A new approach for Bachelor degree in Cybersecurity

Agnes Chan
Northeastern University

Introduction.

With the rise in demand for cybersecurity professionals, comes along a proliferation of training programs. These programs range from online training to traditional degrees, from certification to master degrees, all with the goal of producing qualified cybersecurity workforce within a short period. Unfortunately, with all the programs available to students, the gap between supply and demand in cybersecurity workers remains large. More troublesome is the feedback from potential information technology (IT) employers stating that the product of these programs is underqualified. In the 2015 survey report on Cybersecurity Job Market[1], published by Burning Glass Technology, a workforce study company in Cambridge, it was found that 37% of IT employers indicated that fewer than 25% of the graduates are qualified. This leads us to ask questions such as "What is missing in these programs?", "Are we providing the correct training at the right level?", or is it that in our haste of mass producing cybersecurity workers, we are skimming over the fundamental knowledge of the field? This white paper will discuss the weakness of current practices, and propose a new direction in training cybersecurity professionals.

Cybersecurity and Healthcare Professions.

Cybersecurity concerns the protection of computer systems and networks. It builds on the fundamental knowledge of computer science, such as coding, operating system and network. These topics should be taught with similar depth as expected in computer science. However, it differs from computer science in that it concerns the proper functioning of its protected entities, even when they are under attack, whereas computer science concerns the use of computers to achieve efficient computation and engineering designs. The concerns of the two professions are different, the goals and approaches of the programs should be different. Currently, most of the cybersecurity programs follow the methodologies of IT or computer science education, with modification in requirements by adding essential, non-technical knowledge such as cyber law

[1] ISACA State of Cybersecurity 2017: Current Trends in Workforce Development

and human interaction. One other significant modification is the requirement of laboratory exercises. While laboratory exercise in a course provides hands-on experience in learning a focused cybersecurity concept, it does not provide graduates with a holistic view of the problem or vulnerability itself.

On the other hand, while the technical training expected in cybersecurity and healthcare are vastly different, the objective of being able to detect and protect their clients are similar in both disciplines. Both disciplines require fundamental concepts, upon which their disciplines are built. Nurses require basic understanding of biology and chemistry, while cybersecurity workers require fundamental comprehension of coding, systems and networks. Nurses need to know how to communicate with patients, how to look out for suspicious decease, how to provide simple treatment plans, and know when to notify doctors. These skills are taught in courses such as nursing practices and, nursing care for children or adult patients. A cybersecurity professional may not need to communicate with users often, but he needs to be able to detect possible vulnerabilities, to discuss his findings clearly and succinctly with his cybersecurity teammates, and to explore a possible solution to mitigate losses. Current programs do not provide courses within the curriculum to teach cybersecurity students this needed skill, it is left to the students to pick up the skill set through post graduate work experience or other venues. To remedy this shortcoming of the curriculum, we propose the introduction of practicum courses in the last 2 years of their study. These practicum courses allow students to observe and to learn how professionals work as a team to solve problems; they may even learn to participate in decision making through professional mentorship.

Collaboration: Government, Industry and Academia.

Similar to Nursing programs, cybersecurity programs will not succeed without the collaboration from government and industry. In general, academia lacks the opportunity and facility to provide on field training to cybersecurity students. Government and industry are asked to take students on site, mentor them, show them how decisions are made and how one person's behavior affects the entire system. Opportunities for students to observe and to learn are crucial for the success in the education of a cybersecurity professional. In addition, these practicum courses can serve as work experience required by IT managers.

Cybersecurity is also getting more challenging every day, especially with the introduction of new technology and its ensuing applications. One such example is the Internet of Things (IoT). The communication complexity, together with the intricacies of the technology and network infrastructure, have posted new security and reliability challenges to cybersecurity professionals. As new technologies are introduced, the attack surface grows, so does the variation of attacks. It is difficult for a cybersecurity professional to familiarize himself with all the new technologies. These technologies have to be taught and transferred from government and industry experts to security professionals. In addition, with current shortage of qualified cybersecurity educators, government and industry can help narrowing the gap by allowing their employees to teach part-time in academia.

In short, government needs to create programs that fund industry/government professionals to partake in the teaching of cybersecurity. Industry needs to provide expertise and mentorship in training students. It is only through these collaborations that cybersecurity professionals can be well prepared to face the challenges, now and in the future.

Other Mechanisms to Strengthen Cybersecurity Education.

Other strategies that can strengthen the training of cybersecurity professionals include

- *Textbooks*. Textbooks provide a venue to define cyber security taxonomy uniformly. Furthermore, textbooks provide a certain standard of depth in each topic area.
- *Conferences*. Papers accepted or presented by security conferences should include tutorial on new industry technology and the security issues anticipated. Small group discussions on cybersecurity experiences, such as "A problem I encountered and how I handled it", should be encouraged and arranged in conference meetings. Students, especially the MS students, often attribute their learning from peers. The small group discussion is to facilitate peer learning experience.

The cybersecurity community has been debating for the last decade on what knowledge units are needed to be included in the education program. This debate needs to continue to ensure that cybersecurity professionals possess the needed knowledge. But transfer of knowledge is a relatively easy problem to solve. The teaching of professional behavior and experiences require more thought. We are proposing a new paradigm in educating cybersecurity professionals based on how they are expected to perform as a professional upon graduation.

Biography.

Professor Chan received her PhD in mathematics and joined the Northeastern University faculty in 1977. She is currently the Executive Director of Information Assurance and Cybersecurity. Her research focuses on cryptography and communication security. She works on fast, efficient mutual authentication algorithms for small mobile devices. More recently, she focuses on cybersecurity workforce. Professor Chan holds two patents on stream ciphers. She has published widely in IEEE conferences and journals, as well as in Crypto and Eurocrypt. Her research has been funded by NSA, NSF, DARPA and telecommunication industries. She was awarded the Distinguished Educator Award presented at CISSE in 2016.

Professor Chan led the effort in establishing an interdisciplinary research Institute of Information Assurance at Northeastern University. She is the PI for Center of Academic Excellence in Cyber Defense, Research and Cyber Operations. She designed and launched the interdisciplinary programs in cybersecurityat at Northeastern University: MS in 2005, PhD in 2010 and BS in Cyber Security in 2017. Professor Chan has been active in promoting women in sciences, in particular, she has participated as an invited speaker at NSA's "Women in Mathematics" and "Alumni Mathematicians" at Smith College.