Emily Vandalovsky
May 3, 2018
Spring 2018
EDTC 807
Implementation and Evacuation of Curriculum
Dr. Amerman

Project 3: Curriculum Implementation Plan

Initiative: contribute to closing a gap between supply and demand in cybersecurity workforce by developing and establishing an interdisciplinary Associate degree in Cybersecurity.

Overview and Rationale

As cyber attacks increase in frequency, complexity, and severity around the globe, the need for a highly trained cybersecurity workforce is essential. As with many other countries, cybersecurity is a national priority in the United States (The White House, 2017). According to the executive order on strengthening the cybersecurity of federal networks and critical infrastructure, signed by the President on May 11, 2017, in order to grow and sustain the level of the national cybersecurity workforce in both private and public sectors, the appropriate entities must focus on the "efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education" (The White House, 2017).

With 100,000 information security analyst positions available nationwide in 2016, the US Department of Labor projects this number to grow at the rate of 28% through 2026, resulting in a very high demand for employees (Bureau of Labor and Statistics, 2017). According to CyberSeek, there are over 19,000 cybersecurity job positions open in the metro area of NY-NJ-PA, with nearly 10,000 open positions in the state of New Jersey alone (CyberSeek, 2017). The supply/demand ratio of Cybersecurity workers NY-NJ-PA metro-area is very low at 1:3, and the national average is 1:2.6 (CyberSeek, 2017). The above-mentioned numbers illustrate the tremendous need in the educated and employable workforce in our geographic region and country-wide. Our community college is ready to join the growing army of national and international educational intuitions in delivering quality education in the field.

Prior to describing the approach to cyber education, it is necessary to clarify what is exactly included in the term "cyber" or as Cyber Education Project (CEP) defines it, "cyber sciences":

> The term "Cyber Sciences" reflects a collection of computing-based disciplines involving technology, people, and processes aligned in a way to enable "assured operations" in the presence of risks and adversaries. It involves the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The concept of "Cyber Sciences" refers to a broad collection of such programs, and disciplines under this umbrella often also include aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, many times in the context of an adversary (Cyber Education Project, 2017).

The inclusive understanding of "cyber" broadens the approach to cyber education by incorporating both technical and non-technical fields.

A number of institutions in the United States already adapted such approach and were able to implement a multi-disciplinary framework for cybersecurity education on both undergraduate and graduate levels. The Department of Computer Science at the University of Texas-Pan American reports the following about its Master's in Interdisciplinary Studies program: "taking a multidisciplinary approach to security and more particularly cyber security results in graduates who can think more openly and within alternative systems of thought. They are able to recognize and assess assumptions, implications and particular consequences" (Lawrence-Fowler, 2013).

The team of professors from The University of Central Florida (UFC) researched and evaluated the existing cybersecurity education approaches when they observed a gap in education in the human-centered area of Cybersecurity (Caulkins et al., 2016). Based on their research and recommendation, UFC implemented a graduate-level program Modeling and Simulation of Behavioral Cybersecurity Certification utilizing a holistic approach, inclusive of

technical as well as behavioral aspects of the field. The early results of such approach have been reported by the University as "overwhelmingly positive" (Caulkins et al., 2016).

Some secondary schools implement a multi-disciplinary approach towards cybersecurity education on the undergraduate level. Salve Regina University of Newport, RI, is reportedly the only Rhode Island institution to create an opportunity for all its undergraduate students to receive interdisciplinary cybersecurity education by implementing a 15-credit concentration in cyber resiliency (Salve Regina University, 2017). The concentration is completed by enrolling in 100- and 200- courses only, comparable to offerings at the community college level.

In order to close a gap between the workforce supply and demand in the cybersecurity field and related areas, it is necessary to focus on the interdisciplinary approach to cybersecurity education. A similar approach has already been successfully implemented in a number of institutions on the graduate level. However, there is still an opportunity to develop a similar approach on the associate degree level, equivalent to the first two years of undergraduate education.

Proposal for Implementation

The current paper serves as the systems-based proposal for implementation a multi-disciplinary initiative between the Department of Criminal Justice and the Department of Computer Science and Information Technology in their efforts to create an interdisciplinary associate degree program in cybersecurity. Joining forces between the two academic areas will serve several purposes, such as increasing the student applicant pool, establishing pathways for students to the respective academic areas on both ends and expanding a circle of the industry partners.

Since the field of cybersecurity encompasses multiple areas of technical and non-technical fields, incorporating two educational area of Information Technology and Criminal justice into developing a joint curriculum expands student applicant pool. Potential students, previously interested only in technical aspects (supported by Computer Science and Information Technology education) will be able to explore the criminal and the legal components of the field. Similarly, applicants interested in the criminology and forensics, will be able to gain technical skills, necessary for the field.

For the degree program to exist and be successful at the community college level, it needs to be transferable to four-year institutions. Having a pathway from a two-year school to a four-year schools helps students to meet their long-term educational goals and stay focused on their immediate objectives. Even applied degree programs, such as Associate in Applied Science, may be transferable through an establishing an articulation agreement.

Within the framework of this proposal, the partnering four-year institutions, who currently accept transfer students to the respective areas of Information Technology and Criminal Justice, will be asked to review the newly designed program and provide feedback on its transferability. Provided that the current academic partners already award transfer credit for the respective existing programs, it is hopeful that they will continue to award credit for the joint force initiative. Seeking and receiving letters of support for the newly developed program will be the end-goal result of this process.

In developing a new program at the community college it is essential to seek advice from the industry professionals and experts in the field. Consulting with both advisory boards: one the on the Criminal Justice side, and the other on the Computer Science / Information Technology side, is of tremendous importance. Local organizations, from public and private sectors, are

future hiring managers of today's students, therefore for the students to be employable, it is essential to provide them with the skillsets that the industry needs. Due to the interdisciplinary nature of this initiative and the two markets that this program is preparing for, the recommendation of the local companies play a vital role in its development.

Supporting the new curriculum development by extending the cybersecurity program to a greater audience of applicants, establishing partnerships with the educational counterparts and seeking advice form the local industry advisory boards are the essential components of the degree implementation plan.

Due to the fluency of the curriculum and in order to guarantee its sustainability of the program, the professional development opportunities will be available to the existing faculty and additional human resources qualified in the area, will be acquired. The initiative will incorporate growing support infrastructure, both hardware and software related, to provide students with hands-on learning opportunities.

Evaluation Plan

The evaluation plan of a degree program is based on the assessment criteria that the institution is using. The Associate level degree program in the State of New Jersey, has to comply with the state requirements.

The program learning outcomes (PLO) will be developed to provide program-level evaluation criteria, which will be disseminated further into particular course-level outcomes. According to Brandt and Tyler, "a learning outcome has the same essential character at all levels of planning (hence, the appropriateness of a single term, goal, to describe it) and that the level of

generality used to represent learning varies with the planning requirements at each level of school organization" (1983).

This degree program will include a general education component and the program specific coursework. The program evaluation plan will contain general education learning outcomes, including but not limited to demonstrating an ability to think critically and creatively, applying analytical reasoning to across academic disciplines, demonstrating proficiency in oral and written communication, demonstrating information literacy and technological competency, cultivating ethical values and personal leaning strategies (Bergen Community College, n.d.). The program specific requirements will include the following learning outcomes: demonstrating an understanding of data communication concepts, computer vulnerabilities, forms of cyber attacks, applying cybersecurity skills, implementing policies and protocols to comply with legal and regulatory requirements.

At various levels, the success of the program implementation can be measured differently. At the institutional level, the success of the program can be measure in the number of graduates and transfer students, but for the new program this measure is not immediately attainable.

The more rapid measure of the successful execution for the newly developed program is in its enrollment numbers. Students may feel hesitant enrolling in the recently designed program due to the lack of the proven record. Establishing working relationships with academic and business partners can assist with promoting the program and reassuring its value.

Once the program is fully developed, the evaluation plan will include ongoing assessment of general education and program specific outcomes in accordance with the college's program assessment plan. On the level of the individual course offerings, the evaluation will take place

as part of the program review process and according to the college's posted schedule. Members of the Advisory Boards will be invited to provide their feedback on applicability and validity of the program on a regular basis.

Reflection

Since this degree program is mostly driven by the industry demands and shortage of employable population, its main goal is not only to provide general education but also to focus on the specific and applicable skillsets. As stated by Brandt and Tyler, "[t]he test of whether a goal is stated at the appropriate degree of generality-specificity is its clarity and helpfulness in guiding the educational activities necessary at that level of responsibility" (1983).

Creating new curriculum is dealing with multiple levels of goal setting with their corresponding levels of evaluations. The article of *goals and objectives* by Ronald Brandt and Ralph Tyler was particularly useful for writing this paper and establishing criteria for the designing learning objectives.

On a greater level, modern curriculum is constructed from two large components: a general education and a technical education. From the historical perspective, it has inherited from almost all major movements of the American educational system of the 19th century. The degree is based on the industry demands and technology driven model, whose prototype was established by the social efficiency educators and Jospesh Mayer Rice (Kliebard, 2004).

Overall, creating a new curriculum plan is a multifaceted initiate that spans overtime and needs attention before, during and after the process. With the systematic approach and attention to evaluative strategies, it is a complex but attainable process, which benefit the students and other related constituencies in a given institution.

References:

Bergen Community College. (n.d.). *Professional Studies AS – General Curriculum Degree*. Retrieved from http://bergen.smartcatalogiq.com/en/2017-2018/Catalog/Academic-Programs/AS-Degree-Programs-in-Professional-Studies/Professional-Studies-AS-General-Curriculum-Degree

Brandt, R. S., & Tyler, R. W. (1983). Goals and objectives. *Fundamental curriculum decisions*, 40-52.

Bureau of Labor and Statistics, U.S. Department of Labor. (2017, October 24). *Occupational Outlook Handbook*, Information security analysts. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016, October). Cyber workforce development using a behavioral cybersecurity paradigm. In *Cyber Conflict (CyCon US), International Conference on* (pp. 1-6). IEEE.

CyberSeek. (n.d.). *Cybersecurity supply/demand heat map.* Retrieved from http://cyberseek.org/heatmap.html

Cyber Education Project. (2017). *About Us*. Retrieved from https://cybereducationproject.org/about

Kliebard, H. (2004). *The struggle for the American curriculum, 1893-1958*. New York, NY: Routledge.

Lawrence-Fowler, W. A. (2013, January). Multi-disciplinary Approach to Cyber Security Education. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). Retrieved from http://weblidi.info.unlp.edu.ar/WorldComp2013-Mirror/p2013/SAM9783.pdf

Salve Regina University. (2017, October 25). *Interdisciplinary concentration in cyber resiliency designed for students in all majors*. Retrieved from http://www.salve.edu/news/interdisciplinary-concentration-cyber-resiliency-designed-students-all-majors

The White House. (2017, May 11). *Presidential executive order on strengthening the cybersecurity of Federal networks and critical infrastructure.* Retrieved from Office of the Press Secretary https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal