Idaho Cyber Heroes: Helping Individuals Navigate Career Pathways in Cybersecurity

August 2021

Team Cyber League

Aaron Goin, Boise State University

Cole Branter, University of Idaho

Leah Johnston, Lewis-Clark State College

Ritchie Rodriguez, College of Eastern Idaho

INL Mentor

Jade Hott, Idaho National Laboratory

Abstract

In 2019, there was a shortage of 3.5 million qualified cybersecurity professionals. Cyberattacks are ever on the rise, making it increasingly important these positions be filled quickly. The purpose of this research, as part of the Idaho Cyber Research Project, was to use information collected from open-source materials to depict the career path issues in cybersecurity for individuals. Interviews with professionals from various industry sectors in Idaho also influenced the course of our research. Early research revealed that one of the main problems is an unclear career path for individuals wanting to enter the cybersecurity workforce. Unclear pathways are defined by of a lack of awareness about a career field, uncertainty surrounding the knowledge and skills taught in college due to a lack of standardization between institutions, high qualification standards in hiring, and a lack of diverse representation in the cybersecurity workforce. Additionally, a platform called CyberKnights was assessed as it applies to the individual and their pathway. However, CyberKnights is not the only solution to this problem, and further research is needed to identify additional solutions.

Table of Contents

Introduction

Guards, guns, and gates! Before the time when computers and new technologies were integrated with physical systems, security was very different. Companies had a security guard during the day and ensured they locked their doors at night. Today, a person sitting at a restaurant sipping on coffee could be quietly collecting information from the people around them. The problem is there are not enough qualified people working in the field of cybersecurity to protect cyber assets. As of 2019, there was a shortage of 3.5 million professionals.[1] Cyberattacks are ever on the rise and these empty positions must be filled quickly. However, it is imperative these positions are filled with not just anyone, but with qualified cyber professionals.

The purpose of this research, as part of the greater Idaho Cyber Research Project (ICRP), was to use information collected from open-source materials to depict the career path issues in cybersecurity for individuals. Early research revealed that the main reason for the shortage of qualified professionals is the lack of defined pathways for individuals to obtain the necessary skills to get a job. Identifying the best pathway an individual should take is not an easy task, as there are multiple routes available. This cohort has explored the following solutions to increase the number of qualified individuals in the cybersecurity workforce: helping high schoolers gain awareness of the cybersecurity field, identifying education and experience required by employers, finding a clear career pathway to that education and experience, and increasing diversity in the pipeline. Additionally, the value of the website CyberKnights will be assessed as it applies to the individual and their career pathway, and how effective it is in mitigating issues in the workforce pipeline. CyberKnights is an online system that aims to assess the talents of its users, offering several tools to manage and map career pathways in cybersecurity. CyberKnights provides tools such as Career Track, a certification identifier, resume sharing, and many other helpful resources to allow the user to map a possible pathway in cybersecurity.

Increasing Career Awareness in High Schoolers

Keeping these tools in mind, CyberKnights would be ideal for individuals who are already aware and interested in cybersecurity. However, what about individuals who are not in the know about cybersecurity? The youth of today are making career-related discoveries in high school. Many sources suggest awareness and self-efficacy are key factors in determining whether high school students pursue cybersecurity careers.[2,3] Luckily, the state of Idaho is involved in efforts to positively impact cybersecurity career awareness and the self-efficacy of high schoolers. However, most of Idaho's efforts are only geared towards increasing students' awareness of cybersecurity. These efforts appear to be effective, but they can be improved by having more programs with diverse role models. Research shows that having role models of the same gender and race positively impacts self-efficacy in students.[4]

Idaho is devoted to increasing cybersecurity career awareness for high schoolers. In 2020, Governor Brad Little emphasized programs that help students become aware of cybersecurity while gaining field knowledge.[5] An example of this is CyberStart, a cybersecurity training program that more than 600 students have participated in since 2018.[5] In addition, Cybercore provides a lab at Idaho National Laboratory (INL) where students can explore secure control systems. INL also hosts an annual summer camp that promotes hands-on activities and games.[6] GenCyber is another resource in Idaho, offering camps for teachers and female students.[7] However, more can be done to engage diverse students, as women, African-American, and Hispanic workers make up a minority of the cyber workforce.[8] One solution is to provide a role model for these students.[4] As the number of diverse workers in cybersecurity is still low, Idaho should continue its efforts to provide role models these students can relate to. This will help increase the self-efficacy of diverse students, adding more unique perspectives to the workforce.

Building the cybersecurity workforce starts with students. However, before students pursue a career in cybersecurity, they must have awareness of the field and self-efficacy. CyberKnights could help find qualified individuals if they have a prior interest in cybersecurity. However, for students who do not have this interest, CyberKnights is probably not the best resource, as it doesn't address self-efficacy. For those who have a stronger interest, they can search for educational options that provide relevant, on-the-job skills. When looking at the individual's pathway to cybersecurity, the decision on what college or university to attend can have a major impact on the quality and relevance of the education received.

Centers of Academic Excellence in Cybersecurity

Many jobs in the cybersecurity industry require a bachelor's degree in cybersecurity, or a related field. A 2016 study found, however, that only 3% of graduates' skills were relevant to cybersecurity.[9] Checking to see if a potential college or university is a Center of Academic Excellence (CAE) is a great way to ensure a student gets a quality education. CAE is a federal program managed by the National Security Agency (NSA) that is focused on helping educational institutions teach the most up-to-date information in cybersecurity.[10]

There are many goals an institution must achieve to obtain and keep accreditation as a CAE. The institution must first apply to become a Program of Study (PoS), then officially become designated as a CAE.[11] As part of becoming a PoS, an institution needs to identify all the knowledge, skills, and tasks learned in the program's curriculum using the NICE (National Initiative for Cybersecurity Education) Framework. This provides a method of standardizing the knowledge and skills gained through the individual's time in the degree program. An individual also gains an in-depth knowledge of what will be taught throughout their time in college. There are also many incentives to joining the federal program, including financial grants, recruitment, and support from the CAE community.[12] There are publicly available guides updated by the NSA with full details about how to become a CAE.

Knowing what is going to be taught provides useful insight, but it doesn't help when it comes to what to expect after graduation. CyberKnights can be an answer to this problem and could be utilized to build CAE-approved curriculum. CyberKnights has the same knowledge, skills, and tasks mapped to real jobs in the cybersecurity career industry inside the "TKSs" website tab.[15]

This can help an individual know what job to pursue after college, making the transition from education-to-career easier and more straightforward.

Requirements and Barriers for a Career in Cybersecurity

Cybersecurity students attending CAE-certified institutions with standardized curriculum is a great start. In addition, it is important to understand cybersecurity is an ever-evolving field, and a dynamic system for updating standards would be a prerequisite for such an educational standard model. If the goal is to gain some ground on the workforce gap, the industry would be best served by providing multiple routes to cybersecurity careers. With no clear educational route, the next best option is to examine what most employers seek as job requirements. In an analysis by Burning Glass Technologies, of over 114,000 jobs in cybersecurity, almost 85% of job postings stated a bachelor's degree as an educational requirement.[17] This overwhelming majority is a strong reason to get a bachelor's degree, suggesting employers have found a 4-year degree empowers a cyber tech to enter the workforce with a well-balanced view of the world of information technology (IT) and security.

Although ideal, getting a bachelor's degree might not be feasible for everyone. The price of education varies, but 2019 numbers show that the average cost of tuition and fees for full-time students is $24,696 per academic year.[18] This is the average between public in-state and out-of-state four-year institutes, as well as private nonprofit four-year institutes. In addition to high costs, there are people with jobs and family responsibilities that make it difficult to fit school into their schedule. Still others may be reluctant to dedicate four years to school without a guarantee of getting a job after graduation. More flexible routes need to be considered for educating individuals for a position in cybersecurity. More importantly, those flexible routes need to satisfy the cybersecurity needs of industry in the same way as more traditional paths to be accepted.

An Associate's degree is another option, requiring half the time and at a lower cost. This focused route would still lay a strong foundation for somebody to start an entry-level position, bypassing many of the general education requirements that typically fill out a Bachelor's degree. One benefit of going this route is an individual would get a better insight to the working environment of IT and could continue schooling later, and with a better understanding of exactly what area of cybersecurity they want to focus on.

Upon uncovering the issues with cybersecurity, it became important to consider the emphasis on skilled and qualified cybersecurity professionals. Research has shown that 3-5 years of experience is required for 46% of these jobs.[17] This starts to paint the picture of cybersecurity as something that takes time and experience to get into. As stated by Ean Meyer, an information security professional, "The major argument around the skills gap seems to be the idea that information security isn't an entry-level job." Meyer then goes on to talk about a lack of entry-level jobs stating, "We can close the skills gap by creating a path for entry-level roles."[20] This makes a lot of sense, as it is impossible to become an expert without first being a novice. Qualifications for positions need to be re-examined and the "required" qualifications need to be a necessity, not just desired. In addition, mentoring and apprenticeship models could facilitate on-the-job learning on the exact systems—not merely similar systems—the apprentice would be maintaining at the end of the apprenticeship (see “Benefits of Internships and Apprenticeships below).

Also, nearly 6 in 10 cybersecurity positions request at least one certification.[23] While certifications shouldn’t be a make-it-or-break-it factor, they can be used to help qualify people who otherwise might be lacking in one way or another. Finding people with experience in IT can be measured by various accredited certifications, ostensibly establishing competency levels regardless of where they are in their careers. Those seeking employment in the industry can pursue a specific certification (e.g., CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), etc.) providing specific paths to help close the skills gap. Having entry-level job roles for people with less education or people with skills in other areas of IT is important. Having those more technical roles for people who have had the opportunity to get a well-versed education, possibly utilizing CAE institutions with a standardized education, is also important.

Much like the other areas, CyberKnights can be used to assist with these goals. CyberKnights is a workforce development tool that connects the individual’s knowledge and skills (K&S’s) back to the NICE framework’s defined K&S’s. This has tremendous potential for linking a person to a job based on technical ability instead of resume achievements. In addition, a job seeker can see what K&S’s are missing for a specific position, cross-reference that with which certifications would teach them those missing K&S’s, giving an even clearer path forward. Although useful, the list CyberKnights provides still requires additional development. Some certifications are missing, and often directions on how to apply for and schedule certain certifications are missing. Core certifications covering many fundamental areas with basic knowledge seem to grant many K&S’s, while professional-level certifications grant fewer K&S’s. This is most likely due to how niche advanced certifications can get, though it can create oddly skewed suggestions favoring less-qualified people. Often, those cyber professionals who are more advanced would have no reason to keep core certifications current, and most likely hold only a couple advanced certifications instead.

This workforce gap is the product of multiple problems and needs multiple solutions. One of the next steps toward finding those solutions is re-evaluating job roles and their requirements, allowing more people with varying education and experience to discover a job role that suits them. Using tools such as CyberKnights to connect employers and employees can help. There are still more ways, such as internships and apprenticeships, to help guide individuals into a cybersecurity role.

Benefits of Internships and Apprenticeships

As mentioned previously, unclear career pathways are one of the biggest hurdles individuals face in their journey to become a cybersecurity professional. Aside from college, individuals are not sure if an internship, apprenticeship, or another option will allow them to attain their desired career. Meanwhile, diverse individuals in the workforce pipeline face challenges such as discrimination that prove to be discouraging and disheartening. As ransomware attacks and data breaches only increase, it is imperative solutions are identified to these problems to quickly guide qualified applicants into empty cybersecurity roles. With thorough research, various options have been identified that can make this a reality. Online tools such as CyberKnights will assist the individual in mapping a clear pathway to their desired career. In addition, internships, and apprenticeships can result in more qualified professionals exiting the pipeline and entering the workforce.

CyberKnights provides users with several tools to assist them in mapping a career pathway. One helpful resource is a website called "Career Track." An individual simply states their current job and tasks, as well as their desired occupation, and the site will map the pathway they must take to obtain the job they want. Overall, CyberKnights is a valuable resource, particularly for college students and those in the workforce looking to identify a pathway that is right for them. Once the individual identifies their pathway, however, it is important they are equipped with the proper skills to confidently preform in their role. By utilizing internships and apprenticeships, the individual can not only gain relevant hands-on experience, but assure prospective employers they are skilled in managing their data and system security.

Internships can be valuable to the undergraduate or graduate student. Not only do internships help one gain, develop, and refine their skills, but afford many other opportunities to the individual such as: giving them an edge in the job market, networking, experience, and confidence. Additionally, those who have completed at least one internship will receive 16% more job offers than those who have not.[25]

There are many ways one can find the internship that is right for them. They can utilize websites such as Linkedin and Internships.com. While internships do have their benefits, there are some downsides. Many internship positions are unpaid, and sometimes an intern can be found performing clerical tasks rather than honing their professional skills. Internships are a good way to start, but if possible, it would be preferable the individual completes an apprenticeship program.

Apprenticeship programs offer an opportunity for the individual to gain much needed field experience. These programs are often compared to internships, but in truth are quite different. Apprenticeships are much more focused than internships, with the individual working directly under an expert in the field, with programs usually lasting between 1-2 years.[26] Additionally, while internships are often geared towards students who wish to gain some experience and build their resume, apprenticeships are intended primarily for graduates who are preparing to enter the workforce. Finally, apprenticeships have been proven to help the individual land a job, as 94% of people who complete an apprenticeship retain employment.[27] By participating in an apprenticeship, an individual can greatly mitigate career pathway uncertainty and gain experience in the field.

A Lack of Diversity in the Cybersecurity Workforce

Another problem an individual will have to combat while making their way through the workforce pipeline is a lack of diversity in the cybersecurity field. A recent study found the cybersecurity field is comprised of only 26% minority members with about 39% of the U.S population being a minority according to the 2020 US census[28]. This leaves a 13% workforce disparity. In Microsoft's 2020 Diversity and Inclusion report, they show that even though progress is being made, 4.9% of their U.S. workforce is African American and only 0.7% is Native American.[29] This is alarming to say the least, considering how many vacant cybersecurity positions there are. Strictly from a logical perspective, if these positions are to be filled, the industry will need to target all groups of individuals, especially minorities. Additionally, companies with a greater percentage of minority employment are 35% more likely to have higher financial gain than competitors, as well as having more perspective, ideas, and employee satisfaction within the organization.[30] It is important minorities feel confident to explore and retain a career in cybersecurity, and there are many resources available that can help.

For elementary and secondary students, there are many established organizations ready to assist minorities in becoming successful cyber professionals. Groups such as Girls Who Code and #YesWeCode aim to teach valuable coding and cybersecurity skills while mitigating diversity and financial barriers. [31] In the collegiate environment, there are also diversity resources to help minority students such as diversity clubs and scholarships. While diversity is quite important during one's educational journey, it is equally important to have diversity and inclusion resources for minorities in the cybersecurity workplace. Some diversity organizations that support minority individuals include Latinos in Information Sciences & Technology Association, American Association of Blacks in Energy, and Chinese Software Professionals Association. By helping future professionals with hurdles that appear along the entire cyber pathway, Idaho will have a larger and more qualified cybersecurity workforce.

Results

The initial results of this collective research indicate there are a few main takeaways on the most effective strategies that fill cyber roles. Idaho is devoted to increasing cybersecurity career awareness for high schoolers. An example of Idaho's efforts, which has been emphasized by Governor Little, is a cybersecurity training program called CyberStart. Since 2018, CyberStart has had more than 600 students participate.[5] Research has shown efforts like these increase awareness of cybersecurity and positively affect self-efficacy in high schoolers.

For students looking to get a job in cybersecurity, many job postings require a Bachelor's degree.[22] Deciding on what college or university to attend can have a major impact on the quality and relevance of the education received. A federal program, called CAEs, is focused on helping educational institutions teach the most up-to-date information in cybersecurity.[12] However, only three colleges are currently CAE certified in Idaho, with seven other accredited colleges in the area surrounding Idaho.[16]

Although ideal, getting a Bachelor's degree might not be feasible for everyone due to the high costs of tuition and balancing other responsibilities. Other educational routes need to be taken into consideration. Even if an applicant has a degree, some professionals in the field have expressed that cybersecurity is not an entry-level position.[20] Apprenticeships and internships can help increase the chances of getting a full-time position after graduation by providing an individual with relevant work experience.[27] Another challenge individuals may face when pursuing a job in cybersecurity is a lack of diversity in the field, with only 26% of the workforce made up of minority members.[28]

Discussion

Through the research conducted, it has become apparent there is further work to be done to solve the issues in the career pathways for prospective cyber professionals. CyberKnights may have a wider influence if there is a section designed to help high school students. If a high schooler was given this resource in its current state, they could become overwhelmed or disinterested. Many specifics about cybersecurity career pathways currently on CyberKnights may not pertain to high school students. If the website included a section that promoted information on cybersecurity careers, as well as provided links to fun activities such as CyberStart, this could be much more effective for this age group. This would be worth testing if having this on the website would yield a positive result from high schoolers. This could include whether high school students who visited CyberKnights later participated in CyberStart or studied cybersecurity in college.

Continuing on the cybersecurity pathway from high school to college, CAEs improve the quality and standardization of college curriculum, while providing greater insight on the knowledge and skills learned in the program. Further research and interviews with institution officials about their experience being a CAE could prove valuable. Gaining this understanding could help explain why there are not more CAEs in Idaho. Gaining a degree from CAEs can help the transition into a cybersecurity role. In general, however, employers posting these positions have high standards for work experience as well. More routes into cybersecurity need to be considered. Focusing on creating entry-level jobs would help increase the number of individuals in the workforce and help close the skills gap. Opening opportunities up to people with less education, little work experience, but with highly specific certifications can be a first step towards this.

If an individual wants to take a route where they earn while they learn, apprenticeships can provide a great opportunity to gain work experience. Apprenticeships provide the individual with valuable experience that employers not only want but need as the apprentice continues to learn and become confident – all while providing value to the organization. Academic institutions from high school to university should advocate apprenticeships to their students, as they are appealing even to a non-traditional student who does not have interest in post-secondary education. Additionally, state and federal governments should emphasize the importance of apprenticeships and provide more funding if possible.

Diversity is also important and has been an overlooked issue in the workforce pipeline. The reality is the lack of diversity will prevent cybersecurity jobs from being filled, as well as limit unique perspectives that help organizations grow. Diversity resources should be endorsed by CyberKnights, as well as by companies that do not endorse it already. Schools and organizations should make it their mission to celebrate diversity and give all individuals equal opportunities, no matter their gender or ethnicity.

Conclusion

Time and technology have shifted what we consider secure. Utilizing tools such as CyberKnights will standardize knowledge, skills, and tasks for a job – as well as helping to mitigate unclear career pathways. Instilling confidence in students will help them pursue a career in cybersecurity earlier. Assisting colleges in obtaining the necessary resources will allow them to become a Center of Academic Excellence (CAE) and teach relevant material. Re-evaluating job roles and their requirements, especially for entry-level roles, will bring more people into the cybersecurity field. Apprenticeships and internships help individuals gain relevant experience. Finally, diversity will be at the forefront of these efforts, helping the cyber workforce become larger in quantity and perspectives. The shortage of cybersecurity professionals creates a complex problem that is difficult to solve. But with continued research and efforts from organizations, the cybersecurity workforce pipeline can and will be fixed. For the sake of our country, it must be.

References

[11] Application Process and Adjudication Rubric, Working Group. (2021). *Proposed Designation Requirements and Application Process for Cyber Defense Education*. National Centers of Academic Excellence in Cybersecurity. Link (Retrieved on June 30, 2021).

[7] Boise State. (2021, July 6). *GenCyber - Inspiring the next generation of cyber stars - Computer science.* Computer Science. Link

[12] Bowcut, Steven. (May 5, 2021). *Centers of Academic Excellence in Cybersecuirty (CAE-C) guide.* Cybersecurity Guide. Link (Retrieved on June 22, 2021)

[16] *CAE Instituion Map.* CAE community. Link (Retrieved on June 22, 2021).

[17] Callie Malvik. (03/22/2021). Is a Cyber Security Degree Worth It? Analyzing the Facts. Link

[2] Crandall, K. S., Crandall, K., El-Gayar, O. F., & Noteboom, C. (2019). *High school students? Perceptions of cybersecurity: An explanatory case study*. Issues In Information Systems, 20(3)

[6] CSI Workforce. (2021). *Cybercore summer camp*. CSI Workforce Development and Training. Link

[1] Cybercrime Magazine. (2019, October 24). *Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021*. Link

[5] *CyberStart America encourages Idaho students to pursue cybersecurity education.* (2020, October 30). Office of the Governor. Link

[27] *DISCOVER APPRENTICESHIP: EARN WHILE YOU LEARN TODAY*. (2020, September). APPRENTICESHIP.GOV. Link

[20] Ean Meyer. (08/16/2017). The Skills Gap is an "Entry-Level" Problem. Link

[8] ESG, & ISSA. (2020). *The Life and Times of Cybersecurity Professionals 2020*. Enterprise Strategy Group. Link

[31] G.W. (2021, June 14). *WE'RE BUILDING THE WORLD'S LARGEST PIPELINE OF FUTURE FEMALE ENGINEERS.* Girls Who Code. Link

[30] Hunt, V., Layton, D., & Prince, S. (2021, March 12). *Why diversity matters*. McKinsey & Company. Link

[15] *Knowledge, Skills, and Tasks*. CyberKnights. (n.d.). Link. (Retrieved on July 14, 2021).

[3] Konak, Abdullah (2018) "Experiential Learning Builds Cybersecurity Self-Efficacy in K-12 Students," Journal of Cybersecurity Education, Research and Practice: Vol. 2018 : No. 1 , Article 6.

[4] Kricorian, K., Seu, M., Lopez, D., Ureta, E., & Equils, O. (2020). Factors influencing participation of underrepresented students in STEM fields: Matched mentors and mindsets. International Journal of STEM Education,7(1).

[9] Kroll, Steven (Mar 6, 2019) *Only 3 Percent of U.S. Bachelor's Degree Grads Have Cybersecuirty Related Skills*. Cybercrime Magazine. Link (Retrieved June 16, 2021).

[21] Marc Van Zadelhoff. Lindsey Lurie.(05/03/2017). It's Not Where You Start – It's How You Finish. Addressing the Cybersecurity Skills Gap with a New Collar Approach. Link

[29] McIntyre, L. (2020, October 23). *Microsoft's 2020 Diversity & Inclusion report: A commitment to accelerate progress amidst global change*. The Official Microsoft Blog. Link

[18] Michael Hansen. (05/18/2021). The U.S. Education System Isn't Giving Students What Employers Need. Link (Also See Appendix C Graph 4)

[26] P. (2021, February 28). *Difference Between Apprenticeship and Internship (With Table)*. AskAnyDifference.Com. Link

[28] Reed, J. (2017). *Innovation Through Inclusion: The Multicultural Cybersecurity Workforce*. Ics2.Org. Link

[10] *What is a National Center of Academic Excellence in Cybersecurity (NACE-C)?* (n.d.). National Centers of Academic Excellence. Link (Retrieved on June 17, 2021).

[23] Will Markow, Scott Bittle, Pang-Cheng Liu.(June 2019). Recruiting Watchers for the Virtual Walls. The State of Cybersecurity Hiring. Pg 11. Link

[25] Zuckerman, A. (2020, May 26). *98 Internship Statistics: 2020/2021 Data, Trends & Predictions*. CompareCamp. Link

Appendix A: Summary of Other Summer Projects

To help our cohort's progress, we participated in other activities as part of this INL internship. They are listed below:

- Intern enrichment sessions: These meetings discussed several scientific projects that take place at INL, as well as employment opportunities that help us become equipped with being more prepared to secure employment.

- ICSCOP Briefings: Provided the opportunity to access industry professionals who provided feedback on the research questions we posed.

- Meeting with Organizations: Some of the cohort visited organizations that had an IT department, as well as educational institutions that are involved in this workforce pipeline. Members would discuss with the organization what their needs were, what programs or tools they would be open to implementing, and much more.

- Splash Page Development: Throughout the summer we worked on developing a cohort webpage for INL. The purpose was to inform and educate viewers about Cyber League's progress, research, and findings.

- Cyber Escape Room Development: We shared our ideas on how to create a cyber escape room. Our ideas and suggestions were based off of the content we learned from the 301V course provided by the Cybersecurity and Infrastructure Security Agency (CISA).

- Cybersecurity Training: We were able to get some cybersecurity training from CISA, as well as a 2-day course called CyberFire Toaster. This allowed us to gain perspective on defending ICS systems, as well as the training an individual might partake in.

- Municipality Review: We identified cybersecurity incidents and data breaches that occurred in different towns in Idaho, and then the greater world. Ideas of cybersecurity positions that could have stopped these incidents were also discussed in these reviews.

- University Curriculum Experts: There was also an opportunity to meet with the cybersecurity curriculum experts at University of Idaho and Boise State University. They briefly discussed their efforts in establishing curriculums that would best prepare students for the workforce. Cyber ranges were established as a way to practice on the job skills, as well as having industry professionals be instructors for classes. This perspective was much appreciated, as their efforts were recognized beyond descriptions of curricula on a website.

Appendix B: COSTAR Pitch

This was an opportunity to present our problem statement and solutions to a crowd of other interns. We did it using a sales pitch format, and then received feedback. Here are some takeaways:

- Hook: Our introduction was effective overall, as we asked a series of adaptive questions to a hypothetic boss in an elevator. Some of these included: “How much do you care about cybersecurity workforce problems?” and “What do you think the solution is?”. Overall, the audience appreciated our introduction. As there was not an actual person we were pitching to, it proved challenging to demonstrate this. However, our cohort is confident that this strategy would be effective in a real-life scenario.

- Customer: We identified the main customer as the individual in the cybersecurity workforce pipeline.

- Opportunity: We also identified the problem of unfilled positions in cybersecurity, and the large scale of this opportunity.

- Solution: We provided CyberKnights as a solution, while including other solutions such as resources for diversity and work experience. One criticism for this section was that it wasn’t strong enough of a solution in terms of the belief behind it. Other people thought that it was too strong, and that we were relying on CyberKnights to be the ‘perfect’ answer to everything. As we reassessed our paper after this presentation, we widened our argument of solutions beyond just CyberKnights. This also illustrates the idea that offering multiple solutions with confidence can balance out criticisms we received: having fairly strong solutions to cybersecurity workforce problems that we believe in.

- Team: We then identified who needs to be on the team. We identified as those with educational, curriculum information, CyberKnights users, those with an interest in cybersecurity, and those who are knowledgeable about work qualifications. We also explained how our research is backed by industry professionals in ICS and by the INL.

- Advantage: Finally, our results of our solution indicated more fulfilling careers for individuals, reduced cyberattacks, and more clarity to pursue cybersecurity careers through CyberKnights. Some felt like this section was disjointed and did not present a clear/concise solution. It lends itself back to the research itself, and that there are multiple problems with multiple solutions. It is a problem worth researching on a continual basis, and one that may not have a concise answer that is agreed upon by everyone.

- Results: The most promising thing from this session was the agreement of our problem, and that most people in the COSTAR pitch recognized our problem, and the fact that any solution to it is better than no solution. The pitch itself would have worked better with individuals who may pursue a cybersecurity career, educators, or industry professionals, as that is what it was designed for. In actual elevator pitches that happen outside of a facilitated COSTAR session, you have less time to figure out what the other person values and explain how your solution matches up. This means that there could be parts of the COSTAR format that get abandoned or changed to maintain relevance in the real-world conversation. Our cohort is confident that our pitch is better applied in the worlds of individuals we are addressing, and less applicable in that environment. We have determined that the best way to do that is to have adaptive questions to figure out what the individual values, and then matching that value to anything related in our research.

Overall, despite the feedback being mixed, we believe that our adaptive approach was effective, and that our solutions will adapt to the exact problems each individual has. Since individuals have a variety of values in terms of their career choice, we want to have a solution that has a wide net and can catch a variety of individual values. This will serve more people.

Appendix C: Related Visuals

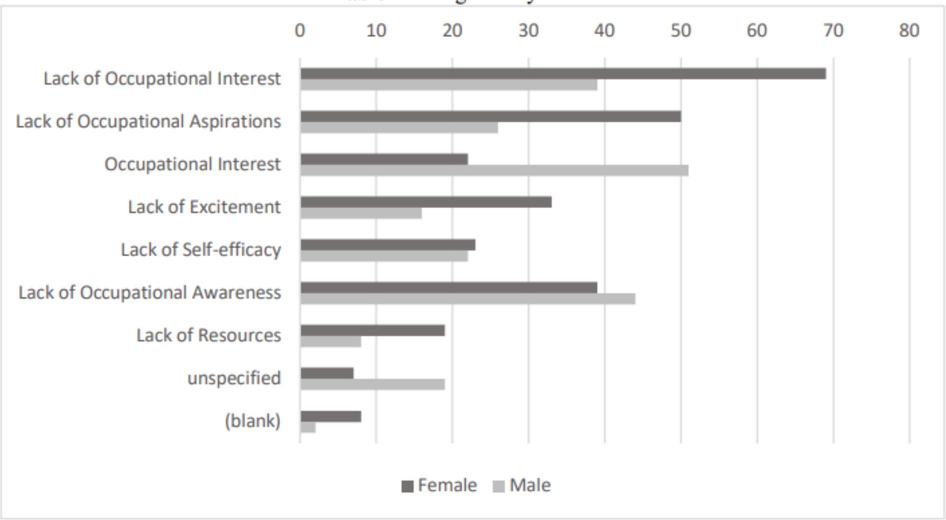
What prevents high school students from pursuing cybersecurity careers? Crandall and fellow researchers conducted a study where they asked high schoolers the things that would prevent them from pursuing a cybersecurity career (2019). Most students responded with the following reasons: lack of occupational interest, occupational awareness, and occupational aspirations. In their research, occupational interest and awareness appeared to be linked to self-efficacy, which is described as how a student views their own abilities [2]. Increasing a student's self-efficacy is the main recommendation from Crandall et al.'s research, which starts with increasing a student's awareness of cybersecurity careers (p. 78-79). This research makes sense, as it would be hard to be interested or inspired about a topic if it is unknown to the individual.

Reason for not pursuing a cyber career	Number of Students
Lack of Occupational Interest	108
Lack of Occupational Awareness	82
Lack of Occupational Aspirations	76
Occupational Interest	74
Lack of Excitement	49
Lack of Self-efficacy	46
Lack of Resources	27
unspecified	26
blank	10

Source: (Crandall et al.,2019, p. 6) Chart 1

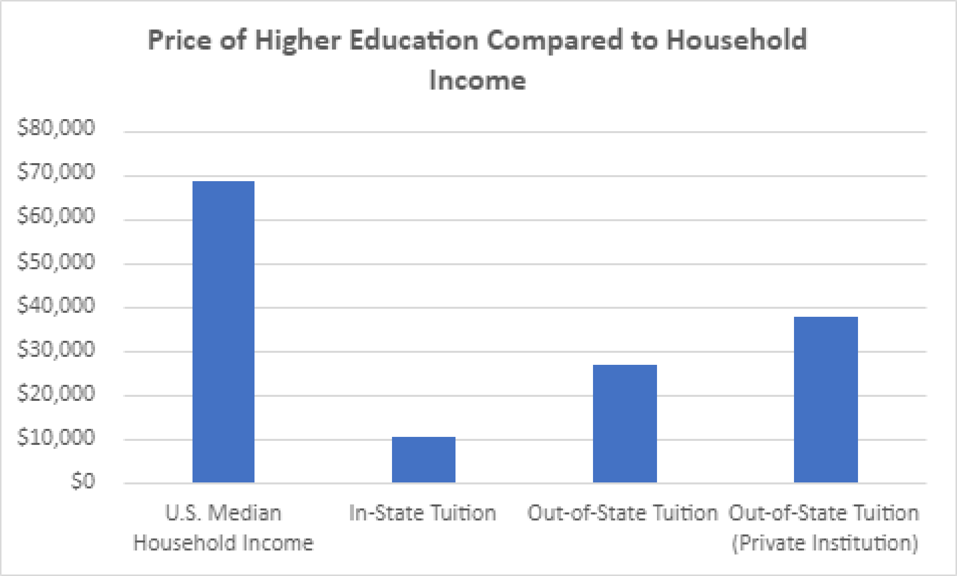
From the same study, here's a graph that separates the responses by gender.

Table 4. Categories by Gender



Source: (Crandall et al.,2019, p. 8) Graph 1

The price of education varies but a statistic shows for the year of 2019, tuition and fees alone reached as high as $10,560 for in-state students at 4-year public institutions. The cost jumps up to $27,020 for out-of-state students and $37,650 for private institutions [18].



Reference 18 - Graph 2