EXCELSIOR COLLEGE®

WWW.EXCELSIOR.EDU

Growing and Sustaining the Nation's Cybersecurity Workforce

Excelsior College’s response to the NIST request for information concerning the nation’s cybersecurity workforce.

The following joint response is from Dr. Andrew Hurd and Dr. Denise Pheils, Faculty Program Directors of Cybersecurity at Excelsior College. The request for information asked for responses to eight questions or other questions. We added a question that pertains to funding. Please do not hesitate to reach out to either of us concerning our responses. We have been active in the CAE community and are willing to help contribute to a stronger national cybersecurity posture.

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?

Companies and organizations have compiled reports assessing various elements of the cybersecurity market. Companies like Burning Glass and Frost and Sullivan compile annual reports that measure or aggregate data from a variety of sources. There is no standard or consistent manner for the selection of participants, collection of data, or the various aspects of the data measured and reported. The data is not industry-wide and fails to reflect all facets of the cybersecurity ecosystem including employment (current, future, skills in demand, salary, education, etc.) and education (numbers enrolled, numbers successfully graduate from accredited programs and National Security Agency (NSA) Centers of Academic Excellence (CAE) schools and non-CAE schools). The current metrics fail to standardize position titles and skills for those positions. The metrics do not standardize job duties or the effect of education and certifications on the market. There are no metrics to evaluate the effectiveness of cybersecurity personnel in thwarting hacking attempts and successful mitigation of threats.

Much of the metrics in use are selected for a specific purpose – there is some subjectivity in the process, which is like conducting a risk assessment internally. As the person evaluating the metrics already has a relationship with the organization, it can be easy to assume security controls that are not actually in place or to misapply a control due to inherent bias and that foundational relationship.

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

No. While the NIST National Initiative for Cybersecurity Education (NICE) attempts to create a common framework and lexicon; it does not include all facets of cybersecurity nor all skills essential for success in the various fields. The NIST Framework states that it is only a suggestion and that it is incomplete. That the entirety of the knowledge, skills, and abilities cannot be covered in the framework. The NIST Framework also states that the framework is a foundation for future growth in cybersecurity, therefore while the framework has a baseline for the categories, it lacks the depth needed to have a proper understanding and uniform classification of duties. Across the levels of business (Fortune 500, etc.), the same titles, skills, expectations, salaries, and entry point to the discipline are not consistent. Part of this stems from the necessary holistic view of cybersecurity that is often overlooked in favor of a niche or popular entry path. Cybersecurity can benefit from a workforce that has the varied background and skills offered by those who studied in and have experience in information technology, information systems, computer science, cybersecurity, and law and legal specialties such as healthcare law, criminal justice, psychology, sociology, and others.

Assuming there is one path to cybersecurity positions and thus security in this country is short-sighted and misguided. Continuing how we always have results in what we have always obtained. Opening the pool of potential cybersecurity professionals to the disciplines mentioned above offers a more holistic view of the problem and strengthens our problem-solving ability as we will have contributors with varying viewpoints, experiences, and expertise who may offer better suggestions and move us from a reactive nation to one that is proactive in cybersecurity.

The NIST Framework also leaves out essential skills that have been identified as needed in the industry. The software skills are not found within the Knowledge Skills and Abilities. There is a lack of categories like oral communication, writing skills, and other soft skills needed in the industry.

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, our college has proper policies in place. In addition to the policies, we require all employees complete a cybersecurity awareness 3-part course annually. We also have awareness prompt like messages on mouse pads, banners, and login prompts and warnings. As threats are ever evolving the awareness training, cybersecurity policies and procedures must also evolve. To our knowledge, the policies are consistently enforced. It would negate the effect of such policies and even make those indefensible if that were not true.

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)?

The list of skills can vary from entry-level with a solid demonstration of soft skills and ethics to certified expert level with several years of experience. In some cases, the expectations are realistic, and in others those are not, as it is difficult for students and entry-level workers to gain the experience mandated by many of the positions as that is the expected experience the person would gain once in that position. It is almost cannibalization of the industry as only those in the industry qualify for most of the positions. This is a constant problem in that *entry-level* jobs need to be more than entry level very quickly. The learning curve for cybersecurity is aggressive and often people are learning as they go. The on the job training model is highly adapted in the industry.

The field needs entry level points so aspiring, talented individuals may gain the necessary experience to secure positions in this area and increase the number of cybersecurity workers and not just allow horizontal movement within the industry. While many faculty seek ways to help students gain the necessary experience, we still have a paucity of positions that will allow for novices in experience, but possessing education and/or certifications is necessary to alleviate the gap in experience. We encourage our students to participate in cyber challenges to gain some of the real-world experience needed for the entry-level jobs.

The way the skills and experience vary by industry is within the context of each area. While all industries require and need cybersecurity expertise, the context for how that expertise is applied differs. For example, when learning to program a student may not understand the reason that no mistakes are allowed in their coded assignments, but once it is explained, or upon entering an industry like healthcare, which had the Therac-25 deaths (because of a coding error patients were subjected to too much radiation) the application of their code is understandable. In a retail environment, a mislabeled component may make a screen show a jumbled display or a phrase with missing characters, but in an SCADA environment, it could cause an entire section of an electrical grid to stop producing or allow for contamination in a water treatment plant. Until one is invested in an industry, it is often difficult for them to understand the full potential ramifications of their actions (or inactions). The issue also arises with the diversity in cybersecurity jobs. It is not enough to just have cybersecurity specialist infused in all areas of the businesses because the cybersecurity specialist may not know the process or responsibilities involved. We need individuals from all facets of the workforce to become intrigued with cybersecurity enough to gain the cyber skills needed to protect their areas of business.

To address these issues, we need more public/private-academic partnerships. This will increase the number of students with hands-on experience, providing the missing context for how their skills are applied and learning the correlation or causation that may result. Incentives for employers would aid in making this more attractive for businesses. Most educators already understand the value of this proposition. An additional benefit is the knowledge employers gain of the academic program and the abilities of graduates.

Employer involvement with academic programs may aid in lessening the entry barriers for students and veterans who have experience but are unable to disclose the specifics of what they have done as they can demonstrate to an employer their knowledge and skills without breaching confidentiality. Incentives for industry partners to get involved with neighboring educational institutions would go a long way to improving the cybersecurity workforce.

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?

Instead of naming names of colleges and programs, the most effective programs share common attributes. Each program is up to date with the current technologies that offer hands-on opportunities and material in a variety of learning styles. Students can learn beyond the classroom as it is impossible for teachers to provide everything one will need to be successful, but the teacher can inspire, motivate, and spread enthusiasm, innovation, and curiosity about cybersecurity. The programs must offer critical thinking skills, and the best programs are not bound by place or time. For some students, on-ground education is most appropriate while others excel in online education. Whatever the venue, all students need hands-on, context based, and current learning opportunities.

The best educational scenarios offer education in a variety of methods. Degree programs are important but educational certificates are also important for individuals who return for a specific skill set that targets a job role.

An effective program is one that is continuously evolving and monitors the trends of the industry. The trends are used as examples in classroom exercises, and they are also used develop new classes for the programs. The consultation of a Faculty Advisory committee and an Industry Advisory committee is also a positive influence on a program.

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

The biggest challenge is always funding. Cyberattacks are only increasing. If we are ever to become cyber resilient and proactive, we must regard cybersecurity and the vulnerabilities in our systems in a different way. Opening the search for solutions to people with multiple skill sets, education, and experience will allow for additional perspectives and different approaches to solving the problems we face now and in the future. To combat the situation most effectively, employers need to view themselves as part of the academic and experience process and not just recipients of the final product.

Organizations that aid in training the workforce should have the opportunity to hire those candidates.

Change is also needed in the corporate and academic worlds to recognize multiple paths to cybersecurity employment. We are not in competition with other academic institutions; we are compliments to each as we offer differences in programs, opportunities, and geographic service. The fact that it is often termed a ‘conversation’ about cybersecurity issues should change to an action item as the conversations have occurred. Now we need solutions so it should be brainstorming and idea generation, synthesis, collaboration, and creation.

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)?

The advances in technology will open additional avenues of specialization and entry but do not change the fundamental need or existing education and training options. What exists will still be needed (as long as it stays current and offers viable, hands-on, experiences to students), and additional specializations will become available to address those changes. Everyone will still need cybersecurity awareness and specific skills in their areas of expertise/practice, and with new advances, there will be additional specialty areas for which one can train, prepare, and progress.

With the advancements in technology, the need for training and education in the specific areas will also need to increase. Research and exploitation of the new technologies will need to be performed, and research will identify if the technology is an extension of previous technologies that have a sound cybersecurity plan or if a new risk management and mitigation process will need to be developed.

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?

There is a place for all programs that offer timely, relevant, hands-on (when applicable to the topic) learning opportunities. What should occur is a broadening of what it means to be an NSA/DHS CAE by limiting the mandatory Knowledge Units (KU) in favor of an increase in the number of KUs a school can choose, which does not diminish the value or prestige of a CAE designation, but rather increases the types and specifications that may now become a CAE. The purpose and designation of being a CAE need to have more meaning than to just the federal government. It is reassuring to know that if you meet the curricular recommendations for the CAE program that your students will be valued and ready for a job with NSA/DHS/DOD and other government regulated agencies, but the private sector needs to be educated on what it means for a student who has graduated from a CAE.

It is not the responsibility of one institution to dictate what steps should be covered by the sectors listed above, but it is up to all entities to work together to make sure the previous seven questions in this survey are covered and implemented.

Here is a prime example where a school would benefit from a CAE designation, but they are not eligible to be one because they do not have a broad enough program. But digital forensic programs are of extreme importance, and they should be promoted.

Currently, an entirely digital forensics program-type cybersecurity school that meets all other criteria (such as infusion of cybersecurity concepts in all programs to the extent appropriate and within the context of the discipline), can’t become a CAE as it has no room in the curriculum for the more main-stream subjects that exist in the CAE KU pool. If the school needs to only meet a limited number of ‘mandatory’ topics and may include those topics that better support digital forensics, that school can continue to meet a need within academia by offering the program, meet the need in industry by supplying specialized cybersecurity workers, and address those issues dealing with digital forensics in this country. The school still achieves excellence, the students benefit from a specialized program, employers have skilled graduates to hire, and it is not in direct competition with the cybersecurity programs offered at neighboring schools.

Additional question:

9. What is the federal government going to do to increase funding to more than the top tier R1 schools?

Funding should be made available to other schools who focus programs on teaching rather than research.

10. What is the federal government doing to discuss evaluation of competencies?

There is a lack of assessment of skillsets in the industry. ISACA has created a competency based certification where individuals must validate their skillset on a given renewal cycle. Most other renewals of the industry certification are based on CPE credits. The CPE credits can be anything in an area of focus, and don’t have to be specific to the desired learning outcomes from the certification.

Validation of skills and competencies within workers will assist decision makers in focusing funding. Focusing funding to the obtainment of needed skillsets should increase the competency of the workers in that area. This could be done by increasing the incentives for educational institutions to offer internships and other on the job skill obtainment.