Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education

Dr. Paul Wagner
paulewagner@arizona.edu

Dr. Robert Honomichl
rjhonomichl@arizona.edu

Crystal Beasley
crbeasley@arizona.edu

Thomas Reid
thomasreid1@arizona.edu

Logan Bradford
lbradford@arizona.edu

Alexandra Urbaszewski
aurbaszewski@azdohs.gov

College of Information Science
University of Arizona
Tucson, Arizona 85747, USA

Abstract

As cybersecurity threats continue to increase in sophistication, frequency, and scale, the demand for a skilled cybersecurity workforce expands. While post-secondary institutions have increased the number of cybersecurity programs, similar growth within high schools has not kept up. High school cybersecurity and computing courses are necessary to develop skills, raise awareness and digital responsibility, introduce career opportunities, and foster critical thinking and problem-solving skills. The CyberSupply data collection was part of the 2020 National Centers for Academic Excellence in Cybersecurity High School Designation Feasibility Study, initially focusing on availability and access to high school cybersecurity courses across 12 states. In 2023, the CyberSupply data collection was expanded to include Arizona. This paper provides an overview of the CyberSupply data collection project and details the Arizona CyberSupply data collection project conducted in fall 2023. Arizona's data is analyzed to identify the profile of Arizona schools and students, key findings, and opportunities for changing access to cybersecurity education in Arizona. These insights can help cybersecurity educators identify availability and access to cybersecurity courses and pathways in their states, areas of opportunities to support K-12 educators, course and pathway development opportunities, and address the cybersecurity workforce needs of the nation.

Keywords: Cybersecurity, Cybersecurity Education, CyberSupply, K-12 Education, Skills Gap, Pathways

Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education

Paul Wagner, Robert Honomichl, Crystal Beasley,
Thomas Reid, Logan Bradford and Alexandra Urbaszewski

1. INTRODUCTION

The cybersecurity skills and workforce gap continue to widen as the threat landscape continues to evolve at an alarming rate. The ability to overcome these issues requires a comprehensive cybersecurity education and training strategy. Collegiate cybersecurity programs continue to increase in availability and access due to increasing demand and support from federal agencies and funding. Despite this growth at post-secondary institutions, cybersecurity education within high schools is somewhat bare, with some pockets of growth (Dark et al., 2020). Only 16% of regular public high schools are estimated to have cybersecurity courses (Dark et al., 2020). The availability of cybersecurity courses is limited due to the availability of qualified teachers, availability of computer labs, crowded curriculum, and sequencing and scheduling. This limits access to cybersecurity courses to an estimated 3.7% of U.S. high school students (Dark et al., 2020). High school cybersecurity programs are important because they provide early skill development, help address the growing demand for cybersecurity professionals, raise awareness and promote responsible digital behavior, introduce diverse career opportunities, develop critical thinking and problem-solving skills, enhance national security, and bridge the digital divide. An added benefit is that these skills transcend the cybersecurity discipline. This paper provides an overview of the CyberSupply data collection project and details the Arizona CyberSupply data collection project conducted in fall 2023. Arizona's data is analyzed to identify the profile of Arizona schools and students and identify key findings and opportunities for changing access to cybersecurity education in Arizona. These insights can help cybersecurity educators identify the availability and access to cybersecurity courses and pathways in their states, identify areas of opportunities to support K-12 educators, course and pathway development, and address the cybersecurity workforce needs of the nation.

2. LITERATURE REVIEW

Cybersecurity Workforce Gap

The cybersecurity workforce shortage continues to be a concern, with over 450,000 unfilled positions within the United States (CyberSeek, 2025) and nearly four million globally (ISC2, 2023). Additionally, the cybersecurity threat continues to grow in sophistication, frequency, and scale, increasing stress on the cybersecurity workforce and leading to high employee turnover. White & Bunce (2023) estimates that nearly 51% of cybersecurity professionals will leave the field due to stressors like staffing and resource limitations, rising complexity of technology, remote work challenges, and compliance and regulatory pressures.

Compounding this problem is the increasing dissatisfaction of employers regarding the knowledge, skills, and abilities of cybersecurity graduates' capacity to fulfill the required tasks of the organization. Ross and Duke (2018) stated, "employers are expressing increasing concern about the relevance of certain cybersecurity-related education programs in meeting the real needs of their organization," in a report to the President of the United States. Additionally, an ISACA report (2023) identified that only 28% of employers surveyed believed that recent cybersecurity graduates were well prepared to meet the cybersecurity challenges of the organization, citing a lack of technical and soft skills. Addressing these concerns requires reviewing cybersecurity programs at the post-secondary level to ensure alignment with industry needs. Additionally, understanding the cybersecurity availability and access at the secondary education level can identify ways to develop competencies earlier in students' educational journey.

Collegiate Cybersecurity Programs

Hundreds of post-secondary institutions provide academic programs in cybersecurity to address the cybersecurity workforce gap and meet the knowledge, skills, and abilities required by employers. The National Security Agency's (NSA) National Cryptologic School partners with several federal partners on the National Centers of

Academic Excellence in Cybersecurity (NCAE-C) program. NCAE-C aims to create and manage a collaborative cybersecurity educational program with post-secondary institutions that:

- Establishes standards for cybersecurity curriculum and academic excellence;
- Includes competency development among students and faculty;
- Values community outreach and leadership in professional development;
- Integrates cybersecurity practice within the institution across disciplines; and
- Actively engages in solutions to challenges facing cybersecurity education (National Security Agency [NSA], 2025).

Currently, 467 institutions (National Centers of Academic Excellence in Cybersecurity [NCAE-C], 2025) maintain one or more of three designations: Cyber Defense, Cyber Operations, and/or Cyber Research. Institutions must complete a program of study validation that meets the desired characteristics required by the program office to produce the qualified workforce needed by the nation (NSA, 2025).

Alternatively, ABET is a nonprofit, non-governmental organization that accredits programs globally. They currently accredit 4,773 programs at 930 colleges and universities in 42 countries (ABET, 2025a). Similar to NCAE-C institutions, ABET-accredited programs ensure that graduates are prepared to enter the global workforce. ABET accredits programs in cybersecurity and similarly named computing programs and cybersecurity engineering and similarly named engineering programs. There are currently 54 institutions with one or both of these accreditations (ABET, 2025b).

It is important to note that additional schools not listed in these databases may also have cybersecurity programs. Additionally, colleges and universities may hold both ABET and NCAE-C designations.

High School Cybersecurity Programs

The availability and access of high school programs are difficult to identify. The National Center for Education Statistics (NCES) is the Department of Education's agency focused on collecting, compiling, analyzing, and reporting the condition of American education (National Center for Education Statistics [NCES], 2025). School statistical data provided by NCES includes directory information, school details, and enrollment characteristics; however, program information is not provided. Aggregate data for programs is typically collected by organizations and nonprofits at the local, state, or federal levels. Identifying program and course availability required the manual inspection of school websites. This is noteworthy as the process is time-intensive and can lead to errors.

Dark et al. (2020) conducted a study to identify (1) the availability of gateway-to-cybersecurity and cybersecurity courses and pathways and (2) the level of access to cybersecurity courses and pathways for 9-12 grade students in the U.S. This comprehensive study of 5,915 regular public high schools (42.5% of schools) and 192 Career and Technical Education (CTE) centers (15.8% of centers) located in Arkansas, Colorado, Florida, Georgia, Illinois, Maryland, Ohio, South Carolina, Texas, Utah, and Virginia provided a confidence level of >99.99% for public schools and 90% for CTE Centers (Dark et al., 2020).

CyberSupply's background and details on the methodology are outlined in the next section. Comprehensive study results can be found in the 2020 NCAE-C High School Designation Feasibility Study (Dark et al., 2020) with compiled results found at CyberSupply.org (Dark Enterprises, 2023). The CyberSupply study provided the template for Arizona's CyberSupply data collection project, which is the focus of this paper.

3. CYBERSUPPLY

Background
CyberSupply was part of the 2020 National Centers for Academic Excellence in Cybersecurity (NCAE-C) High School Designation Feasibility Study. The High School Feasibility study investigated the practicality of a high school cybersecurity recognition program by conducting a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, identifying resources required to implement, and establishing a prospectus for success (Dark et al., 2020). The goals were to identify the availability, attendance, and access to gateway, non-gateway, and cybersecurity courses within public high schools and CTE centers within the U.S.

A gateway course is typically considered the first credit-bearing course in a program of study, which generally applies to the requirements of a degree program (Kwak, 2020). Alternatively, gateway courses can be considered courses that students take, such as English or biology. The CyberSupply study defined gateway courses as "introductory courses that teach necessary prerequisite knowledge that set students up for success during their academic career and their professional lives." (Dark et al., 2020, p.58) The

study further coded gateway courses as Computer Science (CS) gateway or Information Technology (IT) gateway. Table 1 outlines the courses used within the study.

CS Gateway	IT Gateway	Non-Gateway
CSP/AP CSP	IT Fundamentals	Computer Applications
CSP/AP CSA	Networking I	Computer Management and Support
CS Discoveries	Networking II	Database
CS Essentials	Networking III	Digital Media
Exploring CS		Game Design I
Intro to CS		Game Design II
Linux		Mobile Applications
Programming I		Robotics
Programming II		Web Design I
Programming III		Web Design II
		Capstone I
		Capstone

Table 1 – Course Coding (Dark et al., 2020)

Cyber.org's K-12 Cybersecurity Learning Standards (2021) center on three core themes: Computing Systems (CS), Digital Citizenship (DC), and Security (SEC). Within these themes are fundamentals in cybersecurity education focusing on communication and networking, hardware, software, online safety, ethics, policy and legal issues, information security, network security, and physical security (Cyber.org, Cyber Innovation Center, & Cybersecurity and Infrastructure Security Agency, 2021). Additionally, the High School Cybersecurity Curriculum Guidelines & Glossary (Teach Cyber, 2021) are based on four levels: big ideas, enduring understandings, learning objectives, and essential knowledge statements. The big ideas are broad areas of importance within cybersecurity, including ethics, establishing trust, ubiquitous connectivity, data security, system security, adversarial thinking, risk, and implications (Teach Cyber, 2021). In addition to these documents, concepts from the Cybersecurity Curricular Guidelines (ACM, 2017) and the Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs) (Becker et al., 2024) were used to identify cybersecurity courses offered at schools within the study population. The following course titles were identified: Cybersecurity I, Cybersecurity II, Cybersecurity III, Principles of Cybersecurity, Network Security, Cyber Forensics, Cyber Ops, and Advanced Cyber Forensics (Dark et al., 2020).

Research questions were broken down into availability (the provision of courses in schools) and attendance and access (student access to courses in schools). Availability generally means that something can be used or obtained. For this study, availability of courses means that the course is listed within the school's academic catalog. Dark (2020) noted that merely listing a course in a school's catalog does not guarantee that the course has been or is being offered. Access generally refers to the ability to obtain or use a resource. Within this study, access is a function of the percentage of schools with gateway or cybersecurity courses, the number of students served in those schools per year, the number of courses available to those students, and the number of students that could be served with those courses (Dark et al., 2020). The following research questions guided the research study:

Availability
1) What percentage of schools and CTE centers have cybersecurity courses and computing courses that would be foundational to cybersecurity? Foundational courses in this study are called Gateway courses.
2) Are there differences in availability by state, Title I status, size and locale?
3) How many courses are offered by type (Gateway, Non-Gateway, Cybersecurity)?

Attendance and Access
1) How many students attend the schools and CTE centers with gateway and cybersecurity courses?
2) Are there attendance differences by state?
3) Are there attendance differences by race/ethnicity?
4) Given availability levels along with other limitations (limited teachers, computer labs, and available hours), how many high school students have access to gateway computing and cybersecurity courses?
5) Are there differences in access by state?
6) Are there differences in access by student race/ethnicity? (Dark et al., 2020)

4. ARIZONA'S CYBERSUPPLY

Arizona's CyberSupply data collection project partnered with Dark Enterprises' personnel, who conducted the initial CyberSupply data collection in 2020. This partnership allowed researchers to leverage the original research methodology, align with research questions, and benefit from lessons learned and best practices. This project was sponsored by the Center for the Future of Arizona (CFA) in partnership with the University of Arizona during Fall 2023. CFA is a nonprofit, nonpartisan organization that provides education, workforce development, and civic engagement programming. Specifically, the Arizona Pathways to Prosperity (APTP) initiative creates "future opportunity and upward economic mobility for all young Arizonans while supporting state and regional talent needs" (Center for the Future of of Arizona [CFA], 2025). APTP develops career-connected pathways in critical career fields, like cybersecurity, to provide career exploration, early college programs of study, and work-based learning (CFA, 2025). In addition to identifying the availability, attendance, and access of gateway, non-gateway, and cybersecurity courses, Arizona's CyberSupply data collection project had the following additional goals:

1) Identify schools of opportunity to develop cybersecurity courses or programs.
2) Identify schools with cybersecurity courses or programs to articulate pathways to higher education.
3) Identify schools with cybersecurity courses or programs to provide career exploration and career readiness opportunities.

Methodology
As previously mentioned, a subset of the research questions outlined in the High School Designation Feasibility Study was used to develop the research questions for this study. The research questions are:

Availability
1) What percentage of schools and CTE centers have cybersecurity courses and computing courses that would be foundational to cybersecurity? Foundational courses in this study are called Gateway courses.
2) Are there differences in availability by size, Title I status, and locale?
3) How many courses are offered by type (Gateway, Non-Gateway, Cybersecurity)?

Attendance and Access
1) How many students attend the schools and CTE centers with gateway and cybersecurity courses?
2) Given availability levels along with other limitations (limited teachers, computer labs, and available hours), how many high school students have access to gateway computing and cybersecurity courses?

Although state-to-state comparison is briefly reviewed, it is important to note the timeframe between the original data collection and Arizona's data collection. The availability and access to cybersecurity courses in the original 11 states may have changed.

Purposive sampling was used during this study, which refers to a group of non-probability techniques in which units are selected because they have characteristics needed in the sample (Nikolopoulou, 2022). Purposive sampling is best suited to help answer the identified research questions, particularly when a lot of background information is available. Homogeneous sampling was used to reduce variation and simplify the analysis to describe a particular subgroup in depth.

Data Collection
Researchers from the University of Arizona (U of A) and undergraduate students from the U of A, Grand Canyon University (GCU), and Pima Community College (PCC) conducted data collection during the 2023-2024 academic year. Data sources included the Common Core of Data from the National Center for Education Statistics (NCES).

- Data on enrollment, race/ethnicity, free/reduced lunch, Title I status, size, and locale were gathered from NCES.
- Data on course availability were gathered from publicly available websites. Undergraduate students manually collected this data, which was then reviewed by faculty and personnel from Dark Enterprises to validate the findings.

Schools
Arizona's CyberSupply course availability data is reported for 349 schools identified in the final dataset with an estimated total population of 319,079 high school students. Most schools were considered "small schools" with less than 600 students (54.2%), Title I schools (54.4%), and located within a city (43.6%). The breakdown for each category is provided in Tables 2, 3, and 4.

School Size	f	%
<600 Students	189	54.2
600-1200 Students	44	12.6
1201-2000 Students	62	17.8
>2000 Students	54	15.5
Total	349	100.0

Table 2 – School Size

Title I	f	%
Yes	190	54.4
No	159	45.6
Total	349	100.0

Table 3 – Title I Schools

Locale	f	%
City	152	43.6
Suburb	70	20.1
Town	51	14.6
Rural	76	21.8
Total	349	100.0

Table 4 – School Locale

Courses

This study identified 667 computing and 73 cybersecurity courses, as outlined in Tables 5 and 6, respectively. Courses considered computer science gateway are annotated with (CSG), those considered IT gateway are annotated with (ITG), and non-gateway courses are annotated with (NG).

Pathway	Course	f	%
Computer Science Gateway	AP CSP / CSP	73	10.9
	AP CSA	56	8.4
	CS Discoveries	5	0.7
	CS Essentials	8	1.2
	Exploring CS	4	0.6
	Introduction to CS	50	7.5
	Linux	3	0.4
	Programming I	83	12.4
	Programming II	69	10.3
	Programming III	38	5.7
	Exploring CS	4	0.6
Information Technology Gateway	IT Fundamentals	41	6.1
	Networking I	15	2.2
	Networking II	11	1.6
	Networking III	4	0.6
Non-Gateway	Capstone Course I	47	7.0
	Capstone Course II	21	3.1
	Computer Applications	1	0.1
	Computer Management and Support	27	4.0
	Database	0	0
	Digital Media	11	1.6
	Game Design/ Development I	18	2.7
	Game Design /Development II	8	1.2
	Mobile App Design/ Development	10	1.5
	Robotics	33	4.9
	Web Design	20	3.0
	Web Design II	11	1.6
	Total	667	100

Table 5 – Computing Courses

Course	f	%
Intro to Cybersecurity	21	29
Cybersecurity II	17	23
Cybersecurity III	14	19
Principles of Cybersecurity	16	22
Network Security	0	0
Cyber Forensics	0	0
Cyber Ops	1	1
Advanced Cyber Forensics	0	0
Other	4	5
Total	73	100

Table 6 – Cybersecurity Courses

Analysis

The formula for calculating access (Figure 1) is the number of courses (C) multiplied by the number of available seats (P). 30 is used for available seats to align with the feasibility study. C x P is divided by the total number of students (T) divided by four (4) to determine the approximate number of students per grade (4)

$$A = \frac{C \times P}{T/4}$$

Figure 1 – Access Formula

Analysis of the data and available courses identified that 48% of schools provided gateway courses across 460 different courses (667 (total courses)-207 (NG-labeled courses) =460 different courses from Table 5). 70% of total students from the study have access to these courses, providing an estimated 34% access to gateway courses.

Additionally, 10% of schools provided cybersecurity courses across 73 courses. These schools accounted for 2% of total students, providing an estimated 2.7% access to cybersecurity courses. Further, <1% of students have access to a cybersecurity pathway. Pathways are career-themed and college preparatory programs in high schools and CTE centers. Cybersecurity is often found in either the IT or STEM career cluster.

Tables 7 through 15 provide a cross-tabulation of computing courses, gateway computing courses, and cybersecurity courses across school size, Title I status, and locale, respectively, and provide the following information. Profile information and key findings from this data are summarized below.

Profile of Schools and Students
- 78% of AZ public high schools are Urban and 88% of students attend Urban Schools
- 33% of schools have >1200 students and 75% of students attend these schools
- 54% of AZ public high schools have <600 students and 13% of students attend them
- 54% of high schools are Title I

Key Findings
- 40% of schools offering gateway courses are Urban; 8% are rural schools
- 9% of schools offering cyber courses are urban; 1% are rural schools
- 78% of schools with 1200+ students offer gateway courses; 15% offer cybersecurity courses
- 34% of schools with <1200 students offer gateway courses; 7% offer cybersecurity courses

School Size	Computing Courses		
	Yes	No	Total
<600 Students	68	121	189
600-1200 Students	29	15	44
1201-2000 Students	46	16	62
>2000 Students	45	9	54
Total	188	161	349

Table 7 – Computing Courses and School Size

School Size	Gateway Computing		
	Yes	No	Total
<600 Students	54	135	189
600-1200 Students	25	19	44
1201-2000 Students	45	17	62
>2000 Students	45	9	54
Total	169	180	349

Table 8 – Gateway Computing and School Size

	Cybersecurity Courses		
School Size	Yes	No	Total
<600 Students	12	177	189
600-1200 Students	5	39	44
1201-2000 Students	8	54	62
>2000 Students	9	45	54
Total	34	315	349

Table 9 – Cybersecurity Courses and School Size

	Computing Courses		
Title I	Yes	No	Total
Yes	96	94	190
No	92	67	159
Total	188	161	349

Table 10 – Computing Courses and Title I

	Gateway Computing		
Title I	Yes	No	Total
Yes	85	105	190
No	84	75	159
Total	169	180	349

Table 11 – Gateway Computing and Title I

	Cybersecurity Courses		
Title I	Yes	No	Total
Yes	19	171	190
No	15	144	159
Total	34	315	349

Table 12 – Cybersecurity Courses and Title I

	Computing Courses		
Locale	Yes	No	Total
City	86	66	152
Suburb	43	27	70
Town	24	27	51
Rural	35	41	76
Total	188	161	349

Table 13 – Computing Courses and Locale

	Gateway Computing		
Locale	Yes	No	Total
City	79	73	152
Suburb	43	27	70
Town	19	32	51
Rural	28	48	76
Total	169	180	349

Table 14 – Gateway Computing and Locale

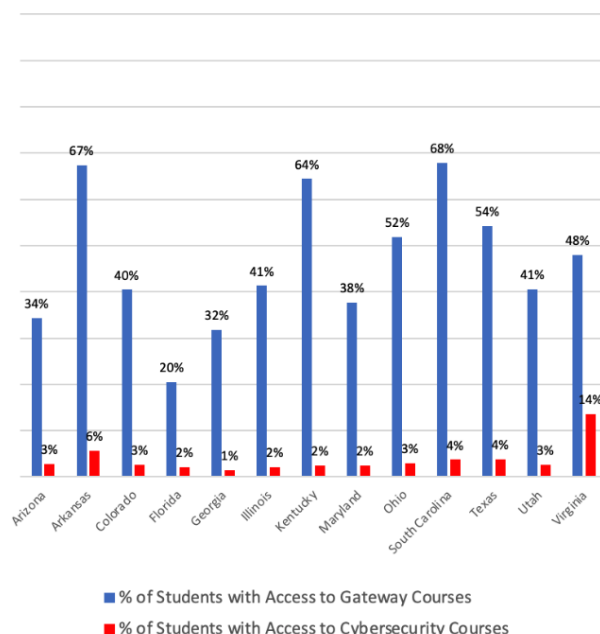|	Cybersecurity Courses		
Locale	Yes	No	Total
City	22	130	152
Suburb	5	65	70
Town	4	47	51
Rural	3	73	76
Total	34	315	349

Table 15 – Cybersecurity Courses and Locale

Arizona's CyberSupply data was compiled into the dataset from other states. Figure 2 outlines the availability of Gateway Computing courses and Cybersecurity courses across 13 states. Figure 3 outlines the access to those courses across states. Several key takeaways are identified by viewing this consolidated data. First, there are prominent outliers in several states. For example, the availability of gateway computing courses in Maryland at 91% is contrasted with the relatively low access to those courses at 38%. Similarly, the availability of cybersecurity courses in Virginia at 61% contrasts with access being calculated at just 14%. Second, the average availability for Gateway Courses is 59% or 56% when removing the Maryland outlier. The average availability for Cybersecurity courses is 16% or 12% after removing the Virginia outlier. There are no significant outliers for Gateway access, resulting in an average access of 46% across states. However, when calculating access for cybersecurity, averages are considered with Virginia and without, resulting in 3.7% or 2.9%, respectively.
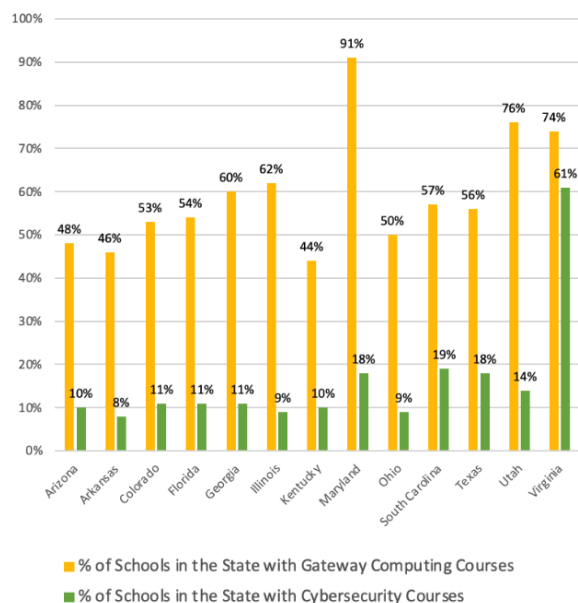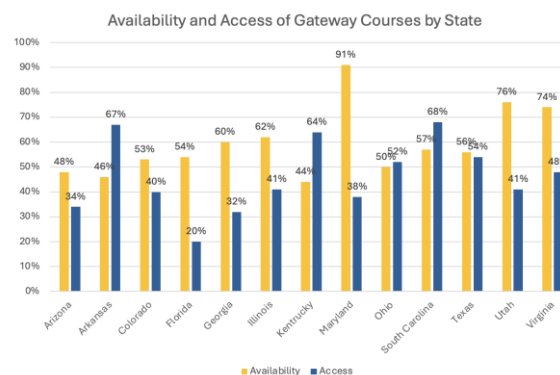
Figure 2 – Availability by State with Gateway Computing vs Cybersecurity Courses (Dark et al., 2020)


Figure 3 – Access by State with Gateway Computing vs Cybersecurity Courses (Dark et al., 2020)

Finally, researchers developed Figures 4 and 5 to highlight the side-by-side comparisons of availability and access from states included in this study. Figure 4 shows that in some instances (Arkansas, Kentucky, Ohio, and South Carolina), there is greater access to courses than availability. Alternatively, Figure 5 shows the

differences between availability and access are proportionally similar except for Virginia.

Figure 4 – Availability and Access of Gateway Courses by State
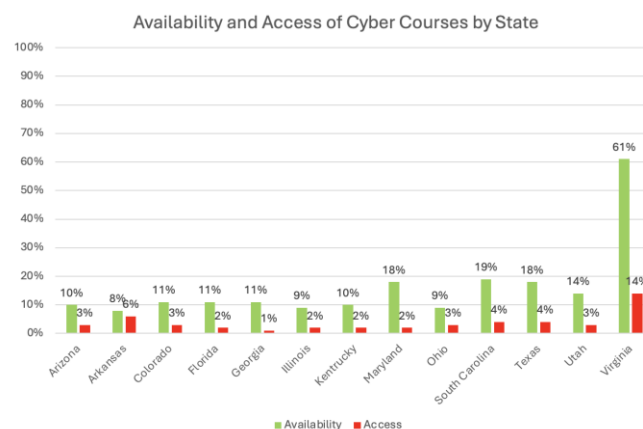
Figure 5 – Availability and Access of Cybersecurity Courses by State

5. FUTURE WORK

This study provides multiple possibilities for future work. Analysis of outlier states and those tat have more access to courses than availability could identify best practices, resources, or methods for developing and increasing the availability and access for gateway and cybersecurity courses within Arizona. Additionally, researchers noted a three to four-year gap between the original data collection and Arizona's data collection. Evaluating the ability to conduct regular data collection and expanding it to other states could further identify areas of opportunity and excellence to inform decision-making. This could also lead to year-over-year trend analysis to identify whether availability and access are increasing or decreasing. Further, researchers will leverage this data to identify schools for development, support, or expansion. It could identify why schools with low, or no availability are not offering gateway or

cybersecurity courses. Finally, this study provides information on schools with gateway and cybersecurity courses. This provides the opportunity to develop a community of practice and connection with schools to ensure districts, teachers, and programs are sustainable. This would enable the development and distribution of best practices, staying current with the evolving nature of cybersecurity, and conducting professional development. The community of practice can be facilitated through statewide initiatives, including GenCyber, Arizona Cybersecurity Initiative, the National Cybersecurity Teaching Academy (NCTA), Arizona Teaching Academy, and the 18-credit Graduate Certificate in Cyber Operations offered by the University of Arizona.

6. CONCLUSIONS

The availability and access to gateway and cybersecurity courses at secondary education institutions are critical to overcoming the cybersecurity skills and workforce shortage. Cybersecurity education at the high school level lacks availability and access, with only 10% of Arizona schools offering cybersecurity courses and less than 1% of students having access to cybersecurity pathways. Changing access in Arizona can occur in several ways. First, leveraging interest in computer science can develop interest in cybersecurity. Since 48% of schools offer gateway to cybersecurity courses it provides an opportunity to develop interest through those courses. Second, offering multiple entry points into cybersecurity pathways can be beneficial. Cybersecurity professionals have diverse backgrounds and enter the career field at different points. Cybersecurity education should provide similar opportunities and a diverse range of pathways. Additionally, states and schools need to invest in teachers and cybersecurity professional development. There are local and national training opportunities ranging from camps and professional development, like GenCyber and Cybersecurity High School Innovations (CHI), to scholarships for a graduate certificate in cybersecurity provided by the NCTA. Finally, Arizona needs to incentivize schools and districts to initiate and grow cybersecurity pathways. This may include implementing state standards and requirements for cybersecurity or developing a dedicated CTE program for cybersecurity.

Actions must be taken to address Arizona's and the nation's critical cybersecurity workforce shortage by expanding access and availability of cybersecurity education in our secondary schools.

Educators, policymakers, and industry leaders should collaborate to leverage existing computer science programs, create diverse entry points into cybersecurity pathways, and invest in teacher training and professional development. By incentivizing schools and districts to build robust cybersecurity programs and adopting clear state standards, states can empower their students with the skills needed for tomorrow's digital challenges.

7. ACKNOWLEDGEMENTS

8. REFERENCES

ABET. (2025). *About ABET.* https://www.abet.org/about-abet/

National Center for Education Statistics. (2025). *About NCES*. https://nces.ed.gov/about/

ABET. (2025). *Accredited programs*. https://amspub.abet.org/aps/category-search?disciplines=91&disciplines=94

Association for Computing Machinery (ACM), IEEE-CS, AIS SIGSEC, & IFIP WG 11.8. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity*. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Becker, A., Blum, Z., Burgin, K., Carlin, A., Chu, B., Cranford-Wesley, D., Frank, S., Ghosh, T., Hamman, S., Joyce, R., Keller, S., Kohnke, A., Levy, Y., Liu, X., Manikas, T., McBride, S., Mierzwa, S., Miller, S., Nagaishi, M., Nowatkowski, M., Pinto, A., Steiner, S., Taylor, B., Tu, M., Weathers, R., West, T., & Zanella, G. (2024). *National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) knowledge units (KUs)*. National Security Agency. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Center for the Future of Arizona (CFA). (2025). *Arizona pathways to prosperity*. https://www.arizonafuture.org/media/ok5pbis5/aptp-flier-statewide-v4.pdf

Cyber.org, Cyber Innovation Center, & Cybersecurity and Infrastructure Security Agency. (2021). *K-12 cybersecurity learning standards*. https://cyber.org/sites/default/files/2021-10/K-

12%20Cybersecurity%20Learning%20Stand
ards_1.0.pdf

CyberSeek. (2025). *Cyberseek supply and demand heat map*. https://www.cyberseek.org/heatmap.html

Dark Enterprises. (2023). *Cybersecurity education: Availability and access in public high schools*. CyberSupply Securing the Workforce. https://cybersupply.org/

Dark, M., Daugherty, J., Williams, T., & Sands, J. (2020). *2020 NCAE-C high school designation feasibility study*. National Cryptologic Foundation. https://caecommunity.org/sites/default/files/initiatives/files/Feasability_Study_Final_NCAE-C_2020.pdf

ISACA. (2023). *State of cybersecurity 2023: Global update on workforce efforts, resources, and cyberoperations*. https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

ISC2. (2023). *How the economy, skills gap, and artificial intelligence are challenging the global cybersecurity workforce*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

Kwak, J. (2020, June). What are gateway courses and why do they matter to equity in higher ed? *Every Learner Everywhere*. https://www.everylearnereverywhere.org/blog/what-are-gateway-courses-and-why-do-they-matter-to-equity-in-higher-ed

Nikolopoulou, K. (2022, August 11). What is purposive sampling? Definition and examples. *Scribbr*. https://www.scribbr.com/methodology/purposive-sampling/

National Centers of Academic Excellence in Cybersecurity (NCAE-C). (2025). *CAE institution map*. https://www.caecommunity.org/cae-map

National Security Agency (NSA). (2025). *National centers of academic excellence in cybersecurity*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Ross, W., & Duke, E. (2018). *Supporting the growth and sustainment of the nation's cybersecurity workforce: Building the foundation for a more secure American future*. U.S. Department of Commerce & Department of Homeland Security. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/supporting-growth-and-sustainment

Teach Cyber & National Cryptologic Foundation. (2021). *High school cybersecurity curriculum guidelines & glossary*. https://teachcyber.org/wp-content/uploads/2022/11/High-School-Cybersecurity-Curriculum-Guidelines-Nov2022.pdf

White, A., & Bunce, J. (2023). *Generative AI and cybersecurity: Bright future or business battleground?* Sapio Research. https://www.deepinstinct.com/pdf/voice-of-secops-4th-edition