Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce

Development – Request for Information Response

Wm. Arthur Conklin, PhD
CISSP, GICSP, GRID, GCFA, CSSLP, CSDP, CRISC, Security+, CASP
Associate Professor, Department of Information & Logistics Technology
Director, Center for Information Security Research and Education
University of Houston, College of Technology
College of Technology Building
4730 Calhoun Road #312
Houston, TX 77204-4023
Waconklin at uh dot edu

General Information

1. 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.

1. Yes. I am an associate professor at a 4 year tier 1 research state university. We are a NSA/DHS Center of Academic Excellence in CyberDefense Education (CAE CDE) and Research (CAE-R).

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 collect the following data and use it in NSA/DHS Center of Academic Excellence in CyberDefense Education reports on an annual basis: # students enrolled in the program, the graduation rate, the number of qualified faculty. There has been talk concerning the collection of additional elements of data to examine things like job placement rates, etc. I feel that we should be very careful in expanding data mandates. Collecting data takes money, time and effort, the latter two which are always in short supply. Data on students after graduation such as employment data is difficult to mandate that students provide it, and collection is difficult to automate. Anecdotal stories, our current source, results in incomplete information and can lead to suboptimal deployment of limited resources.

Before new metrics are introduced in the name of program improvement, determine who has the data, how hard is it to get, and what will it cost. Don't assume schools have the data or the answers, they typically are clueless. Frequently these data requests end up on the desk (or email inbox) of the professor leading the program. This becomes an "additional duty" that can tax an already over-taxed professor.

Meaningful data and metric would assist the program in the delivery of content, production of graduates, something directly related to improving the programs. Rather than count what we have (# students, # instructors), how can we count what we need, the gap, between what we are producing and what is needed. I know there are challenges associated with determining where we are with respect to meeting demand in this changing environment, but putting the data collection onus upon the already overworked, will only slow delivery of the product, both metrics and workforce. We need to find ways to do this without impacting the supply chain itself.

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

As an educator, I say yes. The latest CSWF (800-181) is comprehensive. But from a practical experience model I would say the answer is no. Many companies still bring unrealistic job descriptions and expectations to the marketplace. I see companies wanting CISSP for an introductory job, while the certification calls for years of experience. This disconnect is cross cutting of all firms, all jobs, with the exception of a few tech based companies. A concerted effort has been made to get with Cybersecurity professionals to ensure the information in the workforce categories, specialty areas, work roles, and knowledge/skills/abilities, is accurate from a technical perspective. Now it is time to get this into the HR professionals and hiring managers so that it can be properly employed. This will be a large task because of the diversity of employers, industries and cultural expectations. But the group we need to enjoin in the employment of this information is outside the congregation of our own church and we have to get them in before they join in our efforts.

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

Nothing to comment

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)?

Employer's needs and expectations are realistic, because they are real. We may not like them, but they are real. As employers get overly specific, CISSP, 10+ years' experience, reverse engineering malware abilities, project management . . . and the list goes on, the pool gets smaller and more expensive.

One of the employer's expectations that is often at odds with recent graduates is in the area of soft skills. Can the person present technical material, and then answer non-technical, yet relevant business questions, can they present themselves with confidence, how do they handle situations where they do not know the answer, these are what win interviews, but are rarely covered in detail. These are also highly important qualities among cybersecurity professionals. More time and effort needs to be placed in this area of workforce preparation.

They typically do not match the student exiting a pipeline for two reasons: 1) the pipeline is more than just cybersecurity job skills. A degree has other classes and for good reason, learning how to think, problem solve, and appreciate 2nd and 3rd order consequences requires time and experience. If one is trained for the entry level requirements only, they will not be able to grow and adapt as the field changes and employee wants a career beyond the entry level job. Employers rarely recognize the value of broad based learning abilities.

There is less variance by industry than one would expect, except in the specifics of tools, techniques and procedures. And because of the wide range of tools and differing vendors. And this brings up one of the true dilemmas facing industry and academia: how to partition between training and education. Training tends to be skill based using specific tools, learning how to use a vendors "stuff". Education is more general, theory based and less dependent upon actual instantiation. 100% of either of these, leaves a student unprepared for long term success. !00% training, means they might be ready day one for the entry level job, but have no foundation upon which to grow. 100% education means they might be ready for growth, but lack skills needed to immediately succeed. The challenge is in the balance between the two. Unfortunately, with respect to classical university professors, unless they have connections to industry and the current state of the art, they push too hard towards education, with limited practical skill assessment. Industry driven training programs tend to skip foundational material needed for the long term growth and success during a career.

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 Centers of Academic Excellence program run by NSA/DHS offers a comprehensive set of cybersecurity programs from multiple universities, overseen to ensure that the correct materials are being taught by qualified people. Although not an accreditation program, this group of universities works as a large, diverse collective, sharing the limited resources and reusing rather than recreating – which provides two significant outcomes; improved quality, and at lower costs.

In the early years the CAE program was a workforce training program for a select group of government jobs and all the recognized programs looked alike in their output. Today, the program has shifted to a community based sharing program built upon the breadth of over 200 schools. This sharing between schools has made development of specialty programs possible and allowed the material to spread to schools that otherwise could not have afforded the materials. What makes the CAE program effective is its reliance upon the schools themselves to help vet new member institutions, to help share curricula, to share instructors, to create local pipelines for students to navigate from 2 year schools to 4 year degrees to graduate work. By making the standards high level and open for flexibility among different programs, yet having enough detail to ensure quality – students coming from a CAE program, whether specializing in secure coding, digital forensics, auditing, network security, or any of dozens of other degree plans, they have a solid knowledge base of the foundations of security and a hands-on skill-based education in their specialty.

There are some certification programs, such as SANS, which have similar high standards. The cost basis for a program comprised of SANS classes is fairly high – approximately $50K for a masters level education, and this places it out of reach of many.

There is a highly successful scholarship program run by NSF, scholarship for service. This program allows students to trade work after graduation for education. Right now, the program serves the needs of Federal, State, local, and tribal governments. This program would go further if it would allow graduates that go into education, as we have a dire shortage of qualified cybersecurity professors.

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

Long term:

The greatest challenge is a lack of STEM interest from middle school forward. Rather than seeing more computer science programs in high schools, we are seeing less. Rather than

encouraging better STEM education, we are catering to a system of testing excellence into students. Our countries future lies in STEM – not just cybersecurity, but in a wide range of fields from every discipline STEM touches. Fixing STEM from middle school on forward is a long term project, but without it we will never succeed. When our students at the university level compete in coding challenges on a worldwide stage, we routinely come in far from the leaders. Student who win these contests begin programming by middle school and continue to grow for decade before we try to catch them. Yes, the early years are still rudimentary, but like money in a compound interest account, it builds over time. And it is not just an handful of students taking these paths overseas, but literally millions, as they see this as a pathway out of poverty. We need to invest and build upon those lessons and create millions of students playing with programming, raspberry pi's, robots, etc. in middle schools across the US.

The NSA has begun a program called GenCyber, which tries to kickstart interest by hosting camps across the country to introduce students to the wonders of STEM.

Mid-term:

The workforce development industry: Universities, Colleges, training companies, certification vendors, all need to work their offerings to more closely align with industry workforce needs. And learn to work together rather than acting as competitors.

Double the size of the NSA/DHS Center of Academic Excellence Program. Increase the size and scope of the scholarship for service program in the NSF to include service as faculty member post PhD as qualifying service.

Short term:

Put some money forward to provide incentives to schools with demonstrated records, enabling them to grow their programs. For instance $100K/year per CAE school, would cost a bit over $20 million a year, but if give in an unrestricted form would enable each institution to adapt and grow in ways they see fit, helping the overall diversity aspect as well.

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)?

Advances in technology are only going to exacerbate the problem. Unless structural reforms occur, more and more will move to industry, leaving academic institutions wishing for the good old days (today) to return. The entire realm of OT/CPS (operational technology/cyber physical systems) is understaffed and growing in the awareness they need to solve it. Needs are growing exponentially, while resources are flat.

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?

Introduced: A focused, visible, coordinated workforce initiative that professional/public/private organizations and academia can contribute to instead of duplicated efforts throughout the country – built around NCWF (SP 800-181).

A national STEM effort to put stem back into K-12, specifically 6-9. And make it real education, not just a test requirement. We need to take back technology education leadership – we are far from the top where we should be. This will require national attention and funding.

Modified: We propose an academic track of the CyberCorps program to attract all talents in the top research universities to study security/IA in the U.S. Rather than the current government service requirements, this track would require scholars to teach cybersecurity courses at a US university after getting a PhD. This would serve to both enhance the reach of the CyberCorps program and potentially provide some relief for the severe lack of cybersecurity faculty.

The CAE program (NSA/DHS Center of Academic Excellence) should be expanded. It is ready to double in size and broaden its base, but this will require additional federal funding. Long term a simple pass through of funding to CAE's to help cover their costs will improve the programs as well.

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

Introduced: There needs to be more training opportunities provided to secondary school teachers for them to be qualified to teach cybersecurity courses. Teachers need to be provided with additional incentives for supporting students in programs such as CyberPatriot and other extra-curricular cyber competitions/activities.

Modified: School systems need more incentives and opportunities to encourage development of cybersecurity programs at the secondary school levels. Bring back Computer Science as a real subject. Bring back STEM in middle school and forward.

    iii. By the private sector, including employers?

Modified: More employers need to be engaged with advisory boards throughout all levels of academia – secondary schools, community colleges and higher education.

Modified: More efforts need to be made to encourage partnerships between industry/academia/schools that result in student internships and provide for class instructors

iv. By education and training providers?

Introduced: Curriculum transition programs. These programs would characterized by highly experienced and qualified cybersecurity educators holding workshops for current computer science faculty who are interested in teaching security courses (not necessarily doing research) but do not have the time or depth of knowledge required to prepare the material in a given topic. The master teacher should provide all material (slides, homework, data sets, etc.) to the participating faculty. These professors will them offer courses in their institutions in the following years. This is a quick way of increasing the security curriculum capacity. There have been some curriculum modules developed with federal funding, but the adoption rate is too low. We should make it easy for professors to teach new security courses using proven course material.

Modified: Universities need to examine their own faculty career paths and see where the friction point is between highly qualified candidates from industry and the typical publish or perish cycle. The new world is technologically driven, has full integration of real world reality with deployment of solutions, and the "publish or perish on the aspects of slivers of new knowledge" does not fit well within this model. Rather than discover new knowledge, much of the future growth will be in integrating concepts from a multidisciplinary point of view. Multidisciplinary faculty attempting to navigate traditional academic career paths learn how hard it is to follow this path – we, the university community needs to realize that these are valid paths and find ways to be inclusive of them.

v. By technology providers?

Introduced/modified: Technology providers need to step up to the STEM problem and the resource problem. They benefit from the outcomes, they need to help shape the source of future inputs. When we look at workforce as a supply chain issue for the firms that will be adopting their products and services, the technology sector needs to step up direct involvement in assisting the growth of the supply chain. From donation to education to making their people resources available to assist in the development of the talent, tech has a lot to give, it just needs to happen.