Constructing a Methodology for Developing a Cybersecurity Program

Patrick Ward
Claremont Graduate University
patrick.ward@cgu.edu

Abstract

This paper serves to introduce the problem of constructing a methodology to develop a cybersecurity program. The goal of the program is to prepare students graduating from an accredited two-year college for success in cybersecurity careers. Several challenges must be addressed such as program accreditation, workforce development, and DHS/NSA Center of Academic Excellence in Cyber Defense (CAE-CD) designation. All of these serve as inputs in constructing a methodology to develop such a program to meet local industry needs for cyber professionals.

1. Introduction

The Internet has brought us ubiquitous connectivity to virtually all computing devices, where integrity and confidentiality are now a lower priority than the drive for availability. The ubiquitous connectivity has yielded many benefits including location-based services, home security, online banking, and a convenient alternative to accomplishing many tasks that previously had to be done in person. However, many problems that plague the Internet today result from the focus on availability instead of security as the bulk of Internet usage today is more oriented toward business transactions than ever before. The drive to produce software to make services more available has forced many software companies to market software that is not focused on security, but rather convenience and ease of use.

Recent years have seen a growing awareness of the need to improve cybersecurity and that cybersecurity is important to the national defense of every country. The growing threat of cyberattacks, whether they be denial of service attacks or viruses, has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure. The cybersecurity incidents continue to proliferate due to a shortage of well-educated cybersecurity professionals, almost 3 million globally [1], to combat cybersecurity incidents and defend against cybercriminals. The US government even passed legislation to fund the development of computer security education programs through the Cybersecurity Research and Development Act [2]. Another growing concern is the threat of nation-states engaging in cyberwarfare, and the possibility that business and personal information systems could become casualties if they are undefended [3].

Decreasing the number of cybersecurity incidents can be done by addressing the shortage of well-educated cybersecurity professionals in the workforce [4]. The NSA [5] states that higher education and research in cyber defense can produce professionals with cyber defense expertise to reduce the vulnerabilities that lead to cyber security incidents in the national information infrastructure.

There are many challenges to effectively training cybersecurity professionals to be adequately prepared for the workforce. Various efforts have been made in the past with limited success. These efforts mainly address curriculum development. All these efforts fall short when it comes to training undergraduates in two-year degree programs to be ready to combat the causes of cybersecurity incidents as they fail to address the gap in hands-on skill exercises.

There are various standards that can be used as curriculum development guidelines. The Department of Homeland Security (DHS) in partnership with the National Security Agency (NSA) has created a Center of Academic Excellence Cyber Defense (CAE-CD) designation [5] for programs that meet certain standards. There are also two organizations that accredit cybersecurity programs: Association of Technology, Management, and Applied Engineering (ATMAE) [6] and the Accreditation Board for Engineering and Technology (ABET) [7] There are also industry recognized certifications that can be used to guide curriculum development [8] and there was a joint task force of the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM) that formed the Cyber Security Education Consortium (CSEC) to produce the CSEC2017 standard. [3]

A framework needs to be created to develop an ATMAE-accredited cybersecurity curriculum with a CAE-CD designation that incorporates hands-on skill

URI: https://hdl.handle.net/10125/70617
978-0-9981331-4-0

exercises for an undergraduate program in a two-year college. The methodology is needed because colleges can use it as a framework for developing cybersecurity curricula that meet the needs of their local employers.

I will propose a framework for modeling a cyber defense curriculum based on the National Initiative for Cybersecurity Education (NICE) framework and the Cyber Security Education Consortium (CSEC17) framework [3] that satisfies both the requirements for the NSA CAE-CD designation [5] and the ATMAE accreditation standards [9] for a two-year college offering Associate's Degrees using hands-on skill exercises that sufficiently prepare students for careers that satisfy local employers' cyber defense needs.

2. Literature Review

I will review the literature based on the different components of a methodology: the standards underlying a curriculum (the "what"), the pedagogy involved with a curriculum (the "how"), and a process for implementing a curriculum. All of these are parts of developing a methodology for curriculum development as the college's Computer Information Technology (CIT) department needs to know on what we are basing the curriculum, how it is to be taught, and what the process itself is for developing the curriculum.

2.1. Standards and Accreditation

After having established the need for an undergraduate cybersecurity program curriculum (the "why" of the design), and prior to discussing the methodology that one could use to develop a curriculum; one must realize that many standards are available upon which to base the curriculum, but only two applicable accreditations: ATMAE and ABET.

There have been various efforts using different standards, but only one of them using ATMAE [9]. Some efforts have focused on colleges achieving the NSA/DHS CAE-CD designation [10-15], but the efforts were either for four-year degree programs or for business schools [16]. Some efforts used ABET [16-27], but only for four-year degree programs. Only Doggett [28] described an undergraduate 2-year program applying for ATMAE accreditation, but the author, like the others cited above, failed to address the methodology used for curriculum development.

While many of the papers discuss ABET [23] for one, I have not found a paper that discusses meeting ATMAE accreditation requirements for an undergraduate (2-year) cybersecurity curriculum. ABET only offers its Computing Accreditation Commission (CAC) accreditation to 4-year schools. The ATMAE accreditation is the most appropriate for an IT curriculum at a 2-year college.

None of the efforts cited above have explicitly focused on the development of a methodology for curriculum development. Any proposed cybersecurity curriculum should produce more and better educated and trained cybersecurity professionals to defend against cybersecurity incidents [29]. Educational institutions must maintain both their regional and program accreditations and develop cybersecurity curricula that meet those requirements.

Some of the other standards upon which programs are based include CSEC2017 [30], CAE [31], CS2013 [32], NICE [33] and NISTISSI-4011 [11]). The relevant standard to my problem is that of the DHS/NSA Center of Academic Excellence for Cyber Defense (CAE-CD). I will discuss both the curriculum standards and the process of obtaining the CAE-CD designation for the college's cybersecurity program in 2020.

2.2. Pedagogy

After having examined the standards behind curriculum development (the "what"), I will now focus on how such a cybersecurity curriculum could be delivered (the "how"), what options there are for delivering it; e.g. flipped classroom, blended learning, hands-on exercises and how the prior literature has assessed the effectiveness of these methods. Cybersecurity tasks require students to be able to analyze complex data and to know how and when to use tools. O'Neill and McMahon [34] show that a student-centered learning (SCL) approach can be effective in improving student learning. SCL can manifest itself in many ways: experiential, flexible, and self-directed.

There are a few different approaches that have been shown to be effective in cybersecurity instruction. The approaches are role-based [35], challenge-based [36], e.g. the US Cyber Challenge [37], scenario-based [38], competency-based [39], game-based [40], and inquiry-based [41]. Each of these are explained below.

Toth and Klein [35] describe a role-based approach in which students take on different roles in cybersecurity scenarios and interact with each other using these different roles to gain perspective on how incidents are handled. Apple [36] proposed a challenge-based learning (CBL) methodology that requires students to use their knowledge and technology to solve real-world problems. The challenge-based concept has been applied to the development of cybersecurity skills among high school and college students. The Center for Internet Security (CIS) describes many different cyber-oriented challenge-based events in the US alone to promote workforce development. The challenges can be broad (e.g., keep confidential information safe and keep the network safe from cyber-attacks [19] or narrow (i.e., focused on a specific problem).

Carlton [38] describes a scenario-based approach where students are given various scenarios and use their skills to demonstrate their knowledge. The competency-based approach [39] requires students to demonstrate their competency by completing certain objectives. The game-based approach has students playing games like CyberAware [40] to master the concepts, leading students to a greater sense of cybersecurity awareness. CyberAware is a novel mobile application developed for cybersecurity awareness and education in both formal and informal learning settings for children. The distinguishing feature of the app is that it uses the Attention, Relevance, Confidence, and Satisfaction (ACRS) motivational model. The inquiry-based approach [41] gives students the independence to discover the solution, but it provides guidance when necessary.

Sweller [42] describes cognitive load theory, which states that while providing students explicit instructions in a prescriptive approach is important, it is not clear that the students are learning anything other than how to follow directions. A more goal-oriented, open-ended approach that engages the students to try to independently figure out problems' solutions may be more effective.

The research cited above has shown that each of the pedagogical methods for delivering a cybersecurity curriculum is effective. Each of the methods relies on students applying the skills learned, analyzing problems and scenarios, synthesizing various skills learned, and evaluating their effectiveness [43,44]. Each of these six ways of delivering the curriculum share several commonalities that I have incorporated into a pedagogy: 1) hands-on skills-based assessment, 2) competencies assessed by the students' ability to pass certification exams, and 3) the CBL methodology engaging the students to outperform their peers and to solve real-world problems. Each of the methods outlined above was challenged by the college's decision to close campus due to the COVID-19 outbreak.

2.3. Process

After discussing the pedagogical methods of delivering an undergraduate cybersecurity program curriculum (the "how" of the design), one must now examine the process or methodology for developing the curriculum, I.e. how does one design such a curriculum. Woodward, et. al. [45] describe the process that a large university undergoes to achieve the CAE-CD designation for their program. This process involves several steps involving the faculty, the students, and industry. Clark and Stoker [31] discuss the eight specific program requirements: letter signed by the college president endorsing the program, evidence of the program's existence for at least 3 years with one year of student degrees, evidence that student development and assessment are fostered in the field of Cyber Defense, a virtual "center" for cyber education, evidence of sufficient cyber faculty to ensure continuity, evidence that cyber defense is incorporated in other degree programs, an institutional security plan, and cyber outreach and collaboration efforts outside the institution [5].

In addition to the program requirements, there are specific curricula requirements. The NSA/DHS have defined 11 core cyber defense knowledge units (KU) to which all two-year curricula should map. Each KU includes a definition, topics to be covered, and student learning outcomes. The NIETP web site ("National IA Education & Training Programs", n.d.) lists the following areas: basic data analysis (quantitative literacy), basic scripting, cyber defense, cyber threats, fundamental security design principles, information assurance fundamentals, introduction to cryptography, information technology system components, networking concepts, policy, legal, ethics and compliance and systems administration. Darabi and Cruz [46] describe the common practice of incorporating as many KUs into as few courses as possible to ensure that students are required to take those courses to graduate with cyber defense degrees.

Mew [14] outlines several issues to consider when designing a cybersecurity curriculum. Each of these issues and the discussion of how they apply to the author's college's nascent cybersecurity program is in section 3.

Key success factors in program design are having a faculty project champion, faculty dedication and tenacity, industry partner(s), alumni and student involvement, and continuous improvement. Continuous improvement can be assessed using metrics measuring enrollment, job placement, and the CAE-CD designation. The CAE-CD designation itself requires that cybersecurity awareness be a part of the entire university's curriculum. Students also need to be involved in security activities whether that be in the form of cyber defense competitions, outreach efforts, or other undergraduate research opportunities. Industry needs to be involved to provide input on the level of cybersecurity education that they expect from new employees. Faculty need to be involved in recruiting activities to increase enrollment in cybersecurity programs.

Three of the most recent articles merit closer review of the process outlined in them. Clark and Stoker [31] serve as a good reference for those unfamiliar with the process of obtaining a CAE-CD designation. Dawson, et. al. [25] explain how a CAE-CD designated program can be used for cyber workforce development. Katz [14] explains the challenge of either preparing students extensively in one topic (depth) or exposing students to a variety of topics (breadth).

Kim and Beuran [47] propose a conceptual methodology for designing a cybersecurity education program for higher education. Their paper focuses on the steps involved at a four-year university, but they do not actually implement a program, so there is no empirical data on which to assess their methodology. The authors outline the steps required to design a cybersecurity curriculum including review of existing programs, defining an educational framework, designing a program curriculum, selection appropriate pedagogical methods, developing curriculum content, and testing and revising the content. Kim and Beuran [47] cite the NIST Cybersecurity Framework (NICE) for reference, but they ignore the CAE-CD designation requirements, and other relevant frameworks like CSEC2017 and ACM2013. The authors reference the use of integrative learning theory in developing a holistic cybersecurity education model encompassing curriculum development, experiential learning methods, assessments, and building communities of practice (CoPs). The authors also cite two pedagogical models and methods: Kuzmina-Bespalko-Popovsky (KGP) and Process Oriented Guided Inquiry Learning (POGIL).

The authors present their educational program design methodology in Figure 1 of their paper which helps to visualize their model. The authors further clarify what they mean by defining the educational framework in dimensions: institutional, users: learners and stakeholders, and external. The authors also propose a curriculum design outline in very broad terms, but the more specific examples in other papers provide more guidance. The authors do have a relatively thorough discussion on choosing pedagogy, which is helpful in analyzing the various discussions of pedagogy in other papers. It also helps to put the various pedagogical methods in the context of a cybersecurity education. In developing educational content, the authors recommend holding a workshop. The final step of revising and testing would occur once a program has been in existence for several years.

3. Framework/Methods

As noted above, the author's college is a 2-year college that offers Associate degrees. The college's cybersecurity program has been in existence since the fall 2016 semester, and it is updated every semester to track the ever-changing cybersecurity landscape. It is time to revise and test the program. This provides an opportunity to build a framework that can inform not only the college's program but can be generalized to other college cybersecurity programs. Thus, I propose to use the action design science research (ADR) approach formulated by Sein, et. al. [48] to build such a framework. I chose this approach because of the influence that the organizational context has on the development of the college's cybersecurity program. The organizational context contributes prospective employers for the students, accreditation requirements, a setting as in a trade school or a 4-year university to the cybersecurity program's development. The effect that the organizational context has on the program's development cannot be understated, and hence the need to recognize the organizational context's contribution necessitates the use of an approach that takes the organizational context into account.

In this paper, Orlikowski & Iacono's [49] "ensemble artifact" is the cybersecurity program itself. I will use the ADR method itself to justify its use in this case.

The first stage is problem formulation. Section 1 introduced the problem of developing a program that meets the needs of various stakeholders. These stakeholders are all part of the organizational context. The initial scope of the problem is to develop a program that meets the needs of faculty, students, and cybersecurity professionals addressing the three dimensions addressed by Kim and Beuran [47]: institutional, users, and external as outlined in section 2 above. This problem posed a unique research opportunity using the existing theories as discussed in section 2 above to develop a cybersecurity program fitting the college's organizational context. The formulation of the problem relies on practice-inspired research in which I create knowledge through revising and testing a new cybersecurity program to meet the college's changing organizational context. The "ensemble artifact," i.e., the program itself, in ingrained in Kim and Beuran's, [47] framework as a Gregor [50] Type V design theory.

Kim & Beuran's [47] three dimensions of the institution, the users, and external are useful in describing the situation at the college. The users are represented by both the current and the prospective students, i.e. both the students who are currently seeking employment after graduation and the students who are considering attending the college's cybersecurity program to gain employment in the industry after graduation. The users of the program are also represented by the faculty themselves that provide input based on their own IT and cyber experience into the cybersecurity programs' development. institutional dimension is not only represented by the college itself, but also by the various accreditations that both the college and the program itself need to have to attract and retain students. The ATMAE accreditation that the program needs are mentioned in section 2, and the college itself needs a SACS accreditation. The external dimension is represented by the industry employers, who are, in turn, represented by the local industry advisory board (IAB), which is composed of hiring managers from some of the local companies employing students in the cybersecurity and IT industries.

The second stage is building out, intervening in, and evaluating the artifact, i.e. the program. The program is dominated by the organizational context. The first iteration of the program was solely based on the academic publisher's textbook offerings with courses formed around each textbook's 15 or so chapters corresponding to 15-week semesters. The program initially held an AACSB accreditation, but the requirements for that accreditation changed, and the faculty elected to pursue a new accreditation with ATMAE. Initially, the faculty, representing IT nationwide, deemed the curriculum adequate. However, after conferring with the local IAB the faculty determined that the program needed to have some basis in nationally recognized industry accredited certifications. Each iteration of the program's build-out is based on recursive cycles of decisions made by the stakeholders as the organizational context changes. Even the IAB members themselves changed as either needs were met and the IAB member no longer came, or new needs arose, and a different company would participate in the IAB to help influence the faculty's decisions.

Another input at this second stage is the curriculum committee process of developing, submitting, discussing, and approving curriculum changes. The process of modifying the courses is essentially the same at each iteration as each change to the curriculum needs to be reviewed by a curriculum committee, but how those changes come about varies depending on industry input, accreditation changes, or industry-recognized certification changes. Initially, the cybersecurity program was approved because there was no previous program and there was an industry need. However, as industry needs change, so must the curriculum. Since the IAB meets once a semester (twice a year), there exist ample evaluation opportunities to ensure that the program is meeting those needs. One change to the evaluation process itself is to elicit input from key industry stakeholders to ensure that needs are being met. One such example was a dialogue with representatives of the local utility company and their corresponding staffing agency to ensure that the college's cybersecurity program was meeting their needs. As a result of this, faculty added student preparation for additional industry certification exams to the existing courses by modifying those courses to be more comprehensive in their coverage of topics on the exams. As the exams themselves are updated every few years, there is now a periodic curriculum evaluation for those certification courses to ensure that they meet current certification exam requirements.

4. Discussion

This is an ongoing effort at a community college with a new cybersecurity program since 2016. ATMAE standards were used for accreditation. Local industry is consulted twice yearly for their inputs regarding the program and for suggestions for improvement. Various certification organizations are reviewed for the different certifications offered, their relevance to the program, and local industries' desire for them. The proposed framework with the program development inputs is specified in Figure 1. In each of the following subsections, I will describe the different ways in which each iteration of the second stage of the ADR approach is applied to the existing cybersecurity curriculum. Each cycle provides an opportunity to adapt the curriculum to industry's ever-changing needs

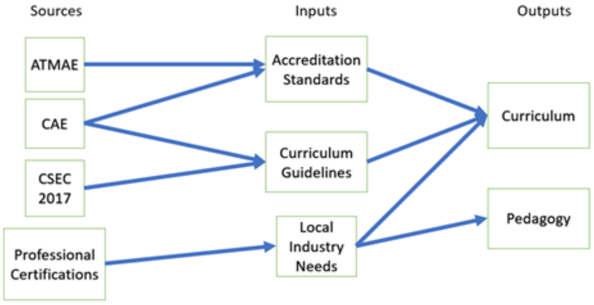

Figure 1. Program development inputs

In total, there were three iterations done through the cybersecurity program development life cycle. The first iteration was the change in accreditation of the program itself from AACSB to ATMAE necessitating the addition of a natural science course to the curriculum. This iteration did not involve any changes to the CIT courses so on impact was assessed. The second iteration was a result of input from the local industry via the IAB, which declared the need for courses to be aligned with existing industry certifications. The third iteration was a result of changing the curriculum to align with CAE-CD KUs. I will address how the changes in each of the iterations impacted the cybersecurity program development in the following subsections with a discussion of the evaluation in the next section.

4.1 New and Modified Courses

New courses needed to be added to the curriculum to accommodate local industry needs and emerging technologies. New courses are offered for two years to assess their effectiveness before they are added to the curriculum. This allows the college to flexibly adapt to local industry needs. Two courses that were adapted to meet industry needs were digital forensics and penetration testing and network defense. The digital forensics courses were adapted to meet local industry needs by providing a more comprehensive foundation for students to be ready to be trained by future employers or to take graduate courses. The penetration testing and network defense course was adapted to cover topics like malware analysis using data analytics and a brief introduction to Python programming. Future courses may include topics like cloud computing, data analytics, and mobile computing.

Proposing new courses requires a one-year lead time for evaluation by the curriculum committee. Currently, we are considering replacing the advanced digital forensics course with a special topics course. The plan is to use this course to introduce students to new topics in this emerging discipline without having the curriculum committee needing to review the course every time topics change. This should allow us to keep our curriculum somewhat flexible.

Modifying existing courses does not require curriculum committee approval if only the course content itself is changing. The courses were aligned with various industry certifications so that graduating students would be able to have attained certifications to make them more employable as requested by the local industry. We were able to incorporate industry's expressed needs for industry certifications in existing courses CITC 1302, CITC 1332, and CITC 2326 without much effort as only a few optics needed to be added or removed depending on their presence in the relevant certification exams: CompTIA Network+, Linux+, and Security+. Future modifications will be made to CITC 2356 for the CompTIA PenTest+ exam. Table 1 lists only the computer information technology courses in the current program curriculum.

Table 1. Current program curriculum

Term/Year	Course	Course Name
Fall/1st	CISP 1010	Computer Science 1
	CITC 1302	Introduction to Networking (CompTIA Network+)
	CITC 1351	Principles of Information Assurance
Spring/1st	CISP 1020	Computer Science 2
	CITC 1303	Database Concepts
	CITC 1332	UNIX/Linux Operating System (CompTIA Linux+)
	CITC 2326	Network Security (CompTIA Security+)
Fall/2nd	CITC 2335	Systems Analysis and Design
	CITC 2352	Digital Forensics
	CITC 2363	Internet Intranet Firewalls and eCommerce
Spring/2nd	CITC 2354	Advanced Digital Forensics
	CITC 2356	Penetration Testing and Network Defense
	CITC 2399	CIT Internship

4.2 Course Sequencing

Course sequencing was also an issue for several reasons. Notably, the course prerequisites needed to be redefined to ensure that students were at least exposed to the concepts prior to applying them in subsequent courses. Another factor that needed to be overcome was the students' reluctance to retain information from one course to apply in another. Initially, students were taking courses that depended on Linux knowledge before they took the Linux course. The students were also expected to understand basic programming concepts before they took courses involving scripting. The students' application of shared concepts was most apparent in the network security course where the students are required to engage in undergraduate research to prepare a paper and a presentation to their peers across the college as part of a student research symposium.

The initial course sequencing was found to be deficient because the students were expected to write research papers in CITC 1302 and research and write security plans in CITC 1351. The prerequisites for these courses were altered to require students to have taken Composition 1. For CITC 2356 and CITC 2363, the Linux knowledge proves to be helpful, so CITC 1332 was added as a prerequisite to the courses. The Penetrating Testing course uses Linux scripts and the CITC 2363 course explores the Cisco IOS in depth where a familiarity with the terminal and the command-line help the students to navigate the Cisco IOS. Changing the course prerequisites required one-year lead time for the campus curriculum committee to evaluate the changes before they were made effective for the following academic year.

4.3 Course Delivery

Course delivery was also challenging as it required the IT group to set up a firewalled classroom/lab environment in which the students could freely practice the techniques they learned. This setup did not provide a satisfactory solution for students unable to come to the classroom, so a cloud-based solution is now being considered. In the meanwhile, to accommodate campus closure, we were able to leverage a textbook publisher provided solution allowing students access to a virtualized online environment. The resulting pedagogy is a combination of a flipped classroom and a tutorial-style approach where students complete their labs during class time, and the instructor is available to render assistance should the students have any difficulties completing the assigned lab work.

5. Evaluation/Assessment

At each of the ADR stages described in section 3, the author performed an evaluation of how the curricula was meeting industry needs through both assessment of student learning outcomes (SLOs) for each course and by the rate of IT industry job placement for each of the graduated students. Each iteration of the ADR second stage required changes in the curriculum: new or modified courses as described in section 4.1, course sequencing as described in section 4.2, course delivery as described in section 4.3. Below, I will briefly describe how each of the categories of changes to the curriculum were evaluated.

When a course is modified or added to meet an industry certification, the evaluation of its effectiveness is limited to the success rate of the students on the certification exam relevant to the course. Both the CITC 1302 and CITC 2326 courses were changed to align with the CompTIA Network+ and Security+ certification exams more closely, and, as a result, more students passed the exams. As this effort is still ongoing, multiple cycles will be necessary to constantly adapt the program to industry's changing needs.

When a course is modified or added to meet an industry need, the evaluation of its effectiveness is done by the employers of the graduates to determine if those graduates are knowledgeable enough in those subject areas to perform their job tasks or if the graduates require more training. As of the 2018 graduating class (the first class having graduated with the curriculum as of fall 2016), each of the employers expressed a desire that the students were taught additional material in existing courses. The college's CIT department modified those courses to meet those needs. With the 2019 graduating class, the employers no longer expressed the same needs, so we determined that the modifications were successful.

When course sequencing is changed, the evaluation of the effectiveness is based on the students' demonstrated knowledge of prior course subjects in subsequent courses. Each course's summative assessments tested the subjects students needed to know for subsequent courses. The assessments were essentially the same while having different questions, but in the same style, structure, format, and difficulty. The assessments needed to be modified each semester to preserve integrity. Assessment were also performed of student's prior knowledge at the beginning of each of the subsequent courses. Overall, the students who had taken the courses in the changed course sequence demonstrated more knowledge (had higher test scores) than those that had not taken the courses in the new sequence. Those students who had taken the courses in the changed course sequence also had higher GPAs.

When course delivery was changed, the evaluation of the effectiveness is based again on the students' demonstrated knowledge when given various problems to solve. A major pedagogical change occurred right after spring break in 2020 with the COVID-19 outbreak. As the outbreak necessitated campus closure for safety reasons, the entire cybersecurity curriculum was moved online. Instruction changed from in-person face-to-face on-ground with lab computers on campus to video conferenced class sessions with lab exercises in a virtualized environment. The students took a few weeks to adapt to the new format as the area was hit by a tornado a month later causing power and internet outages, but the students did adapt to the new format. The drastic change in pedagogical methods seemed to have a negligible impact on test scores as the students in the courses this spring 2020 semester did no better or worse (not statistically significant) than students in prior semesters.

The author also used job placement as an evaluation criterion to evaluate the effectiveness of the curriculum changes. As of the first (2018) graduating class, every cybersecurity student was placed in an IT industry job. Half a dozen local employers place the students, but different employers have different needs every year, so the students are not always placed with the same employers. Some of the students have started working at a local employer and then moved out of the area for work. Since the goal of the two-year college's cybersecurity program is employment, the college's CIT department determined that the program is successful. We hope to increase the number of graduates as our program matures and adapts. The numbers in table 2 below include graduates from the fall, spring, and summer semesters.

Table 2. Graduation Information

Graduation Year	# Students	# Employers
2018	5	4
2019	6	4
2020	6	4

6. Contribution

This paper seeks to offer guidelines to faculty and staff in building a cybersecurity curriculum for a two-year community college. Regardless of the institution, the same issues: local industry, academic accreditation, professional certifications, and curriculum need to be addressed. Although the ATMAE accreditation requirements are not the same as they are for ABET, the same process of applying the standards is used. The contribution here related to the CAE-CD KUs is equally applicable to the ABET knowledge, skills, and abilities (KSAs) and to the recently released Cyber2yr2020 [51] guidelines, which are, mapped to both the NICE and the CAE-CD recommendations.

7. Limitations

The limitations on this case study are that they are specifically relevant to a two-year community college cybersecurity program seeking both a DHS/NSA CAE-CD designation and ATMAE accreditation. Four-year universities have the option of seeking program accreditation with ABET. The NICE framework serves as a guideline to meet the DHS/NSA CAE-CD requirements for the designation, but a college also needs to have their programs accredited to attract, retain, and place students in industry.

8. Conclusion

As ubiquitous connectivity has infiltrated our lives, it is now more important to defend ourselves from the myriad of cyberthreats. We need more and better-educated cybersecurity professionals to defend us. This paper is an attempt to provide institutions of higher learning guidance on developing accredited relevant programs that can be used to prepare students for careers as cybersecurity professionals.

9. References

[1] (ISC)^2 (2018) Cybersecurity Skills Shortage Soars, Nearing 3 Million. Retrieved November 1,2018 from https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html

[2] Cybersecurity Research and Development Act, US House posting on Cyber Security Act (2002): Retrieved November 2, 2018 from https://legcounsel.house.gov/Comps/Cyber%20Security%20Research%20And%20Development%20Act.pdf

[3] Joint Task Force (JTF) on Cybersecurity Education, CyberSecurity Curricula 2017 (CSEC 2017) Retrieved December 10, 2018 from https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

[4] Coulson, Tony; Mason, Megan; and Nestler, Vincent (2018) "Cyber Capability Planning and the Need for an Expanded Cybersecurity Workforce," Communications of the IIMA: 16(2), Article 2.
Available at: https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2

[5] NSA, National Centers of Academic Excellence (CAE) Resource Guide (2018) Retrieved May 1, 2019 from https://niccs.us-cert.gov/sites/default/files/documents/pdf/cae_program_guidance.pdf?trackDocs=cae_program_guidance.pdf

[6] Association of Technology, Management, and Applied Engineering (ATMAE) (2017) programs Retrieved May 1, 2019 from https://www.atmae.org/resource/resmgr/ATMAE_Programs_by_state_as_o.pdf

[7] Accreditation Board for Engineering and Technology, Inc. (ABET), ABET Accredited Program Search, retrieved May 1, 2019 from http://main.abet.org/aps/Accreditedprogramsearch.aspx

[8] Knapp, K., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. Journal of Information Systems Education, 28(2), 101-113.

[9] Association of Technology, Management, and Applied Engineering (ATMAE), 2019 Accreditation Handbook downloaded from https://www.atmae.org/resource/resmgr/accred_2018/2019_Accreditation_Handbook.pdf

[10] Bacon, T., and Tikekar, R. (2003). Experiences with developing a computer security information assurance curriculum. Journal of Computing Sciences in Colleges, 18(4), 254-267.

[11] Dennis, T., El-Gayar, O. F., & Streff, K. (2004). A model program in information assurance and computer security. IACIS International Association for Computer Information Systems 2004, 4(2), 97-102.

[12] Schweitzer, D., Humphries, J., & Baird, L. (2006). Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education. Journal of Computing Sciences in Colleges, 22(1), 151-160.

[13] Mew, L. (2016). The Information Security Undergraduate Curriculum: Evolution of a Small Program. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 3857) downloaded from http://proc.iscap.info/2016/pdf/4071.pdf

[14] Katz, F. H. (2018). Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models. The Cyber Defense Review, 3(2), 65-72.

[15] Yates, D. J., Frydenberg, M., Waguespack, L. J., McDermott, I., OConnell, J., Chen, F., & Babb, J. S. (2018).

Dotting i's and Crossing T's: Integrating Breadth and Depth in an Undergraduate Cybersecurity Course. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 3857).

[16] Yang, Samuel C. & Bo Wen (2017) Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States, Journal of Education for Business, 92:1, 1-8, DOI: 10.1080/08832323.2016.1261790

[17] Mattord, H. J., & Whitman, M. E. (2004, October). Planning, building, and operating the information security and assurance laboratory. In Proceedings of the 1st annual conference on Information security curriculum development, 8-14.

[18] Smith, T., Koohang, A., & Behling, R. (2010). Formulating an effective cybersecurity curriculum. Issues in Information Systems, 11(1), 410-416.

[19] Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011, July). Challenge based learning in cybersecurity education. In Proceedings of the 2011 International Conference on Security & Management (Vol. 1)

[20] Conklin, W. A.; R. E. Cline and T. Roosa, "Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors," 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 2014, 2006-2014.

[21] Koohang, A., Riley, L., Smith, T., & Floyd, K. (2010). Design of an Information Technology Undergraduate Program to Produce IT Versatilists. Journal of Information Technology Education, 9, 99-113.

[22] Greenlaw, R., Phillips, A., & Parrish, A. (2014). Is it Time for ABET Cybersecurity Criteria? ACM Inroads, 5(3), 44-48.

[23] Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. Journal of Information Systems Education, 26(3).

[24] Ekstrom, J. J., Lunt, B. M., Parrish, A., Raj, R. K., & Sobiesk, E. (2017, September). Information technology as a cyber science. In Proceedings of the 18th Annual Conference on Information Technology Education, 33-37.

[25] Dawson, M., Wang, P., & Williams, K. (2018). The role of CAE CDE in cybersecurity education for workforce development. In Information Technology-New Generations, 127-132. Springer, Cham.

[26] de Leon, D. C., Jillepalli, A. A., House, V. J., Alves-Foss, J., & Sheldon, F. T. (2018). Tutorials and laboratory for hands-on OS cybersecurity instruction. Journal of Computing Sciences in Colleges, 34(1), 242-254.

[27] Raj, R. K., & Parrish, A. (2018). Toward standards in undergraduate cybersecurity education in 2018. Computer, 51(2), 72-75.

[28] Doggett, M. (2015). Defining the technology management body of knowledge for ATMAE-accredited programs. Technology Interface International Journal, 16(1), 87-99.

[29] Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74-83.

[30] Conklin, W., & Bishop, M. (2018). Contrasting the CSEC 2017 and the CAE Designation Requirements. In 2018 51st Hawaii International Conference on System Sciences, 2435-2441.

[31] Clark, U., & Stoker, G. (2018). Reflections on Applying for CAE-CDE Designation. In Proceedings of the EDSIG Conference ISSN (2473)3857.

[32] McGettrick, A. (2013). Toward effective cybersecurity education. IEEE Security & Privacy, 11(6), 66-68. doi:10.1109/MSP.2013.155

[33] McGinnis, D. R., & Comstock, K. (2003). The implications of information assurance and security crisis on computing model curricula. Information Systems Education Journal, 1(9), 1-12.

[34] O'Neill, G., & McMahon, T. (2005). Student-centered learning: What does it mean for students and lecturers? In G. O'Neill, S. Moore, & B. McMullin (Eds.), Emerging issues in the practice of university learning and teaching. Dublin: All Ireland Society for Higher Education.

[35] Toth, P., & Klein, P. (2013). A role-based model for federal information technology/cyber security training. NIST special publication, 800(16), 1-152.

[36] Johnson, L., & Brown, S. (2011). Challenge based learning: The report from the implementation project (pp. 1-36). The New Media Consortium.

[37] US Cyber Challenge retrieved from https://www.uscyberchallenge.org/

[38] Carlton, M. (2016). Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses Global. (UMI No. 10240271)

[39] Sabeil, E., Manaf, A. B. A., Ismail, Z., & Abas, M. (2011). Cyber forensics competency-based framework-a review. International Journal of New Computer Architectures and their Applications, 1(4), 991-1000.

[40] Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015, November). CyberAware: A mobile game-based app for cybersecurity education and awareness. In 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL) (pp. 54-58). IEEE.

[41] Weiss, R., Locasto, M. E., & Mache, J. (2016, February). A reflective approach to assessing student performance in cybersecurity exercises. In Proceedings of the 47th ACM Technical Symposium on Computing Science Education (pp. 597-602).

[42] Sweller J. (2016) Cognitive Load Theory, Evolutionary Educational Psychology, and Instructional Design. In: Geary D., Berch D. (eds) Evolutionary Perspectives on Child Development and Education. Evolutionary Psychology. Springer, Cham

[43] Bloom, B. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Longmans, Green.

[44] Anderson L., Krathwohl, D., et al. 2001. A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Addison Wesley Longman, Inc.

[45] Woodward, B., Imboden, T., & Martin, N. L. (2013). An undergraduate information security program: more than a curriculum. Journal of Information Systems Education, 24(1), 63-70.

[46] Darabi, D. M., & Cruz, A. (2015). Meeting the CAE IA/CD Knowledge Units Requirements for the Polytechnic

University of Puerto Rico. In 13th LACCEI Annual International
[47] Kim, E., & Beuran, R. (2018, October). On designing a cybersecurity educational program for higher education. In Proceedings of the 10th International Conference on Education Technology and Computers, 195-200. ACM. dx.doi.org/10.1145/3290511.3290524
[48] Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. MIS quarterly, 37-56.
[49] Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary: Desperately Seeking the 'IT' in IT Research—A Call to Theorizing the IT Artifact," *Information Systems Research* (12:2), pp. 121-134.
[50] Gregor, S. 2006. "The Nature of Theory in Information Systems," MIS Quarterly (30:3), pp. 611-642.
[51] Tang, C., Tucker, C., Servin, C., Geissler, M., & Stange, M. (2020, February). Curricular Guidance for Associate-Degree Cybersecurity Programs. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education, 1285-1285.