Development of a Small Cybersecurity Program at a Community College

Patrick Ward
patrick.ward@cgu.edu
Center for Information Systems and Technology
Claremont Graduate University
Claremont, CA 91711 US

Abstract

This paper introduces 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, pedagogy, existing curriculum standards, and the process to achieve a Department of Homeland Security/National Security Agency Center of Academic Excellence in Cyber Defense (CAE-CD) designation. All of these serve as inputs in constructing a methodology to develop a program to meet local industry needs for cyber professionals.

Keywords: Cyber Security Education, Curriculum Development, Pedagogy

1. INTRODUCTION

This paper seeks to offer guidelines to faculty and staff in building a cybersecurity curriculum for a two-year community college by reporting how a community college has been developing a small cybersecurity program since the fall 2016 semester and discusses the motivation for various changes made as the program has evolved over the last 3 years. This paper shows how the curriculum was adapted to meet various challenges. This paper also addresses how the college has changed course delivery due to campus shutdown. The original program was an Association to Advance Collegiate Schools of Business (AACSB) accredited business information systems program, and this program needed to be changed to both accommodate local industry's evolving need for cybersecurity professionals and to be accredited with Association of Technology, Management, and Applied Engineering (ATMAE). The program also needs to serve the growing demand for cybersecurity professionals nationwide. (Coulson, Mason, & Nestler, 2018) (Burning Glass Technologies, 2019) The new cybersecurity program has been developed from the original because (1) it was cost effective to do so, (2) existing faculty could be used to start the program, and (3) the faculty wished that the program retain its AACSB accreditation. The third goal was later determined to be untenable as the AACSB accreditation requirements changed. These three constraints shaped the curriculum development. This paper discusses the changes made to the original program to support the new cybersecurity program and explains why each change was made.

The Business and Information Technologies (BUS) division at the author's community college (CC) had an information systems technology program since 2009. Information systems is generally considered a business school competence, (Devece Carañana, Peris-Ortiz, & Rueda-Armengot, 2016), and, as information technology has evolved to be more of an engineering disciple, therefore, it was necessary to create a new program and move it to a new division to make the program independent of the BUS division to satisfy the IT needs that a new cybersecurity program needed to fill. Before the fall 2016 semester, the decision was made to create a new Computer Information Technology (CIT) department housed within the Engineering and Information Technology (E&IT) division.

There are numerous needs for a cybersecurity program, among them were: (1), no existing 2-

year cybersecurity program within commuting distance of the local metropolitan area, (2) a need for cybersecurity professionals across many industries, and (3) a local need for cybersecurity professionals as many of the college's graduates are employed within the local area. Faculty and administration considered each of the above needs before deciding to create the new cybersecurity pogram.

The local public 4-year university offers a concentration in cybersecurity that is oriented towards educating cybersecurity professionals to be employed outside the local area, thus the faculty determined that the CC would offer a program that specifically trained cybersecurity technicians needed locally. However, the CC also recognized the need to keep its graduates employable nationally, so the CIT department sought to align the new cybersecurity program with both Center of Academic Excellence in Cyber Defense (CAE-CD) guidelines (National Security Agency (NSA), 2018) and industry recognized certifications. (CompTIA, 2016)

Initially the new cybersecurity program contained business and accounting courses to meet its AACSB accreditation standards. Prior to the fall 2017 semester, the program eliminated those courses and added a natural science course to meet ATMAE accreditation standards. The core CIT department course requirements include networking, systems analysis, database concepts, Linux, and programming to support three concentrations: networking, programming, and cyber defense. New courses were added to support the cyber defense concentration including ethical hacking/penetration testing, firewalls, forensics, network security, and an introduction to information assurance. In all, 7 new courses totaling 21 units were added.

New faculty were hired to teach the additional 7 new courses. The author was among the first new hires to meet this need. The 7 new courses were each chosen to meet needs expressed by local industry. The challenge presented to the faculty was to align the courses both with industry needs and industry-recognized certifications to provide value to the students and to the local and national employers.

The rest of this paper is structured as follows: section 2 is the literature review, section 3 is the discussion, section 4 is the summary, section 5 is the conclusion with the references in section 6.

2. LITERATURE REVIEW

The Association of Computing Machinery (ACM) released the first set of curriculum guidelines for cybersecurity programs for 2-year colleges in 2020. (Tang, Tucker, Servin, Geissler, & Stange, 2020) This provided the long-awaited mapping to the CAE knowledge units (KUs) and a mapping of the competencies into the NICE framework.

What follows is a brief literature review of the various efforts to define a cybersecurity curriculum.

Many of the efforts focus on curriculum design for ABET accreditation for a 4-year degree program: (Mattord & Whitman, 2004); (Smith, Koohang, & Behling, 2010); (Cheung, Cohen, Lo, & Elias, 2011); (Conklin, Cline, & Roosa, Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors,, 2014); (Ekstrom, Lunt, Parrish, Raj, & Sobiesk, 2017); (Knapp, Maurer, & Plachkinova, 2017); (Dawson, Wang, & Williams, 2018); (de Leon, Jillepalli, House, Alves-Foss, & Sheldon, 2018); (Raj & Parrish), but few described undergraduate 2-year programs applying for ATMAE accreditation (Doggett, 2015). One early effort by (Bacon & Tikekar, 2003) attempted to create an information assurance curriculum. (McGinnis & Comstock, 2003) attempt to integrate the NICE framework into a curriculum. Another early effort by (Bogolea & Wijekumar, 2004) described an effort to form a security curriculum from various technology courses. (Dennis, El-Gayar, & Streff, 2004) describe an effort to create a curriculum based on NISTISSI-4011 standards. Both (Schweitzer, Humphries, & Baird, 2006) and (Clark & Stoker, 2018) discuss the process of achieving a CAE designation for a curriculum. (Conklin & Bishop, 2018) do a thorough job of comparing the CSEC2017 (ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8, 2017) curriculum standards with the CAE designation requirements.

Recently, (Costigan & Hennessey, 2016) released a generic reference cybersecurity curriculum for NATO. While the curriculum does focus on national security, its risk-orientation is applicable across many industries. The NATO curriculum emphasizes international cybersecurity organizations, policies, and standards, so it is oriented towards the compliance area of cybersecurity. The curriculum addresses risk management applicable to this author's proposed curriculum.

(Conklin, 2018) proposes 3 new core knowledge units (KUs) for a cybersecurity curriculum. His proposal is based on standard accreditations such as ABET and ATMAE, and on specific curriculum guidelines like CS2008 (ACM and IEEE Computer Society, 2008) and CSEC2017, and on specific industry certifications from CompTIA. He does not address specific industry certifications from organizations like $(ISC)^2$ and EC-Council, which are addressed in (Knapp, et. al., 2017). His proposal includes cybersecurity principles, fundamental concepts, and IT Systems components. The IT Systems components address areas tested by attaining industry certifications from CompTIA. The principles and fundamental concepts are addressed by tests from organizations like $(ISC)^2$.

(Furnell, S., Michael, K., Piper, F., Chris, E., Catherine, H., & Ensor, C., 2018) discuss the national cybersecurity program from the UK's National Cyber Security Centre (NCSC). Initially the program was developed from the CS2013 (ACM, 2013) and later validated by the CSEC2017 curriculum guidelines. Furnell chose to use the Institute of Information Security Professionals' (ISSP) Skills Framework (Institute of Information Security Professionals, 2010) as a starting point to develop a curriculum. This presented challenges when attempting to integrate industry input into curriculum design as the ISSP's focus is on security management and not on the technical skills in which employers need to have graduates trained. The paper does acknowledge the CSEC2017 effort, which also shapes this author's proposed curriculum.

(Harris & Patten, 2015) use learning theory from Bloom's (Bloom & Krathwohl, 1956) and Webb's (Webb, 1997) taxonomies and student learning outcomes to add topics and to create new courses in an existing ABET-accredited curriculum. The authors also provide a useful mapping of curriculum topic areas and examples of student work. This was the first paper that mapped both the curriculum topic areas and courses to learning outcomes including examples of work that students did to achieve them. I map these topic areas and examples to existing courses in section 3.

(Kim & Beuran, 2018) propose a model for educational program design methodology that incorporates many of the inputs referenced in the preceding paragraphs. Their model attempts to incorporate all stakeholders, as in the UK and NATO models, including industry, who ultimately employs the graduates of these programs. Their model also incorporates the changing nature of cybersecurity by proposing that new courses and/or existing courses be modified to accommodate emerging technologies. Finally, their model acknowledges that program development starts with a review of existing programs and pedagogical method selection.

In the discussion, this author will apply a modified Kim & Beuran model to develop a proposed cybersecurity curriculum incorporating a few more inputs.

3. DISCUSSION

The effort to change the program and the curriculum is ongoing at a community college since the fall 2016 semester. As the 2016-2017 academic year progressed, AACSB changed its accreditation requirements necessitating that more business courses be added to the new program's curriculum. Since CIT decided to remain within E&IT, the department elected to seek a new program accreditation that was more aligned with the rest of the E&IT division programs. The decision was made to seek ATMAE (ATMAE, 2019) accreditation for the new program because although many of the programs in the E&IT division were ABET-accredited (Accreditation Board for Engineering and Technology, Inc., 2019), there was no ABET accreditation available for a 2-year cybersecurity program at that time.

The program has been steadily increasing in enrollment from 20 in the Fall 2016 semester to 40 in the Fall 2019 semester. AACSB standards were replaced with ATMAE standards 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 inputs is specified in Figure 1.

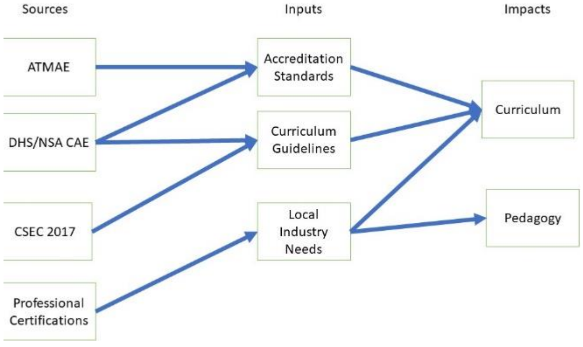

Figure 1. Program Development Inputs

New and Modified Courses

New courses need 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 adapted to meet industry needs were (1) digital forensics and (2) penetration testing and network defense. The digital forensics course was 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. A Special Topics in CIT course was added to accommodate some of the changing trends in the industry, for example, cryptocurrency and Internet of Things (IoT). The examples above illustrate that the ability for curriculum designers to be able to add new courses and modify existing courses is essential to remaining current with industry.

Course Sequencing

Course sequencing is also an issue for several reasons. Notably, the course prerequisites need to be redefined to ensure that students are at least exposed to the concepts in one course prior to applying them in subsequent courses. Another factor that needs to be overcome is the students' reluctance to retain information from one course to apply in another course. Initially, students take courses that depend on Linux knowledge before they take the Introduction to Linux course. The students are also expected to understand basic programming concepts before they take courses involving scripting, a topic covered in the Introduction to Linux course. The students' application of shared concepts is most apparent in the network security course where the students 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 network security course assumes that the students have been exposed to both software and network security issues in Computer Science 1, introduction to Networking, and Principles of Information Assurance. The examples above illustrate how to determine the course prerequisites necessary for the students to begin to master to be able to learn new material.

Course Delivery

Course delivery is also challenging as it requires the campus IT group to set up a firewalled classroom/lab environment in which the students could freely practice the techniques they learned. This setup does not provide a satisfactory solution for students unable to come to the classroom, so a cloud-based solution is under consideration until the spring break when a campus shutdown shifted the faculty's priorities. The college elected to extend the spring break for one week to allow the faculty to investigate alternatives to enable teaching online. The result was a pedagogy consisting of a combination of a flipped classroom and a tutorial-style approach. The idea is to have students come to class with their homework problems, and the instructor would be available to help the students help each other.

This author elected to move two cyber security courses: 1) network security, with 19 students, and 2) penetration testing, with 4 students, completely online. The campus IT group had not setup the firewalled classroom/lab environment, so the program used an online environment from the textbooks' publisher until the end of the spring semester. This author held synchronous video conferenced classroom lab sessions where students could connect via screen sharing to work either singly or in groups with the instructor to work on the assigned laboratory exercises. This provided a rare opportunity for the students to collaborate with the instructor's guidance that was not previously available in the conventional on-ground lecture style. Course delivery depends on subject and with the changing needs of colleges to move more online, these methods will change accordingly. The examples above suggest that helping students work through lab exercises in real-time class sessions may be beneficial.

Industry Standard Alignment

The courses are also aligned with various industry-recognized certifications so that graduating students are able to attain certifications to make them more employable by both the local industry and nationally. Every curriculum developer can benefit from being aware of both local industry needs and industry-recognized certifications when developing or revising a curriculum. Currently, faculty are aligning course material with industry-recognized certifications to make graduates more attractive to employers. Table 1 lists only the computer information technology courses and their associated industry-recognized certifications in the 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 2357	IoT Security
	CITC 2363	Internet Intranet Firewalls and eCommerce
Spring/2nd	CITC 2354	Advanced Digital Forensics
	CITC 2356	Penetration Testing and Network Defense CompTIA PenTest+
	CITC 2391	Special Topics in CIT
	CITC 2399	CIT Internship

Table 1. Proposed Program Curriculum

4. SUMMARY

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: program accreditation, workforce development, pedagogy, existing curriculum standards and CAE-CD designation need to be addressed. Although the ATMAE program 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 DHS/NSA CAE-CD KUs is also equally applicable to the ABET knowledge, skills, and abilities (KSAs) and to the recently released Cyber2yr2020 guidelines (Tang, et. al., 2020), which are, in turn, mapped to both NICE and CAE recommendations.

This case study was limited to the workforce development needs of the local industry. The local firms range from small businesses to somewhat larger employers in various industries from manufacturing to health insurance. Although there are no immediate federal government contract employers in the area, the curriculum standards used are equally applicable.

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 program 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.

The additional pedagogical challenge of having to convert conventional lab/lecture sessions to a completely online format was also met in the spring semester. The students benefited greatly from the experience per their course exit surveys including some who stated that the online exercises helped them understand the material better. This was additionally validated by their exam scores improving after the switch to the online collaborative environment, and the students' final exam scores being better than that of the previous semester's students. The courses that were modified in the spring semester will be modified again this coming spring to take advantage of the opportunities of teaching online. For the fall, one more course: Internet Intranet Firewalls and eCommerce will be modified to be taught online.

5. 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. The recent campus shutdown presented a new challenge to instructors attempting to educate students to prepare them to be cybersecurity professionals. This paper is an attempt to provide institutions of higher learning guidance on developing accredited cyber security programs and give an example of how one two-year institution is developing their program. The lessons learned here are applicable to other two-year programs and to four-year programs looking to either start or revise existing programs.

6. REFERENCES

Accreditation Board for Engineering and Technology, Inc. (2019, May 1). ABET Accredited Program Search. Retrieved from ABET:

http://main.abet.org/aps/Accreditedprogramsearch.aspx

Association for Computing Machinery, IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), "Cybersecurity Curricula 2017: Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity," ed, 2017

ACM, "Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science," ed: Association for Computing Machinery (ACM), 2013, p. 518.

ACM and IEEE Computer Society, "CS 2008: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science," ed: IEEE/ACM Joint Task Force on Computing Curricula, 2008.

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

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

Bloom, B., & Krathwohl, D. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York, NY, US: Longmans, Green.

Bogolea, B., & Wijekumar, K. (2004). Information Security Curriculum Creation: A Case Study. 1st Annual Conference on Information Security Curriculum Development (pp. 59-65). Kennesaw, GA, USA: ACM. doi:10.1145/1059524.1059537

Burning Glass Technologies. (2019). What’s Trending in Jobs and Skills. Retrieved from Burning Glass Technologies: http://www.burning-glass.com/

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elias, F. (2011). Challenge based learning in cybersecurity education. Proceedings of the 2011 International Conference on Security & Management, 1.

Clark, U., & Stoker, G. (2018). Reflections on Applying for CAE-CDE Designation. Proceedings of the EDSIG Conference. 2473, p. 3857. Norfolk, VA, USA: Information Systems & Computing Academic Professionals (ISCAP).

CompTIA, "CompTIA Security+ Certification Exam Objectives," p. 28, 2016

Conklin, W. A. (2018, March). What Constitutes Core in a Cyber Security Curriculum? Journal of The Colloquium for Information System Security Education, 5(2), 14-14.

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors, 47th Hawaii International Conference on System Sciences (pp. 2006-2014). Waikoloa, HI, USA: IEEE. doi:10.1109/HICSS.2014.254

Conklin, W., & Bishop, M. (2018). Contrasting the CSEC 2017 and the CAE Designation Requirements. 2018 51st Hawaii International Conference on System Sciences (pp. 2435-2441). Waikoloa, HI, USA: IEEE.

Costigan, S., & Hennessey, M. (2016). Cybersecurity: A Generic Reference Curriculum. NATO. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber Capability Planning and the Need for an Expanded Cybersecurity Workforce, Communications of the IIMA, 16(2). Retrieved from https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2/

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

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.

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

Devece Carañana, C., Peris-Ortiz, M., & Rueda-Armengot, C. (2016). What are the competencies in information systems required by managers? Curriculum development for management and public administration degrees. Technology Innovations and Education (2), 10. doi:10.1186/s40660-016-0016-2

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

Ekstrom, J. J., Lunt, B. M., Parrish, A., Raj, R. K., & Sobiesk, E. (2017). Information technology as a cyber science. Proceedings of the 18th Annual Conference on Information Technology Education (pp. 33-37). ACM. doi:10.1145/3125659.3125697

Furnell, S., Michael, K., Piper, F., Chris, E., Catherine, H., & Ensor, C. (2018). A national certification programme for academic degrees in cyber security. IFIP World Conference on Information Security Education (pp. 133-145). Springer Cham. doi:10.1007%2F978-3-319-99734-6_11

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), 219-235.

Institute of Information Security Professionals: IISP information security skills framework, V6.3, July 2010. Institute of Information Security Professionals (2010)

Kim, E., & Beuran, R. (2018). On designing a cybersecurity educational program for higher education. Proceedings of the 10th International Conference on Education Technology and Computers (pp. 195-200). ACM. doi:10.1145/3290511.3290524

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.

Mattord, H. J., & Whitman, M. E. (2004). Planning, building, and operating the information security and assurance laboratory. Proceedings of the 1st annual conference on Information security curriculum development (pp. 8-14). Kennesaw: Kennesaw State University.

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.

National Security Agency (NSA). (2018). National Centers of Academic Excellence (CAE) Resource Guide. National Security Agency (NSA). Retrieved from https://niccs.us-cert.gov/sites/default/files/documents/pdf/cae_program_guidance.pdf?trackDocs=cae_program_guidance.pdf

Raj, R. K., & Parrish, A. (n.d.). Toward standards in undergraduate cybersecurity education in 2018. Computer, 51(2), pp. 72-75.

Schweitzer, D., Humphries, J., & Baird, I. (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.

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

Tang, C., Tucker, C., Servin, C., Geissler, M., & Stange, M. (2020). Curricular Guidance for Associate-Degree Cybersecurity Programs. Proceedings of the 51st ACM Technical Symposium on Computer Science Education (pp. 1285-1285). ACM. Retrieved from http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf

Webb, N. (1997). Research Monograph no. 6: Criteria for Alignment of Expectations and Assessments in Mathematics and Science Education. Washington, DC, US: Council of Chief State School Officers.