Cybersecurity High School Innovations: A Path for Educators to Teach Cybersecurity Courses in their Schools

Marc Dupuis
University of Washington Bothell
Bothell, Washington 98011
marcjd@uw.edu
0000-0002-5303-2511

Robert Honomichl
University of Arizona Tucson
Tuscson, Arizona 85721
rjhonomichl@arizona.edu
0009-0001-0968-2277

Morgan Zantua
City University of Seattle
Seattle, Washington 98121
zantuamorgan@cityu.edu
0000-0002-0235-633X

Jenny Ju
City University of Seattle
Seattle, Washington 98121
jujenny@cityu.edu
0000-0002-0770-3177

Abstract—There remains a significant unmet demand for cybersecurity professionals nationwide. Many solutions have been forwarded, but more are needed. Improving opportunities within higher education institutions is important and a critical component of addressing this unmet need, but may do too little too late for many potential cybersecurity professionals. This paper examines the development of an innovative program designed to address this challenge by providing opportunities to secondary educators of all backgrounds. Participants are given an opportunity to learn about cybersecurity and how to bring what they learn back to their own schools and teach it to their students as a standalone course. The program provided a remote component in preparation for an intensive in-person summer summit where participants were brought together at one or more locations. During that time, they would hear from experts in academia, industry, and the military, as well as have an opportunity to practice what they learned through various hands-on labs and activities. Participants from the first year were invited back the second year for a more challenging and advanced experience. During the third year, first and second year participants were invited back such that there were three levels of participants. This paper reports on the findings of this innovative program and provides recommendations for future iterations of similar programs based on lessons learned.

Keywords—*cybersecurity, secondary education, curriculum, courses*

I. INTRODUCTION

The unmet demand for cybersecurity professionals has been a long-standing problem with an urgent need for solutions [1]. According to Cyber Seek, there were over 660,000 openings for cybersecurity positions in the United States alone in 2023 (cited in [2]). This suggests that existing solutions are inadequate alone and the need for innovative approaches are a must.

In this paper, we discuss the development of an innovative program designed to address this challenge by providing opportunities to secondary educators of all backgrounds. This program is known as CHI, or cybersecurity high school innovations. Participants are given an opportunity to learn about cybersecurity and how to bring what they learn back to their own schools and teach it to their students in a standalone course. Essential to this program was helping participants identify appropriate curriculum and resources to ensure they have every opportunity for success. This paper reports on the findings of this innovative three-year program and provides recommendations for future iterations of similar programs based on lessons learned.

The remainder of this paper is structured as follows. First, we discuss some relevant background research and context critical to the development of this program. Next, we examine the development and design of the program. Then, we consider some of the challenges faced and how they may be overcome in future iterations. The results from this program are discussed next. We then offer some concluding remarks as we look toward the future of cybersecurity education at the secondary level.

II. BACKGROUND

The number of unfilled cybersecurity jobs remains incredibly high, both nationally and internationally [2]. Turnover in certain cybersecurity positions is part of the problem [3], but the problem itself is multifaceted and complex. And while college degrees may be required for approximately 60% of these positions, this also suggests that skills and/or certifications in cybersecurity without degrees is sufficient in 40% of the remaining positions [4].

And given the threat this poses to the security of the organizations and countries in which the need for cybersecurity professionals is not being adequately met, it is important to examine this challenge critically. The development of a variety of cybersecurity courses and programs at the college level may be part of the answer [5]–[7], but how do we engage individuals in the idea of pursuing cybersecurity as a career earlier on? Easier access to meaningful certifications and training may be part of the answer, while engaging younger individuals in cybersecurity curriculum at the secondary level may be another critical part of the answer.

The focus on cybersecurity at the secondary level has been advanced both nationally (e.g., [8]–[10]) and internationally (e.g., [11]–[13]). Part of this may be the impact cybersecurity-related threats pose to teens across the world, including on their quality of life (e.g., teens in Jordan) [12]. Another part of this is due to the labor shortage within cybersecurity. Regardless of the specific reason, cybersecurity programs at the high school level have continued to grow.

The pedagogical approaches used for older students may not engage teenagers that are still trying to figure out their interests and what they may want to pursue later in life; more innovation and engagement may be necessary [13]. Many different approaches have been used, including game-based cybersecurity training [14]. Other approaches can also be effective, such as capture-the-flag type activities [2].

Regardless of the modality chosen to engage younger learners, it is important to make such approaches conducive to those that are new to the field. Ultimately, we want to be welcoming to all learners since cybersecurity is a multi-faceted problem requiring people from different backgrounds to address the many challenges. Far too often the approaches used at all levels of education have dissuaded those traditionally underrepresented in the computing fields from engaging with the curriculum, whether due to pre-existing stereotypes [15] or simply not thinking about what may engage others, such as females [16]–[18]. Therefore, as we decide on the appropriate approach(es) to engage secondary students, we must also consider how different factors may influence individuals differently, including due to differences in gender or ethnic background.

And while our focus in the program we describe here was on having secondary educators learn cybersecurity so that they could then teach a cybersecurity course, often times the ability to incorporate a standalone cybersecurity course may be limited initially. Nonetheless, there are often opportunities to incorporate cybersecurity concepts within existing STEM curriculum [8]. Leveraging existing courses to embed cybersecurity concepts may be particularly advantageous to under-represented and under-served individuals as well [10], especially where resources may be limited with respect to developing standalone courses in cybersecurity.

The challenges described thus far and the need to address them have long been recognized by governmental bodies. In the United States, several hundred institutions of two and four year colleges and universities have been deemed National Centers of Academic Excellence (NCAE) by the National Security Agency (NSA). These NCAEs are charged with identifying innovative approaches to expand the cybersecurity workforce. Part of this innovation has been within the K-12 system by developing high school teachers to instruct complete cybersecurity courses. In 2021, a coalition of ten NCAEs responded to a request for proposals to expand the K-12 cybersecurity teaching capacity in seven [redacted for review] states. The remainder of this paper identifies the development and design of the approach employed, as well as the challenges faced and ideas for future iterations.

III. DEVELOPMENT AND DESIGN

From the on-set the coalition realized the CHI (cybersecurity high school innovations) project required a flexible and repeatable training model, supporting teachers at different technical skill sets, across seven states, in rural and urban communities.

Ten participating NCAE personnel shared work roles: teacher recruitment, content management/curriculum development, instructional delivery, and resource development.

A. Recruitment

Faculty from ten participating universities represented seven states. Each faculty member worked to recruit high school teachers from each of their states. Recruitment for the first year of CHI focused on recruiting high school teachers currently teaching a computer science or cybersecurity course or teachers who could create and offer a cybersecurity course within their high school. Because of the rural demographic of areas in each state, many participants taught various content areas and grade levels, including middle school.

Since continued exposure to curriculum and professional development is critical to the participants' success, recruitment for the second year included both a new and continuing cohort. The recruitment for the new cohort followed the same model as during the first year, and recruitment for continuing participants was done by contacting participants who participated in the previous year.

In its third year, the program expanded significantly. It now offers three different curriculum tracks to support both new and returning participants. This expansion, coupled with the project's presence at national conferences, allowed for a national recruitment drive. The aim was to provide more teachers with the opportunity to develop cybersecurity courses, thereby broadening the project's reach and impact. Table I identifies the increasing breadth of geographic participation for each year of the program.

TABLE I. Distribution of Participants by Year of CHI Program

State	Year One	Year Two	Year Three
Arizona			2
Colorado	10	11	6
Connecticut			1
Georgia			2

State	Year One	Year Two	Year Three
Idaho	4	3	2
Nebraska			2
North Carolina			1
North Dakota	2		8
Oregon		1	
South Dakota	3	7	8
Washington	5	7	5
Montana		1	
Illinois		1	
South Carolina			4
Tennessee			1
Utah			1
Totals	**24**	**31**	**44**

B. Curriculum Development

An essential component of the CHI project was the curriculum that would be delivered to the participants. The curriculum developed must provide the opportunity to create new knowledge, build on current participant knowledge, and provide material and resources to integrate into their classrooms. As the CHI project spanned three years, the curriculum was developed in a tiered fashion so that participants would have the ability to return throughout the three-year project.

The first year of the CHI project focused on a curriculum designed to introduce cybersecurity topics and provide the foundation for the participants to add a cybersecurity course as an offering for students. Ideas for topics within the curriculum were developed using the High School Cybersecurity Curriculum Guidelines' Big Eight ideas. Information, lessons, activities, and resources addressing these eight areas were put together using various open-source curriculum developed through other cybersecurity education initiatives. Along with this material, the security team at [redacted for review] developed an additional curriculum focused on the Mitre Kill Chain. Hands-on activities, a key component of the curriculum, were designed to coincide with these topics and would be delivered during the summer summit.

The second year of the CHI project included another cohort of participants who would be working through the introduction to cybersecurity curriculum. Overall, this cohort's curriculum was similar to the previous year's curriculum, with some minor modifications. The second year, however, introduced another curriculum track for returning participants. The second-year curriculum was designed around preparing the participants with the knowledge and material to teach a Security+ course and possibly take the certification exam. The curriculum developed for the second year was a combination of material faculty had used within their courses and the integration of CISCO's Skills for All, a significant addition that brought industry relevance to the curriculum.

The third year of the CHI project not only refined the curriculum from the previous year but also offered a third curriculum track for both returning participants and anyone interested in cybersecurity competitions. The refinement of the curriculum primarily impacted the first-year curriculum and was done based on the feedback of the participants. Many participants had addressed that although there was a lot of great material, they were not as comfortable packaging it into a course. This led to the integration of a fully designed introduction to cybersecurity course that could be easily integrated into a classroom in its entirety or using selected modules.

The year two curriculum had slight refinements. The addition of the third-year curriculum focused on cybersecurity competitions that could be used as supplemental activities within a course or for the development of an after-school competition club.

C. Instructional Delivery

The instructional delivery for each year of the CHI project followed the same format, with a few slight modifications each year. It consisted of five weeks of online instruction and a four-day summer summit. The five-week online portion of the professional development consisted of two-hour online synchronous sessions twice a week from the middle of June to the middle of July. They were also recorded and made available online to provide access for review of the information covered during the synchronous sessions. Course material and resources were disseminated to the participants using a combination of Google Drive and Desire2Learn (D2L). Participants completed and submitted weekly assignments to both of these platforms. The four-day summer summit allowed instructional faculty to provide hands-on cybersecurity labs that reinforced the material covered during the synchronous sessions.

As each year added another curriculum track, the instructional delivery remained relatively the same except for the program's third year. The most significant changes during this time were the learning management system and changes to the summer summit. In previous years, the material for the online portion was hosted through a combination of Google Drive and D2L. D2L created some challenges for both the participants and the instructional team.

To use D2L, the participants needed another account; while the instructional team was waiting for these accounts to be made, they utilized Google Drive and then transitioned to D2L in later weeks; this created some confusion for the participants. The instructional team had to have all the material in the LMS and had little control over making changes as the course continued.

The last challenge was that the participants no longer had easy access to the materials after the professional development opportunity. The LMS challenges from the program's first two years were resolved through a community D2L site in year three. This site allowed participants to sign in using their personal email accounts, gave complete control of content to the instructors, and allowed them to access the site whenever they wanted after the professional development opportunity. This version of the LMS also allows the course to be reused, exported, and enabled new participants to participate.

The other major change to the instructional delivery was the third-year summer summit. During the first two years of the program, the summer summit was held in one location. To help emphasize the ability to replicate this model of professional development, the summer summit was held in three locations to help attract regional participants. This did create some challenges that will be discussed in a later section.

D. Career Focus

Consistent throughout the program was an emphasis on integrating a career focus into the classroom. The American School Counselor Association recommends a 1:250 counselor to student ratio [19]. No high school participating in CHI achieved that ratio; there were a few rural schools sharing counselors between multiple schools. The CHI grant included two strategies to bring relevant cybersecurity career education into the classroom. Teachers each year received access to an online statistically validated career assessment with reports connected to ONET Online. Grant funding provided teachers with codes to administer the assessment in their classes, enabling teachers and students to discuss technology career opportunities and how the curriculum directly related to what they were learning.

A feature of the summer summit design provided teachers with access to industry professionals and opportunities to visit workplace settings to see, firsthand, what the world of cybersecurity work "looked like" to better prepare their students for employment after high school. The summit starts with a visit to an industry site to set the tone for the participants. In the first and second years, [redacted for review] opened their [redacted for review] facility for tours of the manufacturing plant and threat intelligence units. In the third year, the CHI team expanded the summer summit to three locations. [redacted for review]

Input from industry professionals evolved over the three years. During COVID in 2022 speakers presented synchronously online throughout the summer summit. In the second and third years designers moved to an evening dinner with a panel of industry professionals who shared their journey into cybersecurity and what they look for in new hires.

IV. CHALLENGES

A. Curriculum Development

During the first two years, participants resided in seven different states. Many of these states do not have current computer science or cybersecurity standards. For this reason, it can be a barrier for the teachers to be able to offer a course. Requirements to teach specific topics or be CTE certified vary from state to state or even within a state. The curriculum development had to rely on established curriculum aligned with national standards and allow teachers to decide what topics they would use within their courses. The background knowledge and experience of the participants also created a challenge. During the program's first two years, the amount of curriculum and resources from multiple sources created an overwhelming environment where the participants had to try to formulate what and how they would teach the material. There was a need to provide them with a holistic curriculum that could be taught in its entirety or in modules, depending on their course structure.

B. Learning Management System

As previously discussed, the original LMS employed posed challenges for participants and instructors. The lack of customization for the instructional team hindered their ability to tailor the course based on the participants' needs. This is necessary as the background of the participants was unknown when the course was designed. For the participants, the need to switch platforms during the online sessions created confusion. Likewise, the inability to access the material after the professional development impacted the ability to access and review materials while integrating the concepts into their classroom.

C. Summer Summit Remote Locations

The summer summit was held at three locations during the third year to increase regional participation and work on the replicable model. In this method, most of the participants were at the locations with the instructional team, while the other two sites connected through Zoom. This created challenges as the host site was in the Pacific time zone, and the other two were in the Mountain and Central time zones. Other challenges included faculty resources at the remote locations and standardized equipment.

V. RESULTS AND DISCUSSION

Participants were asked to provide feedback to us on a daily basis throughout the intensive summer summit portion of the program. In this section, we discuss some of the feedback received and how it was addressed.

A. CHI Program: Year 1

During the first year of the program, there was only one level available to participants. Thus, all participants were exposed to an introductory cybersecurity curriculum. As often happens when there are learners of various backgrounds and prior experience being exposed to a single unified curriculum, there are several participants that felt the pace was too quick at times. For example, one participant commented on the use of Wireshark: "Have someone walk you through the activity." For several of the labs used during the summer summit, there were detailed instructions and at times, video demonstrations. However, some participants indicated that it would be helpful for the instructor to do a walk-through prior to the class attempting the lab activity. This was a fair point and something we tried to incorporate in the remainder of the summer summit during year one, but more so during years two and three.

Another participant also indicated some challenges with the level of the curriculum and the pace of the delivery: "More time on each subject. It feels like we're going over a whole lot without much time to process." This participant was not alone in expressing this sentiment. Other individuals also noted "Being able to have time to work through everything we're using" and "It will be great to have time to do the labs as a team." During years two and three, we worked diligently to identify which labs and resources would be most beneficial to them in the limited time we had with them. Additionally, in the third year of the program, we sequenced the content and limited the labs to those that were most engaging and straightforward for participants in the introductory curriculum group.

Additionally, several participants wanted less time 'talking' about the content and more time spent working on labs, activities, and exploring curriculum options. For example, one participant noted: "More hands on or activities that involve movement and interaction from participants." Again, a similar sentiment was expressed by others as well. As before, we changed our approach during years two and three. It was more important for participants to have meaningful time on fewer labs and activities than being exposed to a large variety of them. While we made sure they had a large variety of curriculum choices available to them to employ in their own classrooms, we scaled back what we were doing with the participants themselves to allow for more time on each lab and activity with less 'lecture' and more hands-on engagement with the material.

Finally, with any type of program there will be logistical concerns raised. While some meals were provided, such as some breakfast items, participants were tasked with finding lunch on their own. Some participants enjoyed this as it provided them with an opportunity to try different food places in a city they may have been visiting for the first time, while other participants would have preferred to have lunch taken care of for them and on-site: "Having everything here in one place. Not having to go find lunch." During years two and three, breakfast and lunch were provided on-site. The food choices themselves also varied from day-to-day, which the participants seemed to appreciate.

B. CHI Program: Year 2

The feedback we received during year two reflected some of the improvements we made based on feedback from year one. For example, participants appreciated having the food on-site. Along with this though, some participants since it was on-site the lunch break could be shorter: "...could shorten lunch to 30 minutes since lunch is provided." Another participant noted that for breakfast at least, some additional variety would have been nice: "Some additional variety at breakfast would have been good-starch and carb spikes and crashes compounded jet lag. Mid-morning fruit trays were very welcome."

And while some of the content was scaled back for year two, some of it remained too advanced in some respects: "some of the lessons may be too advanced for a student with little to no networking/programming experience." In other words, they were not only thinking about their own experience with the curriculum, but how that might translate to their own students. Another participant noted that the curriculum was good, but due to some connectivity issues we experienced during a couple of the labs, they had a difficult time envisioning conducting some of those labs in their own classroom. Sentiments around labs were a common theme given their central role to most any cybersecurity curriculum: "Would love to spend more time next year learning how to setup and conduct labs."

The logistical issue of labs in high school classrooms was a prevailing theme. This included the aforementioned comment regarding setting labs up in a high school, but also the type of equipment needed, its cost, and perhaps most commonly, questions around obtaining permissions from administrators for their students to conduct ethical hacking in a protected environment. Most school administrators do not understand the benefits, safeguards in place, and how what we are teaching students in a controlled environment regarding 'hacking' is information that is widely available online in an uncontrolled environment.

Other participants were quite enthusiastic about their overall experience: "The hands on activities were great. The learning before we came was useful. Breakfasts and lunches were excellent." Another participant noted: "I enjoyed the online learning and the visit to [redacted for review]. I felt we learned a lot in the physical visit for sure!"

Similar comments were made regarding the more advanced level of curriculum that focused on Security+: "I liked the printed labs as they will work as lesson plans for me. The presenters were very good as well." Likewise, a participant recognized some of the work that went into the lessons learned from year one and how it was applied during year two for both cohorts: "The slower pace was hugely beneficial as well as 'optional' help as we worked through labs."

Other comments reflected the need to continuously be reflective and improve upon our delivery: “There could be better division between labs and direct teaching segments” and “Focus on what teachers need as far as technology support.” Overall, it appeared the improvements we made from year one to year two were largely successful.

C. CHI Program: Year 3

The primary feedback we sought during year three involved the implementation of cybersecurity courses by participants in the program. After all, if the program does not result in cybersecurity courses being taught by the participants then it would be difficult to consider it a success since that was the primary purpose of the program.

Out of 16 participants from year one that completed the survey, 15 indicated that they had taught one or more cybersecurity courses, while the remaining participant indicated they had incorporated five cybersecurity lessons into their other classes and taught them multiple times. A total of over 50 cybersecurity courses have been taught to high school students from the 15 participants that have taught a cybersecurity course.

Beyond direct feedback, we did further revise the introductory cybersecurity curriculum for year three participants. In particular, we re-sequenced the lessons and labs/activities for the in-person summer summit to help better ease them into the more challenging curriculum. For example, instead of leaving social engineering until the end of the summer summit, we explored it during day one given its wide applicability and the generally non-technical nature of the content. This appeared to engage the participants from the very beginning; this carried over until the end. The labs/activities that were more convoluted in some respects were omitted. Overall, we believe this resulted in a smoother experience for both participants and instructors alike.

VI. CONCLUSION

The CHI program was a three-year project designed to teach secondary educators so that they may bring their newfound knowledge and skills back to their own schools to teach cybersecurity courses of their own. While several challenges were faced and improvements made based on feedback from participants and our own internal discussions and reflections, the evidence indicates the program was a success. Participants have been teaching cybersecurity courses in their high schools, including using the curriculum that was made available to them through the program. Current plans are in place to continue offering this program to secondary educators so that additional educators and their students may benefit from it.

What is more difficult to know is how many of those courses will translate to careers in cybersecurity. Regardless, the results suggest that such a program can be successful, both regionally and nationally. And while challenges remain, including schools providing opportunities for such courses to be taught in what is often an already full schedule, there is hope that some of these challenges will begin to fade as governmental mandates requiring cybersecurity in the curriculum become more commonplace. Caution must also be exercised though as often times the schools that are able to offer such courses may be those that have the most resources, which could serve to further exacerbate issues around equity and access, as well as limit the potential for a diverse cybersecurity workforce. And a diverse cybersecurity workforce is critical in our ability to defend against the multitude of threats [20].

REFERENCES

[1] S. Furnell, P. Fischer, and A. Finch, “Can’t get the staff? the growing need for cyber-security skills,” *Computer Fraud & Security*, vol. 2017, no. 2, p. 5–10, 2017.

[2] C. Beauchamp, “A mixed-method study exploring student motivation for participating in cybersecurity CTF competitions,” *CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL*, 2024.

[3] B. Adetoye and R. C.-w. Fong, “Building a resilient cybersecurity workforce: a multidisciplinary solution to the problem of high turnover of cybersecurity analysts,” in *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability*, London, September 2022, p. 61–87, Springer, 2023.

[4] J. Marquardson and A. Elnoshokaty, “Skills, certifications, or degrees: What companies demand for entry-level cybersecurity jobs.,” *Information Systems Education Journal*, vol. 18, no. 1, p. 22–28, 2020.

[5] B. K. Payne, W. He, C. Wang, D. E. Wittkower, and H. Wu, “Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course,” *Journal of Information Systems Education*, vol. 32, no. 2, p. 1334, 2021.

[6] M. Dupuis, “Cyber security for everyone: An introductory course for non-technical majors,” *Journal of Cybersecurity Education, Research, and Practice*, vol. 2017, no. 1, Article 3, p. 17, 2017.

[7] M. Khader, M. Karam, and H. Fares, “Cybersecurity awareness framework for academia,” *Information*, vol. 12, p. 417, Oct. 2021.

[8] L. D. Page, M. Mekni, and E. A. Radday, “Incorporating cybersecurity concepts in Connecticut’s high school stem education,” *Journal of Computing Sciences in Colleges*, vol. 38, no. 8, p. 173–187, 2023.

[9] W. J. Triplett, “Addressing cybersecurity challenges in education,” *International Journal of STEM Education for Sustainability*, vol. 3, no. 1, p. 47–67, 2023.

[10] T. Williams and J. Daugherty, “The state of cybersecurity programs in high schools: A case study analysis of their development, sustainment, and inclusiveness,” in *Proceedings of the 57th Hawaii International Conference on System Sciences*, (Honolulu, HI, USA), p. 10, 2024.

[11] A. W. Fazil, M. Hakimi, S. Sajid, M. M. Quchi, and K. Q. Khaliqyar, “Enhancing internet safety and cybersecurity awareness among secondary and high school students in afghanistan: A case study of badakhshan province,” *American Journal of Education and Technology*, vol. 2, no. 4, p. 50–61, 2023.

[12] A. M. R. AlSobeh, I. AlAzzam, A. M. J. Shatnawi, and I. Khasawneh, “Cybersecurity awareness factors among adolescents in jordan: Mediation effect of cyber scale and personal factors,” *Online Journal of Communication and Media Technologies*, vol. 13, no. 2, p. e202312, 2023.

[13] B. Jerman Blažič and A. Jerman Blažič, “Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity,” *Sustainability*, vol. 14, no. 8, p. 4763, 2022.

[14] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, “Game based cybersecurity training for high school students,” in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, p. 68–73, 2018.

[15] S. Cheryan, A. Master, and A. N. Meltzoff, “Cultural stereotypes as gatekeepers: increasing girls’ interest in computer science and engineering by diversifying stereotypes,” *Frontiers in psychology*, vol. 6, 2015.

[16] J. S. Eccles and M.-T. Wang, “What motivates females and males to pursue careers in mathematics and science?,” *International Journal of Behavioral Development*, vol. 40, no. 2, p. 100–106, 2016.

[17] J. C. Prey and A. C. Weaver, “Fostering gender diversity in computing,” Computer, vol. 46, p. 22–23, Mar. 2013.

[18] J. Wang, H. Hong, J. Ravitz, and M. Ivory, “Gender differences in factors influencing pursuit of computer science and related fields,” in *Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education*, p. 117–122, ACM, 2015.

[19] A. S. C. Association, *School and District Administrators and the School Counselor Role*. ASCA Research Report, 2023.

[20] M. Namukasa, C. Ficke, and I. Piasecki, “Understanding how to diversify the cybersecurity workforce: A qualitative analysis,” *Journal of Cybersecurity Education, Research and Practice*, vol. 2023, no. 2, p. 4, 2023.