low 11% statistic of women in cybersecurity jobs” (wicys.net).

Gonzalez (2015) identifies multiple barriers to women’s participation and advancement in cybersecurity:

- A lack of role models
- Mentors and sponsors
- Problems with supervisory relationships
- Inequities in performance and promotion procedures
- Inflexible work policies that make it difficult to manage competing responsibilities

Organizations such as WiCyS and their annual national conference can help to mitigate some of these barriers. “Companies need to have access to a pipeline of qualified candidates for cybersecurity jobs - both senior-level and students in the field who can join through apprenticeships and internships. It also makes perfect sense to hire women into these jobs, because it’s been proven that workforce diversity improves productivity and also enhances external perceptions. Promoting women into senior, thought leadership positions also adds tremendous value to companies’ positioning with stakeholders and customers” (WiCyS).

2.5 Scholarships

The cost of higher education can be a barrier for some students, likely causing some students to leave the cybersecurity pipeline. This was a factor mentioned previously in the success of dual-enrollment programs, where variations in success were attributed to differing levels of family income. Further, this need was addressed in Recommendation 2.6 of the Report to the President. "Federal and state governments, as well as the private sector, should consider providing greater financial assistance and other incentives to reduce student debt or subsidize the cost of cybersecurity education or training" (Department of Commerce & Department of Homeland Security (2017). Further Action items within this recommendation include:

- Action 2.6.1 - The administration should include … increased federal funding for the CyberCorps: Scholarship for Service (SFS) program administered by the NSF.
- Action 2.6.2 - Modify student loan repayment programs to provide a direct financial incentive for individuals to take cybersecurity jobs in federal, state, local, or tribal governments or economically distressed regions.
- Action 2.6.3 - Provide additional federal or state tax incentives for cybersecurity-related education or training.

Often these scholarships or other incentives are combined with previously discussed efforts to enhance their reach. "Also, there are STEM scholarships available just for women majoring in a STEM program in a post-secondary school. I believe we can extend more federal and state funds to schools to increase their participation in the STEM education. This will ultimately increase the women's pipeline into the IT field" (Gonzalez, 2015).

2.6 Mentoring

The role of mentoring has been discussed in relation to some of the other efforts previously discussed. For instance, one of the barriers mentioned for increasing women's participation in cybersecurity included a lack of role models, and limited opportunities through mentoring. Additionally, the CyberPatriot competition provides for mentoring of high-school and middle-school teams from volunteers in industry and higher education.

3. COMMUNITY BASED LIFE CYCLE

While these efforts have each individually demonstrated significant achievements to increase the flow of students through the Cybersecurity pipeline. Each of these efforts work to increase the entry of students into the pipeline with the hope that they continue their way to ultimately exit the pipeline into a cybersecurity work pathway. This could be thought of as a “push” model, with the intent to push more students into the pipeline and not “leak” out somewhere along the way. “This pipeline is almost always talked about in terms of leaks. If you’ve dripped out, you’ve dropped out” (Garbee, 2017). Indeed, this model of a pipeline is evolving into Pathways, and even Ecosystems. “I prefer to use the metaphor of an ecosystem. It captures the various ways providing students a strong STEM background contributes to economic competitiveness, national security, and an educated citizenry” (Garbee, 2017).

Whatever the approach, or the metaphor, the problems are the same - once in the pipeline, how do we help students stay there? How are students retained in the cybersecurity ecosystem? The solution presented is to implement a systems based approach to help retain students through these various efforts, i.e. to “pull” the students through the cybersecurity pipeline.

3.1 NICE Framework

Whether developing a cybersecurity pipeline, pathway, or ecosystem, the full implementation of the CBLC approach would be assisted by a common language or taxonomy. This is the purpose of the NICE Framework. The National Initiative for Cybersecurity Education (NICE) Framework was developed by the National Institute of Standards and Technology (NIST) as

Special Publication 800-181. "The NICE Framework, establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors" (National Institute of Standards & Technology, 2018). The NICE Framework provides for 33 areas of work in cybersecurity among 7 high-level cybersecurity functions. The incorporation of NICE into the CBLC provides for an alignment of efforts into the proper pathways particularly among potential students, education, and employers (National Institute of Standards & Technology, 2018):

- Current and future cybersecurity workers: to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity jobs and positions. The NICE Framework also enables staffing specialists and guidance counselors to use the NICE Framework as a resource to support these employees or job seekers
- Employers: to help assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions
- Education providers: who use the NICE Framework as a reference to develop curriculum, courses, seminars, and research that cover the KSAs and Tasks described

3.2 Systems Approach

The idea of a systems based approach (through implementation of the Systems Development Life Cycle - SDLC) is not a new approach. "This tried-and-true successful approach is combined with sound project management practices to develop key project milestones, allocate resources, select personnel, and perform the tasks needed to accomplish a project's objectives" (Whitman & Mattord, 2019).

While many of the components of this systems based approach are already in place and discussed previously, there are two elements that are needed to “complete the system” focused specifically on retaining students whose interest in cybersecurity careers is started through these methods: Communities and Mentoring.

3.3 Communities

There is not a shortage of communities in cybersecurity. Each of the efforts previously discussed are themselves part of a community. The Centers of Academic Excellence (CAEs) through the National Security Agency (NSA) and Department of Homeland Security (DHS) are themselves a community of 266 colleges and universities that work together to promote cybersecurity education (https://www.caecommunity.org/).

What is proposed is the development of communities with the specific intent of helping to connect the students in K-12, community colleges, universities, and the cybersecurity workforce, and to retain these students from one effort (e.g. Gen-Cyber) to the next (e.g. CyberPatriot), and to connect them to their own communities (e.g. WiCyS) and provide resources (e.g. Scholarships). The development of a Cyber Education Task Force (CETF) would be able to oversee the overall “system effort” of scanning the Cybersecurity Ecosystem, ensuring the connections from one community to the next. The members of the CETF would include participants from the smaller communities, from education, and from industry to ensure that all of the key players have input on the tasks necessary.

3.4 Mentoring

While the oversight of the CETF would provide the ability to connect the communities together, a more direct method of connecting them together is needed. This could be served through mentoring, and is the key to ensuring the overall success of the system. Mentoring comes in many forms, and some of the communities do directly involve mentoring as part of the model as previously discussed. What is missing from the overall cybersecurity pipeline (or pathways approach) is a more direct, intentional form of mentoring throughout the system. While the current mentoring initiatives are important, a more intentional method is needed. “Research supports a network-based approach to mentoring with a constellation of mentors; that is, an effective mentoring initiative typically draws in people with different skill sets and resources in different stages of their careers (ranging from peer mentors through seasoned professional mentors) and different domains (including college-based mentors and workplace mentors)” (Packard, 2015).

In her discussion, Packard further defines the intentional approach to mentoring as starting with the outcomes you want for students, then consider how mentors can help students achieve them. If you want students to compete in CyberPatriot, then you can determine how a summer camp experience can help to prepare them for it. CyberPatriot incorporates a mentoring aspect into helping students participate effectively in this competition, but doesn’t directly incorporate the intentional method of helping students to bridge the next gap (dual-enrollment, scholarships, college). “Knowing which outcomes you want to achieve will help you decide which mentors you ask to participate and how they can help students in your initiative. For example, mentors can be asked to encourage students by acting as role models, assuring students that they belong in the field, advising students on the pathway toward careers, providing feedback on or strategies for completing academic work, coaching their research process, or acting as a sponsor by recommending students for opportunities” (Packard, 2015).

Many approaches can be used to provide mentoring; we need different approaches to achieve different outcomes (Packard, 2015).

- Events - typically one-time, intensive conferences or seminars.
- Programs - provide mentoring directly to a set of participants through an organized schedule of ongoing meetings or events.
- Practices - initiatives that embed mentoring into teaching and advising to improve the informal mentoring that already occurs in those settings.
- Policies - administrators may choose to develop a policy to increase student access to mentoring events, programs, and practices.

Summer camps would represent the first (Events) approach to mentoring, while competitions such as CyberPatriot would more directly align with the second (Programs) approach. For the Community Based Life Cycle (CBLC) system, multiple mentoring approaches would be used throughout the system as appropriate, with two key considerations:

- Professional mentors: currently used for the CyberPatriot competition, professional mentors are those that can provide career focused mentoring as well as assist with learning specific skills that are used in the professional setting. A CyberPatriot mentor stated, "CyberPatriot is more than just a technical competition. By participating in the program students develop critical thinking and problem solving skills. They learn to work together as a team to accomplish a goal. CyberPatriot is also an excellent way for students to explore a career path and jumpstart their training and education. For adults, it is also a good opportunity to give back to the community as you invest in the lives of students" (https://www.uscyberpatriot.org/about/testimonials).
- Peer mentors: This is, perhaps, the area for greatest success. Packard (2015) directly relates this to STEM Scholar Mentoring Programs, "which improves students' sense of belonging by creating an initial peer group of students with similar academic interests, among other positive outcomes. Scholar programs reinforce the feeling of power that comes with being part of a team; they cultivate a sense of belongingness, which in turn can buffer students in times of struggle and bolster their motivation to persist."

One of the challenges with implementation of a particular mentoring approach is the overall complexity of the cybersecurity ecosystem. It may be worthwhile to design a single approach for implementation into high school with the goal of participating in a security competition, where another approach would be more appropriate for college students completing a cybersecurity degree. The solution would be to implement Cascade Advising, with faculty or employers serving as professional mentors, and peer mentors providing mentorships with to students new to the college/university, or involved with other communities. “In a cascade advising model, faculty or staff supervise upper-level peer mentors, and those peer mentors advise newer students. Cascade advising can provide a vehicle to improve the initial advising for new students and provide a chance to go beyond courses to broaden students' thinking about what is studied in STEM as well as who studies STEM” (Packard, 2015).

4. CONCLUSION

While there is a clear, identifiable need for workers in the cybersecurity workforce, the ability to meet this need is not clear. There are many efforts that are underway to address this workforce shortage, and these are demonstrating positive results. Yet we are still falling short of the needs for the cybersecurity workforce, both now and in the future. The efforts to address this need include many areas:

- Summer camps
- Competitions
- Shared curriculum (Dual enrollment, Articulation)
- Underrepresented populations
- Scholarships
- Mentoring

While this is not meant to be a comprehensive list of many efforts yielding positive results, the need for a more comprehensive method is clear. Developing a Community Based Life Cycle (CBLC) approach to the cybersecurity pipeline will help to serve this need. By using a systems based (life cycle) approach to analyze the cybersecurity ecosystem and determine where potential future cybersecurity workers are “dropping out”, the ability to retain these individuals can be determined.

The first overall approach to determining these areas is through the development of a larger community - a Cyber Education Task Force (CETF) that can work with the communities for the efforts above (summer camps, competitions, etc.) to determine methods for keeping students engaged, or to assist them through the cybersecurity pipeline. These efforts can be aligned through cybersecurity pathways through the use of the NICE Framework to ensure similar objectives. Finally, the use of both professional and peer mentoring is the key to successful implementation. Through the use of a Cascade Advising method, where professional mentors advise and oversee peer mentors, the ability of these peer mentors to advise newer students or assist students participating in summer camps, competitions, and other areas will help to provide more direction for these earlier students and generate a better sense of belonging. This will help to retain more students as they move toward their cybersecurity career.

REFERENCES

[1] Burning Glass. (2015). Job Market Intelligence: Cybersecurity Jobs, 2015. Retrieved from https://www.burning-glass.com/research-project/cybersecurity/

[2] Cyberseek (2018). Cybersecurity Supply/Demand Heatmap. Retrieved from https://www.cyberseek.org/heatmap.html

[3] Department of Commerce & Department of Homeland Security. (2017). A Report to the President on Supporting the Grown and Sustainment of the Nation's Cybersecurity Workforce. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/supporting-growth-and-sustainment

[4] Gonzalez, Matthew D. (2015). Building a Cybersecurity Pipeline to Attract, Train, and Retain Women. Business Journal for Entrepreneurs. Vol. 2015 Issue 3, p24

[5] Infosecurity Magazine. (2013, October 15). The Cybersecurity Pipeline. Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-cybersecurity-pipeline/

[6] Harmon, Tim. (2016, September 14). Cyber Security Capture The Flag (CTF): What Is It? Cisco Blogs. Retrieved from https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it

[7] Air Force Association. (2018, October 29). CyberPatriot Breaks Registration Record Again. Retrieved from https://globenewswire.com/news-release/2018/10/29/1638596/0/en/CyberPatriot-Breaks-Registration-Record-Again.html

[8] Air Force Association. (2016, August 2). CyberPatriot Survey Results Released. Retrieved from https://www.prnewswire.com/news-releases/cyberpatriot-survey-results-released-300307831.html

[9] Fink, J., Jenkins, D., & Yanagirura, T. (2017, September). What Happens to Students Who Take Community College "Dual Enrollment" Courses in High School? Community College Rescource Center.

[10] Packard, B. W. (2015). Successful STEM Mentoring Initiatives for Underrepresented Students: A Research-Based Guide for Faculty and Administrator. Stylus Publishing.

[11] Garbee, E. (2017 October 20). The Problem With the "Pipeline." Slate. Retrieved from https://slate.com/technology/2017/10/the-problem-with-the-pipeline-metaphor-in-stem-education.html

[12] Whitman, M. & Mattord, H. (2019). Management of Information Security. 6th Edition. Boston, MA. Cengage.

[13] National Institute of Standards & Technology (2018). NICE Cybersecurity Workforce Framework. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework