 ISSN 2473-4901
v7 n5507

Preparation for a Cybersecurity Apprenticeship Program (PCAP)

Jonathan Lancelot
lancelotj@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Grace Smith
gls4018@uncw.edu

Chris Nichols
cmn9093@uncw.edu

Ulku Clark
clarku@uncw.edu

Ron Vetter
vetterr@uncw.edu

William Wetherill
wetherillw@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

Despite the coronavirus disease 2019 (COVID-19) disruption to the job market, demand for cybersecurity professionals remains high, with 460,000+ online job listings for US cybersecurity-related positions posted from April 2020 through March 2021 (Cybersecurity Heat Map, 2021). A key effort to generate the talent needed to fill the current shortage involves cybersecurity apprenticeships. While apprenticeships can be win-win-win for employers, students, and schools, there are challenges in getting to that state. Ensuring students have foundational knowledge makes the process easier for employers and leads to more successful apprenticeship programs. This article considers key employer concerns about apprenticeships and describes how a preparation program can satisfy many of their concerns.

Keywords: Cybersecurity, Apprenticeship, Pre-apprenticeship, Certifications, OJT, RIT, RTI

1. INTRODUCTION

Cybersecurity is a demanding field which requires new methods of organization building and skills acquisition. All organizations face the challenge of continuously defending computer networks from attack while periodically dealing with cyber-skilled staff shortages and budget limitations. The International Information System Security Certification Consortium ((ISC)$^{2®}$) reports that the global cybersecurity workforce gap now stands at ~3.1 million ((ISC)^2, 2020), which is a reduction from the gap reported in 2019 but nonetheless still sizeable. As has been noted in many places for several years now, the field of cybersecurity needs actionable and concrete ways to manage the skills gap. A Forbes article from a few years ago captured the prevailing sentiment well:

> Security work is either not getting done, or is being done by people who lack the background or aptitude. … Security teams are either understaffed or under-skilled, and are falling further behind while our adversaries are getting more automated, more mature and more sophisticated in their search for high-value soft targets. (Lloyd, 2017, paragraph 2)

At the same time that organizations are struggling to find needed cybersecurity talent, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reports (FBI, 2021) that cybercrime continues to rise with internet crime complaints up year-over-year nearly 70% in 2020 to a new high of 791,790 (figure 1).

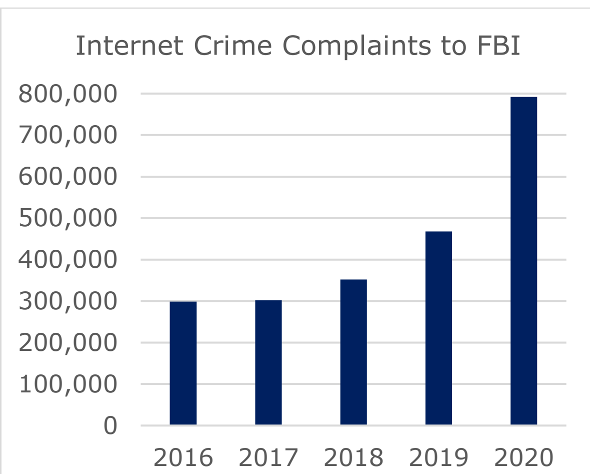

Figure 1 – by year, 2016-2020, number of internet crime complaints to the FBI's IC3

An old chicken-egg problem faced by many new entrants to the job market is the issue of experience. Organizations prefer employees with previous work experience, while new job market entrants need work in order to gain experience.

The latest ISACA (formerly Information Systems Audit and Control Association) State of Cybersecurity report based on survey results from 3,659 cybersecurity professional respondents indicates that 55% of organizations have unfilled cybersecurity positions, that only 28% of hiring managers believe half or more cybersecurity job applicants are well-qualified, and that prior hands-on cybersecurity experience is, by far, the most important factor in determining if a cybersecurity candidate is qualified (figure 2 displays results for the question: "How important is each of the following factors in determining if a cybersecurity candidate is qualified?") (ISACA, 2021). This finding seems to strongly align with the observation that nearly 88% of cybersecurity job postings require at least 3 years of experience. (Burning Glass Technologies, 2019).

Given the requirements for building out and maintaining a competent cybersecurity apparatus, many organizations struggle to figure out how to find the best talent available in the market, while on the other side of the job search continuum, candidates are typically confused by a somewhat hazy recruiting process and are unclear about the knowledge, skills, and abilities (KSAs) needed to fill an entry-level position. One method of bridging the skills gap is via apprenticeship programs.

Apprenticeships have the potential to provide a win-win-win arrangement for employers, students, and schools (Stoker, et al. 2021). However, getting to the point where all three win and feel like they are winning can be a challenge. Apprenticeship sponsors often have concerns that include program cost, apprentice commitment, apprentice qualifications, etc. In this paper, we discuss how many of the problems perceived by employers can be mitigated with programs that support student obtainment of industry certifications and we provide some practical suggestions for sustaining such programs.

2. APPRENTICESHIP REVIEW

Overview and Current Apprenticeship Data

The apprenticeship model – learning by doing – has existed throughout human history and across all cultures (Douglas, 1921). Ancient sources like Hammurabi's Code (rules 188 & 189) circa 1750 BC (King, 2008) make this clear with records of laws and norms governing the obligations of the apprentice and the mentor.

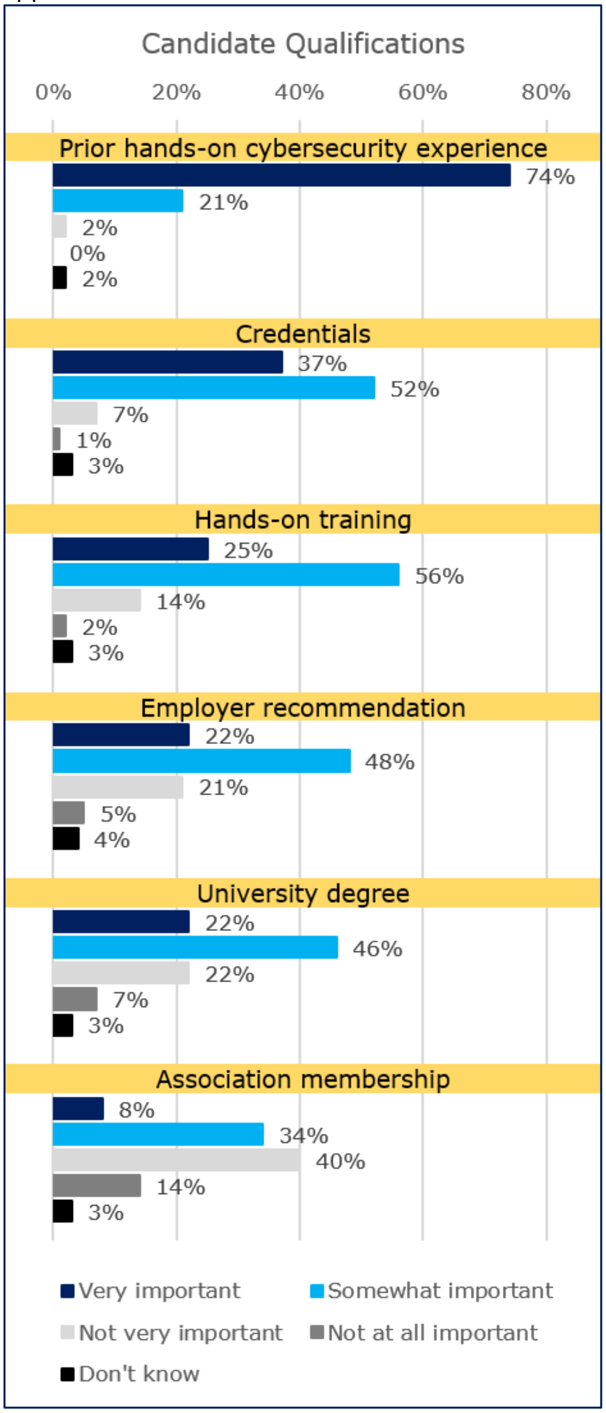

Figure 2 – results for the question: *"How important is each of the following factors in determining if a cybersecurity candidate is qualified?"* (ISACA, 2021)

For centuries, apprenticeships have provided a way to train people for crafts and trades, but should also be understood as a complex social and economic system. Apprenticeships have always involved the exchange of training for labor. Skilled masters host apprentices in the workplace for an agreed period of time. (Frenette, 2015, p. 352)

In classic *everything old is new again* (Allen, 1974) fashion, there has been a sharp turn towards the tried-and-true ancient institution of apprenticeship beyond the trades and into leading-edge industries like cybersecurity (McCarthy, 2021). Compelled, in part, by the existing skills gap and the U.S. Bureau of Labor and Statistics (BLS) projected cybersecurity-related job growth of 31% through 2029 (BLS, 2021b), the U.S. Department of Labor (DoL) has been advocating the creation of new registered apprenticeship programs in areas outside of traditional craft and trade fields.

Using DoL-provided data (DoL, 2021b), figure 3 shows via gray bars and the left-hand y-axis that active participation across all DoL-registered programs has been on the rise over the past five years, including during the heavily COVID-19-affected year of 2020. In addition to the increasing numbers of individual participants, there have been thousands of new apprenticeship programs registered each year during that same time frame as indicated by the dark line with markers and the right-hand y-axis.

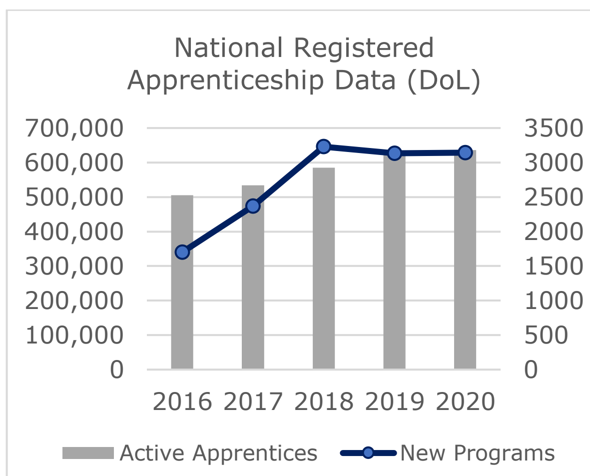

Figure 3 – dual-y-axis chart for years 2016-2020 showing number of active apprentices across all DoL registered programs (left axis) and number of new registered programs (right axis)

Among the DoL industry classifications are "Information" and "Professional, Scientific, and Technical Services" (PSTS), which are the ones most likely to be capturing programs related to

ISSN 2473-4901
v7 n5507

cybersecurity. While currently both constitute quite a small number of apprentices compared to other industries (e.g. construction is 68% of all apprentices), both are experiencing above-average growth in recent years (figure 4).
Normalizing the active apprentice numbers to 2016 data, we see more clearly that the growth rate for Information and PSTS apprentices is markedly more robust than all programs generally (figure 5). While these growth rates are encouraging, the overall number of Information and PSTS apprenticeship programs still appears smaller than warranted given the volume of unfilled cybersecurity positions.

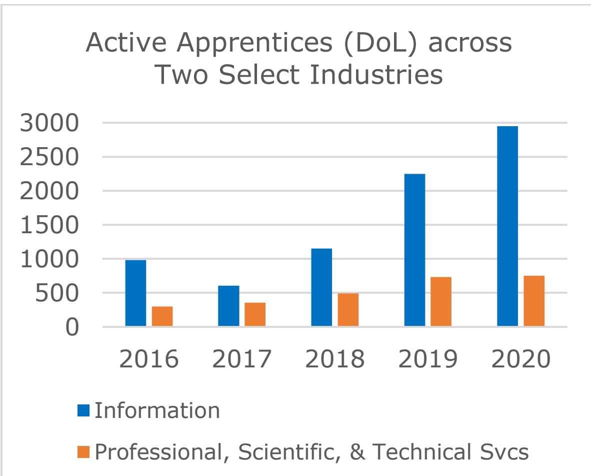

Figure 4 – 2016-2020 yearly data for number of active apprentices in the information industry and the PSTS industry

There were just 2,716 registered apprentices, 0.43% of the more than 630,000 overall, in cybersecurity occupations during 2020 (DoL, 2021a), while total cybersecurity job openings (464,420) plus the total employed cybersecurity workforce (956,314) (Cybersecurity Heat Map, 2021) represents 0.88% of the total labor force (161,086,000) (BLS, 2021a).

Employer Challenges

In spite of the growing enthusiasm for apprenticeship programs, many businesses remain hesitant or feel unable to start such programs. The reasons for this vary a bit from company to company, but we will focus on a group of reasons which seem likely to impact cybersecurity apprenticeship programs and explain how and why we believe they can potentially be mitigated.

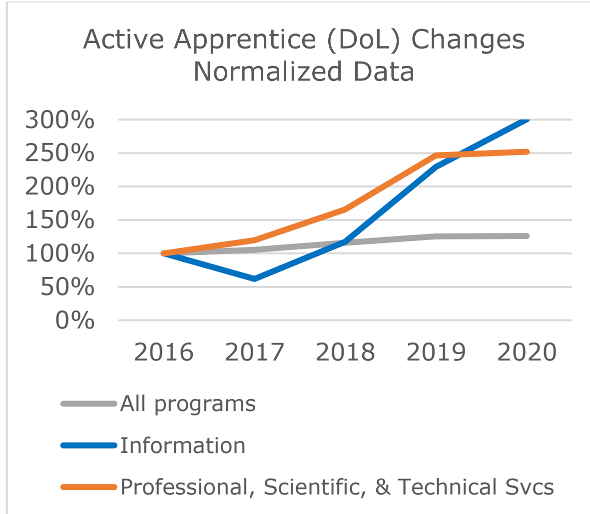

Figure 5 – percent change of active apprentices compared to 2016 base year across all industries, information industry, and PSTS industry.

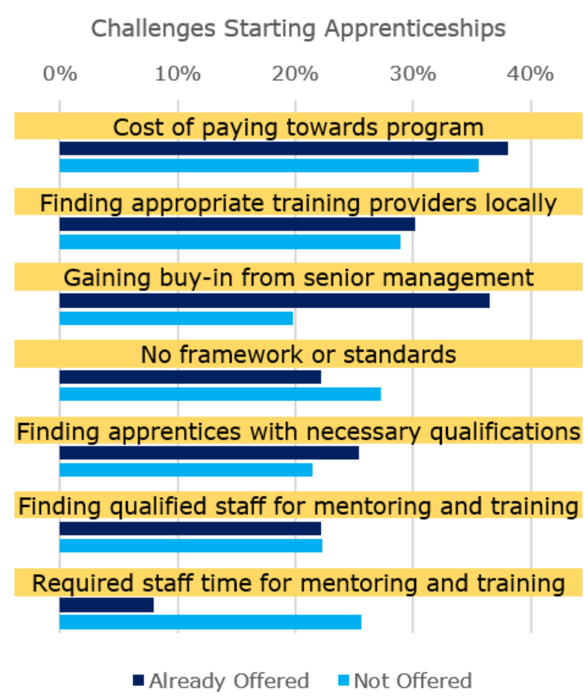

Figure 6 – top responses to the question: "What do you think the challenges are of introducing or embedding Higher Apprenticeships in your company?" (Mieschbuehler, et al., 2015)

Investigating the challenges related to creating apprenticeships, Mieschbuehler, et al., surveyed organizations from across the 9 regions of England – 63 that currently had apprenticeship programs and 121 that did not. (Mieschbuehler,

 ISSN 2473-4901
v7 n5507

et al., 2015). While actual results across different areas of the world would certainly differ, we assume that the differences would not be significant. In figure 6, we show a portion of the results in response to the question: "What do you think the challenges are of introducing or embedding Higher Apprenticeships in your company?" (Higher is equivalent to undergraduate in this context.) We are showing the top half of responses as determined by adding the percentage of respondents from both groups.

Another survey of 947 sponsors of registered apprenticeship programs based in the U.S. done in 2007 presented a fixed list of potential drawbacks and requested that respondents indicate if each was a significant problem, a minor problem, or not a problem (Lerman, Eyster, & Chambers, 2009). These results are presented in figure 7.

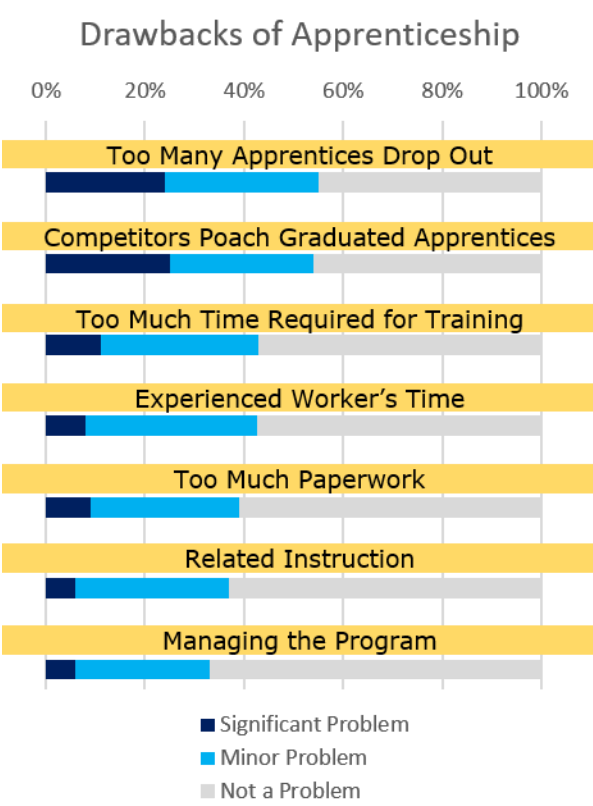

Figure 7 – apprenticeship sponsor views on specific drawbacks of apprenticeship programs (Lerman, et al., 2009)

From these two lists, the challenges/drawbacks that we plan to address are:

- Cost of paying towards program
- Gaining buy-in from senior management
- Finding apprentices with necessary qualifications
- Required staff time for mentoring & training
- Too many apprentices drop out
- Too much time required for training
- Experienced workers' time
- Related instruction

In the rest of this paper, we outline some aspects of a program designed to help close this gap and we explain how we believe it will help allay the challenges and drawbacks identified above.

3. READYING APPRENTICES

The challenges enumerated in the previous section motivate the development of a Preparation for Cybersecurity Apprenticeship Program (PCAP), which looks to close the distance between students seeking qualifications to be eligible for an apprenticeship program and the needs/expectations of the company sponsoring the apprenticeship.

The Question of Cost

While cost concerns are understandable and often uppermost in the minds of organization leaders, studies indicate that apprenticeship programs are usually win-win for firms and workers (Lerman, 2019; Reed, Liu, Kleinman, Mastri, Reed, Sattar, & Ziegler, 2012). The stylized cost/benefit model of apprenticeship in figure 8 depicts this idea.

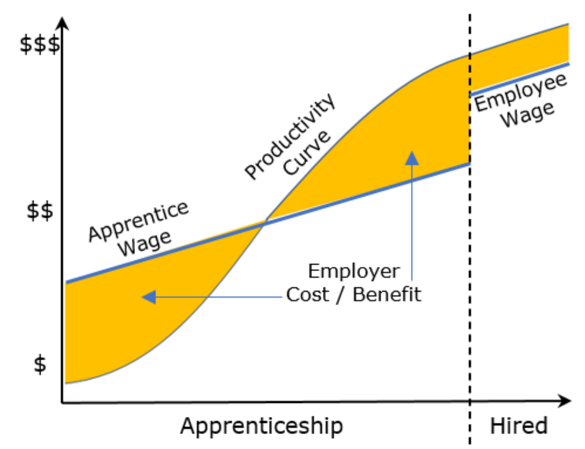

Figure 8 – stylized cost/benefit model of apprenticeship based on (Lerman, 2019) and (Gambin, Hasluck, & Hogarth, 2010).

The model reflects that apprentices are paid a relatively low wage, but at a cost to the employer above the benefit of the apprentice's initial productivity benefit. At some point during the apprenticeship, the productivity benefit overtakes the cost of the apprentice wage, and the employer recoups the initial up-front cost of bringing on the apprentice. Post apprenticeship, the worker is hired at a higher wage and operates at a productivity level above the wage cost to the employer. Later in the paper, we will present a modified version of this chart that shows how the initial employer costs can be reduced.

Apprentice Qualification Standards
The DoL's advocacy for the creation of cybersecurity apprenticeship programs is a key step towards satisfying the industry's requirement and/or desire that job candidates have prior hands-on cybersecurity experience. While this should help future cybersecurity job seekers, it raises the question of what kinds of KSAs cybersecurity apprentice candidates require to be attractive to organizations offering apprenticeships and to motivate other organizations to begin sponsoring apprenticeship programs.

Looking to a well-established apprenticeship program for some clues, we consider requirements for electrical apprentices. The apprenticeship system for electrical workers dates back to 1891 with national standards efforts dating to 1941 (IBEW, 2016). It seems reasonable to believe they have carefully considered the issue of apprentice pre-qualification. Currently, the Electrical Training Alliance (ETA) specifies basic standards to which local programs may have additional, geographic-specific requirements (ETA, 2021).

These basic standards are:
- Minimum age 18
- High school education
- One year of high school algebra
- Qualifying score on an aptitude test
- Drug free

Examples of additional requirements include (ITAP, 2019):
- Pass a color blindness test
- Provide a DMV printout
- Participate in an in-person interview

Through this brief examination of an industry with well-established apprenticeship programs, we can glean some useful hints regarding apprenticeship programs generally and what might make sense when crafting a pre-apprenticeship program for cybersecurity – we enumerate three. First, it will likely take some time to establish industry-wide consensus on basic requirements for cybersecurity apprentices. So, getting started locally with industry-informed ideas while remaining flexible to incorporate slowly shaping national standards is likely a reasonable approach.

Second, while apprenticeship might informally be thought of as a learning process that provides all required KSAs for a given trade or career field, it is clear that each program will have some baseline expectations of apprentices. Apprentice candidates who meet the required baseline will learn and develop job specific KSAs atop this base. Confirmation of this idea comes from the National Initiative for Cybersecurity Education (NICE) Working Group's Apprenticeship Subgroup (NICE, 2021) which has an active project that is investigating this issue and asking, among other things, "What is the preparation and training necessary for success in the On-the-Job Training (OJT) component of the registered apprenticeship?" (Clement, 2021, pg. 22).

The knowledge complement to OJT is often called related instructional training (RIT) or related technical instruction (RTI). The more RTI completed prior to an apprenticeship, the more quickly an apprentice can increase productivity.

Third, the more universally and easily understood the baseline standards, the better. For example, while it is hard to understand the difference between an unweighted grade point average (GPA) of 3.7 from one high school and a weighted GPA of 4.56 from another high school, it is much easier to understand the difference between having graduated high school and having dropped out or having taken one year of algebra compared to having no experience with algebra.

Industry Certification Benefits
The first step in preparing students for cybersecurity apprenticeship is, unsurprisingly, relevant coursework grounded in cybersecurity principles and a robust selection of courses that allows students to move toward their specialty and foster collaboration among students, faculty, and staff.

The next step is a schematic for certifying candidates for an apprenticeship program tailored to target programs or employer requirements. If we re-visit the survey data provided in figure 2 and re-organize it so that the "very important" and "somewhat important" response numbers are combined, we have the result in figure 9.

This slightly different view of the data reveals that cybersecurity hiring managers consider industry credentials as the second most important indicator of a hire's qualification after previous hands-on cybersecurity experience. Industry

ISSN 2473-4901
v7 n5507

certifications range from cyber security specific certifications such as the Security+ certification, the CYSA+ or the Certified Ethical Hacker certification, to certifications with more of a networking focus such as the CCNA, to the CISSP certification which is suitable for those with an ample knowledge of cyber security and a few years of industry experience.

While standardized tests have many detractors, they have the advantage over alternative methods of evaluation of presenting a common standard that permits straightforward comparison (Wainer, 2006). Industry certification exams have the additional advantage that the knowledge being tested is field-specific and presumably more directly applicable to the evaluation of a potential employee's job qualifications.

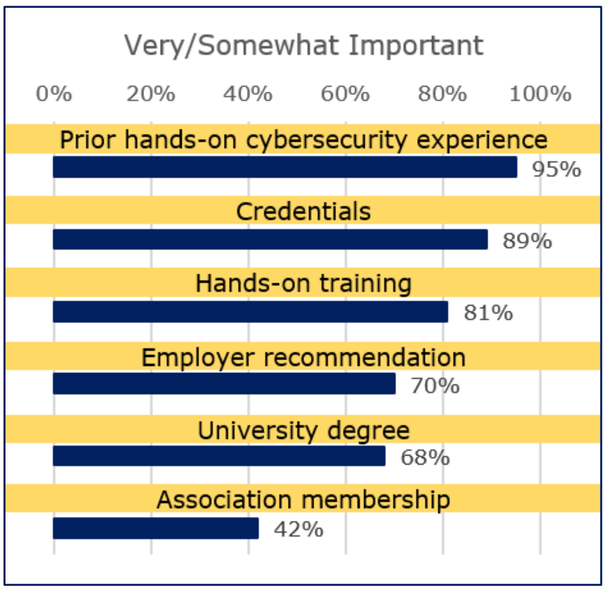

Figure 9 – Combined results of "very" and "somewhat" important for the question: *"How important is each of the following factors in determining if a cybersecurity candidate is qualified?"* (ISACA, 2021).

Looking back at the list of eight employer challenges and drawbacks from the end of section two, we see how industry certifications can serve as a key to easing these concerns. First, we re-consider the question of cost. We modify figure 8 by adding three components: a dotted-dashed curve indicating the remaining RTI an apprentice would be expected to learn, a second y-axis on the right complementing the remaining RTI curve, and a vertical dotted line labeled Certification Advantage.

The idea expressed in figure 10 is that as industry certifications are primarily concerned with industry-specific knowledge, an apprentice possessing a certification will (likely) join the apprenticeship program with necessary foundational knowledge and have less remaining RTI than an apprentice without the same certification. This means the apprentice will be further along the productivity curve and cost the employer less up-front.

The increased amount of knowledge and decreased remaining RTI will presumably have a direct net positive effect on five of the other challenges & drawbacks:

- Finding apprentices with necessary qualifications
- Required staff time for mentoring & training
- Too much time required for training
- Experienced worker's time
- Related instruction

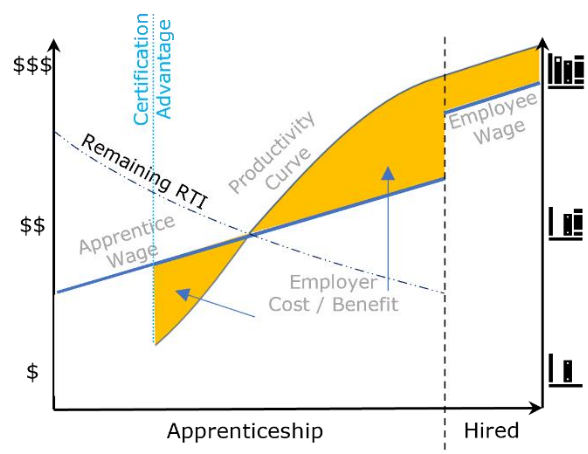

Figure 10 – stylized cost/benefit model of apprenticeship with added "Remaining RTI" curve and "Certification Advantage" line

As certifications are likely to be outside of regular curriculum requirements, attaining one will demonstrate a firmer commitment to the cybersecurity path and plausibly lead to fewer dropouts. The last challenge – gaining buy-in from senior management – should be reduced as a second-order effect of the risk reduction related to the other challenges/drawbacks. For example, per figure 10, the up-front employer cost as well as required staff time for training and mentoring would be reduced.

4. DISCUSSION

Given this reality, we have begun to more directly and aggressively encourage students to sit for industry certification exams after successfully

ISSN 2473-4901
v7 n5507

completing certain classes. The example we will discuss is the Computing Technology Industry Association (CompTIA) Security+ exam. While our efforts to unite course objectives related to attainment of a university degree with certification exam preparation are not unique (Ngo-Ye & Choi, 2016; Al-Rawi & Lansari, 2008; White, 2006), we do have some pragmatic advice that we have not found elsewhere in the literature.

A significant component of a PCAP program is funding for students to sit for the certification exams. Certification exam prices are not generally considered cheap by students. The CompTIA currently retails their Security+ exam, for example, for $370 (CompTIA, 2021b) and offers it to academic partners for $240 (CompTIA, 2021a). Students new to industry certification exams also seem to find them intimidating, regardless of level of preparation. Beyond providing them with knowledge, preparation and encouragement, support in the form of exam fee assistance can help them overcome their reluctance to attempt the exam. Of course, providing financial assistance shifts the financial risk burden to the funds provider and raises concerns that students will not prepare as vigorously as when their personal funds are at risk.

In an effort to balance these concerns, we have piloted two arrangements that seem to work well for the different types of students interested in taking an exam. One arrangement is full reimbursement for passed exams. Students pay for their exam, take it, and, if they pass, submit for reimbursement from our cybersecurity center. There are some administrative challenges with this arrangement that need to be worked out with the finance department, but this option is very low risk to both the well-prepared student and the fee provider.

The second arrangement is a simple cost share regardless of the outcome. Students pay $60 and our cybersecurity center pays $180. This alternative works well for those students who are well-prepared, but just seem to lack confidence that they know "enough." There is potentially more risk involved for the majority fee payer in this case as some students may not see $60 as much of a burden and decide to take an exam without sufficient preparation. While this is not our common experience, i.e. for most students $60 represents real skin-in-the-game and prepare diligently for the exam, this risk can be offset by requiring students to take a pretest before agreeing to pay the $180.

While creating these two arrangements to achieve a high student pass rate is important for showing program value, the challenge to find funds remains non-trivial. We have been able to meet this challenge with both deliberate and ad-hoc approaches.

Our deliberate method involved enlisting the support of our advisory board. We pitched the ideas outlined above and found they were enthusiastic about supporting students in such a tangible and risk-balanced way both on a personal level and as representatives of their respective companies. A number of our advisory board members have hired our students as apprentices for their programs. During the apprentice selection process, the companies utilized the faculty feedback, and were very pleased with the apprentices hired. The majority of the apprentices that went through the local apprenticeship programs have become full-time employees upon graduation. The success of the prior placements has been an incentive for local apprenticeship programs to sponsor even better qualified incoming apprentices. This appears to be a sustainable method for raising exam fees going forward.

Once we had this overall idea in mind, it also became easier to spot ad-hoc opportunities to secure funds for student exam fees. Two examples we encountered were unallocated year-end money from national-level programs and a portion of facilities and administrative (F&A) funds that trickled back to the college and department levels from awarded grants.

5. REFLECTION AND RECOMMENDATIONS

Our university Information Technology Security Department started an apprenticeship program last year, and the apprentices were selected based on their prior academic performance, and their performance in a pilot cybersecurity recruitment program our university participated in. We found that the apprentices completing the pilot recruitment program were focused, well-prepared, and dedicated. When the pilot program was completed, in an attempt to keep the quality of the recruited apprentices high, we designed the PCAP program.

Universities that have apprenticeship programs where students are selected based on university works and achievements are highly selective internal to the university; the quality of candidates is high given the abundance of RIT within the academic environment. Information security teams who are staffers at the university would guide apprentices through OJT and competency building.

Within our institutional program, apprentices demonstrate their ability to adapt and apply their RIT to the OJT, complemented by one-on-one instruction through mentorship. After a brief period of one-on-one instruction, group instruction is the next step, yet not before making sure that each apprentice is on the same page regarding information, access to tools, and methods of investigation. Once group instruction is in progress, team building and communication take place to gain real-world experiences and independence due to confidence-building exercises.

Measuring the competency and knowledge base of the apprentices is the next step before we establish the next step towards program completion and career services. The establishment of a rubric to develop metrics on what the apprentices learned and certifying their capacity for critical thinking and information processing is an achievable goal. Establishing metrics for evaluating apprentices will give employers a holistic perspective on the individual candidate's capabilities and skills.

Significant advancements in the candidates' skills have been observed throughout the first few months of the apprentices working hands-on. The apprentices have demonstrated a degree of independence and trust comparable to an entry-level employee with a reasonable amount of hands-on experience. Success feeds upon itself; therefore, employers are likely to fund programs that yield candidates of the highest caliber. The main factor in accomplishing success is the student's exposure to RIT in the classroom and support preparation for certification exams.

A pre-apprenticeship program sets out to create a standard model for training and designed to bridge two problems: preparing students for entering the field through apprenticeship and belay the employer's fear of hiring apprentices that lack drive, dedication, experience, and knowledge. Suppose employers are informed, satisfied, and eager to employ candidates. This could lead to other apprenticeships forming to the same standard across the board to meet this demand for those who have gained experience through apprenticeship programs.

6. CONCLUSION & FUTURE WORK

Initiatives to create cybersecurity apprenticeships to help close the gap created by negative unemployment in the cybersecurity industry have exposed another gap – between the skills of the available student talent pool and the expectations of organizations willing to offer apprenticeships. In this paper, we examined eight of the key challenges and drawbacks expressed by organizations that are sponsoring or considering sponsoring apprenticeships. We explained how a preparation for cybersecurity apprenticeship program (PCAP) anchored by industry certification attainment would diminish those eight concerns. Because of the cost challenges associated with taking certification exams, we also provided some practical suggestions for making the program sustainable.

In future inquiries into this topic, we plan to deconstruct the "why" behind the employers' concerns. Given the national security implications of negative unemployment in the cybersecurity industry and the increase of cybercriminal activity within the United States, it is critical for employers and universities to recognize the impacts of organizational stagnation. As well, the results in figures 2 and 9 indicate that employers' view of the importance to a cybersecurity career of a university degree is rather dim. It raises the question of whether universities can keep up with the demands and innovations within the field of cybersecurity. The industry certifications are valued highly by recruiters for entry-level analyst positions and hands-on experience is the number one criterion for selection into a cybersecurity job (Figure 9). "The prediction is there will be a variety of entrants moving into the higher education space, offering valuable credentials and providing the skills needed to launch professionally" (Weinberg, 2020). Given this challenge to the traditional liberal arts university model, the higher education should adapt to the current environment in cybersecurity and the tech industry as a whole.

As our PCAP and in-house apprenticeship programs mature, we will evaluate them together, along with partnering company programs, for sustainability and viability moving forward. Solutions in funding, budgets, and marketing will be explored and scrutinized for long-term planning. The development of metrics and rubrics will be critical in overall analysis and data acquisition, which would yield a holistic view of the programs progress and results.

7. REFERENCES

Allen, P. (1974). Everything Old is New Again. https://www.songfacts.com/facts/peter-allen/everything-old-is-new-again

ISSN 2473-4901
v7 n5507

Al-Rawi, A., & Lansari, A. (2008, June). Integrating the Security+ exam objectives into information technology curricula. In 2008 Annual Conference & Exposition (pp. 13-768). https://peer.asee.org/integrating-the-security-exam-objectives-into-information-technology-curricula.pdf

Burning Glass Technologies. (2019, June). Recruiting Watchers for the Virtual Walls; The State of Cybersecurity Hiring. https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf

Clement, K. (2021, May 27). DRAFT Comparative Analysis Cybersecurity Education Models Project white paper.

Computing Technology Industry Association (CompTIA). (2021a). CompTIA ACAD Security+ (Exam SY0-501) Voucher. https://academic-store.comptia.org/comptia-acad-security-plus-exam-voucher/p/ACADCompTIAS

Computing Technology Industry Association (CompTIA). (2021b). Exam prices. https://www.comptia.org/testing/exam-vouchers/exam-prices#security

Cybersecurity Supply and Demand Heat Map. (2021, March). CyberSeek Project Web site. https://www.cyberseek.org/heatmap.html

Douglas, P.H. (1921). American Apprenticeship and Industrial Education [Google Books version]. https://books.google.com/books?id=uQIwYkwa4cwC&dq=apprenticeship&lr&pg=PA209

Electrical Training Alliance (ETA). (2021). Apprenticeship Training. https://electricaltrainingalliance.org/training/apprenticeshipTraining

Federal Bureau of Investigation (FBI). (2021, March). Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Frenette, A. (2015). From apprenticeship to internship: The social and legal antecedents of the intern economy. TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 13(2), 351-360. https://www.triple-c.at/index.php/tripleC/article/view/625

Gambin, L., Hasluck, C., & Hogarth, T. (2010). Recouping the costs of apprenticeship training: employer case study evidence from England. Empirical research in vocational education and training, 2(2), 127-146. https://ervet-journal.springeropen.com/track/pdf/10.1007/BF03546492.pdf

Independent Training & Apprenticeship Program (ITAP). (2019, October 11). Electrician Apprenticeship – How to Become an Electrician. https://itap.edu/electrician-apprenticeship-how-to-become-an-electrician/

International Brotherhood of Electrical Workers (IBEW). (2016, July). History & Structure, Celebrating 125 Years of IBEW Excellence. http://www.ibew.org/Portals/31/documents/Form%20169%20-%20History%20and%20Structure.pdf

International Information System Security Certification Consortium (ISC)2. (2020, November). Cybersecurity Professionals Stand Up to a Pandemic. Cybersecurity Workforce Study 2020. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

ISACA. (2021). State of Cybersecurity 2021. Part 1: Global Update on Workforce Efforts, Resources and Budgets. https://www.isaca.org/go/state-of-cybersecurity-2021

King, L. W. (Trans.). (2008). The Code of Hammurabi. Lillian Goldman Law Library, Yale Law School, Avalon Project Web site. https://avalon.law.yale.edu/ancient/hamframe.asp

Lerman, R. (2019). Do firms benefit from apprenticeship investments?. IZA World of Labor. https://wol.iza.org/articles/do-firms-benefit-from-apprenticeship-investments/long

Lerman, R., Eyster, L., & Chambers, K. (2009). The Benefits and Challenges of Registered Apprenticeship: The Sponsors' Perspective. Urban Institute (NJ1). https://files.eric.ed.gov/fulltext/ED508268.pdf

Lloyd, M. (2017, September 8). Negative Unemployment: That Giant Sucking Sound In Security. Forbes. https://www.forbes.com/sites/forbestechcouncil/2017/03/21/negative-unemployment-that-giant-sucking-sound-in-security/?sh=60d2b07c7206

McCarthy, M. A. (2021). 19. Past as Prologue: Apprenticeship and the Future of Work. In The Great Skills Gap (pp. 184-193). Stanford University Press. https://www.degruyter.com

/document/doi/10.1515/9781503628076-027/html

Mieschbuehler, R., Hooley, T., & Neary, S. (2015). Employers' Experience of Higher Apprenticeships: Benefits and Barriers. Derby and Melton Mowbray: International Centre for Guidance Studies, University of Derby and Pera Training. https://derby.openrepository.com/handle/10545/576935

National Initiative for Cybersecurity Education (NICE). (2021). Apprenticeships in Cybersecurity Community of Interest. https://www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/apprenticeships-cybersecurity

Ngo-Ye, T. L., & Choi, J. (2016). PREPARING STUDENTS FOR SECURITY CERTIFICATION: AN EXPLORATORY EXPERIMENT. Issues in Information Systems, 17(3). https://iacis.org/iis/2016/3_iis_2016_59-69.pdf

Reed, D., Liu, A. Y. H., Kleinman, R., Mastri, A., Reed, D., Sattar, S., & Ziegler, J. (2012). An effectiveness assessment and cost-benefit analysis of registered apprenticeship in 10 states (No. 1b5795d01e8a42239b3c98dcc1e1161a). Mathematica Policy Research. https://wdr.doleta.gov/research/FullText_Documents/ETAOP_2012_10.pdf

Stoker, G., Clark, U., Vanajakumari, M., & Wetherill, W. (2021). Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned. Information Systems Education Journal, 19(2), 2. http://isedj.org/2021-19/n2/ISEDJv19n2p35.pdf

U.S. Bureau of Labor Statistics (BLS). (2020, September). Employment by major industry sector. https://www.bls.gov/emp/tables/employment-by-major-industry-sector.htm

U.S. Bureau of Labor Statistics (BLS). (2021, July). Table A-1. Employment status of the civilian population by sex and age. https://www.bls.gov/news.release/empsit.t01.htm

U.S. Bureau of Labor Statistics (BLS). (2021, April). Occupational Outlook Handbook; Information Security Analysts. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

U.S. Department of Labor (DoL). (2021a). Cybersecurity. https://www.apprenticeship.gov/apprenticeship-industries/cybersecurity

U.S. Department of Labor (DoL). (2021b). Data and Statistics: Registered Apprenticeship National Results Fiscal Year 2020. https://www.dol.gov/agencies/eta/apprenticeship/about/statistics/2020

Wainer, H. (2006). Book Review: Defending Standardized Testing. Journal of Educational Measurement 43(1), 77-84. https://www.jstor.org/stable/pdf/20461810.pdf

Weinberg, A. (2020, September 13). Google just changed the higher education game. Colleges and universities should be paying attention. Business Insider. https://www.businessinsider.com/google-careers-certificate-program-changed-game-universities-should-pay-attention-2020-9.

White, G. L. (2006). Vendor/industry certifications and a college degree: A proposed concentration for network infrastructure. Information Systems Education Journal, 4(48), 07. http://isedj.org/4/48/ISEDJ.4(48).White.pdf