Request for Information – submit date 8/2/2017

Tamarind Tech, LLC

Responses in blue

General Information

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

We are cyber security educators and curriculum developers working on evaluating and determining how we can participate in bridging the skills gap.

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?

There are numerous reports and metrics about the skills gap, but not much about the education, training and workforce development needed to bridge the gap. What we need is a portal or hub through which employers can "request assistance" to fill the gaps. A central repository owned by the federal government would support metrics collection and provide a futuristic view of the needs for workforce development.

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

There is some limited movement towards standard language among cyber security education and certification practitioners in the NICE subgroup but not within the general cyber security population.

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

The organizations I work with have some policies in place but there is very little enforcement. Some organizations have a structure in place to educate new employees, but not existing cyber professionals. The demands for a cyber security professional (eg. analyst's) time outweighs heavily the need to further develop their skills.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce?

Employer needs vary but the common theme include individuals with the following skills:

Identity and Access Control | Pen Testing | Vulnerability Management | Risk Assessment | Policy Compliance | Forensic Analysis | Business Continuity | Security Intelligence | Knowledge of and experience in a Security Operations Center | Soft skills including Decision-making and Communication skills

- Are employer expectations realistic? Why or why not?
  To a certain extent they are. Companies that are successful in avoiding or reducing breaches are diligent about filling all the roles needed to ensure a complete and comprehensive Security Program. The challenge they have in meeting these expectations has more to do with retaining top talent or acquiring talent with the requisite experience.
- Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline?
  They are not even close. The existing workforce consists of two groups: (i) individuals with the knowledge but limited experience in the niche areas that companies need and (ii) a limited number of individuals with the experience
- How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors)?
  The difference per sector is usually determined by the devices that need to be secured. In the case of energy, healthcare, automotive/transportation, there are devices that are not traditional IT devices. These include industrial control systems, medical devices, connected car components etc. These type of Operational Technology (OT) skills are very difficult to find.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today?

Two programs that are sponsored by corporations and managed by non-profit organizations are successful in training and placing cyber security professionals. They are:

1. YearUP - based in 16 states in the US, over 16,000 students served, 3000+ in 2016 (90% placement rate)

2. NPower – 6 states in the US.

- What makes those programs effective?
  The collaboration between corporations, the federal government and non-profit schools
- What are the goals for these programs and how are they successful in reaching their goals?
  The mission is to utilize the unemployed or underemployed to fill the gaps
- Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?
  YearUp (see above) is an example.

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

One challenge is to embrace the need for automation and to do it quickly. While we address that challenge we must be willing to embrace diverse and underrepresented employees as a “market” for employees. By focusing on individuals who are keen to learn and do their part in securing the nation’s and our companies’ valuable data as opposed to the possession of a four-year college degree will allow the paradigm shift of value-based education to take place.

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?

AI systems can both protect infrastructure and become the target of attacks. Not enough is known about these systems to determine if we have sufficient AI security experts to prevent breaches. A timely article discussing this issue can be found in the Harvard Business Review.

The Internet of Things is already facing unique breaches targeted at non-IT devices. Again, the specialized skills needed to secure a medical device or a SCADA system are very hard to come by. The solution would be for a consortium in each industry/sector to create internship programs that provide the hands-on training and experience needed to address these needs. These organizations also need to bridge the gap between “IT Security” and “OT management”.

- How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?
  No response as we are still evaluating this.

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? Provide grants for small businesses focused on cyber security education

ii. At the state or local level, including school systems? Provide incentives for community colleges to build dynamic and fluid infrastructures partnered with private sector to inform students as the threat landscape changes.

iii. By the private sector, including employers? Work with community colleges and private cyber security educators to extend apprenticeship programs and be willing to hire below the 4-yr degree.

iv. By education and training providers? Partner with private sector as above

v. By technology providers? Be willing to support/fund initiatives to build eSOC environments to provide more hands-on training and real-world experience for students.