Leveraging High Schools to Build the Cyber Talent Pipeline

Benjamin Dougherty

Director of IT Pathways, Cybersecurity

The College Board

University *of* Dayton
Center for
Cybersecurity &
Data Intelligence

OHIO CYBER
RANGE INSTITUTE

Overview

A significant cyber workforce shortage is impacting organizations' ability to protect themselves and their customers. In southwest Ohio, Lakota Local Schools is partnering with local businesses to revolutionize the way businesses recruit the next generation of cyber defenders. This paper outlines proven strategies schools can explore to build the cyber talent pipeline through local partnerships; alignment to professional certifications; and internship opportunities and site visits for students.

About the Author

Benjamin Dougherty is the Director of IT Pathways at The College Board. From 2019-2023 Ben was one of the lead instructors and principal architects of the Lakota Cyber Academy where he created a sequence of three high school courses in which students earn college credit, have professional mentors, compete in national cybersecurity competitions, earn industry-recognized credentials, and participate in paid cybersecurity internships. In 2022 the US Department of Education recognized Ben with the Presidential Cybersecurity Educator Award. In 2023 Ben joined the Career Kickstart team at College Board as Director of IT Pathways, Cybersecurity where he is developing a new AP-style cybersecurity pathway of courses that will be available to students in schools across the country.

University of Dayton
Center for Cybersecurity and Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at **go.udayton.edu/cybersecurity**

Leveraging High Schools to Build the Cyber Talent Pipeline

Benjamin Dougherty
Director of IT Pathways, Cybersecurity
The College Board

Introduction

In May 2023, there were more than 750,000 unfilled cybersecurity jobs in the United States alone.[1] For businesses, the inability to recruit and retain cybersecurity talent is costly. According to a report from IBM Security, the average cost of a data breach in the United States in 2022 was $9.44 million, with 83% of the organizations in their research experiencing more than one data breach. The average amount of time for a company to identify and contain a data breach in the study was 277 days. Among the organizations studied, 62% said that their security team was not sufficiently staffed, and the average cost of a data breach for organizations not sufficiently staffed was $550,000 more than the cost for organizations with a sufficiently staffed security team.[2]

There is a significant cyber workforce shortage, and it is impacting organizations' ability to protect themselves and their customers. In 2021, colleges and universities in the United States graduated 60,000 computer science majors (most of whom went to work in non-cyber fields like software and web development).[3] The work-force demand is orders of magnitude greater than the supply of college graduates being produced. According to the National Center for Education Statistics (NCES), there were 15.4 million high school students in the United States.[4] They represent a vast, untapped potential pool of cyber talent. If juniors and seniors make up 7.5 million of all high school students, and 3% of them chose to go into cybersecurity, that would go a long way toward closing the workforce gap in just a few years.

In southwest Ohio, Lakota Local Schools is partnering with local businesses to revolutionize the way businesses recruit the next generation of cyber defenders. In 2019, inspired by the need for local cyber talent, Lakota launched the Lakota Cyber Academy (LCA). Over the past four years the program has grown to include over 250 students enrolled in three cybersecurity courses in grades 10-12. The first year course in the program is open to all students with no prerequisites; the goal of the first year course is to introduce students to the big ideas of information security and ensure that students have the necessary background in technology (e.g. operating systems, networking, etc). Years two and three of the program focus on network defense and ethical hacking. As students progress through the program they have professional mentors from the local information security community, access to paid internships, and the opportunity to earn college credits through dual enrollment opportunities. Students' coursework is also aligned with industry certifications such as CompTIA Security+, AWS Cloud Practitioner, and TestOut Ethical Hacker Pro.

One of the distinguishing features of the Lakota Cyber Academy is that from its inception work-force development has been at the heart of the program. The local business

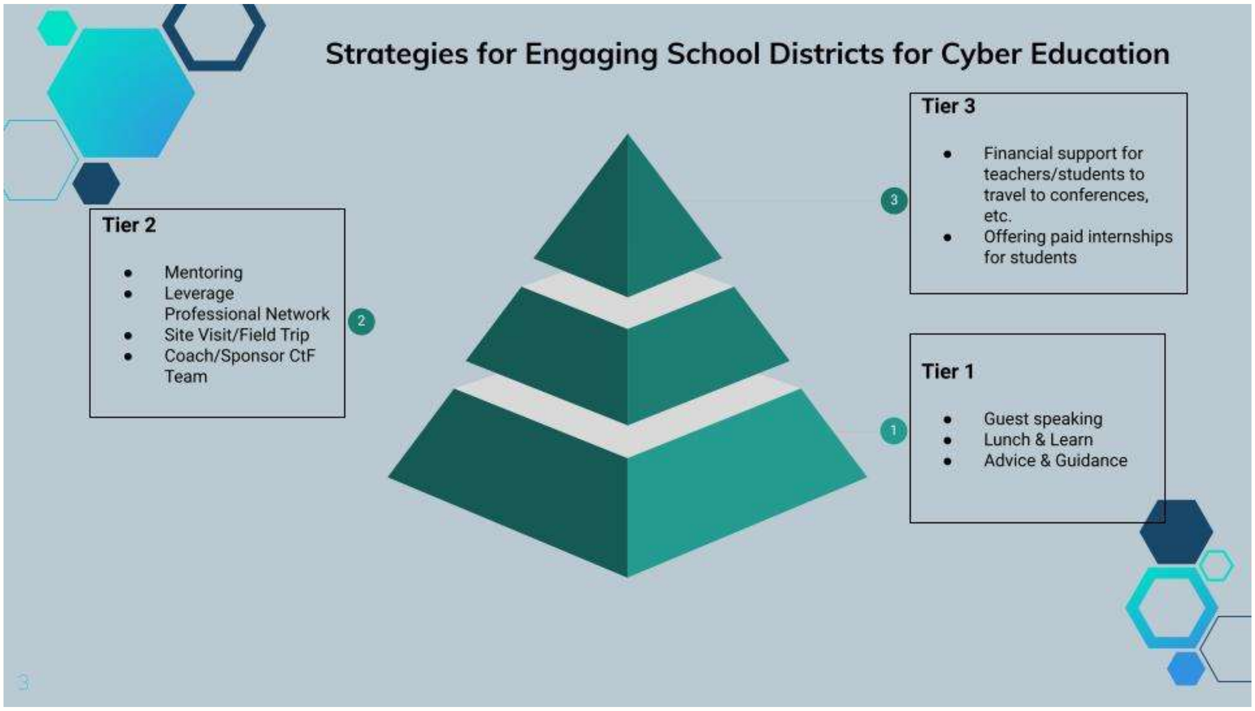
[1] https://www.cyberseek.org
[2] "Cost of a Data Breach Report 2022", IBM Security (https://www.ibm.com/reports/data-breach)
[3] https://www.collegefactual.com
[4] https://nces.ed.gov/fastfacts/display.asp?id=372

community has been instrumental in the development of the course sequence, alignment to professional certifications, and creating internship opportunities and site visits for students. Two business partners in particular have provided strong support from the beginning: Standex Electronics, Inc. and US Bank.

Early in the program Standex offered two paid internship positions for students in their security department, and were so impressed by the quality of the students that they expanded the internship program and increased the number of student interns they took in successive years. Standex assigns interns a mentor who helps them learn how to work in a business environment, and students work on meaningful security projects for the company throughout the school year. Standex has always understood that the interns are students first and has been flexible with their schedule as they participate in sports and when students need extra time to study (e.g. for semester exams). Some Standex interns who have graduated from the program have even returned from college to intern again in the summer.

US Bank has generously provided mentors and engaging site visits for students since the beginning of the program. In 2023, US Bank began a pilot program that is an eight-week summer internship which gives students hands-on experience in different aspects of cybersecurity: DFIR, Blue Team, Red Team, etc. Although these internship models are very different, both have provided great work-based learning opportunities for students.

A Framework for Engagement



Strategies for Engaging School Districts for Cyber Education

Tier 3

- Financial support for teachers/students to travel to conferences, etc.
- Offering paid internships for students

Tier 2

- Mentoring
- Leverage Professional Network
- Site Visit/Field Trip
- Coach/Sponsor CtF Team

Tier 1

- Guest speaking
- Lunch & Learn
- Advice & Guidance

One of the goals of this paper is to lay out a framework that businesses can use to begin engaging with their local school district in an effort to recruit and retain local cyber talent. This framework will focus on three main considerations for a specific engagement strategy between a business partner and a school: impact, time commitment, and financial commitment. The individual strategies are classified in tiers. Tier 1 strategies are lower commitment and are a good way for businesses to begin to develop a relationship with a school or district. Tier 2 strategies involve more commitment, and are oriented toward helping a program grow. Tier 3 contains high commitment high impact strategies.

Tier 1: Low-Commitment Strategies
These strategies are good starting places for engagement with a school district.

Strategy: Guest Speaking
Impact: Varies
Time Commitment: 30-90 minutes
Financial Commitment: None

Guest speaking scenarios include the following:

- Talking about the cybersecurity career field at a school career day/night
- Talking to a cybersecurity class about day-to-day work in cybersecurity
- Partnering with a cyber teacher to teach a class about a topic in your expertise
- Talking to students about cyber "hygiene" and online safety

High-impact	Low-impact
Students have the technical/conceptual background knowledge/skills to understand the topic of the talk	Talk deals with aspects of cyber that are beyond students' current level of understanding; or is overly technical for the audience
Presentation is engaging; students are involved in doing some type of activity	Students are sitting passively only listening
Using relevant specific examples to illustrate point (e.g. discussing specific vulnerabilities related to an app/website that is popular among students)	Speaking in broad generalities about your topic

Strategy: Lunch and Learn
Impact: Medium
Time Commitment: ~60 minutes
Financial Commitment: $25 - $75

Lunch and learns are a popular model for getting students interested in cybersecurity. Students are offered free food (pizza is a popular and affordable choice!) in exchange for coming to learn something about cybersecurity. This could be a way to try to recruit students into a cyber class/club. As mentioned in the "guest speaker" strategy, keep the talking light and direct, and make sure there are opportunities for students to ask questions.

Strategy: Provide Guidance/Advice
Impact: Medium-High
Time Commitment: Varies
Financial Commitment: None

Most school districts don't know where to begin with regard to offering a cybersecurity class/club to students. They are often looking for guidance around questions like: what topics to teach, what materials students need to learn cybersecurity (hardware, software, etc.), what certifications students should work toward, etc. A local expert has the potential to have high impact on a program by providing guidance on these topics. This guidance can range from being informally available via email (low time commitment) to meeting 2-4 times per month with someone in the district to provide on-going advice as the program develops.

Tier 2: Medium-Commitment Strategies
Some of these strategies are more effective for a program that has gone through the "initialization" phase into the "implementation/growth" phase.

Strategy: Mentor Students
Impact: High
Time Commitment: ~1-2 hours per month during school year
Financial Commitment: None

Students want to know what a career in cybersecurity will be like, what opportunities there are for growth/advancement, where they should go to college, if they should go to college, what they should major in, where they can intern, etc. These types of questions can be hard for a teacher to answer. Mentoring provides an opportunity for members of the local information security community to spend high-impact quality time sharing their stories and insights in small group settings with students. If mentors meet consistently (about once each month) with a small group of students over the course of the school year, they cultivate a strong professional relationship that is mutually beneficial. Mentors can serve as professional references and make students aware of opportunities in the information security community.

Two suggestions:

- Small group mentoring is often more effective than 1-on-1 mentoring: 1-on-1 can be intimidating for students; and if a student is sick or on a field trip the small group can still proceed without that one student.
- While some general "getting to know you" sessions are important at the beginning of the school year, the more structure the mentoring sessions have the better they tend to run. Dedicate a mentoring session to any of the following potential topics: resume review, practice interview questions, solving practice CtF questions, tackling/clarifying a tricky concept from class, etc.

Strategy: Leverage Professional Network
Impact: Medium-High
Time Commitment: Minimal
Financial Commitment: $0

Professionals in the information security field are often connected to others in the field and know about local opportunities like conferences, contests, or speakers. Invite other professionals to present at the local school district or be a mentor. The personal invitation model is powerful to enlarging the support network for the school. If there is a conference, ask conference organizers if they would provide free admission for a small group of students or the program teacher to come and learn more about cybersecurity. This request coming from a local professional carries weight, and most conference organizers can afford to let a few students and/or a teacher attend for free. If a local security business is bringing in a guest speaker for a conference or for some professional learning, ask if the speaker would be willing to stop by the school and talk to students in the cyber class/club for 30-45 minutes.

Strategy: Host a Student Field Trip
Impact: High
Time Commitment: 1-5 hours
Financial Commitment: $0-150 (depending on whether the business pays for transportation or lunch)

Providing an opportunity for students to get out of the classroom and see cybersecurity in action in your local business is a great way to support a program. Students learn a lot from these field trips (or site visits) and have the opportunity to ask cyber professionals questions about what it is like working in the field. Some districts have transportation available for these types of trips, but if the business can cover the cost of getting a bus for the field trip that often helps. One technique that has worked well is to schedule the student visit over lunch, buy pizza and ask employees to take a lunch break and have some free pizza with the students and talk with them about the field and their jobs.

Strategy: Sponsor/Coach Student CtF Team
Impact: High
Time Commitment: ~1-2 hours per week leading up to competition
Financial Commitment: Varies depending on the competition ($0 - $200 per team)

Capture the Flag (CtF) style competitions are a great way for students to get hands-on experience with different aspects of cybersecurity in a controlled and safe environment. There are typically challenges for beginner, intermediate, and advanced students, so everyone can learn and play at their own level of comfort. Many students enjoy the competitive gamified environment that CtF competitions offer. This can work equally well for a cyber club or a cyber class. Some CtF competitions are free, others have a (usually small) fee associated with them. Although the fees to participate are often small, school districts don't always have discretionary funds to cover those fees. Funding the students' entry fees can provide an opportunity for students to participate whose families might not be able to afford the entry fee.

Coaching a group of students prior to participating in a CtF competition is a great way to interact with motivated students in a structured goal-driven environment: students want to learn how to solve the challenges and the industry expert has the knowledge and skills to share. This lends itself to a very hands-on activity-based coaching scenario. Most competitions prohibit direct coaching during the competition, but meeting with students for 1 hour each week for a few weeks leading up to the competition can go a long way toward preparing students to be competitive in the CtF. Some suggested competitions:

> *CyberStart America*
> Frequency / Duration: Annually (Oct. – Apr.)
> Cost: Free
> Comments: Wide range of challenges (beginner through advanced); Awards for students who achieve high scores; Opportunities for students to earn free GIAC courses & certifications
>
> *picoCTF*
> Frequency / Duration: Annually (Mar.) for 2 weeks
> Cost: Free
> Comments: Excellent learning resources (handbook, community discussion boards, etc.); Practice challenges available year round; Built-in web-based shell for students to use for free (i.e. no VMs needed)

CyberPatriot
Frequency / Duration: Annually (Sept. – Apr.); Practice Rounds Aug. - Sept; Three preliminary rounds (all teams) Oct. - Dec.; Semi-finals & National Championship (select teams) Jan. – Apr.
Cost: $165/team for early registration; $210/team for regular registration; Teams can have up to 6 students; Teams composed entirely of young women are free
Comments: Students load VMs that are pre-configured with vulnerabilities; students earn points by finding and fixing vulnerabilities; Students get experience with different operating systems; Defensive focused competition; Team-based; Students learn how to use Cisco Packet Tracer

US Cyber Games
Frequency / Duration: Annually (Jun.) for 2 weeks
Cost: Free
Comments: More advanced challenges; Goal is to find/train the best cyber talent in the nation; Opportunities for top players to compete at higher levels

National Cyber League
Frequency / Duration: Fall & spring seasons, each lasting 8-10 weeks
Cost: $35/student for each season
Comments: Excellent user interface; “Gym” available for CtF practice prior to competition; Individual and team competitions; Good variety of challenges; Provides “scouting report” that students can add to their resume showing strengths; Aligned with CompTIA Security+ exam objectives

Tier 3: High-Commitment Strategies
These strategies involve more significant investment of time and money. They are best suited for businesses with an established relationship with the local school and experience providing support through Tier 1 and 2 strategies.

Strategy: Create Student Internships
Impact: High
Time Commitment: Varies
Financial Commitment: $12-15/hour/intern

There’s no substitute for work-based learning opportunities for students. Students gain experience crafting a resume and honing their interview skills during the application process, and then students who are hired on as interns begin developing a professional network, apply the concepts they’ve learned in class in a real business setting, and learn how to operate as a responsible member of a team delivering on objectives that benefit the company. Companies that offer these internship positions are actively building their own talent pipeline. They are identifying the best local cyber talent, and embedding them in their corporate culture. Students who intern with a company in high school often want to return to that company to intern in college, and frequently want to apply to work there after graduation. Students develop a sense of loyalty to the company and deep relationships with the staff members they work with during their internship. It is important to have an intern supervisor who is excited about working with young people and has a positive attitude toward training the next generation of cyber defenders.

The structure of the internship can vary widely. It could be an 8-10 week experience during the summer, or a longer experience during the school year. Some students have flexibility in their school day (e.g. early release) and could work a few hours after school a few days each week. Coordinating with the local district to understand student availability is an important part of designing an internship program that will work for students.

Strategy: Financial Support
Impact: High
Time Commitment: Minimal
Financial Commitment: Varies

Most school districts operate on small financial margins, and it can be hard to justify extra expenses for a special program (especially when the program is starting up and may only have a few students). Providing financial support for things like t-shirts, pizza lunches, and student competition fees can go a long way toward helping the program grow. Another important part of building a program is supporting professional development for the teacher. Sending the teacher to a professional development conference can be expensive for the district (costs include the conference registration fee as well as expenses associated with the teacher traveling to the conference). Similarly, providing financial support for students to attend conferences, events, or field trips is very helpful.