1897 BAY PATH UNIVERSITY

Are you involved in cybersecurity workforce education or training (*e.g.,* curriculum-based programs)? If so, in what capacity ?

Yes, I am an Associate Professor of CyberSecurity Management at Bay Path University, and also serve as the Director of the MS in CyberSecurity Management program, and Chair of the BS in Cybersecurity. Bay Path University serves women exclusively at the undergraduate level. In my role, I oversee the development and delivery of undergraduate and graduate degree programs (on-ground and online) in cybersecurity and computer science, with input from a CyberSecurity Education Advisory Council comprised of cybersecurity leaders and professionals from national and local companies who provide guidance and expertise. As a women's university serving a diverse student population, we are well aware of the career opportunities that abound in this field for women, and we are keenly focused on delivering academic programs and experiential learning opportunities in cybersecurity that directly address the nation's need for a diverse and well-trained cybersecurity workforce. Bay Path University's President, Dr. Carol A. Leary, was invited to join the Department of Homeland Security Academic Advisory Council in 2016, serving in this role as an influential champion on a national scale for women in cybersecurity.

We offer undergraduate and graduate coursework in a variety of formats. Our online accelerated baccalaureate degree programs in cybersecurity, where we have seen particular growth in enrollment among adult women, are offered through The American Women's College at Bay Path University. Launched in 2013, The American Women's College is the focus of a recent award from the Online Learning Consortium, funded by a grant from The Bill & Melinda Gates Foundation Postsecondary Success Program, and the Lumina Foundation 2017 LIFTed Prize, each in recognition of our innovative use of adaptive learning technology in delivering online accelerated baccalaureate degree programs solely for adult women. We are currently funded by a $3.5 million "First in the World" grant from the U.S. Department of Education, Fund for the Improvement of Postsecondary Education (FIPSE), to assess the efficacy of this online model, which we call "Social Online Universal Learning" or SOUL, to improve baccalaureate degree completion among adult women in programs such as cybersecurity, in less time and more affordably, and to take the model to scale nationally.

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Currently there are no standard metrics or data for cybersecurity education, training, and workforce development programs. There are several organizations, including NICE, Burning Glass, and CompTIA, who regularly conduct surveys of workforce developments like job demand, and the skill sets employers indicate they are seeking in future employees. Unfortunately, due to the vast differences among industry standards and organizational structure it is difficult to project their findings onto a more general population. This lack of data can lead to disconnect between employers and those individuals in the education, training, and workforce development industries.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

The most promising analysis of workforce categories, specialty areas, work roles, and knowledge/skill/abilities is the NICE Cybersecurity Workforce Framework (NCWF). NCWF conducted a thorough analysis of cybersecurity positions, by identifying and describing key specialty areas and the associated skills needed to work in that space. From an academic perspective, the work role descriptions are easily translatable to student learning outcomes.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Yes, Bay Path University has developed and published extensive cybersecurity policies and procedures for all of the communities of interest (faculty, staff, and students).

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors)?

There are several primary skills individuals need to be successful in the field of cybersecurity. First they need to have strong analytical skills. Cybersecurity is about solving problems through innovative thinking. The ability to "think outside the box" is essential for success in an environment that is constantly shifting.

Cybersecurity professionals must have people skills, in that they must to have the ability to explain complex issues to a variety of different people within an organization. The days of using fear of loss or fear of being out of compliance with a regulation is long past for the cybersecurity field. Cyber professionals have to be able to position the cybersecurity function within an organization as a business partner through collaboration and cooperation.

Data analytics is a critical skill set for cyber professionals. As organizations begin to understand the volume and types of data they create through the use of their networks, cybersecurity professionals must be able to capture, manipulate, analyze, and utilize organizational data to proactively address security concerns.

Cybersecurity professionals must have an understanding of the business environment in which they function. There is no one size fits all in cybersecurity; even the most well established "best practices" will not address every organization's needs. Cybersecurity professionals have to be able to adapt both to changing needs of the businesses in which they dwell, but also be responsive to every changing threatscape they operate by taking a risk based approach to identify vulnerabilities within their organization and addressing issues proactively.

Finally, cybersecurity professionals have to think more like a "hacker" and less like a security professional. Looking at systems, controls, policies, and procedures to identify vulnerabilities is critical. Testing the veracity of polices and procedure, the effectiveness controls, and the completeness of response plans are an essential skill set for cybersecurity professionals.

Unfortunately, given the environment of compliance and regulations, organizations do not have realistic expectations and are not in line with the knowledge and skills of the existing workforce or student pipeline. The majority of organizations seem to be more interested in two attributes: hiring cybersecurity professionals to administer technology, and hiring cybersecurity professionals with years of experience. There are two things we know for certain in this industry: first, an individual's value is not determined by the number of years they have worked, but by the breadth and depth of knowledge they bring to an organization; and second, the rate of change in information tools and technology is so rapid that skill sets associated with specific tools will be irrelevant within a few years of hiring an individual.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

The most effective cybersecurity education programs are those that are a combination of:

- A strong liberal arts education, particularly focusing on communication skills;
- A robust foundational knowledge of cybersecurity skills based on a risk based approach to cybersecurity. They offer students a significant amount of hands-on experience through the implementation of project based learning that requires students to solve real-world cybersecurity issues; and
- A balanced approach to mathematical requirements.

This type of program is most likely found in small liberal arts or comprehensive colleges and universities, like Bay Path University, that do not have their roots in computer science and technology. They will offer curricula that results in a more rounded cybersecurity professional who understands the threats and concerns of the cybersecurity issues, possesses strong analytical skills, and has a robust understanding of the future of technology in general and of cybersecurity specifically. These types of programs are often more agile, are able to respond to industry trends, thus ensuring graduating students have the best skill sets when entering the workforce.

Developing diversity in the cybersecurity workforce will be critical. One strategy to consider is the development of a coordinated approach to cybersecurity education through partnerships among women's colleges and universities that includes paid internship opportunities with corporate and federal employers. Research conducted by Linda J. Sax, Ph.D. and colleagues indicates that women's colleges serve a student population that is more racially and ethnically diverse than comparison coeducational institutions, while attracting students with strong intellectual orientations who have high expectations for engagement with faculty and care deeply about the world around them.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The greatest challenge in terms of cybersecurity education, training, and workforce development we face as a nation is the lack of a K-20 pipeline. There are many colleges and universities offering degrees in cybersecurity in the United States, but as we know there is a shortage of individuals interested in this field. The missing component is the K-12 portion of the pipeline. Public schools generally do not include any computer science or cybersecurity course offerings to students. Even with the raised awareness of the importance of STEM, technology education in K-12 is basically non-existent. This means that when a student enters a cybersecurity program at a college, they must spend their first year learning fundamental computer science content before they are able to understand the more complex issues relating to cybersecurity. Imagine if the same were true in other STEM areas, for instance the first time a student took a science class was in their freshman year at college. The effect on the scientific world would be catastrophic. There is no way, as a nation, we will be able to address the shortage of cybersecurity professionals without the implementation of computer science and/or cybersecurity course requirements throughout the K-12 pipeline.

In the meantime, it will be critical to make increased federal grant funds available to colleges and universities and other organizations to strengthen their cyber education, training and workforce development programs, including support for paid internships, for institutions and organizations focused on improving the diversity of the cyber workforce. For example, Bay Path University is partnering with a non-profit organization, TechFoundry, to increase the number of low-income women, with or without a college degree, who are prepared with the precise information technology skills that local employers need in entry-level job candidates. The 14-week training program includes an internship with local employers, typically unpaid. Bay Path is working with TechFoundry to adapt the curriculum for online delivery, making it easier for low-income working women to participate, and expand the curriculum to include cybersecurity. Federal funding to support paid internships would be a game-changer.

7. How will advances in technology (*e.g.,* artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

Clearly, as technology changes, the cybersecurity workforce will need to adapt to those changes. Educational programs, particularly those focused on a breadth and depth of knowledge only obtainable thorough practices like project based learning will be well positioned to react to changes within the industry. If they are rooted in a theory to practice methodology, the challenges of changes in technology will be minimal.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

ii. At the state or local level, including school systems?

iii. By the private sector, including employers?

iv. By education and training providers?

v. By technology providers?

The following steps are suggested to grow the Nation's cybersecurity workforce:

1. States must introduce computer science and cybersecurity curriculums, other than robotics and certain AP courses, which are found in many schools, at the K-12. Computer science and cybersecurity education at the K-12 level is an essential element, not only in developing future professions, but is critical in the development of solid global community members.
2. States and Federal governments should provide funding for organizations to partner with colleges and universities to establish long term internships and work study programs. This would address the issue of the lack of experience new graduates face when trying to enter the workforce as well as addressing the perceived shortage of qualified cyber professionals.
3. Employers should be encouraged and/or incentivized to provide paid student internships in cybersecurity that could be supported by Federal funding. One example to look at is the Massachusetts Life Science Center through which state funds are made available to employers that provide paid internships in the life sciences industry in Massachusetts.
4. Educational institutions must integrate cybersecurity courses across all curriculum offerings. This will serve to improve the overall cybersecurity awareness of students and future professionals regardless of their career choice. They should also consider integrating industry certifications into their curriculum, such as Security+.
5. Technology providers must work with colleges, universities, and training providers to provide cutting edge tools and technologies in the classrooms and labs. Providing these tools at low or no cost will allow education institutions to offer the best learning environment possible.

Dr. Lawrence Snyder
Director Cybersecurity Management and Computer Science
Assistant Professor
Bay Path Univeristy