Virtual Extension
The Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air

Seeking to improve the educational mechanisms for efficiently training large numbers of information security workers.

Although recent hiring forecasts (some thousands of new cyber-security professionals over the next three years) by both the NSA and DHS show a strong demand for cyber-security skills, such a hiring spree seems ambitious, to say the least. The current rate of production of skilled cyber-security workers satisfies the appetite of neither the public nor private sector, and if we do not make a concerted effort to drastically increase this work force, then the U.S. will export high-paying information security jobs. In a global economy, such a situation isn’t necessarily a bad outcome, but it poses several challenges to the U.S.’s stated cyber-security plans. We believe the creation of a significant cyber-security work force is not only feasible, but also will help ensure the economic strength of the U.S.

A large cyber-security work force would provide a strong pillar for the domestic high-tech industry. Beyond offering immediate economic stimulus, the nature of these jobs demands that they remain in the U.S. for the long term, and they would directly support efforts to introduce information technology into the health care and energy systems in a secure and reliable fashion. Without a commitment to educating such a work force, it is impossible to hire such a work force into existence.

The Washington Post article “Cyber-help Wanted” highlighted the need for a dramatically different approach to cyber-security education, outreach, and hiring by the federal government. From our point of view, far too few workers are adequately trained mostly because traditional educational mechanisms lack the resources to effectively train large numbers of experienced, knowledgeable cyber-security special-
ists. The government’s incredibly diverse cyber-security needs complicate matters: operational, analytical, and strategic technology roles span both the military and civilian parts of government. Even finding a figurehead to direct and coordinate government cyber-security efforts is a monumental task.

We see the central problem as one of both scaling and competency; academic departments often wrongly eschew the teaching of the informal “Hacker Curriculum” as being too tied to a specific technology to teach abstract computer science concepts, and current amounts of cyber-security research and education funding leave sizeable gaps in our ability to meaningfully educate large numbers of students. Indeed, those educators most capable of passing along information security and assurance skills are often restrained in their ability to dedicate a large amount of time to the classroom because they must spend their time chasing more prestigious research dollars.

Although professional certification courses exist, the NSF has the Scholarship-for-Service (SFS) program, and the NSA has designated many college and university cyber-security programs as Centers of Academic Excellence (CAE), in reality, only a small number of quality educational programs are funded, equipped, and willing to quickly educate large numbers of information security workers.

Furthermore, existing funding for cyber-security education or retraining pales in comparison to the amount of funding available for pure research. Just as importantly, many of the commercial training programs and certifications focus on teaching skills useful for fighting the last cyberwar, not the current, nor future ones. University education serves a pivotal role in providing the core skills necessary for a professional work force to be adaptive to a threat that is hyper-adaptive. Plans for training government cyber-security workers should focus on educating a new work force rather than mass certification of existing workers.

Hope for the future exists: we have seen the enthusiasm that previously bored students have when they get a chance to manipulate real network packets, modify real operating systems and hardware, assess real-world security policies and access control mechanisms, and analyze real vulnerabilities and exploits. We have a number of colleagues in academia who do a tremendous job communicating their talent to small batches of undergraduates or master’s-level students. These efforts need to be scaled up.

To most folks trying to find another job, pay for health care, or deal with a mortgage that is under water, the urgency of educating a cyber-security work force may seem like a low-priority issue. Despite these challenges, the Obama administration has laudably held cyber-security as an important national priority, and we believe that educating large numbers of cyber-security professionals must be a front-line priority, particularly since information security underpins the future success of the strategic priorities of simultaneously reinventing both the health care and energy systems. In fact, the demand for cyber-security professionals far outstrips the current supply—indicating one sector of the economy that is primed for growth if adequate number of professionals can be trained. With the declaration of “National Computer Science Education Week” in December 2009 and December 2010, Congress has recognized that computer science is a vital national interest.

Since most current government and private sector endeavors rely on the presumption of a stable, dependable, and secure computing infrastructure, we recommend the following initiatives:

- Significant funding for cyber-security education: Create a sustained funding program with substantial award amounts to encourage research in educational technology specialized for cyber-security problems that will result in scalable education. The prestige and profile of such awards must match that of awards for pure research.
- Augment the NSA Center of Academic Excellence program: Build educational capacity by leveraging the existing CAE program to have each CAE institution partner with high schools, community colleges, and liberal arts colleges. The CAE program has been criticized as not providing a vehicle for real leadership in moving cyber security forward, but rather serving only as an accreditation program.
- High school pilot program: Work with the Department of Education and local school boards to create a nationwide pilot program in information security curriculum at the high school level. We risk prematurely turning away talented young adults who would benefit from cyber-security training. It is precisely at this point in time that young adults are choosing career paths, and it is here where we can attract them to the broad array of information assurance, privacy, and security problems that exist in the very technology they use on a daily basis: social networking; mobile phones, gaming devices, and embedded devices; email and instant messenger software, and so forth. The wide variety of interesting problems in this space should serve as a draw even for students who don’t think of themselves as computer or math geeks.
- Reach out to the hacker community: Fund workshops for educators to bridge the gap between white hat hackers and the typical academic who has an interest in information security, but little available resources or guidance. Although most ethical hackers have a healthy skepticism about the assurances of security from vendors, they also have a principled, responsible approach to identifying flaws in systems. This segment of the computing community has many valuable things to teach us, as Communications has previously recognized with a special issue.
- Dramatically grow university security expertise: Endow a significant number of National Information Security Scholar Chairs at public and
private universities and colleges. Removing the burden of allocating a tenure line in uncertain economic times would have a multiplicative impact on the amount and quality of cybersecurity education available around the U.S.

We realize that some might argue with these specific recommendations and have others to suggest. We hope the efforts we have listed here stimulate enough discussion to create meaningful, effective, and significant changes in both the quality and scale of cybersecurity education in the U.S. We believe there is a fundamental discrepancy between the expectations of users and employers (including the government) and the reality of a scarce work force and underdeveloped educational mechanism.

Cybersecurity presents a difficult and important challenge because the fight is fundamentally unbalanced: an attacker need only find a single weakness, whereas a defender must scramble to protect everything. If the U.S. cannot produce highly competent defenders of its military, civilian, financial, energy, health care, and transportation information systems, then it will cease to be a meaningful international presence.

References

Michael E. Locasto (locasto@ucalgary.ca) is an assistant professor of computer science at the University of Calgary, Alberta, Canada.

Anup K. Ghosh (aghosh1@gmu.edu) is the chief scientist in the Center for Secure Information Systems at George Mason University in Fairfax, VA.

Sushil Jajodia (jajodia@gmu.edu) is the director of the Center for Secure Information Systems at George Mason University in Fairfax, VA.

Angelos Stavrou (astavrou@gmu.edu) is an assistant professor in the Department of Computer Science at George Mason University in Fairfax, VA.

Copyright held by author.