Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 16, 2017

Challenges in Cybersecurity Education and Workforce Development

Introduction

Increasing awareness of cyberattacks—and the increasing connectedness of cyber and cyberphysical systems—have led to concerns about whether U.S. homes, businesses, and government are prepared to secure themselves in a digitally integrated world. One of the most frequently raised concerns pertains to the sufficiency of cybersecurity education, training, and workforce development in the United States. Federal policymakers have raised questions about the quality and quantity of U.S. postsecondary education graduates with cybersecurity credentials (in general) and have raised concerns about the civilian and military workforce needs of the federal government (in particular).

A number of federal programs across several agencies have been implemented in an attempt to address what many believe to be a nationwide skill shortage in the public and private cybersecurity workforces. Some of these programs have focused on offering education benefits, such as scholarships or specific training, as a tool for attracting cybersecurity workers. Others have focused on enhancing or certifying the quality of cybersecurity education programs, or on expanding interest in cybersecurity careers among youths.

Challenges

There is a widespread general perception that a shortage of qualified and highly skilled cybersecurity personnel exists in the United States and abroad. This perception is supported by results from the 2017 Global Information Security Workforce Study (GISWS), which predicts a worldwide shortage of 1.8 million cybersecurity professionals by 2022.

A broad consensus exists over the need to train and hire cybersecurity professionals in response to increased threats of cyberattacks; however, whether or not this need constitutes a shortage is debated by various researchers and stakeholders. For example, the 2015 study "Hackers Wanted" carried out by the RAND Corporation suggests that existing federal initiatives, combined with natural market forces, are sufficient to supply the necessary quantity and quality of cybersecurity workers for the public and private sectors in coming years.

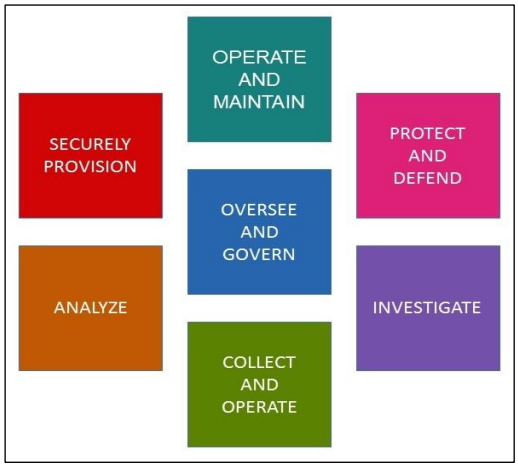
A number of challenges exist in successfully hiring and retaining cybersecurity professionals. This is especially true in the federal government, where often cited concerns include the rigidity of the federal pay scales, higher salaries for comparable jobs in the private sector, time-consuming and opaque hiring processes, and identifying and articulating the full range of cybersecurity positions and needed skillsets across the government. General challenges in the training of cybersecurity workers include the rapidly changing nature of the cybersecurity field and the need to continually maintain and enhance the skill levels of incumbent workers within the field.

Private employers and federal agencies have experienced difficulty in identifying the specific skills and types of positions required to successfully protect their systems from cyberattacks. In response to this, the National Initiative for Cybersecurity Education (NICE), authorized by the Cybersecurity Enhancement Act of 2014, created the NICE Cybersecurity Workforce Framework. The purpose of the framework is to develop a "common language" (for private industry, government, and academia) that both categorizes cybersecurity jobs and describes the knowledge, skills, and abilities necessary to perform them successfully.

In particular, the NICE Cybersecurity Workforce Framework created a high-level grouping of common cybersecurity functions into seven categories that are shown in **Figure 1**. This organizing structure is based on extensive job analyses and groups together work and workers that share common major functions, regardless of job titles or other occupational terms. These seven categories are further subdivided into specialty areas and work roles that more precisely define the specific knowledge, skills, and abilities required to perform cybersecurity tasks.

According to the 2017 GISWS, approximately 30% of the cybersecurity professionals responding to the survey stated that their organizations have partially or fully adopted the NICE Cybersecurity Workforce Framework and used it to match skills and content between training and employment.

Figure 1. Cybersecurity Work Categories Under the NICE Cybersecurity Workforce Framework



Source: National Initiative for Cybersecurity Education (NICE), http://csrc.nist.gov/nice/framework/.

Another challenge commonly faced by employers in both the private sector and the federal government is worker retention. The respondents to the 2017 GISWS identified the following as the employer initiatives most important to the retention of cybersecurity professionals:

- offering training programs,
- paying for professional security certification expenses,
- improving compensation packages, and
- offering flexible work schedules.

Selected Federal Cybersecurity Education Initiatives

The federal effort in cybersecurity education, training, and workforce development, though still nascent compared to federal investments in other educational sectors, spans all stages of education and types of learners. This includes children and teachers in elementary and secondary schools, students and faculty at the postsecondary education level, and incumbent workers in both the federal and private workforces. Federally supported programs in cybersecurity training include activities such as scholarship and grant programs, summer camps and academic competitions, and research on teaching and learning in cybersecurity fields.

The following sections of this InFocus provide an overview of selected high-profile programs that are broadly illustrative of the primary approaches taken by federal initiatives in cybersecurity education and training. This is not a complete list of federal efforts in these areas. A number of federal agencies, including the Department of Defense (DOD), the Department of Energy (DOE), the Department of Homeland Security (DHS), the Department of Labor (DOL), the National Science Foundation (NSF), and the National Security Agency (NSA) host agency-specific programs and activities in cybersecurity education, training, and workforce development.

National Centers of Academic Excellence in Cyber Defense

A joint effort of the NSA and DHS, the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program accredits cybersecurity education programs at selected institutions of higher education (IHEs). To obtain CAE-CD accreditation, an IHE must demonstrate that its cybersecurity education program has met certain criteria and maps "curricula to a core set of cyber defense knowledge." There are currently over 200 CAE-CD designated institutions across the United States.

CyberCorps: Scholarship for Service

The NSF's CyberCorps: Scholarship for Service (SFS) program is a primary source of dedicated federal funding for scholarships to undergraduate and graduate students in cybersecurity-related majors. In addition to CyberCorps scholarships, SFS program funding may be awarded to IHEs for capacity building purposes (e.g., institutional development) in cybersecurity education. As the name implies, the CyberCorps scholarship requires a service commitment of participants. Students who receive an award must agree to work for a federal agency—or state, local, tribal, or territorial government—for a period equal to the length of time they received scholarship support. Data provided to CRS by the NSF in December 2016 indicated that the placement rate for CyberCorps graduates is 94% and that total placement since 2002 is 1,980 graduates.

CyberPatriot

Partnering with the private sector and academia, DHS and DOD help cosponsor the Air Force Association's (AFA) CyberPatriot program. The program focuses on middle and high school students and has three main components: (1) the National Youth Cyber Defense Competition, (2) AFA CyberCamps, and (3) the Elementary School Cyber Education Initiative.

The National Youth Cyber Defense Competition is the longest-running CyberPatriot program activity. It began as a competition between seven teams in 2009. In 2015-2016, the competition field included 3,379 registered teams (comprised of middle or high school students). During the competition, teams are tasked with managing the network of a small company and must find cybersecurity vulnerabilities while maintaining critical services. Northup-Grumman Corporation has provided scholarships to members of the top three teams since 2011.

National Collegiate Cyber Defense Competition

Partnering with the private sector and academia, the NSA, DHS, and the Departments of the Navy and the Army help cosponsor the National Collegiate Cyber Defense Competition (CCDC). The CCDC was launched in 2005 as a college-level cyber competition focusing on the operational aspects of managing and protecting an existing network infrastructure. The competition is regionally organized. Finalist teams compete for a national championship. According to a press release on the Raytheon website (Raytheon was the main sponsor in 2017), teams from more than 230 IHEs participated in the 2017 competition.

GenCyber

The GenCyber program sponsors cybersecurity-focused summer camps for students and teachers throughout the United States. Program goals include increasing interest in cybersecurity careers, helping students practice safe online behaviors and understand the foundational principles of cybersecurity, and improving teaching methods for the cybersecurity content in the computer science curricula of elementary and secondary schools. GenCyber is jointly funded by the NSA and NSF. A 2015 NSF press release notes that in that year, 29 universities in 19 states hosted 43 camps serving 1,400 participants (half of whom were female).

Boris Granovskiy, Analyst in Education Policy

IF10654

Disclaimer