Agencies Plan New Strategies to Train Cybersecurity Workforce

As a global shortage of cybersecurity professionals grows, the government looks to expand pool of applicants.

James Mersol

Thu, 03/21/2019 - 17:13

Leo Wolfert/iStock

One of the biggest challenges in improving cybersecurity for the federal government is hiring information security professionals, which agencies are determined to combat.

Based on the Center for Cyber Safety and Education's 2017 Global Information Security Workforce Study – the most recent survey conducted – nearly two-thirds of employers have had difficulty finding qualified information security professionals, even as 70 percent of companies plan on expanding their cybersecurity teams. Without a new approach to training, hiring and retaining information security professionals, the survey predicted that there will be a shortage of approximately 1.8 million cybersecurity professionals in the next five years.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency are examining paths to train people who are making a career shift to cybersecurity.

One way the agencies are doing so is through workshops for those interested in the field. "It's important to maintain that love for STEM and excitement about technology in everyone," said Deborah Frincke, research director for the NSA, during the DHS Science & Technology Cybersecurity and Innovation Showcase Tuesday. "Diversity of perspective is key to success."

The current length of time that it takes for someone to obtain a security clearance presents another hurdle for government agencies looking to hire new cybersecurity professionals. As of late 2018, the average Top Secret security clearance took 459 days to process.

"We need to rethink how to hire those who take longer to get through that process," Frincke said, noting that first-generation immigrants' clearances are often delayed even longer as investigators examine their connections abroad. She recommended starting new employees in internships or positions where they could work on unclassified material as a remedy.

"It comes down to expanding the pipeline," said Martin Gross, speaking at the showcase for the Office of Cybersecurity and Communications at CISA. "We need to streamline the process so we can hire people right away," rather than allowing positions to remain unfilled for a year or longer.

Additionally, Gross suggested that the government needed to look beyond those with science and engineering degrees, seeking out those with basic skills in coding. The 2017 survey indicated that 87 percent of cybersecurity professionals began their careers in a different field, but 90 percent of hiring managers consider experience in cybersecurity to be an important consideration. Once they've been tested for basic knowledge, the government could develop those skills through a training program, qualifying them for cybersecurity positions in government and the private sector.

The Next Generation

DHS is also examining ways to begin cybersecurity education in grade school. Brian Gattoni, chief technology officer for CISA, said he was amazed by the level of innovation he saw at high school science fairs, from one student who showed how long it takes to break passwords of different strengths to another who had reconfigured an Amazon Dash button to send a message to his parents letting them know he was safe in the event of an active shooter or other emergency at school.

"We need to find a way to tap into their expertise," Gattoni said.

Alan Paller, founder of the SANS Institute, highlighted that a key problem has been training "elites," professionals with both the skills and the aptitudes to innovate in the cybersecurity field rather than simply operate or test existing tools.

At the showcase Tuesday, Paller highlighted the United Kingdom's Cyber Discovery Program, a series of exercises designed to identify and train not only those with the skills knowledge, but also those with the "cybermetrics" – the characteristics of information security innovators – needed to become elite professionals in the field.

Those who scored highly in the interactive exercise were invited to take part in Cyberstart Essentials, a series of hands-on online training modules designed to teach students the fundamentals of computer science. The goal was to find 600 talented specialists at the elite level in the next four years, said Paller. The U.K. program found 700 in six months and are adjusting future targets based on those results.

Starting March 20, SANS and the National Governors Association will launch two pilot programs based on the Cyber Discovery Program in 27 states. The first, Girls Go CyberStart — for high school girls interested in cybersecurity — will offer three series of challenges where students can compete to earn money for their schools as well as college scholarships. The second, Cyber FastTrack — for college students who want to pursue a career in cybersecurity — will follow the same model, offering scholarships to cybersecurity programs to high-scoring students.

A similar program, CyberPatriot, began in 2009 and has yielded impressive results, especially as it expanded beyond its original JROTC focus and extended to students from high school down to elementary school.

“I’m excited about the opportunities these kids will have,” said Timothy Amerson, director of cybersecurity management in the Office of Information Technology for the Department of Veterans Affairs. Amerson, who began coaching a high school CyberPatriot team four years ago, said several of his students have received full scholarships to pursue STEM majors in college, including some who changed their plans for college and their career after participating in CyberPatriot.

Amerson’s experience is not unique – as of 2017, 77 percent of CyberPatriot students have gone on to pursue college degrees in STEM. This year, 6,387 teams participated in the CyberPatriot challenge, where students conducted practical exercises in network security.

“CyberPatriot has given me an opportunity to look forward to my future,” said one participant. “As a young woman especially, I feel like there are many opportunities for me to succeed in the cyber field and I am beyond excited to work hard and earn my way to the top.”

View printer friendly version
Federal Cybersecurity
Department of Homeland Security
Federal Workforce
training
Standard