Man in the Middle Inc.: Non-Profit Social Mission

Sarah Vakos

Group G

Old Dominion University

CYSE 494 33718: Entrepreneurship in Cybersecurity

Professor Porcher

Due: 6/21/2023

Introduction

The resource allocation available to the cybersecurity curricula and individuals who are studying on their own to be workforce ready whether it be an internship job to get hands-on experience, a part time job, or a full-time career is not effectively preparing individuals to be fully equipped for the field. With the information sharing that is offered now comprises of conflicting sources about skillsets and which certifications that the private industry is requiring. Other issues that stem from the information sharing are when individuals who are applying for a job in the workforce and gets denied the position, they are left with no explanation on why they did not get picked for the job and why someone else did.

The issue is most companies require at least a year experience in IT alone along with customer service skills, programming skills, certain soft or technical skills etc., depending on the specific job title. It's not a one size fits all situation either so those who are interested in a cybersecurity related job whether they have a degree or not are still having issues knowing what exactly is valued in each company and or business. The issue here is that there is a great deal of inconsistent data that is not updated and that is not applied to most employers in the private sector today in terms of skillsets and the kind of experience they want to see with applicants.

What is clear is that there is a communication barrier between employers, students, autodidacts and the education system with no sense of realistic expectations or qualifications that employers need to see on resumes for specific job positions. Some companies want to see that you have certain certifications like CompTIA Security + and others don't, some companies want to know what specific skills you know how to do and can explain it step by step. Then there are other jobs that need to see you know how to work with Windows systems and know the ins and outs of management and security because that's the operating system the company work with.

Colleges and universities need up to date information and resources to better guide these cybersecurity students and a platform for those studying on their own without the help of an institution or school to obtain a degree, towards the right path to getting their next job to further their career. But also, to know why they did not get the job they applied for once denied is necessary for growth so those individuals can have a sense of direction on where to go next to learn the skillset that is needed for that job role, so they don't lose hope or interest in the career field.

Many educational institutions struggle to keep up with the rapidly evolving field of cybersecurity. The curriculum may not reflect the latest industry trends, technologies, or best practices. As a result, graduates lack the real-world skills required by employers. Traditional educational programs often focus more on theoretical knowledge rather than hands-on experience. This leaves cybersecurity students and graduates with a gap in practical skills needed to address actual challenges in the field.

Cybersecurity is constantly growing with new threats and attack vectors emerging regularly. It is challenging for educational institutions to keep up with the pace of change and incorporate the latest knowledge into their programs. By fostering collaboration, sharing resources, and keeping up with industry demands, the ecosystem can better prepare cybersecurity professionals for the workforce with ease and less frustration. Man in the Middle will fill this market gap by providing consultation services to employers and educators in the region by acting as a man-in-the-middle to bridge the workforce skills shortage gap between those who are cybersecurity affiliated and specialists in the workforce by providing resources to every customer segment that is involved. In this development, we will streamline the process and make it less exasperating for everyone.

We will use updated consultation research that is industry-backed to improve the system that is being used today. By acting as an information broker, we will be able to improve data sharing at all segments that will make it easier to pick qualified candidates for hiring managers and it will help align current employees with the best practices that are being used today. Overtime this could improve the cybersecurity curriculum at the college and university levels and that information from resources provided can easily be accustomed by everyone in the field. Creating an application for cybersecurity individuals and students with the right guidance and direction towards success in job readiness with the expected skills for each job title is the solution.

Literature Review

The cybersecurity skills crisis continues on a downward, multi-year trend of bad to worse and has impacted more than half (57%) of organizations, as revealed today in the fifth annual global study of cybersecurity professionals by the Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG) (Kesselring, 2021). The new research report, The Life and Times of Cybersecurity Professionals 2021, surveyed 489 cybersecurity professionals and reveals several nuances surrounding the well-documented cybersecurity skills shortage. The top ramifications of the skills shortage include an increasing workload for the cybersecurity team (62%), unfilled open job requisitions (38%), and high burnout among staff (38%). Further, 95% of respondents state the cybersecurity skills shortage and its associated impacts have not improved over the past few years and 44% say it has only gotten worse (Kesselring, 2021).

In America alone, employers struggle to fill nearly 200,000 new job openings requiring cybersecurity-related skills each year, including 5,000 information security analyst positions, the

most common job in the field (Lord & Roseen, 2019). There is no often traveled single path to becoming a cybersecurity professional, and professionals come from all different backgrounds. According to one study, 87 percent of today's global cybersecurity workforce did not start out in cybersecurity, and 30 percent did not even come from an engineering or IT background. As receptive as this seems on its face, the lack of clear paths means that people interested in cybersecurity may not know how best to gain skills and find a job (Lord & Roseen, 2019). That is where Man in the Middle jumps in with all the research already done with our consulting services and our application, Helping Hand, to provide a platform for those who want to know exactly what employers want to see from their education background and professional experiences with resources on how to obtain them.

According to cybersecurity practitioners, employers are dissatisfied because they perceive the graduates of these programs as lacking practical experience as well as an understanding of the fundamentals of computing and information security. As a result, many graduates require extensive on-the-job training before they can begin work. In addition, employers often find cybersecurity graduates lacking in essential soft skills like teamwork, problem-solving, and communication. Organizations are also frustrated by the current cybersecurity education ecosystem, which lacks common metrics or rankings to help employers understand what programs, certifications, and degrees are the most effective. Addressing these issues would help the United States strengthen its cybersecurity talent pipeline (Crumpler & Lewis, 2019).

There is a lack of understanding between the cyber professional side and the business side of organizations that is exacerbating the cyber skills gap problem," said Candy Alexander, Board President, ISSA International. "Both sides need to re-evaluate the cybersecurity efforts to

align with the organization's business goals to provide the value that a strong cybersecurity program brings towards achieving the goals of keeping the business running. Cybersecurity leaders should be able to link the security efforts directly to strategic business goals" (Kesselring, 2021). In order for cybersecurity professionals and businesses to be on the same page there needs to be a clear and transparent list of skills and experience for each and every cyber role a business chooses to post for new potential employee(s). We need to ensure this evaluation is reliable and current to allow cybersecurity individuals to gain the skillsets needed in today's businesses in order to be seen and valued as an asset in the industry.

Extensive on-the-job training cost the company more than they should be spending to prepare their employees that they should already have or adopted but in today's market it is difficult to find them all at one destination or platform. Helping Hand will investigate and collect all those resources that are industry approved and allow those individuals to learn and acquire as many skillsets as they can on one free application. Helping Hand will help employers by not having to train new employees instead they will have more candidates with practical experience and skillsets at hand because users can obtain those skillsets if they don't have it already by learning themselves with the appropriate websites and sources provided to them before applying for the job. Our services are not only for those not in the workforce yet but for those who are and want to touch up on their skills or for those who would like to learn something new to add to their list of know-hows because the field of cybersecurity is constantly improving and evolving to adapt to the current technologies out.

Cybersecurity encompasses a broad range of specialty areas and work roles, and no single education program can be expected to cover all of the specialized skills and sector-specific knowledge desired by each employer. However, there are certain knowledge sets and skills that

are essential for any new employee in a critical technical work role, regardless of the field they are in or the specialty they adopt. This includes an understanding of computer architecture, data, cryptography, networking, secure coding principles, and operating system internals, as well as working proficiency with Linux-based systems, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques. Employers are finding that graduates are lacking this foundation. One recent response from a major corporation to a request for information issued by NICE indicated that "the current [education] environment does not provide a common baseline set of skills from which to build the role specific knowledge necessary to meet employer workforce requirements" (Crumpler & Lewis, 2019).

Relatively newer positions have less vision and scope due to poor job descriptions and lessened awareness of pre-requisite knowledge. Moreover, career paths related to the newer work roles are not covered in CyberSeek, a tool based on the NCWF framework to help employers, students, educators and policy makers to make decisions in pursuing careers or recruiting a cybersecurity workforce. As a result, a sector of candidates aspiring to get into those work roles suffer due to a fragmented focus on education and skills development (Jacob et al., 2018). Cybersecurity as a multidisciplinary field is often misunderstood as requiring input only from Computer Science and not from other fields such as Economics, Mathematics, Accounting, Political Science, Social Science, etc. As a result, the workforce that results from such an education becomes siloed and stove-piped, keeping them within a shell of a specific career path (or a discipline). On a much higher level, previous research indicates that "Cybersecurity workforce members tend to be less bound to organizationally constructed career paths. Rather, they have a tendency towards a boundaryless career precisely motivated by personal achievement and external career dimensions, such as organizational position, mobility, flexibility

and organizational goals" (Hoffman et al., 2012). The NICE framework should consider such non-traditional conceptualizations of career management too (Jacob et al., 2018).

Educators, scholars and practitioners are now more than ever concerned about the gap between what students are being taught in school and the skills required for them to thrive in cybersecurity workforce. In our view, faculty can narrow this gap by creating opportunities for students to gain work experience needed by the field (Javidi & Sheybani, 2019). In addition, many organizations claim that today's graduates lack the soft skills needed to succeed in their careers. This issue becomes more critical in cybersecurity field since there is not only a shortage of technical savvy professionals to fill cybersecurity roles but there is also a dearth of cybersecurity job applicants who possess the soft skills, such as strategic planning, change management, and human cognition and behavior (Javidi & Sheybani, 2019).

There is a lack of understanding of the types of cybersecurity instructional programs that can be designed and implemented to effectively address the cybersecurity workforce skills shortage. The challenge is exacerbated by the rapid evolution of software tools, systems, and processes in this highly complex, dynamic, and adaptive IS domain, where the typical post-secondary education program teaches skills that are outdated at the time of training on tools with a technology half-life of less than two years (Daniel et al., 2022). A lack of effective, accessible, hands-on training platforms is a barrier for students and professionals who seek to gain the skills and abilities necessary to enter the workforce. Additionally, the lack of adequate training makes it difficult for industry experts to upskill or stay up to date on new advancements within the field of cybersecurity. Hands-on experience is necessary to create workforce ready professionals, yet it is underutilized by students and professionals of cybersecurity due to costs, availability, and ease of use (Beason et al., 2021). The shortage of experts in the field results in professional burn-out

and understaffed organizations. By unclogging the academia to industry pipeline, students, professionals, and organizations will benefit (Beason et al., 2021).

In the cybersecurity discipline, there are multiple pathways an individual can take to gain an education. It is common for people to attend college and receive a degree, but a non-traditional route through self-teaching is also an option (Maennel, 2020). Regardless of which path is taken, having hands-on training resources is vital to becoming a productive worker in the cybersecurity field. Due to the everchanging nature of cybersecurity, professionals need access to resources to keep their skills up to date. Hands-on labs and courses need to be readily accessible for anyone interested in maintaining their skillset (Beason et al., 2021).

The demand for cybersecurity talent keeps increasing over time and not only has nearly every organization become completely dependent on technology, but technology also continues to become more complex. Securing today's systems, networks and data against cyber attacks is tougher than ever, with even more security technologies and processes needed to work in concert with each other. So, organizations need their cyber workforces to be larger and have a wider range of skills than ever before (Scarfone, 2022). Cybersecurity job descriptions often require college degrees, multiple certifications and years and years of experience in a variety of security disciplines. Many candidates who would be assets to organizations don't apply for these jobs because they assume that the requirements are truly required. Others do apply but don't even get a call back because they lack a degree or sufficient hands-on experience (Scarfone, 2022).

Alarmingly, a recent survey commissioned by Trellix found that over one-third of the cybersecurity workforce are planning to change careers. There's a major employee retention problem, due in large part to constant staffing shortages and the incredible pressure of many cybersecurity jobs. As people leave the field, the shortages become even worse, which causes

more people to leave the field (Scarfone, 2022). This is the last thing we need for our nation because we need to have fully equipped cybersecurity professionals ready to defend our government, private sector networks from cyber criminals and IT professionals to protect and secure their company's assets from competitors and hackers.

From employers' perspective, the hiring issues come from their HR team and department. According to ISACA's 2020 State of Cybersecurity report, 72% of companies say their HR department doesn't understand their hiring needs. To avoid a similar situation, clearly communicate the job requirements to the HR staff, so they have a complete understanding of the cybersecurity skills they should be looking for in candidates (Cox, 2022). Also, letting those who did not make the cut and why another candidate got the job needs to be clearly stated otherwise, the same issue with hiring the right employee will keep repeating itself. But more importantly the company or business will continue to suffer without the right security needs which is where Man in the Middle comes in to combat those issues by enabling cybersecurity individuals to know exactly what is expected from employers and the private sector along with resources and links to learn them and be workforce ready.

Since job requirements in the cybersecurity field change rapidly due to evolving technologies and threat landscapes it can make it difficult for colleges to keep their curriculum up to date and ensure that students are adopting the latest skills required by employers. With the help of a consultation service, this can maintain an ongoing relationship with colleges, providing regular feedback and recommendations for improvement. They can conduct evaluations of the cybersecurity programs and suggest updates or adjustments based on industry feedback and changing market demands. This ensures that the curriculum remains relevant, and students are competently prepared for employment.

While there are educational services and apps available in the cybersecurity industry that can help individuals acquire specific skill sets and prepare for applying to a job, they're not at a low cost expense or even free and do not offer direct job placement or consultation services specific to job listings. That is why we want to make it easier for everyone in the industry wanting to be job ready with all the resources at hand and in one spot. We are the information broker and have done all the research already, so it is streamlining the investigation and research process for users, while also reducing the time and efforts of employers and their HR team going through the application process. We are providing job listings from numerous employers in the private industry and resources to obtain skills for each job role. It is on the user to take those resources and learn the skillset(s) and then if they want to apply for the job we will offer them updates to their application process from start to finish so no more wondering if the company has reviewed their application or not and will provide a thorough explanation as to why they were not chosen if that's the case, so they can improve on or get more experience in a specific area of expertise.

Overview of Innovation/ Material Taken Outside of Major

Design thinking emphasizes understanding the needs and challenges of users or stakeholders. In the case of individuals aspiring to enter the cybersecurity industry, design thinking encourages empathy towards their concerns, limitations, and gaps in skills. Design thinking emphasizes defining the problem statement clearly before generating solutions. In this case, the problem could be framed as "How might we help individuals acquire the specific skill sets required to enter the cybersecurity workforce?" This helps focus the design process and ensures that the solutions address the core challenges faced by cybersecurity individuals. Ideas

might include creating online platforms, virtual mentoring programs, community-based initiatives, or partnerships with educational institutions to offer affordable cybersecurity training.

Creating prototypes to gather feedback and iterate on the solutions is a crucial part of design thinking. In this context, one could prototype and test different consultation service models to determine their effectiveness, usability, and impact on job readiness. This iterative approach helps refine and improve the solutions over time. Design thinking often emphasizes collaboration and multidisciplinary approaches. To address the challenge of job readiness in the cybersecurity industry, collaboration between cybersecurity professionals, educators, industry experts, and policymakers can lead to more holistic solutions. By involving diverse stakeholders, the design process can benefit from a wide range of perspectives and expertise. By applying design thinking principles and methods, it is possible to develop innovative and user-centric solutions to help individuals become job-ready in the cybersecurity industry. Identifying opportunities and planning, when taken outside of a cybersecurity major, can be relevant in addressing the issue of individuals not being skillfully ready to enter the cybersecurity workforce with market analysis, developing a business model, resource planning, and implementation strategy.

When considering the issue of individuals lacking the necessary skills to enter the cybersecurity workforce, identifying opportunities involves recognizing the demand for skilled cybersecurity professionals. This could be done by researching industry trends, analyzing the job market, and understanding the specific skill sets in demand. By identifying the gaps between available job opportunities and the skills of aspiring professionals, one can find opportunities to provide consultation services that bridge this gap. Conducting a comprehensive market analysis includes understanding the target audience, such as individuals aspiring to enter the industry,

their current skill levels, and the resources available to them. Additionally, analyzing the existing consultation services in the market, their offerings, pricing models, and effectiveness can help identify gaps and areas for improvement.

Planning also entails developing a business model for the consultation service aimed at helping individuals become job-ready in cybersecurity. This includes defining the value proposition, revenue streams, cost structure, and pricing strategy. By considering the financial aspects, scalability, and sustainability of the service, one can ensure its long-term viability and effectiveness in addressing the skill gap. Resource allocation and management involves identifying the necessary resources, such as subject matter experts, mentors, training resources, and technology infrastructure. Additionally, resource planning includes determining the optimal utilization of available resources to deliver the consultation service efficiently and effectively.

Planning also encompasses developing an implementation strategy for the consultation service. This involves defining the steps, timelines, and milestones to establish and deliver the service. It includes creating a platform or infrastructure for delivery, and outlining the support mechanisms, such as community engagement from employers and partners, to ensure the success of aspiring professionals. By applying the principles of identifying opportunities and planning, one can develop a comprehensive strategy to address the skill gap in the cybersecurity industry. This strategy can involve the creation of a consultation service that aligns with the demand for skilled professionals, leverages market insights, and ensures efficient resource allocation and implementation.

Effectiveness of Innovation. To determine whether our consultation application is and will be effective to ensure longevity of our non-profit social mission for the cybersecurity community, we will have to measure certain metrics to see is we are successfully making a

positive impact on the information sharing in the field between individuals, employers, educators, and the government. We will measure social impact since the whole subject-matter around a mission based business is to see the effects that actions have on people, communities, and societies that way we can continue helping more employers, more educators, and more cybersecurity individuals. Establishing the effectiveness of programs is crucial to secure continued funding from partners and investors. We are minimizing the information gap and improving the ecosystem, entry-level avenues, and knowledge/skill standards with academic collaboration by incorporating NICE cybersecurity workforce framework and connecting with their close partners to ultimately have a more integrated cybersecurity industry for job seekers in the field. We will promise improvement rates in the workforce skill shortage gap in the regions of Northern Virginia and the Hampton Roads area, improved ratings on new hires that are qualified for the job role, and success rates with students obtaining skill sets using the app.

Effectiveness will be determined by sensible budgeting and what is found through cost structure, our cash flow statements and a worthwhile balance sheet. We will measure how effective our consultation services are working by refining and enabling the cybersecurity community to obtain job specific skills with a social cost benefit analysis (SCBA). This analysis focuses on the social returns from a venture on the enterprise and the community (*Social Cost Benefit Analysis*, 2021). First, we will need to define the objectives of the application which is to aid and provide individuals with resources to obtain and learn specific skills to be workforce ready, to bridge the skills gap, and enhance the employment process between job seekers and employers in the industry. Next, we need to identify key metrics that align with the objectives which is a 50% improvement rate on workforce shortage gap in the specified regions through HR practices and consulting hiring managers to have clarifications on the correct standards at a

charge for employers in the industry ensuing in a substantial return on investment to private enterprises. For every training partnership and educator, we will guarantee an annual curriculum report that is accurate and up to date. Another feature would be working with partners and the private industry to create 20 internships for educators annually to allow students to get hands-on experience so they will market the Helping Hand application to their students which will help in advertising costs.

As for the Helping Hand app, it will be free to download and will include a minimal charge for specialized updates from the app (progress reports), with a greater income stream obtained from the HR consulting services to private enterprises. For cybersecurity students using Helping Hand through their school, we promise 5,000 students to acquire job specific skillsets and 50% of them will go on to secure a job position in the industry. Another metric is skill acquisition, which will be at least a 50% satisfaction rate by evaluating the effectiveness of the learning resources by assessing the user's skill development over time. Job placement will be a metric to measure the rate at which users secure job placements that match their skillsets acquired through the application but will not be guaranteed to users. User feedback is another metric by collecting feedback through surveys from users regarding their satisfaction on the learning resources, perceived value, and the impact of the application on their career progression.

Turning Innovation into Reality. To make Man in the Middle into a reality we will determine the specific areas within the cybersecurity field that we are focusing on which is workforce development, curriculum design, training programs/resources, and certification pathways. By doing so we will need to familiarize ourselves with the resources provided by organizations in the field and understand their frameworks, standards, certifications, curriculum offerings and staying alert on any of their updates or releases. Attend conferences, webinars, and

workshops related to cybersecurity and engage with industry experts. Establish partnerships with NIST/NICE, CompTIA, Cyberseek.org, HRCyberAlliance, NOVA's CCI (Commonwealth Cyber Initiative) to gain access to their resources and leverage their expertise in return of seeing a positive social impact on the cybersecurity community is important since these organizations have similar goals and visions to aid in the workforce skills shortage.

Reaching out to these organizations, explaining the consulting service's objectives, and exploring opportunities for collaboration is necessary. Aligning ourselves with these like-minded organizations is a key part of our resource strategy, utilizing existing experts with multi-disciplinary knowledge in the industry, which could lead to grant sharing prospects. As well as applying for grants to the DOL, NSF, and local government that offer funding opportunities for workforce development and research. Another source for funding would be from venture capitalist firms also interested in missions like ours, but with an incentive of tax deductions for their donations apart from us being able to quantify an accurate return on investment. Then we will need to highlight how our service can add value to each partner offerings and how we can benefit their target audience. Most importantly, utilize various marketing channels, including our app, social media platforms, industry publications, and professional networks, to raise awareness about our service.

Collaborate with other consultants or firms specializing in related areas to broaden our reach and expertise this will ensure that we consistently provide high-quality consulting services to our clients. Tailor our approach to each client's workforce needs and goals to ensure they are occupying the best practices. Stay updated with industry trends and regulatory changes, and continuously enhance our knowledge base to remain a trusted advisor in the field of cybersecurity. Regularly seek feedback from clients and stakeholders to evaluate the

effectiveness of the consulting services and incorporate their suggestions and continuously improve our offerings to meet evolving industry demands.

To make this entrepreneurship vision into reality we will define the scope and objectives of the consultation application to determine the specific features and functionalities it will include. Helping Hand will provide the specific skills that each job listing from employers are requiring from job seekers and resources on how to obtain them to enter the workforce if they choose to do so. Conduct thorough market research to understand the needs and preferences of cybersecurity professionals, employers, and job seekers. Identify the existing gaps in the market and evaluate potential competitors. This research will help us refine the application's features and ensure its uniqueness and value proposition.

Most of our initial funding will be with NIST research grants and like-minded cybersecurity venture capitalists. As well as considering how we will monetize the application, such as through subscription fees, partnerships, and advertising. Cloud hosting will be the best route for dealing with our application rather than managing our own servers and network. Our skilled development team will comprise of software engineers, UX/UI designers, and cybersecurity experts. We will collaborate with them to design the application's architecture, user interface, and backend infrastructure. Ensuring that the team members have experience in developing secure applications and are well-versed in the latest cybersecurity practices is part of the task in building a development team we can rely on and that have the same goals and visions as us.

The process of submitting required documents and credentials of incorporation as a Virginia nonprofit business and filing with the state for tax-exempt status will be required under state laws. We would successfully be tax-exempt regarding federal income taxation as well as

have noteworthy responsibility protections along with honest public service terms. Fundamentally, in order to be held accountable for compensations per state law, a dissatisfied client would have to be able to prove a form of negligence on our behalf to the extent we were deliberately trying to harm them, which will be rare.

We will employ an iterative development approach, allowing for user testing and feedback at each stage. Prioritize user experience, ensuring that the application is intuitive, easy to navigate, and responsive across different devices. Since the application will handle sensitive user information and educational resources we have to prioritize the implementation of robust security measures. Following industry best practices is crucial for data encryption, secure user authentication, and secure API integrations with third-party resources. Regularly conduct security audits and maintain compliance with relevant data protection regulations. Planning a strategic launch to generate awareness and attract users is another big step in getting the application out into the market. Leverage various marketing channels such as social media, industry forums, partnerships with cybersecurity organizations, and targeted advertising campaigns. We will highlight the unique value proposition of the application and its benefits for cybersecurity professionals, students, and those interested in cybersecurity seeking job-specific skill sets.

Next Steps. Reflecting what was learned throughout this entrepreneurial venture is important for growth and professional development. Identifying lessons learned will involve considering the challenges that were faced, the successes achieved, and mistakes made. Challenges were finding the right organizations and partners that share the same goals as our innovation, to use their resources and data to facilitate our services and application. Identifying the key metrics on how to measure the success and effectiveness of the consultation service and

application was another challenge that was faced. Success in finding no other company or consulting firm like us was something that was achieved. Mistakes made were in the beginning where we only were targeting students at our university (Old Dominion University), but the issue was the amount of people had to be a bigger audience and customer segment, so we decided to reach out to regions of Hampton Roads and Northern Virginia since that is where a lot of jobs in the field are found near Washington D.C area.

My personal perspectives have changed and evolved from the start of this entrepreneurial venture mainly on the target market. We went from just cybersecurity students to helping out the private sector, educators (colleges and universities), professionals, and students going the traditional and non-traditional route. I've learned certain things like what skills are the most in demand for employers, the certain job roles that are needed the most, and most importantly why cybersecurity individual are having troubles finding the resources to obtain the skillsets to be able to be workforce ready. By seeking feedback from mentors, advisors, or peers can provide valuable insight towards this experience and will help gain a broader understanding. Analyzing the impact on future ventures and taking action from insights gained to further develop skills, refine our content, or adjust perspectives is part of the ongoing reflection process. A key takeaway is to embrace the lessons learned, celebrate the successes, and use our reflections as a foundation for future entrepreneurial endeavors.

References

Beason, R. E., Phelan, M., Devine, S., Aiken, M., & Orban, J. (2021). *Evaluation of Hands-On Cybersecurity Skills Development* (No. INL/EXT-21-64359-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).

Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap* (p. 10). Washington, DC, USA: Center for Strategic and International Studies (CSIS).

Cox, T. (2022, July 20). How To Tackle the Cybersecurity Skills Shortage. GetApp. Retrieved June 10, 2023, from https://www.getapp.com/resources/how-to-tackle-cybersecurity-shortage/

Daniel, C., Mullarkey, M., Agrawal, M. (2022). RQ Labs: A Cybersecurity Workforce Talent Program Design. In: Krishnan, R., Rao, H.R., Sahay, S.K., Samtani, S., Zhao, Z. (eds) Secure Knowledge Management In The Artificial Intelligence Era. SKM 2021. Communications in Computer and Information Science, vol 1549. Springer, Cham.

Hoffman, L., Burley, D., and Toregas, C. (2012). Holistically Building the Cybersecurity Workforce, IEEE Security & Privacy Magazine, vol. 10, no. 2, pp. 33-39.

Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T. A. (2018). Is the nice cybersecurity workforce framework (ncwf) effective for a workforce comprising of interdisciplinary majors?. In *Proceedings of the 16th International Conference on Scientific Computing (CSC'18). Las Vegas, USA.*

Javidi, G., & Sheybani, E. (2019). Transforming Cybersecurity Education through Consulting. *Journal of Systemics, Cybernetics and Informatics*, *17*(1), 1690–4524. https://www.iiisci.org/Journal/pdv/sci/pdfs/ZA240IJ19.pdf

Kesselring, L. (2021, July 28). Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment. Bloomberg. Retrieved June 12, 2023, from https://www.bloomberg.com/press-releases/2021-07-28/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment

Lord, R., & Roseen, D. (2019). Workforce. In *Do No Harm 2.0* (pp. 60–74). New America. http://www.jstor.org/stable/resrep19972.10

Maennel, K. (2020). Learning Analytics Perspective: Evidencing Learning from Digital Datasets in Cybersecurity Exercises. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). https://ieeexplore.ieee.org/abstract/document/9229751.

Scarfone, K. (2022, August 15). Cybersecurity skills gap: Why it exists and how to address it. *TechTarget* | *Security*. Retrieved June 10, 2023, from https://www.techtarget.com/searchsecurity/tip/Cybersecurity-skills-gap-Why-it-exists-and-how-to-address-it

Social Cost Benefit Analysis. (2021, July 19). Decisio. Retrieved June 12, 2023, from https://decisio.nl/en/services/social-cost-benefit-analysis/