The State of Cybersecurity Programs in High Schools: A Case Study Analysis of Their Development, Sustainment, and Inclusiveness

Tania Williams
University of Alabama in Huntsville
tania.williams@uah.edu

Jenny L. Daugherty, Ph.D.
DARK Enterprises, Inc.
jenny.daugherty@darkenterprisesinc.com

Abstract

As the field of cybersecurity evolves, so does the field of cybersecurity education. Formal instruction of cybersecurity-related concepts has migrated down to the secondary level, with high schools around the country looking for ways to integrate cybersecurity programs into their existing student offerings. This paper provides the findings of case study research at four high school cybersecurity programs in order to understand how these programs were developed and sustained and their inclusiveness of students from underrepresented, vulnerable, and underserved populations. It provides a brief background of cybersecurity education at the secondary level, describes the methodology used, and provides data analysis and results. Included are recommendations for further study.

Keywords: cybersecurity education, high school, secondary, inclusiveness.

1. Introduction and Motivation

To meet the growing need for cybersecurity experts, high schools across the nation are increasing their emphasis on cybersecurity topics. While the topics vary from school to school, cybersecurity programs are beginning to emerge. This results in the need to make sure students across the nation have access to these resources, including students from underrepresented, vulnerable, and underserved communities. This paper provides the results of an exploratory multiple case study, which examined high school programs to better understand the landscape of cybersecurity education in existing high school cybersecurity programs.

A large cybersecurity workforce is needed to support industry and to provide for national security; however, the demand for workers outstrips the supply (Locasto et al., 2011). This need for cybersecurity workers is evidenced through sites like CyberSeek and through workforce studies by organizations like (ISC)2 (*Cybersecurity Supply And Demand Heat Map*, n.d.; *ISC2 Cybersecurity Workforce Study, 2021*, 2021). Employers, academic leaders, and government officials "must look to construct a road map to provide flexibility in terms of content, delivery mechanism, and education financing for cybersecurity students" (Hoffman et al., 2012, p. 38).

The U.S. has been building the cybersecurity workforce from the top down; early efforts focused on building graduate programs in cybersecurity, followed by baccalaureate and then associate degree programs. Recently K-12 courses and programs have emerged to provide earlier entry points into cybersecurity. For example, the K-12 environment was listed by the Joint Task Force on Cybersecurity Education (2018), as a space to raise user awareness and prepare students to enter post-secondary cybersecurity studies. Efforts to engage students on this path include integrating cybersecurity into existing STEM content, building engagement through summer camps, creating various national-level cybersecurity-related clubs and competitions that target middle school and high school students, and providing dedicated cybersecurity courses (*About GenCyber*, n.d.; *CyberPatriot XII*, n.d.; Ileleji & Joseph, 2018). Also, to help build this path, groups have provided guidelines and standards to outline what should be taught at the high school level (*High School Cybersecurity Curriculum Guidelines*, n.d.; *K-12 Cybersecurity Learning Standards | Cyber.Org*, n.d.).

Schools have used these resources to create STEM-related high schools that include a cybersecurity focus. Similarly, U.S. government agencies are taking an interest in formal cybersecurity education, with the Army piloting a four-year curriculum for use in high schools across the nation (*U.S. Army JROTC Cyber Pilot*, n.d.). As these curriculum programs expand, there is also a push for students with no existing cybersecurity programs to have access to cybersecurity education. For example, the Centers of Academic Excellence (CAE) partnered to offer free curriculum and a free virtual course to students lacking access (*K-12 Pathway Program: RING | CAE Community*, n.d.).

URI: https://hdl.handle.net/10125/107246
978-0-9981331-7-1

As cybersecurity education at the K-12 level forms and grows from clubs and competitions to formal classes and multiple course programs, researchers can **examine this progression to determine relevant features, factors, or issues that apply to the development and sustainment of such programs** (Myers, 2013).

In order to better understand the development and sustainment of these formalized high school programs, this research looked at four high school cybersecurity programs to determine how these programs developed and are sustained, including how they attempt to ensure students receive equal access to resources and instruction. The goal of the research is the answer the following research questions:

How do high schools develop and sustain cybersecurity programs?

How do high schools prioritize making the cybersecurity programs inclusive to students from underrepresented, vulnerable, and underserved communities?

The paper provides background regarding the current state of cybersecurity programs at the high school level and the associated constructs, and it describes the methodology used for the case studies, including data collection and analysis techniques. Finally, the paper discusses findings related to program development, sustainment, and inclusiveness and provides findings and recommendations for future research.

2. Background

CyberSupply (Dark Enterprises, n.d.) collected publicly available data from 42.5% of public high schools in the US from 11 states concerning **availability** of cyber courses/pathways and **access** to those courses. This included 5,915 schools and 192 CTE centers. **Availability** data reflected what school websites report as available courses. This did not mean that the courses were actually offered. Availability was dependent upon student interest and teachers. **Access** was a function of the number of courses available and the number of times in a school day/year the courses are offered. For example, if one course was offered at a school, the entire school population would not be able to take the course.

CyberSupply reports that only 16% of the schools in the sample had a cybersecurity course available. And 3.7% of students had access to those cybersecurity courses. The research data also indicated that ~657 public high schools in the U.S. currently had sufficient CS, IT and a minimum of 2 cybersecurity courses to make a cybersecurity pathway. This does not mean that these schools/CTE centers *actually had* a cybersecurity pathway. Rather, the numbers simply report the number of schools that appeared to have enough courses to make a pathway if the school wanted to do so.

Another important finding pertaining to access was that twice as many Non-Title 1 schools than Title 1 schools offered a cybersecurity course. And 16% more Non-Title 1 schools had computing/IT courses or gateway-to-cybersecurity courses than Title 1 schools. Generally speaking, the most disadvantaged students are those in Title I, small schools.

2.1. Need for cybersecurity education

Cybersecurity education initiatives are supported by the departments of education, energy, homeland security, and labor. Additionally, the National Security Agency and the National Science Foundation have their own efforts (Herold, 2017). The need for high school cybersecurity courses was further alluded to in Executive Order 13870, which instituted a program to begin recognizing secondary school educators who are impactful in the area of cybersecurity (*America's Cybersecurity Workforce*, 2019).

Researchers report the need for cybersecurity education at the secondary level. The lack of exposure to cybersecurity in high school negatively impacts the student seeing cybersecurity as a career choice. A student's career interest starting in high school is a strong predictor of the student's career interest when leaving high school (Sadler et al., 2012). Additionally, grades 7 through 9 are a key period of time for influencing a STEM-related career interest (Blotnicky et al., 2018). However, if students are not exposed to the field of cybersecurity, how will they consider it as a career? Ileleji and Joseph (2018) examine high school students' interest in cybersecurity and found that it had the lowest rating of the six STEM disciplines studied in the research. They attribute this to students having no awareness of the field. This assertion is supported by Amo et al. (2019), who concluded that targeted cybersecurity engagement with pre-teenagers and teenagers can increase interest in the field.

2.2. Cybersecurity courses

Despite the recent focus on cybersecurity education, Herold (2017) describes the scale and quality of cybersecurity education in high schools as spotty, with offerings being decided at the state and district level (further supported by the CyberSupply project). These findings reiterate the need to understand how cybersecurity programs are developed and sustained at the secondary level and how they meet the needs of their student populations.

2.3. Characteristics of a program

For this study, the concept of a program is aligned to the one used to define tech-prep programs. This means that the program should have a clear curricular structure with substance and focus instead of a "smorgasbord of courses without focus" (Frainer, 1996). Barrette (n.d.) differentiates between a course and a program by the level of preparation and integration associated with it. A program's associated outcome is the student's learning across the courses. This is supported by the definition provided in the Perkins Act, which also requires competence through a sequential course of study (Hawkins, 1990).

3. Methodology

The research focused on how and why high schools develop and sustain cybersecurity programs, as well as how these programs meet the needs of underrepresented, vulnerable, and underserved communities; therefore, organizational theories were considered. However, the focus was on the process of program implementation rather than how to make the program more effective (Yin, 2014, pp. 39&40).

A multiple-case design best suited the purpose of the study as it allowed for embedded units of analysis (Yin, 2014, p. 50). By examining the embedded units, program development, program sustainment, and student characteristics, using multiple high schools, the study allowed for literal replication within each case study (Yin, 2014, p. 63). Additionally, the use of multiple cases was considered more compelling and robust (Yin, 2014, p. 57). Therefore, in order to determine the number of cases, the researchers met with other researchers, and through group discussion, determined that four cases were an adequate number of cases. The group also determined that the cases must have cybersecurity programs (multiple courses), with the inclusion of at least one course that focused on cybersecurity specific topics, such as topics of data security, access control, and legal and ethical issues. Additionally, the team decided to include cases that were diverse (Pettigrew, 1990). This was further defined by the team as being geographically diverse, varied in school and program structure, and having varied sizes.

Due to the limited number of high schools with cybersecurity programs, the pool of candidate sites was limited. The researchers identified 11 possible sites that meet the criteria. These candidate sites were determined using recommendations from team members and parties active in cybersecurity high school education.

The boundaries within each site location were also defined. Considerations for these boundaries comprised of the people who should be included, which services should be considered, the time boundaries, the types of evidence to collect, and the priorities of data collection. The researchers identified the following roles to be included in the study: school administrators and counselors, cybersecurity instructors, students, and parents and active stakeholders. The study was limited to the development, sustainment, and student characteristics of the cybersecurity program, with a limit of one day per site. The researchers conducted interviews and collected physical artifacts, such as a course syllabus or course descriptions. The researchers also relied on direct observation of the school's facilities. The researchers prioritized data related to program development, sustainment, and student characteristics (Yin, 2014, pp. 33-36 & 110-118).

The researchers developed a case study protocol, which included the data collection instruments. This protocol consisted of an overview of the case study, the data collection procedures, the data collection questions, and a guide for the case study report. This protocol was a way to increase reliability (Yin, 2014, p. 84).

The data collection questions centered on the high school cybersecurity program's development, sustainment, and student characteristics. It included questions to be asked of specific interviewees, as well as questions asked of the individual case, asked of the pattern of findings across multiple cases, asked of the entire study, and asked to determine recommendations and conclusions (levels II-V) (Yin, 2014, pp. 84 & 90). The guide for the case study report consisted of audience considerations, how data was to be used and presented, and bibliographical information (Yin, 2014, pp. 84-86).

In addition to creating a case study protocol, the researchers utilized a case study database. This database included: field notes, case study documents, tabular material (data counts), and narrative compilations. The use of this database increased the reliability of the study (Yin, 2014, p. 124). Also, to assist with reliability, the researchers maintained a chain of evidence. This included a description of the circumstances, including the time and place of the interview, documentation showing consistency with the case study protocol, and a link between the protocol questions and original study questions (Yin, 2014, p. 128).

As there were multiple sources of evidence, the researchers triangulated the data to measure the convergence of evidence associated with the same phenomenon at each site. This was to strengthen construct validity (Yin, 2014, p.121).

The researchers utilized a computer-assisted tool (ATLAS.ti) to code and analyze the data, with the use of a descriptive framework that aligned with the created data collection instruments (Yin, 2014, p. 140). As for an analytical strategy, the researchers pattern matched; building toward explaining how and why something happened (Yin, 2014, p. 147). Cross-case synthesis was also used, treating each individual site as a separate study (Yin, 2014, p. 165).

4. Data analysis

To better understand how high school cybersecurity programs are developed and sustained, the researchers used ATLAS.ti to code and analyze the transcripts from four school visits. The data set consisted of 29 interviews from four different states having cybersecurity programs: Troy High School in California, Spotsylvania High School in Virginia, and CyberSecurity and Innovation (iCSI) in Texas. One school wished to have its name and state withheld and will be referred to as Program A. Table 1 provides a breakdown of the interviews by school.

Table 1. Distribution of interviewees

School	Role	# of Interviewees
Troy	Administrators and / or counselors	2
	Teachers	1
	Students	3
	Community Members	1
Spotsylvania	Administrators and / or counselors	3
	Teachers	1
	Students	4
	Community Members	1
A	Administrators and / or counselors	1
	Teachers	1
	Students	6
	Community Members	0
iCSI	Administrators and / or counselors	1
	Teachers	1
	Students	1
	Community Members	2

In the interviews, the participants answered open-ended questions detailing how their affiliated high school's cybersecurity program was created and is sustained, as well as unique characteristics about the program's student population.

4.1 Approach

4.1.1. Constant Comparative Coding. Open coding, which is using close examination of data to name and categorize phenomena, involves breaking the information down into parts (Smit, 2002). Using the constant comparative method of simultaneous coding and analysis outlined by Glaser and Strauss, the researchers compared new data sets with the older ones, constantly adjusting the constructs as each data set was analyzed (O'Reilly et al., 2012). This resulted in continuous reflection and adjustment of coding of the data categories, ensuring fit and relevance (O'Reilly et al., 2012). For example, in trying to capture the methods of roadblocks to program sustainment, the researchers often had to add or rename code types as they progressed through the data. Additionally, as the coding progressed, it became important that the researchers capture any problem areas noted by the interviewees. This resulted in the researchers returning to previous data sets to capture that information. This happened again as the researchers noted that several interviewees discussed student recruitment strategies. The researchers decided this was also something they wanted to capture in their analysis, and they returned to previous data sets to code this information.

Using ATLAS.ti, the researchers attached labels to segments of text, usually sentences or paragraphs; however, occasionally, single words or word groups were sufficient (Smit, 2002). As the coding progressed, certain concepts and categories emerged. In the end, the efforts resulted in 3 overarching code groups (creation, description, and sustainment), with program creation having 4 subgroups, program description having 9 subgroups, and sustainment having 3 subgroups. The study also resulted in 276 instances of coding across the 29 interviews (see Figure 1). The average number of codes per interview was 9.5, with the highest number of codes in a document being 25 and the lowest being 2.

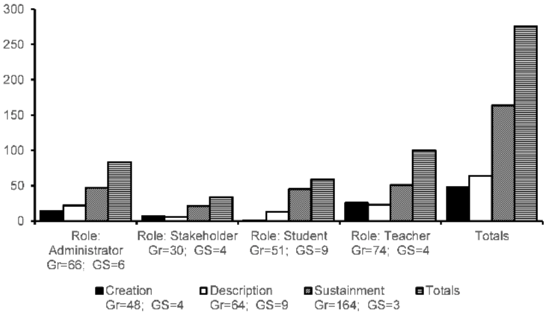

Figure 1. Codes by interviewee's role

Next, the researchers put similar concepts into groups (O'Reilly et al., 2012). For instance, the research team noted 3 different factors related to sustainment: student recruitment, other sustainment factors, and roadblocks to sustainment. Creation and description groupings were similarly broken down. This axial coding allowed the team to make sense of the data and detect patterns.

4.1.2. Theoretical Sampling and Saturation. As the number of interviews was constrained by the availability of the participants at the location, theoretical sampling as means to guide the next data source was limited. Instead of being naturally led "from participant to participant as new conceptual ideas are captured," the researchers used the available participants as a means to see the theory develop. In the spirit of theoretical sampling, the research team did allow the available data set to guide and shape what it was searching for and why (O'Reilly et al., 2012). The data set of four sites defined the theoretical saturation of the analysis, as no other data sets were sought.

Working off the existing open codes, an insight to the data's meaning began to emerge (O'Reilly et al., 2012). As the focus of the research was the creation and sustainment of high school cybersecurity programs and understanding how the programs meet the needs of underrepresented, vulnerable, and underserved communities, patterns related to this research focus were identified and categorized.

5. Results

5.1. Program descriptions

The sites located in four different states varied in school type, cyber program type, and years of existence. Although this was partially reflective of differences in school budgets and local resources, the focus of the study was on the development and sustainment of the cybersecurity program at each school. When those factors arose as impacting the development or sustainment of the cybersecurity program, they were noted. Table 2 provides an overview of each program.

Table 2. Distribution of interviewees

School	Type	Cyber program	Yrs
iCSI	CTE center	CTE	1
Program A	Magnet	Cyber, engineering, and tech focus / cyber integrated into core courses	2
Spotsylvania H.S.	Rural public	CTE	3+
Troy H.S.	Magnet	CTE	3+

5.2. Program creation

The first part of the first research question focused on program creation. The schools were established from action at the state or district levels, which impacted their budgets and access to resources. Program A was created in 2018, when the governor of the state signed legislation creating the school, and in 2020 the school opened its doors to students in the middle of the COVID pandemic. Troy High School and Spotsylvania High School were created at the district levels. For Spotsylvania High School, the district created the program at five of their schools and recruited interested existing teachers to develop the curriculum and teach the courses. However, Troy High School was established upon the suggestion of the teacher as a means to increase school recruitment and build upon the interest in cybersecurity that already existed through cybersecurity competitions. iCSI grew out of existing programs that also originated from participation in cybersecurity competitions, allowing the district to consolidate instructional resources and provide a centralized and isolated network for student instruction.

When establishing a cybersecurity program at the K-12 level, several roadblocks emerged. All listed factors, such as fear of students' actions, lack of money, lack of teacher resources, lack of teacher training, and a lack of understanding of cybersecurity careers as roadblocks to program creation (see Figure 2).

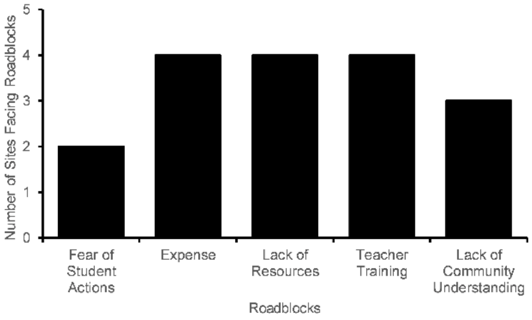

Figure 2. Roadblocks to program creation

Two sites mentioned fear of student actions on the schools' networks as a roadblock to program creation. As one stakeholder described, "One of the issues that we have nowadays is some people are so scared of the term virus or malware or hacking or things like that. And so, what they actually do is hinder a lot of our students from progressing and learning." Another recalled having issues accessing VM images because IT personnel restricted their use. The schools mentioned that educating stakeholders and putting students on isolated networks (either a physical network or using a cyber range) were ways of overcoming this roadblock to creation.

Another barrier was budgetary concerns, specifically, the expense of creating a cybersecurity program. One volunteer mentor mentioned spending money out-of-pocket for resources. He noted, "I've dumped about $10,000 of my own funding into it [the program], just because it's a passion." A teacher at a different location mentioned having to find funding for monitors. Another teacher, who saw the program grow from a cybersecurity competition, noted, "The school network was not good enough. We had to compete at one of the kid's houses." The need for a network (either physical or virtual) was noted as a roadblock among three of the sites, with the remaining site having access to a state-sponsored cyber range.

One of the administrators expressed concerns about finding space to even house the program, noting the district had to invest in new facilities at a considerable expense. To overcome funding and space concerns, the sites reported strategies ranging from relying on equipment and monetary donations, soliciting funds through legislation or grants, or even using school bonds for new facilities.

In addition to finding funds for needed equipment and space, sites also noted the difficulty in finding teaching resources. Teachers at all four sites noted the lack of existing cybersecurity curricular resources at the creation point of their programs. They reported patching together teaching materials from GenCyber camps and CyberPatiot resources. Many reported making their own learning modules for students to use, with all four teachers trying to align with industry certifications to varying degrees. One teacher spoke of writing all of the curriculum and another created a pacing guide.

Not only do teachers need the resources to teach, the administrators and teachers at the sites stressed the need for trained cybersecurity teachers. Among the four sites, two schools had teachers with computer science or IT backgrounds. The other two teachers switched over to cybersecurity from a different content area. One of these teachers noted, "We did TestOut the first year, and it was me staying ahead by two weeks." The teacher, who is self-taught, now has several industry certifications.

Both of the teachers without formalized computer science or IT training also relied on mentors to assist with instruction. "I was trying to find experts to come in and teach us . . . It was very painful the first year." One site mentioned the difficulty in getting teachers credentialed by the state to teach cybersecurity as a roadblock. All four sites saw the need for trained teachers as an ongoing problem. For example at one of the sites, a teacher in the program area noted, "My background is programming . . .The intent was to hire a cyber SME [subject matter expert]. . .The SME was to go on and develop what we were going to do. Now we've kind of gone a different route with that." To meet these challenges, both administrators and teachers mentioned the need for professional development and for access to subject matter experts to allow teachers the time to develop their expertise.

The final roadblock to program creation mentioned by the sites was the lack of understanding of cyber careers. This lack of understanding was seen when dealing with administrators, counselors, parents, and students. "A previous superintendent walked into my classroom one day, and I showed him the CyberSeek.org website," one teacher recalled, "and then a lightbulb went off for him. He was like 'You're offering my grads jobs. What do you need?'"

Student benefits had to be communicated to counselors as well. As one teacher noted, it was important to make sure that the counselors understand the program. This messaging extended to communication with parents and the general community and stressing the benefits of the program and the purpose of the content. One teacher noted, "We were very purposeful…to kind of sell it to all the adults out there."

Another administrator noted the difficulty in making the community understand the field of cybersecurity and the opportunities the field offers. The administrator described a survey that was conducted within their community where results indicated not much awareness of the importance of cybersecurity as a career. To get around this obstacle, the schools mentioned several strategies including leveraging extracurricular activities, hosting parent nights, working closely with counselors, touting program achievements, and developing connections with industry.

5.3. Program sustainment

The second part of the first research question was focused on program sustainment. In addition to understanding how high school cybersecurity programs develop, it is also important to understand how they are sustained. When interviewing individuals tied to the cybersecurity program at the four sites, discussion of sustainment focused on the need for student recruitment. However, other sustainment requirements unique to their program were identified.

The need to actively recruit students varied among the four sites. Admission to two of the programs was competitive, with one site requiring potential students to complete an application, obtain a letter of reference, and undergo an interview. The other site had a lottery system where interested students' names were randomly selected to fill the limited number of seats in the program. A teacher at one of the other two sites mentioned having a heathy program with a steady pool of interested students, and the teacher credited this to good counselors. The last site mentioned student recruitment as a big concern, with one of the counselors stating was as a challenge. The teacher also expressed concern about student numbers and stated, “We’ve got to keep our numbers up.” To maintain student interest in the programs, stakeholders mentioned several similar strategies as identified in Table 3.

Table 3. Strategies to Maintain Interest

Strategies	No. of Schools
Community outreach	2
Competitions	4
Counselors	4
Parent nights/classroom visits	3
Student awards/certifications	4
Student internships	4
Mentoring/teaching younger students	3

While the need for students was a commonality among the sites, the schools mentioned other sustainment factors unique to their programs. For example, at one of the schools, every interviewee mentioned having an inspiring/passionate teacher was the most important factor to the program’s success. When talking about why the school’s program was successful, one parent noted, “I can’t say enough good things about the program. Oh, I think with all the things with all programs, a majority of the program is who’s leading it and who’s teaching.” The administrator of the school echoed the parent’s praise stating, “Yeah, some [programs] are more successful than others, but I think it’s because of the instructor.” The students interviewed also mentioned being inspired by the teacher’s passion for “helping people learn more about cybersecurity and what it means in every aspect of your life.”

For another school, the key was industry partners and parents. The counselors at the school noted the students attending the school had unique internship opportunities that made cybersecurity attractive to students and beneficial to the community. In fact, students get 150 hours of internship placement between their junior and senior years. This connection with industry allows the students to make connections to businesses and allows them to build other employable skills. Additionally, the teacher runs the cybersecurity program similar to a sports team – complete with a parent booster club responsible for fundraising.

Two of the schools felt a major factor in sustainment was their use of mentors. At one school, adult mentors were used to maintain equipment and coach extracurricular teams. Additionally, student mentors were used to teach/tutor younger students, serving as teaching assistants for the classes. Stakeholders and students at the school both stressed the value of peer-to-peer collaboration. “I find that my peers are my greatest encouragement in learning new concepts,” one student said. Another student echoed that “…the most important thing is not only do you learn the knowledge but can share the knowledge with others. It’s awareness and soft skills. Teaching is the big thing.” The other school used students to mentor middle school students, helping to grow the program.

One of the four schools stressed that maintaining rigor was an important factor to school sustainment, noting that the rigor of their program helped set it apart from other programs. This theme was echoed by the student interviewees. “It’s a big thing that they actually go more in depth with security than other schools do.” Other students stressed the importance of rigor, with one student saying that the teachers “do more actual work application. . . They walk you through how it’s going to affect your actual work, and that’s the main focus of our school is to get us prepared for an actual job. So, as soon as we graduate, we can take a job wherever we want and know what we’re doing.”

Of course, just as there are factors required for program sustainment, there are also challenges that stand in the way of the program continuing. The four schools mentioned 12 challenges related to their programs (see Figure 3). The challenges are as follows:

- Disinterested students: one school mentioned some students enrolling in the course who do not find it engaging enough to continue. This impacted retention numbers. The actions and attitudes of these students also impacted the experiences of other students in the course.
- Funding: Administrators from two schools noted the programs were expensive to maintain. One school will not be able to expand the program as planned without extensive renovation of a building.
- Keeping up with growth: Three schools mentioned concerns about being able to meet the current demand for the courses associated with their programs. Two schools had already exceeded capacity, while another school was nearing maximum capacity.
- Being in a rural area: One school mentioned that being in an area that was not near a lot of cybersecurity related jobs made it more difficult to build interest in the program.
- Scheduling: One school found scheduling students for the courses a challenge.
- Student recruitment: As mentioned earlier, one school felt that they had to maintain a high level of student interest for the program to continue. All schools saw student recruitment as a priority.
- Teacher retention: All the schools mentioned the programs were currently very dependent on keeping their cybersecurity teachers. One school had

experienced a high turnover in cybersecurity teachers, which impacted the continuity of the classes.

- Teacher training: All of the teachers expressed a desire for more training. Some wanted content specific training, while other desired training on pedagogical strategies. Of interest, one student also noted the gap in teaching expertise: "Teachers that come in aren't actually teachers. They're just professionals now doing stuff with students. We have that kind of gap in like education training."
- Technology: Teachers noted two frustrations with technology. One was the expense to acquire and maintain technology. The other was working with the IT departments at the schools in using the technology. Two teachers expressed problems with blocked sites and difficulty in getting the sites whitelisted.
- Undeveloped curriculum: All the schools mentioned the lack of curriculum options, especially for 2nd to 4th year students in the program. All the teachers mentioned the burden of having to make their own materials. At one location, the students also commented on the lack of an established curriculum.
- Updating curriculum: Two of the teachers expressed concern with using outdated resources and constantly updating lessons due to changes in the field.
- Varied student skills: Interviewees from all roles and from three of the schools mentioned the range of student ability in the classes and the difficulty of teaching students with very limited computer skills in the same class with students who already have a high level of technical expertise.

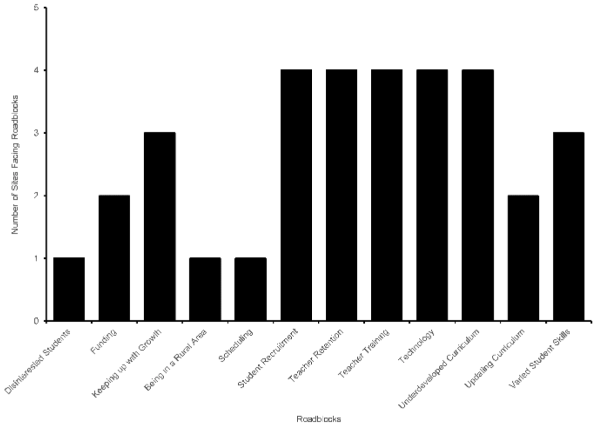

Figure 3. Roadblocks to program sustainment

5.3. Program inclusiveness

The second research question focused on program inclusiveness. Although all of the programs indicated an intention to be inclusive to all students, the programs developed approaches to include specific populations of students in the cybersecurity program. Table 4 lists the strategies used by each of the schools and the population targeted. Some of the strategies were more organic, developing based on student interest, and others were more intentional, created as policy or through targeted strategies.

Table 4. Inclusivity Strategies

School	Inclusivity Strategies	Targeted Population
iCSI	Lottery-based selection	Holistic
Program A	Geographic selection	Holistic
Spotsylvania H.S.	Teacher/school recruitment Role models	Autistic / learning divergent students
Troy H.S.	Peer leadership "Girls' room" Girls in Technology Engineering club	Female / female identifying students

The Troy program encourages the development of peer leadership and instruction, and through that, an effort to increase the number of females in tech. The school supports a girls' room, where girls can explore and experiment without fear of judgment. This room is led by female students, who instruct on topics such as intermediate and offensive Linux. Additionally, the students have formed their own club called Girls in Technology Engineering (GTech). This club goes beyond traditional cybersecurity topics to also cover topics such as coding and web development. "The idea is to teach middle school and high school girls, especially those who are just starting…the skills they need to feel comfortable and confident in the field," explained one student. The club has resulted in an increase in female students taking on teaching duties and engaging with the program.

Spotsylvania's program has a different approach to inclusiveness. This program has built a reputation for its work with students who are autistic. According to a parent of one of the students, his son was recommended to the program during an Individualized Educational Program (IEP) meetings. This student has achieved multiple industry certifications. Another parent discussed the use of role models, stating that, "One of the people in the IT department is also functioning autistic. She shared her story with him [the son], and that was kind of huge for him to see that somebody else was like him. It's incredible." Another parent related how the school's club and field trips helped his son with social interactions. This student plans to further his cybersecurity education after graduation.

Program A and iCSI seek to provide cybersecurity offerings to students who would not have access to cybersecurity education at their home institution. Program A is a residential school that focuses on geographic diversity in the state. Pulling from rural and under-resourced communities, the school actively promotes equity and opportunity. “So, we’re going into school systems that may not have strong science or strong STEM programs and extending those opportunities to students to enroll here,” explained one of the school’s counselors. “We’re really proud of our female representation, our students of color representation, but diversity also means geographic diversity.” With students coming from under-resourced schools, the school has safety nets in place to help students bridge any academic gaps. “There is a very strong, student-centered approach,” explained the counselor. “We put net after net after net after net under them that allows for a very high retention rate.” One of the nets is community building by putting students in teams. Additionally, students receive individualized instruction to help them tackle more difficult concepts.

iCSI is a bit different than the other programs in that their enrollment is lottery-based, meaning there are no specific inclusivity strategies related to recruitment; but there are strategies related to retaining students. To ensure that students have an equal chance at one of the limited seats in the program, they use a lottery system. Out of the students who apply each year, only about half get selected. The students vary in socioeconomic status and ethnicity, and the students vary with incoming ability needs. As the instructor explained, “The trick is differentiating successfully on a daily basis.” To break down any barriers among students, the program promotes peer teaching. The program also utilizes guest speakers and community mentors who work with the students to help them find success.

6. Conclusion

The case study data set indicates that nationally recognized cybersecurity programs can be created in a variety of school structures and program formats. Two of the school programs started as student competitions, one started through state legislation, and the other was created by a decision at the district level in response to a state mandate. Each school was geographically dispersed and varied in size and structure. The programs themselves were also dissimilar. However, there were common challenges in program creation. Challenges included fear of student actions on the school’s network, the expense, lack of resources, lack of teacher training, and lack of community understanding regarding the field of cybersecurity. Even after overcoming these roadblocks, there still exists challenges to program sustainment. Common roadblocks faced by all four sites are student recruitment, teacher retention, teacher training, technology, and underdeveloped curriculum.

Perhaps one of the most interesting facets among the schools was their differing approaches in meeting the needs of underrepresented, vulnerable, and underserved communities. The intention to make cybersecurity accessible to underrepresented and underserved is critical to ensuring access, as well as reaching more students who might be interested in pursuing cybersecurity as a career.

6.1. Recommendations

Based on the findings from the case studies, recommendations for furthering the establishment of high school cybersecurity programs that prioritize making their programs inclusive to all students include

- Being intentional with strategies to encourage students from underrepresented groups to not only enroll (i.e., recruitment), but participate actively in the program (i.e., retention). This may mean instructors become skilled at culturally relevant pedagogy and become intentional in including students who might not typically enroll these types of courses.
- Integrating peer and/or industry mentors and role models that are representative of students from underrepresented groups.
- Differentiating instruction to meet students where they are when entering the program. Incoming students have a wide variety of computing skills and cybersecurity knowledge, requiring flexible instruction and expectations tailored to individual students.

Recommendations for furthering research on the establishment of high school cybersecurity programs that prioritize making their programs inclusive to all students, include

- Further research to identify lessons learned in sustaining inclusive cybersecurity programs. Cybersecurity is relatively new to the K-12 curriculum thus best practices are needed to inform future practice.
- More research to explore how students from underrepresented groups relate to and experience cybersecurity education.
- Specifically, research on how schools decide which “nets” (or supports) to provide to students and when.

Ethical Approval

The study obtained ethical approval from The University of Alabama in Huntsville’s Institutional

Review Board of Human Subjects Committee (EE20228). All participants consented to take part in the study.

Acknowledgements

This research was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-20-1-0292), which is part of the National Security Agency. The authors would like to thank Dr. Melissa Dark, Dr. John Sands, and Mark Loepker for their contributions to the research.

12. References

About GenCyber. (n.d.). Retrieved November 23, 2020, from https://www.gen-cyber.com/about/

America's Cybersecurity Workforce. (2019, May 9). Federal Register. https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce

Amo, L. C., Liao, R., Frank, E., Rao, H. R., & Upadhyaya, S. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education*, *62*(2), 134–140. https://doi.org/10.1109/TE.2018.2877182

Barrette, C. (n.d.). *Course vs. Program Learning Outcomes: Analogies and Examples* [PowerPoint]. Retrieved November 15, 2021, from https://wayne.edu/assessment/files/course_vs_program_learning_outcomes.pptx

Blotnicky, K. A., Franz-Odendaal, T., French, F., & Joy, P. (2018). A study of the correlation between STEM career knowledge, mathematics self-efficacy, career interests, and career activities on the likelihood of pursuing a STEM career among middle school students. *International Journal of STEM Education*, *5*(1), 22. https://doi.org/10.1186/s40594-018-0118-3

CyberPatriot XII. (n.d.). Retrieved November 24, 2020, from https://www.uscyberpatriot.org/Pages/Competition/Season%20History/CyberPatriot-XII.aspx

Cybersecurity Supply And Demand Heat Map. (n.d.). Retrieved October 19, 2020, from https://www.cyberseek.org/heatmap.html

Dark Enterprises. (n.d.). *Cybersupply*. CyberSupply. https://cybersupply.org.

Frainer, M. (1996). *A study of the success factors, roadblocks, and strategies/practices leading to the successful implementation of Tech Prep programs in California public high schools—ProQuest* [Dissertation]. https://www.proquest.com/docview/304330882?pq-origsite=primo

Hawkins, A. F. (1990, September 25). *H.R.7 - 101st Congress (1989-1990): Carl D. Perkins Vocational and Applied Technology Education Act Amendments of 1990* (1989/1990) [Legislation]. https://www.congress.gov/bill/101st-congress/house-bill/7

Herold, B. (2017, March 22). With Hacking in Headlines, K-12 Cybersecurity Ed. Gets More Attention—Education Week. *Education Week*. https://www.edweek.org/ew/articles/2017/03/22/with-hacking-in-headlines-k-12-cybersecurity-ed.html

High School Cybersecurity Curriculum Guidelines. (n.d.). National Cryptologic Museum Foundation. Retrieved November 25, 2020, from https://cryptologicfoundation.org/what-we-do/educate/high-school-cybersecurity-curriculum-guidelines.html

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically Building the Cybersecurity Workforce. *IEEE Security Privacy*, *10*(2), 33–39. https://doi.org/10.1109/MSP.2011.181

Ileleji, T., & Joseph, A. (2018). Cybersecurity Talent Shortage and High School Students' Career Interests. *Annual International Conference on Computer Science Education: Innovation & Technology*, 105–113. https://doi.org/10.5176/2251-2195_CSEIT18.141

ISC2 Cybersecurity Workforce Study, 2021 (pp. 1–42). (2021). ISC2. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Joint Task Force on Cybersecurity E. (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. ACM. https://doi.org/10.1145/3422808

K-12 Cybersecurity Learning Standards | Cyber.org. (n.d.). Retrieved November 13, 2021, from https://cyber.org/standards

K-12 Pathway Program: RING | CAE Community. (n.d.). Retrieved February 21, 2023, from https://caecommunity.org/initiative/k12-ring

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). Virtual Extension The Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air. *Communications of the ACM*, *54*(1), 129–131. https://doi.org/10.1145/1866739.1866764

Myers, M. D. (2013). *Qualitative Research in Business and Management* (2nd ed.). SAGE Publications.

O'Reilly, K., Paper, D., & Marx, S. (2012). Demystifying Grounded Theory for Business Research-2012-O-Reilly-247-62—2020 Fall—Qualitative Research Methods (INFS-810-DT1). *Organizational Research Methods*, *15*(2), 247–262.

Pettigrew, A. M. (1990). Longitudinal Field Research on Change: Theory and Practice. *Organization Science*, *1*(3), 267–292.

Sadler, P. M., Sonnert, G., Hazari, Z., & Tai, R. (2012). Stability and volatility of STEM career interest in high school: A gender study. *Science Education*, *96*(3), 411–427. https://doi.org/10.1002/sce.21007

Smit, B. (2002). Atlas.ti for qualitative data analysis. *Perspectives in Education*, *20*(3), 65–76.

U.S. Army JROTC Cyber Pilot. (n.d.). Retrieved November 13, 2021, from http://www.usarmyjrotc.com/employment/cyber_pilot.php

Yin, R. K. (2014). *Case Study Research: Design and Methods* (5th ed.). SAGE Publications