NACE Workshop Position Statement – Cybersecurity Education and Competency Challenges

Nancy R. Mead, PhD, SEI Fellow Emeritus, CMU Adjunct Professor of Software Engineering, nrmcmu@gmail.com

Bio Sketch: Dr. Nancy R. Mead is a Fellow Emeritus of the Software Engineering Institute (SEI), and an Adjunct Professor of Software Engineering at Carnegie Mellon University. Her research areas are security requirements engineering and software assurance curricula. The Nancy Mead Award for Excellence in Software Engineering Education is named for her.

Prior to joining the SEI, Mead was a senior technical staff member at IBM Federal Systems, where she spent most of her career in the development and management of large real-time systems. She also worked in IBM's software engineering technology area and managed IBM Federal Systems' software engineering education department. She has developed and taught numerous courses on software engineering topics, both at universities and in professional education courses.

Mead has more than 150 publications and invited presentations. She is a Life Fellow of the IEEE, a Distinguished Member of the ACM, and was named the 2015 Distinguished Educator by IEEE TCSE. Dr. Mead received her PhD in mathematics from the Polytechnic Institute of New York.

Position Statement: Let us consider challenges in cybersecurity education and its associated competencies:

- Cybersecurity these days must consider much more than shoring up an existing system's defenses and applying patches.

  Although cybersecurity was once limited to mechanisms like patch management, firewalls, and encryption, it has become clear that such methods are far from adequate for today's threats. Unfortunately, many managers are still stuck in a time warp that leads them to think that cybersecurity is something that only needs to be considered after a system is fielded. As a consequence, systems are developed that can never be adequately secured due to poor architecture and implementation decisions. There is a substantial need to educate people who are still laboring under these misconceptions.

  These same folks do not know what to do with graduates of modern cybersecurity programs, and relegate them to low-level positions in system administration just to fill a slot (I call this "cannon fodder"). The highly qualified individuals hired into these slots can't wait to "do their time" and find a more interesting job, and some of them even buy their way out of a contractual obligation in order to do so.

- When they hire, employers tend to look for experience in specific languages and tools, rather than more substantial competencies. Moreover, career advancement in cybersecurity seldom includes defined competencies as a consideration.

  It's probably been at least 5 years since I pointed out that classified ads do not seek individuals with substantial educational background. Instead, they advertise for expertise in specific languages, specific static analysis tools, and so on. Moreover, many organizations don't want to train new employees, but expect them to be productive out of the box. This occurs in part because people change jobs often, and employers don't want to invest in growing the skills of people who will be gone in a year.

  On the plus side, there are some organizations who have developed competency models for cybersecurity and software assurance. How they are being used, however, is largely unknown. More data collection is needed to understand the status quo.

- At all levels of education, there is a dearth of faculty who are qualified to teach cybersecurity.

  In attempting to transition software assurance curriculum recommendations, especially at the community college and high school levels, it is clear that there are not enough qualified faculty to do this. If the school has degree offerings in computer science or information systems, then the existing faculty can learn

enough about the field to be able to teach it. However, faculty members who are set in their ways are not necessarily motivated to change. One possible solution is to bring in adjunct faculty to teach these courses, but quite frankly, if you consider all the hours put in, the typical adjunct salary doesn't even amount to minimum wage.

On the plus side, whenever software security and software assurance degrees are offered, there seem to be an ample number of students who are interested in these offerings. In undergraduate and graduate programs, more cybersecurity degree offerings exist than at the lower levels, but there is a risk that students will rush into these programs because the field is "hot", and later as graduates, lose interest and drop out of the field, much as we saw in computer science some years ago. The NACE Workshop benefited greatly from the participation of students. We need to step down from our pedestals and ask students as well as recent graduates what they need, rather than trying to invent things in a vacuum.

- For the most part, standard sets of material for teaching a cybersecurity or software assurance curriculum at any level are not publicly available.

  Although some faculty are willing to make their material publicly available, and they are to be commended for this, it is often the case that the material is considered the intellectual property of the university or the individual faculty member. Individual faculty members who use the same material to do consulting or teach industry workshops are reluctant to share their materials with others who may have similar consulting arrangements. Universities may be reluctant to have material shared if they think it helps a competing university. With online and distance education offerings, any university can be considered a competitor, regardless of their physical location.

  Government-funded projects have helped to address this, but the funding is usually insufficient to support fielding an entire program, and it can't be counted on for the long-term investment that is needed. If it is done, it is usually a one-time effort, with no opportunity to refresh and modify the material at a later time. The funding, when it exists, is often used to support making course materials available "as is", without consideration of how to make it useful to other instructors who are not teaching the exact same course at the same university. By and large, there is no data collected on how many faculty use publicly-provided material, or how effective it was, assuming measures of effectiveness even exist. Needless to say, the same applies to students who are on the receiving end. Sad to say, it's possible to get a grant to support a single workshop, or what is otherwise a volunteer effort, but grants to support a substantial amount of work are seldom available.

- Possible solutions

  I believe that a cooperative, appropriately funded, multi-year effort between government, industry, and academe could go a long way towards addressing these problems. The NACE workshop was an excellent start, and the organizers are to be commended for their initiative.

  The NICE framework attempts to address some of the issues, once again depends on voluntary participation and donated materials. I would like to see ongoing funding for it, so that it can serve as more than just a clearing house for materials. The Scholarship for Service program has produced a number of graduates with excellent background. The same is true of the Centers of Academic Excellence. Certainly government needs to be a part of the solution.

  Industry needs to recognize that this is not simply a case of getting graduates who are productive from day one. Higher education is intended to produce individuals who have learned the fundamentals that will serve them well over the course of their careers – the ability to create, learn, apply, and analyze problems, approaches, and methods that may not even exist when they graduate. From an industry perspective, this means that the graduates they hire will be productive for many years to come.

  Considering the fact that information systems and cybersecurity now concern all of us in our daily lives, educational institutions at all levels need to collaborate to support the development and delivery of appropriate course materials.

  Measures of effectiveness need to be defined and built into educational program follow-up. It is not sufficient to do something once and then declare victory. It takes resources to track graduates over a period of years, collect feedback, and use the feedback to improve present and future programs.

  All of this takes dedication, and resources. It's not something that can be tossed off in a year or two. While it is certainly the case that progress has been made, more is needed. Workshops such as NACE can be great catalysts for change, provided the appropriate follow-on activities are planned, funded, and executed.

  Please visit the SEI website for curriculum recommendations, competency materials, and course materials available for free download: https://www.sei.cmu.edu/education-outreach/curricula/index.cfm