Growing and Sustaining the Nation's Cybersecurity Workforce

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?

   We are limited to internal enrollment and graduation data relative to credit and non-credit (workforce) statistics. External sources such as EMSI and BLS.

   The improvements we need are to find out industry credentials "downstream" from when a student completes their education/training with us. Often times the students need additional exam prep time following their course completion with us and this time gap contributes to our inability to find out certification outcomes.

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

   Probably not and perhaps won't be any time soon. The areas are so broad, and at the same time becoming so specialized, that definitions will always lag behind.

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 – assuming we understand what you are referring to about policies.

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 two extremes developing in this regard. We have employers who are requesting an emphasis on "soft skills" over technical skills, which is creating some unreal expectations about what a community college should be providing. It also becomes a moving target between employers about what each one deems as appropriate soft skills and the balance with how much technical is needed too. There is no middle area after this. The opposite end of the employer spectrum is that they want exceedingly talented people, but these are very difficult to develop given the security clearance requirements needed in order to get that level of experience and

expertise to qualify as a high-end cyber professional. It is becoming obvious that registered apprenticeship programs are the answer to bringing order out of chaos.

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?

   I don't have a definitive example I can cite in this area. We contend that development of several registered apprenticeship types and levels will be needed to get us and our students where they need to go.

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

   The potential population of students/workers for cybersecurity have a very myopic vision of what cybersecurity is about. Primarily this vision focuses on blinking computer lights and networks. They do not envision the vast majority of cybersecurity areas that do not involve networking skills.

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)?

   See the brief answer to #2 above. I believe the critical concepts of cybersecurity need to be embedded within the curricula of other programs relying upon data. This is to say, virtually all programs.

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?

Charles B. Swaim

Dean – Business, Public Services, Information Systems and Mathematics

Thomas Nelson Community College

99 Thomas Nelson Drive

Hampton, VA 23666

(757) 825-2900

SwaimC@TNCC.edu