Addressing the US Cybersecurity Workforce Demand

Computing is a fundamental part of our daily lives. Our energy grid, national defense, finance and healthcare are just a few examples of systems that depend on computing. With the growth of the Internet of Things, our homes, cars, appliances, phones, and children's toys all depend on technology. Both adults and children are exposed to cyber threats, and must be computer and cyber aware at increasingly younger ages. Attacks on these systems continue to grow in sophistication and frequency. Addressing these threats requires developing a larger cybersecurity workforce within the US. And we must start building this foundation in our K-12 system when youth are first exposed to both the advantages and threats from technology.

Filling the Pipeline

The role and significance of computing has increased in society and the economy, yet students often do not have access to high-quality quality IT and computer science education. Although 69% of 7-12 students report that computer science is taught in their school, only 21% of these schools offer an Advanced Placement course[1].

Because of the unique role cybersecurity specialists play in our country's security, the most sensitive jobs in this field must be filled by US citizens. And it's clear we are not producing enough highly skilled security specialists to address our growing cybersecurity needs. According to the Bureau of Labor and Statistics, in 2014 there were 82,900 Information Security Analyst jobs nationwide, and there was an expectation for this to grow by 18% over the next decade[2]. Equally dramatic, the number of Software Developers was expected to grow from 1,114,000 in 2014 to 1,300,000 in 2024[3].

Cybersecurity cuts across many domains of study, but one focus area is computer science. The number of US computer science bachelor's degrees being awarded peaked in 2003-04 at almost 60,000, fell by over a third by 2008-9 and is only now beginning to approach a similar level[4]. Expanding access to K-12 computer science will help build the interest in computer science degrees, which will help meet the specialized needs of the cybersecurity workforce needs in the long run. As our overall pipeline of diverse students in the US interested in and willing to study computer science in higher education expands, so will the potential pool of students specializing in the technical aspects of cybersecurity.

K- 12 Cybersecurity and Computer Science Synergy

Cybersecurity is an important component of computer science. Principles such as process isolation, resource encapsulation, domain separation, least privilege, modularity, simplicity, minimization, and layering are concepts that are necessary for security to be achieved. Principles such as these should be taught when computer science is taught, because they matter to computer science in general, not just cybersecurity. Therefore, cybersecurity concepts should be embedded within all K-12 computer science initiatives, such as the refresh of the new Computer Science Standards, refresh of the AP Computer Science coursework, development of the Computing Science Framework, and implementation of the Computer Science for All initiative. However, it should be noted that cybersecurity is not restricted to computer science. There are other disciplines, such as mathematics, engineering, business and others where cybersecurity concepts must also be incorporated.

[1] https://services.google.com/fh/files/misc/searching-for-computer-science_report.pdf

[2] http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[3] http://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm

[4] http://nces.ed.gov/programs/digest/d15/tables/dt15_322.10.asp?current=yes