

Preparing Adjunct Faculty Cybersecurity Experts to Teach at the Post-Secondary Level¹

Shelly Heller, Lance Hoffman and Costis Toregas
The George Washington University
Washington DC 20052

in order for the United States to maintain and expand its capabilities in the world of cybersecurity – whether planning for the deployment of new technologies and the internet of Things (IoT), preparing defenses, constructing offensive tactics, or developing appropriate policies – a well-educated government workforce is needed. To fill the numerous jobs which are emerging, many educational pathways have to be opened to provide appropriate skills and experience – including job training, community college programs and traditional four year and graduate programs. Each of these avenues educates and trains individuals to work at different levels and in different capacities in our ‘cyber’ world. Currently there is a capacity issue: students cannot readily be added to the education system because faculty with professional and pedagogical experience are scarce. especially at the community college level. The weak link in the cybersecurity workforce supply chain is often finding faculty who can be effective and who can provide the proper encouragement to students to join the cyber workforce. Success in achieving the educated Cybersecurity workforce will depend, in large part, on the capabilities of these educators and on the capacity of educational institutions to scale up and absorb increased numbers of students by offering attractive and impactful courses.

Community colleges are currently an untapped source of cybersecurity workers. “Community colleges can play a critical role in giving students the hands-on skills that are needed on the front lines (of) defending computer networks” (NSF, 2013). According to the American Association of Community Colleges, there has been huge growth in the percentage of higher education faculty teaching in community colleges and the biggest group contributing to that growth are part time faculty. And, while some community colleges have existing programs in cybersecurity and have dedicated full time faculty, according to the Center for Community College Student Engagement, more than 58% of community college classes are taught by adjunct faculty (Fain, 2014). While the data is not broken out by discipline, informal conversations with local community college professors imply that they rely heavily on adjunct faculty, and many of these adjuncts have no prior teaching experience. A typical advertisement for a cyber-security faculty member at a community college includes “Bachelor's degree (Master's preferred)

¹ Work supported in part by U. S. Defense Department Grant H98230-17-1-0371

and five years of work experience as Computer Forensics professional, technical qualifications: (CompTIA Network+, CompTIA Security+, CISCO certifications, CISSP, SANS, Certified Ethical Hacker (CEH)), knowledge of Programming Languages, excellent written and oral communications skills, experience in leadership including a history initiating and managing change, working with others toward shared goals and developing others.” These requirements can act as a barrier to many aspiring faculty members, thereby extending the mismatch between demand and supply, since there is a shortage of individuals with those characteristics who wish to teach part-time in a community college.

Our answer: Tapping into cybersecurity experts as adjunct faculty. Cybersecurity experts already in the workforce have the potential to fill the need for part-time cybersecurity faculty at the community college level. These individuals from government positions and the private sector have backgrounds that approximate the typical qualifications listed above, and thus can fit into a viable long term strategy for filling the faculty gap. They often work with cybersecurity issues daily, have access to the latest technologies, wrestle with contemporary problems, and develop policies for their organizations. They often have a wide network of peers who might also be called upon to teach.

Currently the Cybersecurity Teaching Corps project at GW is exploring these possibilities through a research effort and a pilot online course “Teaching Cybersecurity at Community Colleges” (See Figure 1).

Introduction to Community Colleges, Ethics and general structure of a course
The typical Community College student, Faculty codes, Crafting goals and objectives
Teaching concepts – moving from concrete to abstract
Teaching concepts – using group work in your class
Teaching concepts – using case studies in your class
Teaching concepts – using discussions during a class

Figure 1: Cybersecurity Teaching Corps Sessions

The course targets CyberCorps (OPM, 2018) alumni with 3 to 5 years of work experience to address the typical requirements for adjunct faculty in community colleges; these recent CyberCorps graduates generally possess the requisite cybersecurity content knowledge and experience to teach at a Community College level, but usually do not have teaching experience or knowledge of diverse learning and assessment techniques. Furthermore, many of them are not a product of the community college pathway and often they do not appreciate the challenges and opportunities associated with community college students in the classroom.

There are six sessions as noted in Figure 1. Each session has three general content areas: presentations related to the history and context of community colleges, ethics within the professions of teaching, and cybersecurity and pedagogy tools for teaching at a community college. Each hour-long session is unmoderated; any questions posed in session presentations are addressed in subsequent slides or sessions. The sessions will be made available to a focus group during the summer of 2018 and based on its feedback, adjusted pilot sessions are expected to be available for fall 2018.

Obviously, the Reach to Teach concept could be modified to target faculty who would be appropriate to teach as adjuncts in four-year colleges. And the targeted experts could be expanded well beyond CyberCorps alumni to include others currently working in the field and retired cybersecurity professionals who wish to give back. Monetary inducements might also be provided, such as partial or complete forgiveness of student loan debt, tuition rebates at colleges and universities for those wishing to get an advanced degree, and other strategies.

It is expected that the outcome of this GW effort will be an on-line course pilot-tested in a small number of institutions during the summer of 2018 and then made available to a broader number of individuals and institutions.

REFERENCES

(NSF 2013) Community College Cybersecurity Program Trains 21st Century Workforce
https://www.nsf.gov/news/special_reports/science_nation/cybersecurity.jsp

(OPM 2018) U. S. OPM, CyberCorps Scholarship for Service, <https://www.sfs.opm.gov/StudFAQ.aspx>

(Fain 2014) P. Fain, "Low Expectations, High Stakes", Inside Higher Ed, April 7, 2014,
<https://www.insidehighered.com/news/2014/04/07/part-time-professors-teach-most-community-college-students-report-finds>
