Implementation of Raspberry Pis: How to Decrease the Cybersecurity Diversity Gap

Eli Bryant Roberts

April 25th, 2025

University of Virginia

For fulfillment of the UVA CS Capstone

Abstract

Everything in today's world is revolved around the expansion of technology. From cloud server providers making data centers to using VLANs to segment different hosts in a small business, technology is at the forefront for these operations. This diversification of technology leaves vulnerabilities open to be exploited. The gap between zero-day attacks versus the vacant cybersecurity positions that are unfilled is tremendously concerning. In a world filled with technology, why are we not able to protect our data? In a condensed and simplified answer the root issue is the lack of exposure and preparation from our educational system. Without proper education or training, it makes it an obstacle course for people to break into the cyber world. This issue is correlated to the lack of diversification in the workforce.

To address this issue, a raspberry pi is being proposed. By implementing this affordable and compact teaching tool into our school systems, people who are a part of the minority will be able to experiment and later on pursue an occupation in IT. Diversification allows for different perspectives, the more diversification means the more security added onto protecting our complex networks.

Introduction

In a world filled with diversity, the cybersecurity workforce does not accurately reflect this. Data has shown that adding different perspectives into any workforce will enhance problem solving and give different perspectives on how to tackle an obstacle (Gomez & Bernet, 2019). If diversity is important and technology is the backbone of Americans infrastructure, why are we not looking for a way to fix this? From common talk especially at UVa, it's rare to hear someone pursue a field in security or IT. Even from my own personal experience, being someone who is pursuing cybersecurity rather than aspiring to be a software engineer, I feel as if I am being

looked at cockeyed. A research was conducted that “2,300 security managers reported that 59% of their security positions were unfilled, although 82% anticipated cyberattacks to their systems” (Mountrouidou et al., 2019) . If cybersecurity is important to keep our organizations up and running; Why do these two not correlate? If vulnerabilities are present and increasing diversity can help aid this problem, what is the hold up?

Tables one and two present data on the composition of the current cybersecurity and computer-based workforce in the United States (Chamlou, 20222). Table one illustrates the distribution of individuals in cybersecurity and STEM positions by race, indicating a workforce predominantly composed of white employees. Table two highlights the gender disparity within the IT workforce, revealing a significant gap. These data, derived from a research study, suggest that the cybersecurity and IT sectors currently lack diversity, with representation leaning towards white male employees.

RACE OF EMPLOYEES	% OF ALL JOBS	% OF ALL STEM JOBS	% OF COMPUTER SCIENCE JOBS (INCLUDING CYBERSECURITY)
White	63	67	62
Asian	6	13	20
Black or African American	11	9	7
Hispanic or Latino	17	8	8
Other	3	3	3

Table 1: Distribution of cybersecurity & STEM jobs based on race

GENDER OF EMPLOYEES	% IN CYBERSECURITY CAREERS
Man	76
Woman	24

Table 2: Distribution of cybersecurity jobs based on gender

It is often said that inclusion in the workspace or lack of role models is the reasoning behind this diversification; while this is true in some sense these are only consequences for why diversity is not occurring.

The root issue is from the lack of preparation and exposure. If someone wants a career in cybersecurity they either A. do not know how to get in because of the lack of guidance or B. start their cybersecurity journey and end up giving up because they do not have efficient resources or support. If someone wants to pursue a career in cyber there are a lot of obstacles to overcome. All of these factors could be avoided if children were given the opportunity to experiment with cyber based technology. The public school system does not do this, K-12 learning requirements do not prepare children for technology based occupations post high school. Students are pushed and influenced by teachers to go to a university post high school but this does not set children up properly for the workforce.

To address this issue, I want to implement the raspberry pi to help teach students about cybersecurity at a young age. Implementing this technology would help teach students technological skills and allow them to experiment and decide if they want to pursue a career in cybersecurity or not.

Related Works

CS Experience, created by the Raspberry Pi Foundation is an amazing example of how this can be accomplished (Colligan, 2025). The raspberry pi just recently released a computer science based curriculum aimed at children between the ages of 8 and 14. These plans are used to conduct a safe and creative learning experience for everyone involved. Each device is programmed for easy use, meaning that computer science qualifications are not needed. This

allows easy access for teachers to educate their students with ease. The best thing about this curriculum is that it's free and available to anyone. Depending on the age range, curriculums are laid out in full, a teacher's guide is provided and units are provided with their own individual side projects. Table three depicts the learning targets prioritized for students in year 2 (ages between 5-7) who are learning computing systems and networks. The resources are here, they need to be implemented across our national school system. Raspberry Pi's goal behind all of this is to reduce the digital skills gap.

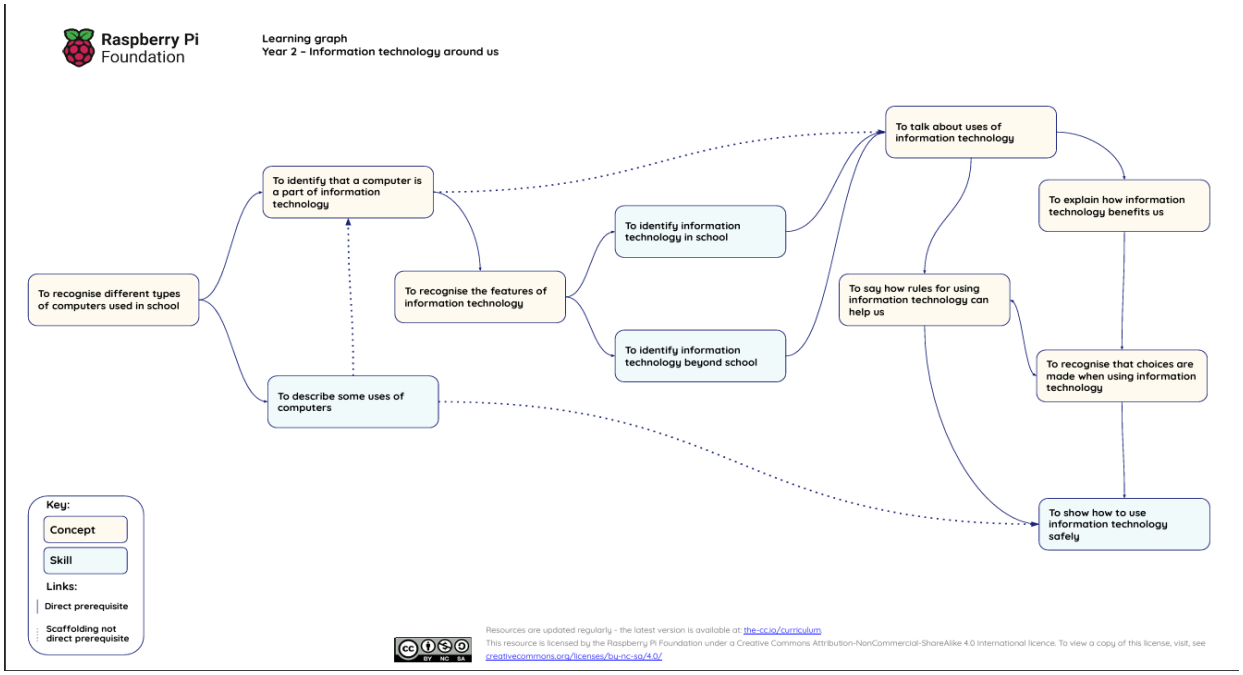

Table 3: Raspberry Pis Year Two(age 5-7) Learning Graph for Information & technology

Another example where the raspberry pi has been implemented into our school system is from a research investigation that was conducted at the University of West England (Legg et al., 2023). In this research cyber range, a commonly used platform used to teach technical skills, is used to teach offensive and defensive cyber concepts in schools. Compared to the CS Experience, this goes a step farther and exposes children to the difference between red vs blue

teaming and what each team entails. In this demonstration, children are given the opportunity to perform blue team skills (ex. harden our security, etc) or become offensive tactics like tampering with desktop files or conducting a nmap scan on a vulnerable computer.

Proposal

My proposal is to implement raspberry pi devices into our public schools to expose children to cybersecurity skills. Similar to what CS Experience has produced and the researchers at University of West England, I want to combine these ideas together. I am proposing a national curriculum that can be implemented all across the country. Just how CS experience made classes for computer science skills, I want this to become a mandatory thing across schools nationwide.

How math, english and science is a requirement for children in elementary school, technology should be another addition. In elementary school, a curriculum like the CS experience should be implemented. Fundamentals of IT and technology should be taught, this will be the place for where technology can be introduced. Later leading into middle and highschool would be when more cybersecurity based projects would be introduced. This allows students to learn technology and be able to gain these skills throughout their academic career while reducing the digital gap in America. Even if children decide that they do not want to pursue a career in cybersecurity, when leaving high school they will be more technologically prepared when entering the workforce.

I have chosen this specific device because of its inexpensive cost and multipurpose capabilities. The cost to set up a raspberry pi is no more than fifty dollars per breadboard. Each pi can be hooked up onto a monitor and used as a small computing device, almost similar in function to a computer that costs on average 600 - 700 dollars. The cost to distribute these devices to each school would be literally nothing in comparison to giving schools thinkpads.

Aside from the cost, raspberry pi's can be used for everything: what can be done on a computer can also be complete on a pi, plus more. Below is a mocked up curriculum of how these cybersecurity topics would be taught:

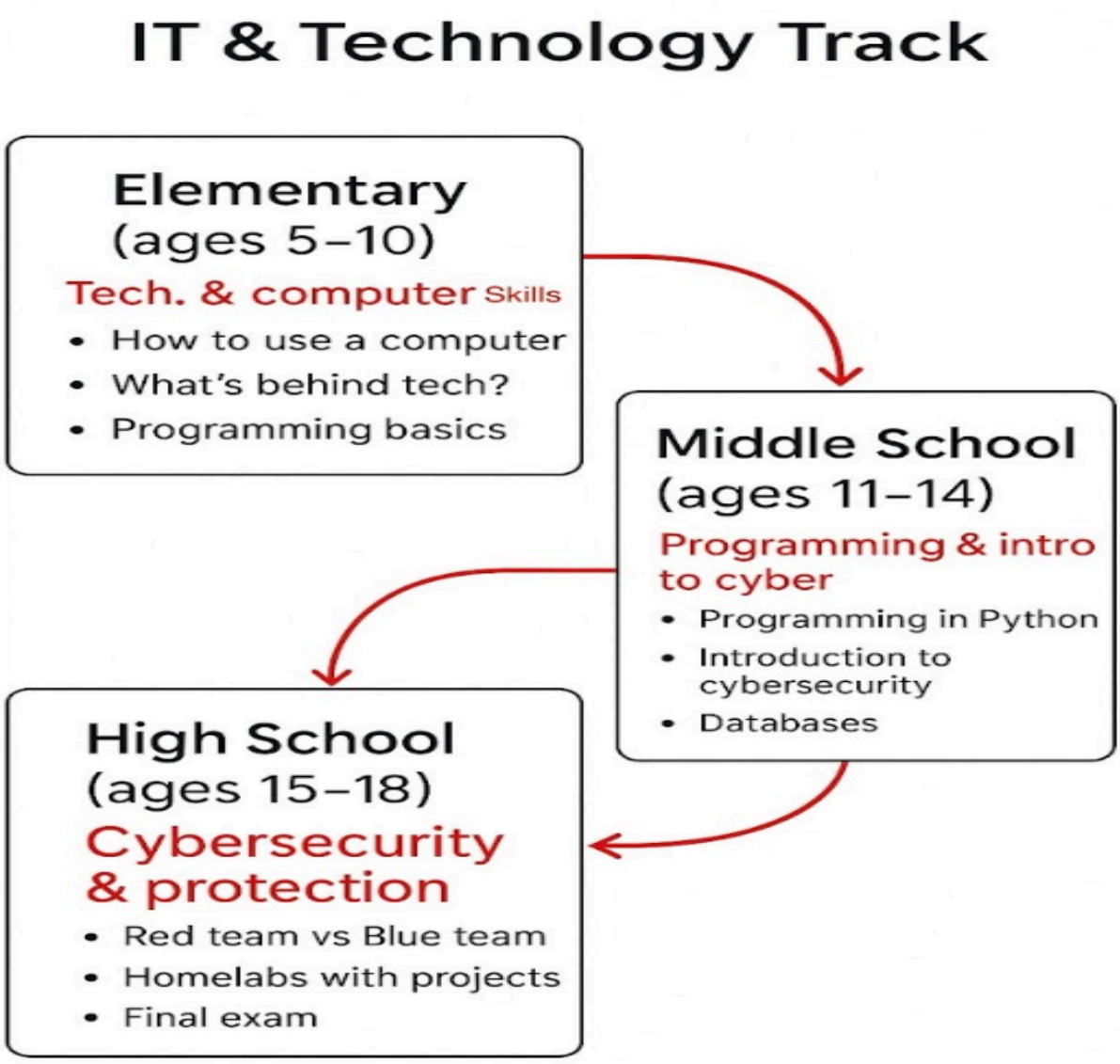

Table 4: Ideal Cybersecurity & Technology Proposal

Table 4 contains a small example of how this curriculum would be implemented into our public school. Starting off at elementary schools the first core concept that would be taught

would be “Technology & Computer skills”. During this time children will become acclimated with how to use a computer (i.e. improving mouse skills, learning how to navigate through a computer, etc), the overall high level concept for how the internet and networks work together, and lastly a small introduction into programming. Middle school students would learn the concepts of programming and have an introduction of cybersecurity. During their time at school they would be introduced to python programming and also learn some key concepts like how data is stored via online and how cybersecurity is incorporated in protecting this data. Lastly in high school is when more hands-on cybersecurity projects would be implemented. Children would learn what the meaning behind red vs blue teaming while also experimenting with hands-on projects like homelabs. Once all of this is complete students will be evaluated and be given a final project or exam to determine the successfulness of their training. This final assessment will contain all of the previous modules that have been taught, since each unit and core concept is based on another, each unit will be included in this evaluation.

Including this technology into our school systems would allow for exposure. This exposure will allow students to be able to experiment with these security concepts at an early age to help them decide if they want to pursue a career in cybersecurity. By implementing and approving this proposal, this will allow an increase of diversification in the current cyberwork force.

Conclusion

Cybersecurity is the backbone of American infrastructure, in order to strengthen this and reduce the technological skill gap, diversity needs to be increased. The way for this to be accomplished is through exposure. How can this be accomplished?

Implementing the Raspberry Pi into our educational system is a great way to improve diversity in the cybersecurity industry. Allowing students at a young age to experiment with

these technical skills will allow them to learn technical skills which will better close the technological gap in America. By allowing more students to be exposed to these cybersecurity concepts will allow a wider range of people aspiring to break into the cybersecurity field. By incorporating more people into the industry, this will allow for different perspectives to protect our networks while also being able to expand our technological network capabilities.

References

P;, G. L. (n.d.). *Diversity improves performance and outcomes*. Journal of the National Medical Association. https://pubmed.ncbi.nlm.nih.gov/30765101/

Mountrouidou. (2019, December 18). *Securing the human | proceedings of the Working Group reports on innovation and Technology in computer science education*. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. https://dl.acm.org/doi/abs/10.1145/3344429.3372507

Why diversity in Cybersecurity Matters. Explore Cybersecurity Degrees and Careers | CyberDegrees.org. (2022, November 16). https://www.cyberdegrees.org/resources/diversity-in-cybersecurity/

Colligan, P. (2025, March 27). *Experience CS: A new way to teach computer science*. Raspberry Pi Foundation. https://www.raspberrypi.org/blog/experience-cs-a-new-way-to-teach-computer-science/

Arthur, R. (2025, January 24). *Addressing the Digital Skills Gap*. Raspberry Pi Foundation. https://www.raspberrypi.org/blog/addressing-the-digital-skills-gap/

View of teaching offensive and defensive cyber security in schools using A raspberry pi cyber range: Journal of the colloquium for information systems security education. View of Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range | Journal of The Colloquium for Information Systems Security Education. (n.d.). https://cisse.info/journal/index.php/cisse/article/view/172/172

Cooks-Campbell, A. (2025, January 21). *What diversity in the workplace means and why it's essential for teams*. BetterUp. https://www.betterup.com/blog/what-diversity-really-means-and-why-its-crucial-in-the-workplace