Essay: Cyberpath One Stop Application

Faith Weems

Old Dominion University

CYSE 595: Entrepreneurship in Cybersecurity

Dr. Brian Payne

June 20, 2022

Overview

In this paper, it will address a recent concern pertaining to cybersecurity that has been an issue for the past few years. This matter pertains to the lack of cybersecurity professionals that are in the workforce. As technology continues to advance, there becomes more of a need to protect it. It cannot be efficiently protected if there are not enough professionals to ensure its safety. In this review, there are multiple problems being addressed. These problems include:

- The increasingly amount of cybersecurity attacks
- The lack of cybersecurity professionals in the private and government sectors
- The lack of women and minorities that are cybersecurity professionals
- Lack of curricular in cybersecurity at colleges and universities

Throughout this paper, I will detail the offerings that the Cyberpath One stop Application has and how it will solve the problems mentioned above. In order to increase the amount of working cybersecurity professionals, they must be given the tools to successfully enter this career. This application is a one stop for all upcoming and current cybersecurity professionals. The application has resources for individuals from each skill level. The application offerings include:

- Mentoring from cybersecurity experts that are currently in the field working
- Access to information pertaining to bootcamps and certificates from colleges and universities
- Ability to chat with others via private chat or through forums.
- Ability to participate in 1 of 10 paid apprenticeships offered throughout the year

- Job board that will help assist in the job search, which includes detail description of requirements
- Resources and tools (videos and literature that assists with continued learning in risk assessment, phishing, and awareness)
- Study plans for additional certifications
    - CompTIA A+ (foundations)
    - CompTIA Network+
    - CompTIA Security+ (requirement for many positions)
    - CompTIA PenTest+ (specialized)
    - CompTIA CASP+

Literature Review: Problem

In recent years, there have been numerous data breaches and attacks brought to light by the media. The most well-known kind of attack being the ransomware attack. For example, the media and internet blew up over last year's ransomware attack, known as the Colonial Pipeline attack. Colonial Pipeline is one of the largest fuel pipelines in the United States. This attack was detrimental, compromising thousands of individuals personal information and causing the pipeline to go offline. As a result of this shutdown, Americans were in fear that this would cause a shortage at gas stations. Eventually, this shortage became widespread and caused an uproar in the media. To remedy the situation, Colonial Pipeline paid a ransom of almost 4.5 million dollars to the hacking group. In the end, the government was able to recover much of the money paid in ransom to the hackers. Without cybersecurity professionals, Colonial Pipeline might have never recovered from that attack.

Experts have stated that the United States is just as or even more vulnerable to cyberattacks (Marks & Schaffer, 2022). This vulnerability is due to the constant improvement of cybersecurity and the complexity of our digital society outpacing the efforts to keep up. The nation has become more reliant on technology, which increases the targets that hackers can aim at. There is a clear issue with the reliance on technology because most technology is built without security being the top priority. One of the easiest targets has been an array of Internet-connected devices, such as cameras and refrigerators. These Internet-connected devices are commonly referred to as Internet of things or IoT. These IoT devices are known for relying on default passwords and being difficult to update software patches. Because these devices have weak security, they are extremely easy to hack.

Cybersecurity has received a great amount of attention lately. This media attention started with the SolarWinds cyber-attack that occurred in 2020. The SolarWinds attack is known to be the most sophisticated in history that had a global impact. It was a software supply chain attack that compromised a large amount of SolarWinds' clients. These clients include government agencies and top businesses, such as Microsoft and FireEye. The frequency of malicious breaches continues to increase. In fact, there is a current attack plaguing the nation, which is known as the log4j vulnerability. This vulnerability is known to allow hackers to run code on any machine or application that is vulnerable. Many companies don't even know that they have it unless they are looking for it, even then, sometimes it can't be found. Due to the increased number of attacks, the demand for cybersecurity professionals is great.

The lack of cybersecurity professionals has not only affected the private sector, but also the government. The government is struggling to hire cybersecurity specialists, while it is facing

an unprecedented increase of hacking threats. The shortage of cyber workers is making it difficult to protect government data from being stolen by hackers. This has resulted in the diminishment of the governments abilities to help improve cybersecurity in industries that are vital to national and economic security (Marks, 2021). It also continues to increase the dangers posed by the government's systems, which are known to be outdated.

For the government to be able to resolve some of these issues, they will need more trained cyber specialists. Although there is a lack of cybersecurity professionals, the government's cyber workforce has increased by 8 percent since 2016 (Marks, 2021). The increase in the government's workforce is a positive thing, but it is nowhere near sufficient to meet and combat the cyber threats. At some federal agencies, including the Labor and Agriculture departments, the cyber workforce since 2016 has shrunk. Only 25 percent of government cyber workers are females and there are 16 times more federal IT workers older than 50 than there is younger than 30 (Marks, 2021). This trend implies that most of the government's cybersecurity workers are not new to the profession.

What are a few ways that the government can resolve this lack of cyber workers? First, they should hold the government officials accountable because their agencies can't retain cyber workers. Second, they should create paid internships for young cybersecurity professionals and make it easier for them to move into government jobs. Lastly, they should increase the salaries of cyber professionals that will compete with the private sector. The government has a lack of cybersecurity workers because of the lengthy hiring process that is difficult to navigate and the inflexibility, which turns younger workers off. Using these techniques will not only increase the governments cyber workforce, but also increase employee retention.

Amongst the shortage of cybersecurity professionals, women and minorities are underrepresented. The underrepresentation of minorities and women in computer science has been a concern to industry, government, and universities for over 10 years (Burrell & Nobles, 2018). In fact, only 3% of cybersecurity analysts in the United States are African Americans. Today, only 11% of cybersecurity professionals are women (Gonser, 2019). Diversity can enhance knowledge and provoke new practices by adding to the organization's intellectual capacity and innovative ideology. According to Gonser (2019), the Bureau of Labor predicts that jobs for cybersecurity specialists in the United States will grow 28% by 2026. Corporations can benefit by providing women and minority students with internship opportunities to gain real-world work experience and to highlight the qualities and capabilities of those desiring to enter the cybersecurity workforce.

When looking at the statistics of cybersecurity professionals across the nation, there is a clear deficit. In fact, there are nearly 465,000 unfilled positions in cybersecurity across the nation (Marks, 2021). The number of unfilled positions will increase if there isn't a change in the way that the government and private sector trains and hires individuals. Colleges and universities have initiated cybersecurity bootcamps and programs. Given the newness and lack of curricular consensus in cybersecurity, education providers have struggled to keep up (Sobel et al., 2019). Typically, cybersecurity work requires a bachelor's degree in computer science, programming, cybersecurity, or systems engineering (Gonser, 2019). In many cases, certifications are required, such as CompTIA A+, Security+, and Network+. These programs are intended to introduce growing professionals to a possible career in cybersecurity. Although there are new educational offerings, there is still a need for more engagement from the cybersecurity education community.

Literature Review: Innovation

One of the most important offerings that the Cyberpath One Stop Application has is the high-quality mentoring. Mentoring is the process by which an individual with advanced experience and knowledge assists, guides, and supports a less experienced person. This support and guidance can concern the mentee's personal life, professional life, or career development. Mentoring services are offered for individuals that are at all levels. These services are provided to individuals that are seeking a career in cybersecurity, new to the career, and more experienced cybersecurity professionals. Companies and businesses can use these services as well by joining the program that provides mentors, while also having individuals that are mentees. This ensures that there is a revolving, steady flow of mentors and mentees. The mentoring services provided are considered formal mentoring services. Formal mentoring is assigned through the organization and are sometimes assigned at initiation or developed through mentoring programs (Fowler et al., 2021). In this case, the mentoring is formal because it is developed through mentoring programs.

When done effectively, formal mentoring programs are a great value for mentees, mentors, and the organizations in which they work. In fact, organizations who benefit from the implementation of formal mentoring programs use those services to enhance their organizational effectiveness (Fowler et al., 2021). Organizations benefit from mentorships, but what affect does it have on mentors and mentees? Studies have proposed a vast range of positive outcomes for mentees. For example, being a mentee has been associated with increased job satisfaction, self-

esteem, opportunities for promotion, career opportunity and mobility, career planning, and lower stress levels (Fowler et al., 2021).

Having the opportunity to be a mentee myself, it was a truly enriching experience. People don't always speak on their experiences but switching careers and/or majors is very intimidating. Starting from earning a Political Science/ Pre-Law degree to then working on a degree in Cybersecurity was extremely stressful and frightening. Oftentimes, it is still a shock how many trials were faced, confronted, and succeeded through. Without having a mentor for the past year, I am not sure where my career would be. There were times that giving up seemed to be the best option, but after speaking to my mentor, giving up was completely off the table. Coming from a small town, I never expected to have so much support from individuals outside of my family and friends. Mentoring has been extremely impactful in my life, so giving others that same opportunity is a passion of mine. Mentoring can be life-changing and having that encouragement in your life is very impactful.

Not only does mentoring impact the organization and mentee, but also positively affects the mentor. Studies show, the mentors reported higher levels of job performance, organizational commitment, job gratification, and better retention rates (Fowler et al., 2021). Mentors have also shown an advancement in technical expertise, managerial skills, and leadership. The man that mentored me and gave me my start, asked if I would like to mentor others. After being a mentee for a year, I had the pleasure of mentoring others. It is rewarding helping someone else, while also remembering the great mentoring that you received and remaining humble in that.

Mentoring has a lot of excellent benefits. In fact, it was concluded that employees prefer to function and remain in a work environment that provides challenges, offers new opportunities, and provides the opportunity to advance while assisting personal development (Fowler et al.,

2021). These are important factors in a mentoring relationship. While being mentored, I received a different outlook on my career and goals. At the beginning of being mentored, there was a complete lack of motivation. Accountability in mentoring is beneficial, which is what it provides. Some individuals need to hear what they are doing wrong from someone that is not a friend or family member. This essentially motivates that individual into realizing that something must change. In other words, mentoring can give someone a completely different perspective then what they once thought.

Lastly, employees that are involved in mentoring relationships feel more support, are more committed and pleased, and are less likely to leave than employees that do not have a mentorship relationship (Fowler et al., 2021). Employees involved in mentoring are also more likely to mentor others in the future. In order to ensure the success of the Cyberpath One Stop Application, those that start out being mentees should eventually elevate to become mentors. This will ensure that there are plenty of mentors and will reveal the quality of the mentoring services.

Another offering that the Cyberpath One Stop Application has is the ability to chat with others via private chat or through forums. This provides everyone using the app the ability to network and aid in career development. Networking is an important aspect of career development and can be beneficial in starting a new career. There are many opinions pertaining to the definition of networking. Networking is a supportive system of sharing information and connections among individuals that have a common interest (Dinning, 2017). In other words, networking is not about collecting as many business cards as you can get your hands on, it is about building relationships.

One of the reasons that I am successful in my life is due to the networking that I am constantly building and maintaining. For example, I decided to take a temporary job through a temp agency working as an Administrative Assistant. My job duties included scanning paperwork, checking Covid-19 vaccination cards, and inputting them into the system. The job was set to only last a little over a month. The man I worked for was head of HR and he saw the efforts I made and the thoroughness of my work.

Once the job was near its conclusion, my boss suggested that I apply for a full-time position directly through the company. The week before the job was set to end, my boss and the only contact I had at the company to speak on my behalf, went into retirement. When the role was complete, I decided not to come back, and I thought all hope was lost. A few weeks after, there was a position posted at that same company for an Engineering Program Compliance Coordinator. Soon after applying, my old boss sent me a text message checking in on me and asking if there were any jobs that I applied for. Shortly after, he spoke on my behalf to the hiring manager, and I was able to secure the job that I applied for.

After experiencing what networking has done for me in my professional life, it is important that the application has a feature to help others get their start as well. You never know who is listening or who is watching. Networking can give an individual the big break that they needed. In fact, networking enables us to gain new information, understand others' viewpoints, develop ourselves, and gain new friendships and connections (Dinning, 2017). We can learn through these relationships and must be open to what experiences can come from them.

In order to get the most out of networking, it is important to utilize a record-keeping system. An example of a quality record-keeping system is LinkedIn. LinkedIn is a great application to make connections, stay connected, and find connections. How does an individual

network? In order to network, one must be visible, both online and in person. Visibility and putting yourself out there are the main aspects of quality networking. After visibility is achieved, connect and reconnect. Outreach is extremely important, but it should be done frequently instead of just once. For the connections to grow, the seed must be planted, which in this case is done by reconnecting and follow-up.

The Cyberpath One Stop Application provides information on bootcamps, certification programs, and undergraduate programs from colleges and universities. Instead of having to go through tedious processes to find a school and cybersecurity programs, the application does that all-in-one click. Education is imperative to start a career in cybersecurity. In fact, an educated workforce is essential to building systems that are trustworthy (Schneider, 2013). In most cases, a bachelor's degree is required to pursue a career in cybersecurity, but it varies based on the position applied for, certifications received, and years of experience.

Along with information on furthering education, Cyberpath One Stop offers training modules, videos, and literature that assists with continued learning in risk assessment, phishing, and awareness. These services are offered to the daily user and/or businesses and corporations that seek to enhance awareness and training. As cyber-attacks have continued to increase exponentially, the need for and importance of security training for employees is growing as well. According to Kweon et al (2021), security training and education are effective methods for cyber-attacks within academia and industries.

With Cyberpath One Stop, businesses can get up-to-date awareness training for their employees to reduce or eliminate cyber threats. It is known that many cyber threats occur from human errors. For example, assets can be leaked due to an employee's careless behavior. This can be done by downloading e-mails send by an unidentified sender, checking linked pages

without caution, or setting passwords that are easy to guess. Employees are considered the weakest point of firms when it comes to information security (Kweon, 2021). In other words, employees and their human errors are most likely to cause cyber threats, whether done intentionally or unintentionally. In order to prevent this, implementing information security training and education is used to effectively enhance security capability.

To compliment the training and educational offerings that Cyberpath One Stop has, it provides the user with study plans for additional certifications. These certifications include:

- CompTIA A+ (foundations)
- CompTIA Network+
- CompTIA Security+ (requirement for many positions)
- CompTIA PenTest+ (specialized)
- CompTIA CASP+
- CompTIA CySA+

In addition to the many offerings that Cyberpath One Stop has, it provides an updated job board so the user can see what jobs are currently in their location or nearby. It is important to read and understand the requirements for each role in order to find the position that best suits the individual and their qualifications. If there is a role that peaks the user's interest, but they do not have all the qualifications needed, the user can take advantage of the other services offered. This will allow the user to focus on the qualifications still needed and they can apply later for positions in that role.

Lastly, the Cyberpath One Stop Application will offer ten paid apprenticeships per year. In order to decide who will receive these apprenticeships, there will be an application process to

ensure the candidates are deserving and serious about entering a career in cybersecurity. The paid apprenticeship includes:

- One year of work experience: Includes a paid internship at a partnering company located near apprentice
- Work at your own pace courses from an accredited college/university
- Mentoring services to guide the apprentice along the way
- Completion of courses will result in an ungraduated certificate in Cybersecurity
- Free access to all Cyberpath One Stop services for a year

The apprenticeships being offered are intended to change someone's life in a positive way, while assisting them in their future career in cybersecurity. Having been a cybersecurity apprentice myself, the experience was overwhelming. I never thought that I would be given the opportunity to learn and discover my passion as easily as I did. After completing the apprenticeship program, I found out that I was one of eight people chosen from over one thousand candidates. Knowing the joy that the apprenticeship brought me, made me want to help others in their cybersecurity journey.

Relation to Material Outside of Cybersecurity

The innovation and problem closely relate to material covered in my communications class. The Cyberpath One Stop application is focused on communication, such as the use of networking and mentoring. For these problems to be addressed, individuals need to start openly communicating about their expectations and goals. Some fear the thought of communication, but most results happen when open communication is welcomed. The news and media have communicated these issues with the public and government officials, but nothing seems to get

resolved. When will enough be enough and we start to see results? How many more cybersecurity attacks must occur before changes are made?

One could say that the lack of cybersecurity professionals is a lack of communication, a lack of trying, or a lack of caring. This application is only a small step, but the bigger picture begins with the government. Private sector jobs in cybersecurity have started to pay more than government jobs. This has only made the lack of cybersecurity professionals an even bigger issue. The government needs the most help when it pertains to cybersecurity and attacks. Along with communication, comes effective listening. The government will only continue to lose money because they choose not to effectively listen to issues concerning cybersecurity.

Determining Effectiveness

When creating an application like Cyberpath One stop, there are multiple ways to determine effectiveness. First, the mentors will be evaluated by each mentee that they are assigned to. This will ensure that the mentor services are of a high quality. Along with these evaluations, the mentors will evaluate their experiences assisting the mentees. This evaluation must be done to ensure the mentors are receiving all the tools and support needed to guarantee the success of the mentees.

Second, it is important to receive feedback from the businesses and their employees concerning the effectiveness of the videos and literature on awareness. Surveys will be provided to each person that receives services, but it will not be the sole method used to evaluate effectiveness. One of the main aspects I will consider when gauging effectiveness, is the number of downloads and in app purchases. This will tell me what services are most effective to the users and which ones may need improvement. Another way to gauge effectiveness is by assessing

customer retention. If customers use our services for a prolonged amount of time and/or purchase multiple services, this can be an indication that those services are effective.

What is needed to turn innovation into a reality?

In order to turn this innovation into a reality, a lot of funding will be needed. Most of the funding needed will have to come from grants. This grant money will be used to create the application and provide funding for the ten paid apprenticeships per year. Secondly, I would have to get businesses, colleges, and universities to partner with me and assist with the apprenticeships and mentoring. Third, I would have to find places or companies to advertise the application where it would reach the right and most amount of people possible. It is important that the group of individuals viewing the application and using its services provide a diverse demographic of women and men of all races, ethnicities, and geography.

Self-Reflection

Dear Director,

Creating my own cybersecurity company has been an enriching experience. While brainstorming ideas for the innovation, I included things that I wish I was able to experience while in my apprenticeship. I took both the positive and negative experiences in the apprenticeship that I had and used personal experiences to drive this project. Cybersecurity has been a passion of mine since getting introduced to it two years ago. This project means a lot to me because before cybersecurity, I felt lost and did not know what I wanted to do with my life. I constantly put a lot of pressure on myself and assumed that law school would be my passion.

Overtime, I learned that being a lawyer is not my calling. My goal in life is to make an impact and promote change. By creating this innovation, I was able to do just that.

While speaking to other apprentices in my cohort, they had the exact same concerns that I did. If I could impact and help at least one other person, I would be extremely happy. Although this project may only be an idea, I hope one day that I am able to have the tools needed to create this innovation. If I had more time to create a plan, I would offer a lot more services. Overall, this project has taught me a lot about myself and made me feel the deep passion again for cybersecurity that I felt when I first started.

Best Regards,

Faith Weems

References

Burrell, D., & Nobles, C. (2018). Recommendation to Develop and Hire More Highly Qualified Women and Minorities Cybersecurity Professionals. In Proceedings of the 13th International Conference on Cyber Warfare and security: ICCWS 2018: Hosted by National Defense University, Washington DC, USA: 8-9 March 2018 (pp. 75–80). essay, Academic Conferences and Publishing International Limited.

DINNING, A. (2017). The Lifelong Pursuit of Networking. TD: Talent Development, 71(8), 72–73

Fowler, J. L., Fowler, D. S., & O'Gorman, J. G. (2021). Worth the investment? An examination of the organisational outcomes of a formal structured mentoring program. Asia Pacific Journal of Human Resources, 59(1), 109–131. https://doi-org.proxy.lib.odu.edu/10.1111/1744-7941.12252

Gonser, S. (2019). Jobs in Cybersecurity Are Exploding: Why Are Women Locked Out? How high schools are trying to attract girls to this lucrative tech field. Tech Directions, 78(7), 24–26.

Kweon, E., Lee, H., Chai, S. et al. The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Inf Syst Front 23, 361–373 (2021). https://doi.org/10.1007/s10796-019-09977-z

Marks, J. (2021, August 2). *Analysis | the cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most*. The Washington Post. Retrieved

June 18, 2022, from https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/

Marks, J., & Schaffer, A. (2022, June 6). *Analysis | the U.S. isn't getting ahead of the cyber threat, experts say*. The Washington Post. Retrieved June 18, 2022, from https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/

Schneider, F. (2013), "Cybersecurity Education in Universities," in IEEE Security & Privacy, vol. 11, no. 4, pp. 3-4, July-Aug. 2013, doi: 10.1109/MSP.2013.84.

Sobel, A., Parrish, A., & Raj, R. K. (2019). Curricular Foundations for Cybersecurity. *Computer (00189162), 52*(3), 14–17. https://doi-org.proxy.lib.odu.edu/10.1109/MC.2019.2898240