Emily Vandalovsky November 19, 2017
EDTC 805 Cross-Discipline Studies
DYI my PDP White Paper

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

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 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).

As the team of professors from The University of Central Florida (UFC) researched and evaluated the existing cybersecurity education approaches, 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 could be completed by enrolling in 100- and 200- courses only.

In order to close a gap between the workforce supply and demand in the cybersecurity field and its 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 room for improvement for developing a similar approach on the associate degree level, which oftentimes completes the first two years of the undergraduate education.

The current paper serves as the beginning of the grant proposal, mostly its rationale part, for supporting a multi-disciplinary initiative between the Department of Criminal Justice and the Department of Computer Science and Information Technology in their efforts to implement an inter-disciplinary associate degree program in cybersecurity.

The new curriculum development initiative will be supported by establishing partnerships with the local industry for outreach opportunities and advisory boards. It will provide necessary professional development for the existing faculty and seek additional human resources experienced in the area. It will incorporate growing support infrastructure, both hardware and software related, which will provide students with hands-on learning opportunities.

In addition to exploring a multidisciplinary approach to establishing an Associate degree in cybersecurity through collaboration with my colleagues from other disciplines and departments, I will expand my PDP goals further by completing the following tasks:

- Research what kind of similar programs are already in place in sister community colleges in this region and collaborate on best practices and idea;
- Research what kind of Bachelor degree programs are already in place in our 4-year educational partners, so that we can develop articulation agreements with those schools and create 2+2 cybersecurity pathways for students;
- Reach out to the Advisory Board to participate in the discussion on the current field demands;
- Research specific grant opportunities available to support curriculum development, professional development and computer lab infrastructure to support cybersecurity education in my school;
- Attend professional local and regional conferences on broadening participating in cyber education.

References:

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

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