The Role of the Community College in Educating the Cybersecurity Workforce

Robert D. Campbell  
Vice President for Information Technology, IL  
Rock Valley College  
United States  
b.campbell@rvc.cc.il.us

Abstract: The issue of national security and the need to protect the nation’s information systems, networks, and infrastructures could not be more prevalent. President Bush recently directed the development of a National Strategy to Secure Cyberspace to ensure that America has a clear roadmap to protect its important infrastructures. In conjunction with this national call to secure cyberspace, leaders of higher education have worked to identify strategies and resources to help meet the nation’s educational and workforce needs in this critical high-tech area. This poster presentation will focus on the key findings and recommendations that came out of the National Science Foundation workshop on “The Role of Community Colleges in Cybersecurity Education.” Topics include the issues of certifications and skill standards; preparation for cybersecurity positions; specification of topics, courses, and curricula; and advancing the role of community colleges in cybersecurity education.

In June 2002, the National Science Foundation and the American Association of Community Colleges assembled approximately 90 experts in computer, network, and information security from community colleges, four-year colleges and universities, business, industry, and government to consider how resources at community colleges can be harnessed and expanded to educate a cybersecurity workforce.

Technical education about cybersecurity issues is needed for employment in a wide range of fields, including software engineering, network administration, banking, e-business, and law enforcement. The relevant occupations cover a vast spectrum of knowledge and skills. Part of this spectrum, which accounts for a significant share of the workforce demand, can be effectively addressed by courses and programs at community colleges.

Community colleges are at the forefront of technological education improvement in this country. As community-based institutions, they are strongly positioned to provide workforce development and technician training in response to growing industry needs. Serving over 40% of all students enrolled in postsecondary education and accounting for approximately 34% of all undergraduate science, technology, engineering, and mathematics enrollments, community colleges are uniquely situated to address the rising concerns of technician shortages and faculty pipelines issues.

The poster session will focus on the key findings and recommendations that came out of the National Science Foundation workshop on the “Role of Community Colleges in Cybersecurity Education.” Three overarching issues to be addressed by this poster session are:

1. Role of certification and skill standards. The distinction between certification and skill standards is clarified and specified. Skill standards recommend foundational elements for programs and provide a set of core competencies. Skill standards can assist in the definition of the field, provide uniformity across institutions, map programs to specific jobs, and provide guidelines that assist educational programs in evolving and adapting changes in the field and in job requirements. Certification can be an assessment of an applicant’s qualifications as measured by performance on a standardized test, a mechanism for establishing articulation agreements between and among institutions, a way to encourage the formation of education and business/industry partnerships, and a system for continuing on-going professional development and life-long learning.

2. Establishment and maintenance of a cybersecurity program at a community college. Establishing and maintaining a cybersecurity program will require initial and on-going investment. Collaboration among two-year and four-year institutions of higher education, business, industry, and government at all levels can assist in securing the necessary
resources to meet the demand for a high quality cybersecurity workforce. This includes resource support from internal and external sources for educational materials and curricula, dedicated state-of-the-art facilities, access to educational and training opportunities through diverse modes of instructional delivery systems, continuous opportunities for professional development and enhancement, and student recruitment and support systems.

3. Specification of topics, courses, curricula, and programs. Community colleges prepare a wide range of cybersecurity professionals. They train entry-level workers, provide workers with opportunities to maintain high levels of skills and knowledge, serve workers who are trying to change jobs or positions, and prepare students for transfer to four-year programs. To navigate this diversity, students need to have a clear understanding of their options, responsibilities, and the goals of the programs in which they are enrolled. A framework of six core areas was developed as part of the workshop for specifying topics, courses, curricula, and programs for linking them to hands-on real world activities.