COMMUNITY COLLEGE CORNER

Elizabeth K. Hawthorne

Multifarious Initiatives in Cybersecurity Education

ACCORDING TO THE NATIONAL SECURITY COUNCIL, "President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter [2]." In May of 2009, the President supported the recommendations from his commissioned Cyberspace Policy Review that, among other endorsements, included promoting cybersecurity awareness and building the digital workforce of the 21st century. The recommendations from the Cyberspace Policy Review were based upon the 2008 Comprehensive National Cybersecurity Initiative (CNCI), which consists of 12 individual initiatives designed to help secure the United States in cyberspace. This column will focus on Initiative 8 – expand cyber education – as it relates to two-year college programs.

First a little background on CNCI Initiative 8. Presently, an insufficient number of cybersecurity practitioners and professionals exist to protect and defend the United States in cyberspace. The current cybersecurity training and education programs are limited in focus and lack unity of effort. Evolving from CNCI initiative 8, the National Initiative for Cybersecurity Education (NICE) was established with the goal of creating "operational, sustainable and continually improving" cybersecurity education that will enhance the nation's security [8]. The Department of Education and the National Science Foundation (NSF) are serving as co-leads for this NICE component called *Formal Cybersecurity Education*. The mission of this component is to bolster cybersecurity education programs from kindergarten through graduate school, with an emphasis on science, technology, engineering and mathematics (STEM) disciplines to fill the pipeline with technologically-skilled and cyber-savvy personnel.

During the summer of 2011, an ACM Innovation and Technology in Computer Science Education (ITiCSE) working group studied 16 associate-degree programs in information assurance (a.k.a. cybersecurity). The findings are revealing and in concert with CNCI Initiative 8. "A lack of consensus of what constitutes information assurance (IA) education has led to IA degree programs with widely varying curricula [10]." Associate degree IA programs vary in their particular emphases, their curricular structure, and whether they are meant to place graduates into the workforce or to matriculate students into baccalaureate degree programs. Of the 16 associate-degree programs examined by the 2011 working group, 14 were Associate of Applied Science (A.A.S.) degrees and 2 were Associate of Science (A.S.) degrees. Of the A.A.S. career programs, two areas of concentration emerged, network security and computer forensics. Figure 1 depicts the composition of a typical network security degree, while Figure 2 illustrates the composition of a typical computer forensics

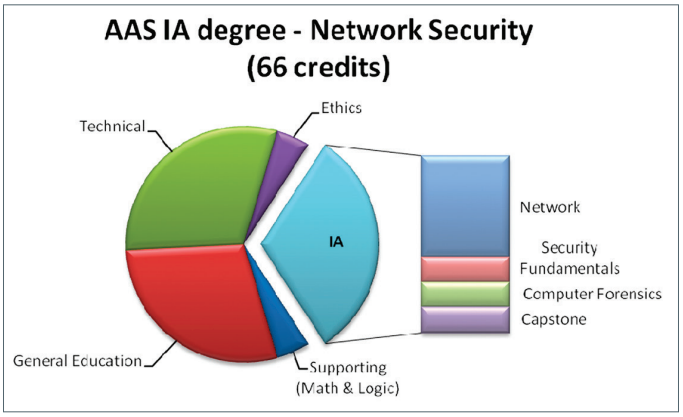

Figure 1: Typical A.A.S. degree in network security

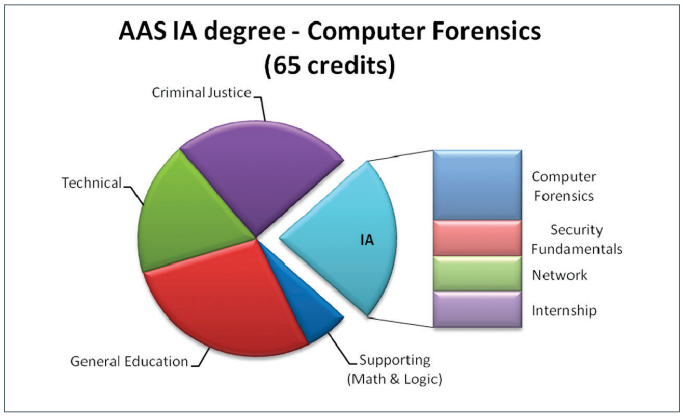

Figure 2: Typical A.A.S. degree in computer forensics

ILLUSTRATION: ISTOCKPHOTO/@SMARTBOY10

degree. The computer forensics degree resembles the network security degree with criminal justice courses taking the place of some of the network courses.

Of the 16 associate- and 9 baccalaureate- degree programs investigated by the 2011 working group, a clear pathway for course articulation between two- and four-year information assurance degree programs did not emerge. Figure 3 portrays a modified A.S. degree in computer science with the inclusion of a Security Fundamentals course that would provide the typical connection points enabling the transfer between a traditional AS in CS and a traditional BS in CS with an IA track.

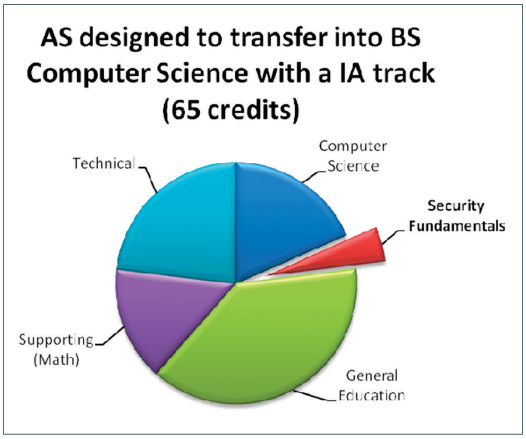

Figure 3: Modified A.S. CS degree designed to transfer into a baccalaureate CS degree with an IA track

Another cyber education initiative aimed at the two-year college level includes the four NSF-sponsored Advanced Technological Education (ATE) Centers [1] located strategically throughout the country. The ATE Centers provide community colleges with technology resources, faculty training, and varying model curricula that align to the Committee on National Security System (CNSS) standards in information assurance. Each ATE Center has unique resources and accomplishments.

One of the centers is CyberWatch [5], which is located on the East coast at Prince George's Community College in Largo, MD. A fairly new sister center, CyberWatch West [6] is located on the West coast at Mt. San Antonio College in Walnut, California. Working with the NSA, DHS, and the NSF, CyberWatch played a key role in developing and implementing the National Centers of Academic Excellence in Information Assurance Two-Year Education (CAE2Y) program. CyberWatch continues to mentor aspiring CAE2Y designated community colleges, helping to document their degree programs in order to meet the stringent NSA requirements (primarily, CNSS 4011 and 4013). In 2010 CyberWatch mentored the first six community colleges that received the CAE2Y designation from NSA. To date, there are approximately two dozen CAE2Y designated community colleges. However, drastic changes for obtaining the CAE2Y designation are on the horizon. Instead of mapping to the CNSS standards, the NSA will soon require alignment to "Knowledge Units" that map to the National Cybersecurity Workforce Framework [7]. Both CyberWatch and CyberWatch West are providing input for the "Knowledge Units" as well as offering assistance to existing and prospective CAE2Y institutions.

A third ATE Center is the Cyber Security Education Consortium (CSEC) [3], headquartered at the University of Tulsa. CSEC consists of a partnership between community colleges and career and technology centers in Oklahoma, Arkansas, Colorado, Kansas, Louisiana, Missouri, Tennessee, and Texas. A primary mission of CSEC is to develop and disseminate cybersecurity curricula for two-year institutions as well as assist faculty to build programs of study.

The fourth is the Center for Systems Security and Information Assurance (CSSIA) [4] located at Moraine Valley Community College in Palos Hills, Illinois. CSSIA not only serves community colleges in the mid-west region, but is also considered a National Resource Center by the NSF. CSSIA operates national models for skills and learning events based on the creation of scalable and affordable remote virtual laboratory environments. CSSIA also delivers faculty professional development workshops via its national infrastructure and has hosted three annual Cyber Defense and Disaster Recovery Conferences. CSSIA has been featured on NSF's Science Nation [9].

Another NSF-funded and complimentary teaching resource for community college faculty is Security Injections from Towson University. "Security injections are strategically-placed security-related modules for existing undergraduate classes. The combination of lab exercises and student-completed checklists has helped teach security across the curriculum without adding extra pressure on already overburdened undergraduate degree programs [11]."

In summary, there are multifarious cybersecurity education initiatives and resources intended for community colleges of which only a few are highlighted in this column. Faculty and administrators at two-year colleges should avail themselves of these resources to create certificate and degree programs in cybersecurity that assist in fulfilling the needs of local government, business and industry. With over 1,200 community colleges from coast to coast, together we can help respond to the nation's urgent need to secure our cyberspace. **Ir**

References

[1] ATE Centers, http://www.atecenters.org/ Accessed 2013 March 1

[2] Comprehensive National Cybersecurity Initiative, National Security Council, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative/ Accessed 2013 March 1

[3] CSEC, University of Tulsa, http://atecenters.org/csec/ Accessed 2013 March 1

4] CSSIA, Moraine Valley Community College, http://atecenters.org/cssia/ Accessed 2013 March 1

[5] CyberWatch, Prince George's Community College, http://atecenters.org/cyberwatch/ Accessed 2013 March 1

[6] CyberWatch West, Mt. San Antonio College, http://www.cyberwatchwest.org/ Accessed 2013 March 1

[7] National Cybersecurity Workforce Framework, National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/framework/ Accessed 2013 March 1

[8] National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/ Accessed 2013 March 1

[9] O'Brien, M. & Kellan A. (January 28, 2013). *Community College Cybersecurity Program Trains 21st Century Workforce*, Science Nation, National Science Foundation, http://www.nsf.gov/news/special_reports/science_nation/cybersecurity.jsp?WT.mc_id=USNSF_51 Accessed 2013 March 1

[10] Perez, L., Cooper, S., Hawthorne, E., Wetzel, S., Bryniels-son, J., Gökce, A., Impagliazzo, J., Khmelevsky, Y., Klee, K., Leary, M., Philips, A., Pohlmann, N., Taylor, B., Upadhyaya, S. *Information assurance education in two- and four-year institutions* (2011), ACM ITiCSE-WGR '11 Proceedings of the 16th annual conference reports on Innovation and technology in computer science education - working group reports; doi: 10.1145/2078856.2078860

[11] Taylor, B. & Kaza, S. Security Injections, Towson University, http://www.towson.edu/securityinjections/ Accessed 2013 March 1

Elizabeth K. Hawthorne
Computer Science Department
Union County College
Cranford, New Jersey 07016 USA
Hawthorne@ucc.edu

DOI: 10.1145/2505990.2505999