INFORMATION SYSTEMS EDUCATION JOURNAL

Volume 19, No. 2
April 2021
ISSN: 1545-679X

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is six times per year. The first year of publication was 2003.

ISEDJ is published online (https://isedj.org). Our sister publication, the Proceedings of EDSIGCON (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the EDSIGCON conference. At that point papers are divided into award papers (top 15%), other journal papers (top 25%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for ISEDJ.

INFORMATION SYSTEMS EDUCATION JOURNAL

Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned

Geoff Stoker
stokerg@uncw.edu

Ulku Clark
clarku@uncw.edu

Manoj Vanajakumari
vanajakumarim@uncw.edu
Congdon School

William Wetherill
wetherillw@uncw.edu
Information Technology Services
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

The United States, along with the rest of the developed world, is experiencing a shortage of cybersecurity talent in the workforce ((ISC)^2,2019). Among the strategies being encouraged and used to close this workforce gap are work-based learning programs like cybersecurity apprenticeships. Well-designed apprenticeships can provide a win-win-win situation for employers, students, and schools. This article describes our experiences to date working to establish a meaningful cybersecurity apprenticeship program. We share the early success we have found as well as some lessons learned.

Keywords: Cybersecurity, Apprenticeship, Work-based Learning

1. INTRODUCTION

Our university was designated in September 2018 as a Center of Academic Excellence in Cyber Defense Education (CAE-CDE) by the National Security Agency (NSA) and Department of Homeland Security (DHS). The CAE designation criteria checklists, which assign points for meeting programmatic criteria, provide credit for existing internships (and, by extension, apprenticeships) related to cybersecurity (Criteria for Measurement, 2019), but do not require they exist for designation if aspects related to providing students access to cybersecurity practitioners and facilitating business/industry collaboration are met in other ways (e.g. guest speakers/lectures, obtaining curriculum input). However, once designated and immersed in the CAE in Cybersecurity Community, it is clear that internships and apprenticeships are key among the strategies being heavily emphasized for accelerating the growth of the nation's cybersecurity workforce.

The heavy emphasis on internships and apprenticeships is part of the response to the large cybersecurity talent gap that currently exists in the United States and throughout the rest of the developed world. The International Information System Security Certification Consortium (ISC)$^{2®}$ reported in their 2019 Cybersecurity Workforce Study ((ISC)^2,2019),

that a global cybersecurity workforce gap of over 4 million currently exists while a gap of ~561,000 skilled cybersecurity workers exists in North America (up from ~498,000 the year before ((ISC)^2,2018)). While CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, maintains a cybersecurity supply/demand heat map that indicates there were over 500,000 cybersecurity job openings listed from October 2018 through September 2019 in the United States ("Cybersecurity Supply and Demand Heat Map," n.d.). The site also notes that openings requesting various common cybersecurity-related certifications typically outnumber current certification holders. For example, the CyberSeek site indicates that there are 84,802 Certified Information Systems Security Professional (CISSP) certification holders vs. 112,428 job listings requiring the certification. Cybersecurity company Tripwire surveyed 342 security professionals for its 2020 Skills Gap Report and noted that 85% of the respondents found it harder to hire IT security staff with needed skills now than it was a few years ago (Tripwire, 2020). Making matters worse, 55% responded that the workers they are able to recruit need extensive training to get them up to speed.

The importance of reducing the gap is recognized at the highest level of the government. On May 2, 2019, the President of the United States signed an executive order (Exec. Order No. 13870, 2019) that included the following in Section 1. Policy. (d) (**emphasis** added):

> The Nation is experiencing a shortage of cybersecurity talent and capability, and innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities. Training opportunities, such as **work-based learning**, **apprenticeships**, and **blended learning approaches** must be enhanced for both new workforce entrants and those who are advanced in their careers.

That same day, following the signing of the executive order, all National CAE-CDEs were invited to attend a White House telecon briefing on the order's importance. Apprenticeships were not the only thing discussed, but it was clear that they are to be a key pillar in the effort to strengthen the nation's cybersecurity workforce.

There is extensive literature demonstrating the benefits of work-based learning (WBL) and applied learning for producing work-force ready graduates (Raelin, 1997; Costley, 2007; Lester & Costley, 2010; Brook & Corbridge, 2016). WBL practices help students build on the theoretical knowledge gained in the classroom and integrate theory with its industry implementation by building pathways to careers.

Though internships and apprenticeships are widely recognized as being valuable, well-established plans that layout steps for building a cybersecurity internship and apprenticeship program seem hard to come by. The NICE Apprenticeship Group recently conducted a survey to better understand WBL in higher education. Figure 1 shows the distribution of participating colleges by type where WBL exists in institutions with cybersecurity programs.

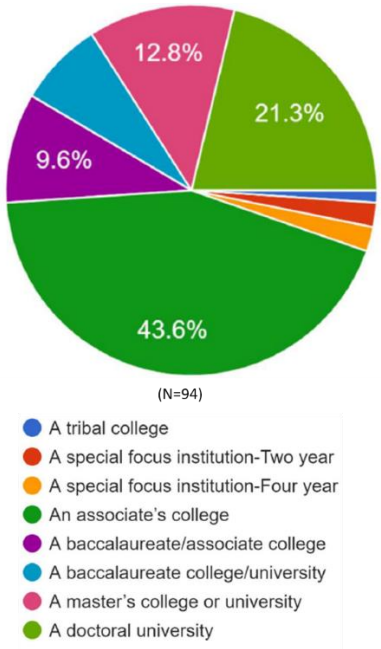

Figure 1 – WBL in participating colleges (by type) with cybersecurity programs (chart from Seshagiri, et al., 2020)

Figure 2 shows the density among NICE suvey respondents of the different types of WBL offered. It is not readily apparent how internship, apprenticeship, and externship were defined, but however defined, apprenticeship programs (20% of institutions) noticeably lag internship programs (78%).

The Department of Labor (DOL) initiated a number of projects to increase the number of apprenticeship programs. Even though there are no federal apprenticeship programs established, there are a few nationally recognized registered apprenticeship programs (RAP) like IBM's New Collar Apprenticeship program. There are a number of motivating factors for companies to partner with education institutes and become a part of a registered apprenticeship program. Some of these are the local labor shortage, opportunity to test potential employees, and access to a pool of qualified workers. Despite these benefits, many companies are hesitant to initiate a program due to concerns, such as, lost productivity for trainers, lack of staff/time/money to be dedicated to WBL, uncertain economic climate, and student knowledge/maturity levels.

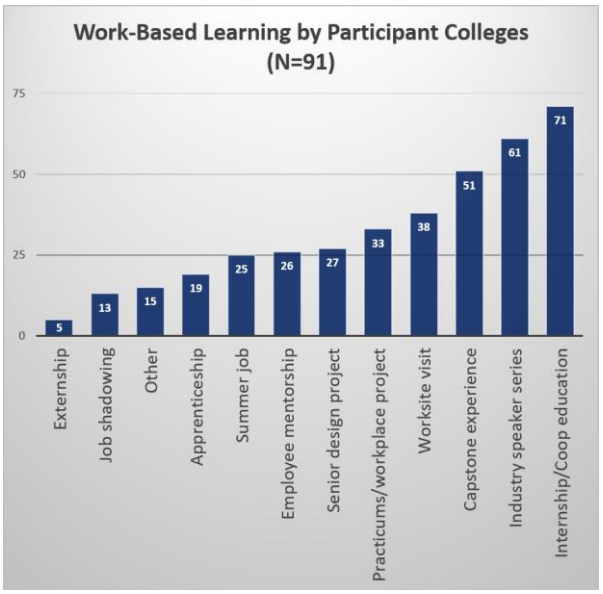

Figure 2 – types of WBL offered by NICE survey respondents (data from Seshagiri, et al., 2020)

DOL RAP's key elements can be summarized as (Jones & Lerman, 2017):

1. Apprentices are full time employees
2. Apprentices need to have at least 2,000 hours on the job training
3. Apprentices need to be paid at least the minimum wage
4. On the job training needs to be a formal and structured training

Recognizing the benefits and challenges of starting an apprenticeship program in a small city that is ~150 miles away from the closest metropolitan area, we have spent the past two years working to build our program and in this paper, we share the details of some of our early success in the hopes of benefiting the larger cybersecurity education community. Due to the geographical limitations, which impact the number and size of potential recruiters, and hesitation on the part of companies to commit to the minimum 2,000 hours on the job training requirements, we initially steered away from RAP, but still followed some of the key RAP guidelines. Along with our successes there have been missteps as well which we will present more thoroughly in the future.

This paper is organized as follows: section 2 briefly describes the history of apprenticeship in order to establish a working definition for this discussion; section 3 provides details of several of our experiences with organizations and programs that support/promote apprenticeship programs; section 4 presents a reflection of our progress thus far and offers some lessons learned; section 5 concludes the paper.

2. APPRENTICESHIP VS. INTERNSHIP, A QUICK DISCUSSION OF TERMS

Ancient in origin and universal across world cultures, apprenticeship is at its essence, learning by doing (Douglas, 1921). The Code of Hammurabi (King, 2008) from ancient Mesopotamia dating to ~1750 BC includes rules related to the regulation of apprenticeship arrangements:

> *188. If an artizan has undertaken to rear a child and teaches him his craft, he can not be demanded back.*
> *189. If he has not taught him his craft, this adopted son may return to his father's house.*

Intern, according to TIME® (Haire & Oloffson, 2009), is a term that initially meant a person with a medical degree, but still without a license to practice. Following World War I, it simply meant a physician in training. Politicians subsequently borrowed the word as an alternative to apprentice and now the word often means something like an apprentice, but with differing details which only the speaker may truly understand.

The distinction between interns and apprentices can be somewhat blurry today and the words, when used loosely, are often interchangeable. To generalize the difference, we might say an intern is most commonly understood to be someone working to gain experience and an apprentice might fundamentally be thought of as

someone learning a specific skillset by doing. The purpose and process of the internship might be said to involve surface-level exploration of a possible field of interest in order to "gain experience" while an apprenticeship often involves in-depth, hands-on skill accrual in a selected career. The U.S. Department of Labor (DOL) enumerates six key (general) differences between internships and apprenticeships as follows in Table 1 (Apprenticeship, 2019):

Internship
1. Length: 1-3 months
2. Structure: Often unstructured with focus on entry-level general work experience
3. Mentorship: Generally, not included
4. Pay: Often unpaid
5. Credential: No credentialing
6. College Credit: Often granted
Apprenticeship
1. Length: 1-3 years
2. Structure: Structured training plan with focus on mastering specific skills that an employer is typically looking to fill
3. Mentorship: Individualized training is provided/ overseen by an experienced mentor
4. Pay: Paid experience that can often lead to full-time employment
5. Credential: Often leads to an industry-recognized credential
6. College Credit: Often granted; sometimes significant

Table 1 – DOL differentiation between internship and apprenticeship.

For the purposes of this paper, we will lean most heavily on the first three points when differentiating between the two. An apprenticeship is meant to:

1. operate over a longer time horizon (6+ months).
2. focus on gaining skills specific to cybersecurity entry-level occupations (vice general office experience).
3. provide oversight from an experienced cybersecurity professional.

3. APPRENTICESHIP EFFORTS

Overview

In this section, we will detail some of our experiences engaging with various organizations and programs that promote cybersecurity internship/apprenticeship opportunities. These include:

-nationwide bank headquartered locally that specializes in originating business loans guaranteed by the Small Business Administration (hereafter referred to as SBA-Bank).

-specialized cybersecurity and cybercompliance company built to serve the banking community that provides banks and credit unions a co-managed, cloud-based compliance-automated solution that unifies detection, investigation, resolution, reporting, and compliance (hereafter referred to as C&CC).

-national gamified cybersecurity pilot initiative – CyberStart.

Our university is part of a 17-campus system and currently offers 56 baccalaureate, 36 masters, and 4 doctoral degrees to its ~14,700 undergraduates and ~2,700 graduate students. It is located in a city of ~120,000+ and county of ~230,000+ residents. The Information Technology (IT) degree is an interdisciplinary program offered by the Business School and the College of Arts and Sciences. The particular curriculum path mapped to the CAE-CDE Knowledge Units (KU) is the BS in IT with Cybersecurity Minor. There are currently 35 students following this path.

For a little over two years, our faculty, especially those associated with the University's Center for Cyber Defense Education (CCDE), have been working to build a cybersecurity apprenticeship program for the students involved in our CAE-CDE designated curriculum path (IT major with cybersecurity minor). In this section, we will enumerate many of the steps taken during this time in order to illuminate how some fairly innocuous steps end up having a big impact, while other, seemingly promising steps have yet to bear much fruit.

C&CC Apprenticeship

In fall 2017, our Department of Computer Science from the College of Arts and Sciences and the School of Supply Chain, Business Analytics, and Information Systems from the Business School reinvigorated pursuit of CAE-CDE designation by creating a full-time designation committee. One of many actions

resulting from this effort was that the first cybersecurity subcommittee was created, and a meeting held during the spring 2018 advisory board meeting for our Information Systems (IS)/Master of Science in Computer Science and Information Systems (MS CSIS) programs. Key events from this timeline are enumerated in Figure 3. In the run-up to this meeting, current advisory board members and faculty reached out to cybersecurity professionals from local/regional businesses/organizations to invite them to attend. Among the many who answered the call to advise us in our cybersecurity education efforts was the Chief Information Security Officer (CISO) of SBA-Bank. This nascent organizational effort led directly to the first substantial cybersecurity apprenticeship outcome for our students and largely flowed through the relationship with the CISO.

In the fall of 2018, we were notified of our designation as a CAE-CDE, news we shared with the attendees from the spring meeting and which seemed to help bolster and/or solidify our cybersecurity bona fides with them. By mid-October of 2018, we were able to hold the first cybersecurity advisory board meeting – an outgrowth of the subcommittee meeting from the spring. During that meeting, participants began to speak and brainstorm more broadly about many aspects of our burgeoning cybersecurity program, including potential interactions between local/regional businesses and cybersecurity students. A key outcome of the meeting, which we learned more fully about later, was that the SBA-Bank CISO departed motivated to seek to create more concrete links between the local cybersecurity professionals and our students.

At the spring cybersecurity advisory board meeting in mid-February 2019, we came up with an idea to hold a cybersecurity workshop in April 2019 as an opportunity for local cybersecurity professionals and students to meet and interact. As well, the CISO informed us that he had been working with C&CC, a cybersecurity startup, to create a local/regional security operations center (SOC) and was promoting the idea of establishing an apprenticeship program. A meeting in late February 2019 quickly followed, hosted by the CISO and including members of the leadership of C&CC. At that meeting, representatives from our university, SBA-Bank, and C&CC sketched out a process to explore the creation of a cybersecurity apprenticeship program for our students.

Step one in the process involved using the April 2019 workshop to expose university students to key cybersecurity professionals from local/regional businesses as well as provide an opportunity for those professionals to get a sense of the students. During that workshop, the following sessions were held by representatives from local businesses:

- "Cyber Resilience – How to Respond and Recover During a Breach"
- "Know Thyself: The Art of Risk Assessment and Threat Modeling"
- "Prioritizing Security – How Security is Integrated into the Software Development Lifecyle at an Agile Company"

Figure 3 – C&CC Apprenticeship key event timeline

Step two was a meeting in late May 2019 where the CISO convened a meeting at SBA-Bank with

key personnel from the university cybersecurity advisory board, C&CC and two other local businesses tied to the fintech industry:

-a software company specializing in delivering an end-to-end bank operating system to financial institutions around the world (hereafter referred to as BankOS).

-a digital banking services and support company for banks and credit unions (hereafter referred to as DigiSVC).

In advance of the meeting, the CISO laid out our CAE-CDE background, the general apprenticeship idea, and the potential value (win-win-win for students-businesses-school) in setting up a local security operations center (SOC) and staffing it with university cybersecurity students overseen by C&CC cybersecurity professionals. The meeting concluded with strong support from all attendees and a general agreement to move ahead with implementation. SBA-Bank leased building space on their campus to C&CC for the establishment of a SOC to serve SBA-Bank cybersecurity/cybercompliance needs as well as other local/regional customers like BankOS and DigiSVC.

Step three involved SBA-Bank and C&CC visiting our campus in September 2019 to interview about a dozen students, from which they ended up directly hiring a senior (with fairly extensive past work experience) graduating in December 2019 as a cybersecurity engineer and selecting three seniors (May 2020 grads) to participate in the apprenticeship program for six months.

In February 2020, C&CC began a company reorganization which has delayed a second round of apprentice selections (and now further delayed due to Coronavirus Disease 2019 [COVID-19] impacts), but in May, all three initial apprentices were hired full-time as cybersecurity analysts. And, in July, one other student slated to be an apprentice was instead interviewed for and offered a full-time position that starts in August.

CyberStart Apprenticeship

The CAE in Cybersecurity Community sends out weekly digest emails. The digest on October 28, 2019 included in the Recent News section an announcement titled, CyberStart Student Apprentice Workshop and Onboarding NSF. The notice presented an opportunity for 10 universities to attend a workshop at New York University (NYU) Tandon School of Engineering to facilitate implementing a program similar to one done as a proof-of-concept at Stony Brook University (SBU).

In a March 2019 article, Matt Nappi, SBU CISO, described how he ran a student employment/apprentice/intern program, but that it didn't seem to be attracting candidates from a sufficiently wide pool (Nappi, 2019). So, partnering with the SysAdmin, Audit, Network, and Security (SANS) Institute, he advertised a gaming/pizza party for student participants to find out if they were an "extraordinary problem solver." He emphasized no prior technical experience was necessary and that if the game playing went well, it could potentially lead to a paid apprenticeship with his office. The web banner (Figure 4) is well-crafted to catch students' interest and reach out to those who had not previously thought they may have cybersecurity interest or skills.

Figure 4 – CyberStart web banner

The game, called CyberStart Go, features 12 introductory problem-solving challenges (5 easy, 6 medium, 1 hard) related to subjects like cryptography, forensics, and Linux. For example, one of the medium challenges categorized under cryptography displayed the electronic keypad in Figure 5 and asked players to help determine the four-digit PIN using the fingerprints as a clue. Readers curious about the game can peruse it here: https://go.joincyberstart.com/.

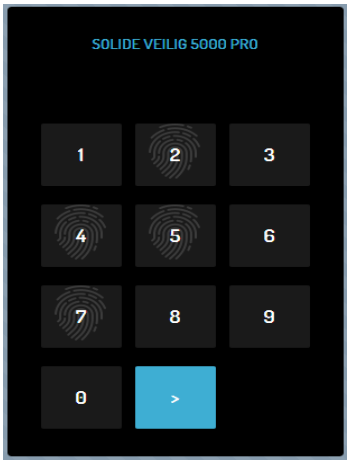

Figure 5 – CyberStart Go medium challenge

What we found compelling about Matt's story was his report that the game-based program generated "a buzz around campus, catching the attention of non-STEM as well as STEM students." Too often students with exceptional problem-solving skills, but low/no tech skills self-select out of cybersecurity-related programs. The CyberStart program strongly appealed to us since we had been looking for ways to excite latent interest, provide affordable (and fun!) IT/cybersecurity fundamentals training in an engaging and easily accessible platform format, and identify those truly interested students for potential engagement as university apprentices/interns and/or student employees.

Partnering with our university's Director of Information Security, we generated the required letter of intent with a brief summary of why we were interested/committed to participate in the program. We submitted the letter in November, heard back that we were selected in December, and attended the workshop on January 9, 2020.

On January 31, 2020 we held the game/pizza party and then left the game open until February 22. Participants who enjoyed the 12 problem-solving challenges could submit an online form noting their two favorite challenges and requesting full access to the game. We had 100 students request full game access. The full game (approximately 300 challenges) could be played until May 31, 2020 at which time elite performers were given tokens to CyberStart Essentials curriculum. Of those who requested full game access, we had 61 students play it to some degree. Elite scorers (about 10 students) completed over 40% of the challenges with the top performer completing 75% of the challenges. These candidates will also have interview opportunities for the apprenticeship program with the Information Technology Services (ITS) – primarily centered about SOC operations which monitor over 300 million network events each day.

The COVID-19 impacts resulted in campus operations being mostly closed since mid-March, so ITS has yet to actually interview and on-board any interns/apprentices.

NICE Apprenticeship Subgroup

The National Initiative for Cybersecurity Education (NICE) has an official working group (NICEWG) comprised of six subgroups that meet independently of the NICEWG. The Apprenticeship subgroup is one of the six and was created to assist anyone interested in learning more about how apprenticeships work in technology occupations. There are no special requirements for joining the NICEWG and the subgroup beyond personal interest. It is a relatively simple matter of sending some emailing requests (Petrella, 2020).

We did not become aware of the Apprenticeship subgroup until early in 2020 and were especially interested in the fact that one of the focus areas was discussion of the steps to building a cybersecurity apprenticeship program. Though we have only participated in the subgroup for a couple of months, it seems likely to be helpful. And, while there is no particular published set of steps advocated for creating apprenticeship programs, the subgroup has turned us on to a couple of initiatives to investigate such as the Inner City Fund (ICF) Cybersecurity Youth Apprenticeship Initiative (CYAI) and IQ4.

The CYAI initiative was launched in June 2019 by ICF with support from the DOL, Employment & Training Administration, Office of Apprenticeship. Their specific goal is to create at least 900 new cybersecurity apprenticeships by the year 2024 by supporting educational institutions wanting to expand the number of cybersecurity registered apprenticeship programs (RAP) serving in-school youth ages 16-21. In addition to providing technical assistance to schools developing cybersecurity RAPs, ICF will reimburse $350 to the apprentice business/sponsor for each new enrolled youth. Participation in this program requires completion of an application cover page and a 1-2 page narrative covering basic information about the apprenticeship program being registered.
IQ4 founded the Cybersecurity Workforce Alliance (CWA) in 2015 with a mission to ramp up the development of the cybersecurity workforce. It provides a workforce platform that offers solutions to students, academia, and industry. For academia they offer internship modules that review the NICE framework. Throughout the program the students investigate each framework function using a case study and present their findings as a cybersecurity consulting firm (each student has a different cybersecurity professional role) to the mentors, who are seasoned cybersecurity professionals that are partnered with IQ4.

4. REFLECTION AND LESSONS LEARNED

Building a cybersecurity apprenticeship program is neither simple nor straightforward. Even with governmental advocacy and a like-minded support community, much of the guidance feels

ad-hoc and efforts seem like discovery learning. After reflecting on our two years of effort so far, we feel we can offer the following lessons learned/recommendations.

Apprenticeship Is Very Valuable
This might be obvious, but it merits explicit assertion. The three students in the first cohort of C&CC apprentices were good students in our classes – diligent, motivated, and conscientious. But, once they were working on real-world problems with real effects and consequences for live business operations their motivation, understanding, and learning all spiked. The increase in the apprentices' ability to link theory, practice, and outcomes became more obvious the longer they were engaged in the program. So, the complexity and difficulty of building an apprenticeship program is worth it, at least so far.

Building An Apprenticeship Program Is Somewhat Like Sales
Building an apprenticeship program seems to resemble the sales process. Though the authors' experience with the sales process is quite limited, as much as we are aware of sales steps that include understanding a customer's goals, challenges, and budget we see parallels in trying to build an apprenticeship program. With the C&CC program, the concept of finding a champion (Weinstein, 2014) was particularly germane. The CISO of the SBA-Bank was clearly the champion with this program and without them, it is not clear we would have had the relationships, credibility, and business process understanding to establish the program as rapidly – if at all. We really do believe the apprenticeship programs can be win-win-win for employers-students-schools, but it is the employers that require the convincing and at the end of the day, it is a bit like sales. While this particular example (bank CISO champion) may not be replicated by readers, we believe the general "sales process" is and recommend approaching the challenge with this mindset.

Identify Potential Apprenticeship Partners
An apprenticeship program is obviously going to need partners from industry, government, non-profit, etc. to provide apprentice opportunities for students. A key aspect of identification is having labor market information for your geographical area. With a report like that, you will be able to identify the companies that are hiring for cybersecurity positions or that are likely to be. Data like annual revenue, industry, current employment, projected employment, etc. can be used as indicators to help you prioritize which organizations you approach with partnership in mind. Some organizations may be obvious fits and could be immediately approached regarding apprenticeships. Others will be better cultivated with invitations to campus cybersecurity events or advisory board meetings to expose them first to university capabilities and allow them to warm to the idea of partnering. Being and staying open-minded is key to finding the people with whom you can create a connection that will potentially lead to an apprenticeship program champion-style relationship.

Prime the Pump
Eventually, we hope to have a robust apprenticeship program in which all students can participate and from which all partner companies will benefit. It became clear during the interview process with the first round of C&CC apprentices that the stakeholders were a bit cautious and really wanted (needed?) a win with the first group. To that end, even with the interviews, they sought a lot of our input regarding the students' hard skills, soft skills, and ability to perform in a team environment. We were much more heavily involved in helping determine students who were a "best fit" than expected. And, while we did not play favorites with anyone, we realized the importance of getting it right with the inaugural group, so worked very closely with C&CC and provided as much relevant information as possible. Recognize with the first steps of a program that you are building trust and reputation. Without these things, the program will likely not last.

Join the NICE Apprenticeship Subgroup
It probably took us longer to discover that this group existed than it should have. Unsurprisingly, there are a lot of benefits to being part of a subgroup with like-minded people. These include networking with other institutions (academic and business) that have apprenticeship programs; learning about DOL apprenticeship updates; and hearing about, as well as getting involved with, new national apprenticeship-related initiatives.

5. CONCLUSIONS

With our world becoming more digital every day, cybersecurity graduates seeking entry level jobs in the US need to be prepared to rapidly translate their academic knowledge into specific skills useful to employers. WBL training gives students the opportunity to implement the theory learned in class to real-world situations

and become workforce ready. The companies that provide apprenticeship programs benefit from the training offered to the participants and have highly skilled hires that are experienced in the specialty areas that they need filled and have previously had a hard time filling. Most companies are not aware of the programs or hesitant to start one due to lack of knowledge, but with the lead of the educational institutions, the companies that have the capacity to start apprenticeship programs can become long-term partners and this relationship would lead to a highly qualified cybersecurity workforce.

6. REFERENCES

Apprenticeship, O. of. (2019, November 13). What is the difference between an apprenticeship and an internship? Retrieved May 22, 2020, from https://www.apprenticeship.gov/faq/what-difference-between-apprenticeship-and-internship.

Brook, C. & Corbridge, M. (2016) Work-based Learning in a Business School Context: Artefcats, Contracts, Learning and Challenges. Higher Education, Skills and Work-Based Learning, Vol. 6 No. 3, pp. 249-260. https://doi.org/10.1108/HESWBL-12-2015-0060

Costley, C. (2007). Work-based learning: assessment and evaluation in higher education, Assessment & Evaluation in Higher Education, 32:1, 1-9, DOI: 10.1080/02602930600848184

Criteria for Measurement (2019). National IA Education & Training Programs Web site. Retrieved from https://www.iad.gov/NIETP/documents/Requirements/CAE-CDE_Criteria_2020.pdf

Cybersecurity Supply and Demand Heat Map. (n.d.). CyberSeek Project Web site. Retrieved May 22, 2020, from https://www.cyberseek.org/heatmap.html

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

Exec. Order No. 13870, (2019, May 2). American's Cybersecurity Workforce. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

Haire, M. & Oloffson, K. (2009, July 30). Brief History, Interns. TIME. Retrieved May 22, 2020, from http://content.time.com/time/nation/article/0,8599,1913474,00.html

(ISC)^2. (2018, October 17). International Information System Security Certification Consortium (ISC)2® Web site. Retrieved from https://www.isc2.org/News-and-Events/Press-Room/Posts/2018/10/17/ISC2-Report-Finds-Cybersecurity-Workforce-Gap-Has-Increased-to-More-Than-2-9-Million-Globally

(ISC)^2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 Cybersecurity Workforce Study, 2019. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Jones, D. & Lerman, R. (2017, June). Starting a Registered Apprenticeship Program. The Urban Institute. Retrieved from https://innovativeapprenticeship.org/wp-content/uploads/2017/06/Employer-Guide_June-2017.pdf

King, L. W. (Trans.). (2008). The Code of Hammurabi. Lillian Goldman Law Library, Yale Law School, Avalon Project Web site. Retrieved May 22, 2020, from https://avalon.law.yale.edu/ancient/hamframe.asp

Lester, S. and C. Costley. (2010). Work-based learning at higher education level: value, practice and critique. Studies in Higher Education. 35, no 5: 561-575

Nappi, M. (2019, March 11). Cybersecurity Apprentice Program: A CyberStart JumpStart. Retrieved May 22, 2020, from https://you.stonybrook.edu/matthewnappi/2019/03/11/cybersecurity-apprentice-program-a-cyberstart-jumpstart/

Petrella, E. (2020, June 11). National Initiative for Cybersecurity Education (NICE) Working Group. Retrieved June 24, 2020, from https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group

Raelin, J. (1997). A Model of Work-Based Learning. Organization Science. https://doi.org/10.1287/orsc.8.6.563

Seshagiri, G., Ghosh, T., & Aliaga, O. (2020, June). Survey results on work-based learning in colleges with cybersecurity programs.

Tripwire. (2020, February). Cybersecurity Skills Gap Report 2020. Retrieved from https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Tripwire-Dimensional-Research-Skills-Gap-2020.pdf

Weinstein, P. V. (2014, November 05). To Close a Deal, Find a Champion. Retrieved June 24, 2020, from https://hbr.org/2014/09/to-close-a-deal-find-a-champion