Growing and Sustaining the Nation's Cybersecurity Workforce

Are you involved in cybersecurity workforce education or training (*e.g.,* curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? *Note:* Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

I am involved in cybersecurity workforce education at a public two-year college and private four year college. I am also a CyberPatriot mentor. I develop cybersecurity curriculum for college and high school students.

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?**

   The NICE Cybersecurity Workforce Framework (NIST) is available. However, I don't believe many faculty in computer science (who aren't involved with cybersecurity) have even heard of it. CAE has knowledge units that provide a framework. However, there are many other independent organizations who have made their own.

   Some of the metrics have information that is duplicated. It's hard to find the information, because there doesn't seem to be one definitive best source and new sources seem to appear frequently. We need a turnkey national training program that would provide labs to colleges, high schools or workforce programs.

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

   It's hard to agree on categories or specialty areas because they are changing all the time. Also, not all the categories and specialty areas are available for employment in every location across the country, so everyone may not be as familiar with all of them. In addition, many of the specialty areas are very similar to each other.

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

We do have workforce education programs and policies. However, it's hard for the small number of cybersecurity faculty to find time to educate high school students, two and four year college students and to add workforce training to such a big workload. If we had a greater number of cybersecurity educators available then more opportunities would be available to train everyone.

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)?**

   They are telling us they value communication, problem solving, adaptability and flexibility the most. Apparently, many of their new employees are lacking these skills. They feel like they can teach them the technical skills that they need, but they aren't getting people who are willing to change at a fast pace.

   Their expectations are realistic, but most of the training programs are not teaching the skills they are looking for. Students are not challenged and tested in stressful situations to fix problems. Many students are expecting the instructors to fix all their problems. Rather than do a Google search for an answer, they just email or ask the instructor. Students need to learn to be self-sufficient, but work well as a team member and to try to solve their own problems – before they look for help.

   Schools also don't have enough resources for in depth knowledge of business sectors. For example, each industry has different assets to protect. It would be helpful if students knew which assets were most important to protect before they were already employed in cybersecurity.

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?**

   There are a lot of effective programs, but those programs are heavily based on hands-on learning and apprenticeship/internship opportunities. The goals for the programs are to produce employees who have the skills they need to be successful in their new workplace. Those skills need to include more than just cybersecurity skills. Effective communication, teamwork and problem solving are equally important in producing workers that are prepared to succeed. They also need to take classes with content that will actually be used in the workplace. They need to learn in a multidimensional environment that includes not just fragmented skills or knowledge, but be able to use all their skills in an environment that simulates the workplace. The NICE Challenge Project is a good type of training for students who already have reached an intermediate skill level, but it doesn't allow for physical challenges.

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

   One of the biggest challenges for the government is that they almost always require a Bachelor's degree, when many students with an Associate's degree would be completely capable of being successful at the job. As much as they say they are trying to be more friendly to two year graduates, they aren't. There is a huge shortage in cybersecurity which could be partially filled by two year graduates. Cybersecurity is at a state when the government just can't afford to be that picky. Also, employers keep asking for the wrong type of degrees. They think if they hire someone with a computer science degree, they should be able to handle any type of computer work. In reality, most of the computer science four year degrees in our area are heavily based in programming and business systems/analysis. They expect these students to design a network, when many of them either have not even had a network class or only one class worth only a few credits. They are not prepared to troubleshoot big networks, because they don't have any experience in that. Employers need to take a good hard look at the coursework that is included in the type of degree that is on their job descriptions.

   We have a huge pool of talent in our high school students. They grew up with computers and are digitally connected in more ways than we can count. They have more time on their hands than students who have graduated from high school and have a job and significant other. High school students have little to no actual knowledge of the opportunities in cybersecurity careers. If they have heard about them at all, they don't know what would be involved in the daily work or how big the salary would be. In fact, high school students aren't as concerned with high salaries as traditional college students – probably because they haven't been paying the bills yet. These students are just looking to find a passion and goal in their life. They have so much energy and passion, they should be involved in helping the cybersecurity community on projects – at least for research. That would spark their interest and help the cybersecurity community.

   If the US would make some type of cybersecurity education mandatory, it would help everyone. Those students would learn to avoid phishing attacks before they even get into the workplace. High schools in our area need to trim their budgets and are cutting most of the electives, leaving just math, science, English and social studies. Many states have state tests that need to be passed, so they focus on what will help them pass the tests. If cybersecurity was on their state tests, they would make sure they taught it.

   Another challenge is for educators to keep up on the latest cybersecurity technologies. Even though colleges can hire adjuncts who are currently in the cybersecurity field, sometimes their lack of organization and teaching skills overcomes whatever benefit students could get from them having more current technological knowledge.

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)?**

   Internet of Things is one of the greatest dangers to the cybersecurity welfare of the country, because people see these devices as safe. They are like wolves in sheep's clothing. Many are produced with little to no security. There aren't any laws that require minimum security for any products of this type, so without laws they will continue to produce them as cheaply as possible – which is without any security. People have no realization of how much information is collected about them from all these devices or who companies are sharing it with. There are no laws that protect peoples personal information either when it pertains to the steps they walked, what they ordered, etc. Perhaps in the future, someone could use this type of information to blackmail someone. Where are the companies keeping all this information? Likely not in a secure place.

   Working in Computer Information Systems we expect to always be changing our curriculum. However, it is hard to find information when many times textbooks are not available for new technologies and faculty have little training in it. I think most programs are ready to adapt, they just need a reliable constant source of information so that they can be trained and provide the appropriate resources to students.

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?** It seems like the Federal government has many agencies that do very similar work. They do seem to be working towards sharing much more than in the past, but I think that communication could be improved. Part of the problem is all the layers of "classified" material, layers that cause things like public phonebooks to be classified. The government is making partnerships with industries, but that partnership could be strengthened and enhanced. Much government time is wasted by people flying from place to place, when they could increase meetings via secure online communications. When it comes to most cybersecurity education communication, it doesn't need to be kept secret. More stakeholders could be involved in decisions if they didn't have to lose days of work to travel to remote locations to discuss information with the government. We could all get a lot more work done if a secure web sharing platform was developed that would make it easier for us to work together without using an airplane.

ii. **At the state or local level, including school systems?** All state, local and school systems should have cybersecurity education. Real cybersecurity education, not just a quiz that asks if it's safe to give your bank account numbers to your long lost cousin who wants to send you a few million dollars. Social engineering is a huge problem and everyone needs to be aware of the possibilities involved. Everyone needs to know a lot more about iOT, because so many people have houses filled with wolves in sheep's clothing. They don't see these devices as any type of danger, but not seeing the danger makes may make them the most dangerous of all.

Computer classes in general are being cut out of the school systems to save money. Many states are concerned with just teaching what is needed to pass state mandated tests. Cybersecurity should be on the state mandated test and every school should be required to provide some type of cybersecurity education. Many of the high school teachers say they don't have anyone qualified to teach a cybersecurity class in high school. For that reason, the government should provide an online cybersecurity class that teachers could use.

iii. **By the private sector, including employers?** The private sector should require employees to spend more time on cybersecurity training and have regular pentesting to find vulnerabilities.

iv. **By education and training providers?** Education and training providers need more easily available and current training. It would really help if the training was free and they didn't have to travel that far, because some college employees have a lot of paperwork to fill out. For example, at our school the president, vice president and Dean need to sign before I can leave the state and they aren't always around. I also need to fill out a professional development request form and tie whatever I do to the schools mission and goals. Then I have to save all original receipts and when I sometimes can't get one I need to go find a notary to sign before I can get reimbursed. So, it can be very time consuming for people to travel, in more ways than one. I think the paperwork involved with traveling, prevents many employees from traveling at all.

v. **v. By technology providers?** Technology providers should take security a lot more seriously, even if it costs them a little more money and takes them a lot more time. Perhaps they government could give them some type of benefit if they reached a certain level of security in their organization. Every secure step from point A to point Z will help everyone. If the providers can block more malicious traffic, it would reduce the load on local firewalls and the chance that some user would inadvertently follow a damaging link.