Cybersecurity Leaders Discuss New Strategies to Narrow the Growing Workforce Gap

'Aptitude' is among government's top focus for potential recruits.

James Mersol
Thu, 11/21/2019 - 13:05

Earlier this year, a study on the workforce gap in cybersecurity estimated that shortage to be “2.93 million unfilled cybersecurity positions worldwide.” The most recent study published this month from the International Information System Security Certification Consortium, known as (ISC)2, indicates that gap has grown, now totaling 4.07 million unfilled positions — an estimated 500,000 of which are in the U.S. The lack of skilled or experienced cybersecurity personnel was again cited as the top job concern for the 3,237 cybersecurity professionals surveyed.
Job satisfaction, however, for those within the cybersecurity field is high, with 66% of survey respondents saying they were “somewhat satisfied” or “very satisfied” with their job. Moreover, most view their job as part of a long-term career — 65% of respondents said they “intend to work in cybersecurity for the rest of their careers.”

While retention cannot be ignored entirely — if nothing else, cybersecurity training must be ongoing to reflect the nature of continually-evolving threats — some recommend focusing on the hiring pipeline. The federal IT sector has an aging workforce, and the gap may widen further if there is no strategy to increase the replacement rate for retiring employees. Some agencies view this situation as a three-pronged issue: agencies need to find ways to attract more to entry-level positions straight out of college; encourage employees under 30 to develop their careers, even if that means a stint in the private sector; and efficiently onboard mid-career professionals in senior-level roles in cybersecurity.

The Entry-Level Strategy

One area of workforce recruitment that needs improvement is hiring entry-level cybersecurity professionals from college programs and then attracting them to the public sector.

“How do you pitch working in a cleared environment to a college student?” asked Jonathan Lee, deputy chief of risk management for the National Geospatial-Intelligence Agency, at the Defense One Cyber Summit Nov. 19. He suggested that the gap between public-sector and private-sector salaries is only half of the problem. The other is the culture; public-sector jobs lack many of the office perks Silicon Valley companies offer, and working in a secure facility means leaving your smartphone in your car and using the agency’s computers, which are unlikely to be cutting-edge systems. College students, especially those who have not been planning for a cybersecurity career in the public sector, prove difficult to sway.

One strategy Lee gave was to offer students a job opportunity that doesn’t carry a life-long career commitment. If they’re offered a contract to work for the government for a few years, he said, and they receive training along the way, even if they opt to work for the private sector, that increases the overall amount of cybersecurity talent in the U.S.
“The challenge that we see is the long-term pipeline issue,” said Jim Cook, vice president of strategic engagement and partnerships at MITRE. “Not just looking at existing pipelines and how to extend them, but also new pathways and even new sources of talent.”

Another strategy is to change the way agencies describe job roles.

“Universities are getting really good at this — they’re changing the conversation away from the job and more to the problem,” said Cook.

Technical job requirements are important, but “wanting to do good,” such as securing medical devices and countering disinformation, is a powerful incentive to many students, he explained.

The opportunity to increase talent nationwide is one of the driving factors behind the Cyber Talent Initiative, a partnership between several federal agencies, including the departments of Veterans Affairs, Health and Human Services, Homeland Security and Defense, as well as the FBI, private-sector firms including MasterCard and Microsoft, and CyberVista as a technical partner. The Cyber Talent Initiative encourages students in a cybersecurity-related major to apply. If selected, they will be placed in a cybersecurity position with one of the partner agencies for two years. If they complete their rotation with the agency, they can apply for a job with the private-sector partners. Once employed, they will receive $75,000 in student-loan assistance.

“[We're looking for] the engineering mindset in a liberal arts major brain,” explained Simone Petrella, CEO of CyberVista, in an interview Nov. 1.

Applicants are assessed not on their cybersecurity coursework, she said, as few will have received formal training as part of their program, but on their aptitudes and interests. The ideal cohort will be made up of recent graduates that have a demonstrated interest in keeping up with the fast-paced evolution of threats and security practices, a history of following cyber hygiene practices themselves and an ability to answer “theoretical questions” about cybersecurity that indicate their ability to quickly respond to incidents once they are trained practitioners.
The program address three challenges: student loan debt, the cybersecurity workforce gap, and the financial losses both public- and private-sector enterprises incur from breaches. The goal is to “identify alternative sources of talent” to the traditional pipeline of engineers and data scientists that go into cybersecurity roles, Petrella said. The program also flips the traditional school of thought on its head — a lot of agencies and companies do not know exactly what cybersecurity roles they need to fill; instead, CyberVista has asked them what they’re looking to accomplish and has tailored the positions accordingly.

The FBI has taken a similar approach in filling its cybersecurity needs, recognizing the mission required more than a standalone cybersecurity division.

“Our focus over the past few years has been defining what we really mean by the cyber workforce,” said Tonya Ugoretz, deputy assistant director of the Cyber Readiness, Outreach, and Intelligence Branch of the FBI. “As you might imagine, there’s rarely a type of crime that we investigate that doesn’t have some sort of digital or cyber component.”

Her office has coordinated not only staffing the Cyber Division, which focuses on cyber intrusions, but also providing “data analysts, digital operations specialists, computer scientists, [and] IT specialists” to join teams both at FBI headquarters and in field offices around the nation.

“Some of the people in [our] hiring pool have cybersecurity-related skills, but many will not,” she said. “We’re employing aptitude testing among our new hires to see who among that pool ... might have the aptitude and the capability to have a cyber-focused career.” This testing allows the FBI to identify new employees who might be able to train to fill the gaps within the agency.

Data suggests the approach of identifying aptitudes and training those with the interest in cybersecurity has been a historically effective approach. The (ISC)2 Cybersecurity Workforce Study reports that 56% of respondents intended to work in cybersecurity, while only 42% started their careers in the field. Moreover, those who have the aptitudes and interest in cybersecurity stay in that career, as indicated by the earlier data showing that 65% of cybersecurity professionals intend to stay in the field for the rest of their career.
Hiring at All Levels

As junior cybersecurity employees take time to work up to more advanced positions, agencies are also exploring new hiring methods to court experienced cybersecurity professionals.

“We’re pivoting from a very passive recruitment approach,” said Travis Hoadley, senior advisor to the chief human capital officer at the Department of Homeland Security. “Most of the federal government tends to post jobs and hope that the right person will apply [and] make it through that process ... Waiting for the right person to click USAJobs is not really enough. We’re focused on trying to target cyber talent where we think that talent is, including individuals who are experienced professionals.”

As the agency with the highest number of cybersecurity positions, DHS received special congressional authority in 2014 to create the Cyber Talent Management System, a new platform for hiring these roles. The authority has empowered the agency to develop a process for hiring cybersecurity professionals influenced in large part by how the private sector hires the same talent.

“We’ve taken a step back and said that we think cybersecurity as a mission space represents the type of challenge where we can’t really replicate a system from the middle of the 20th century,” Hoadley said, which was the impetus to move away from traditional titles and classifications for government positions. “We’ve thought very hard about what the private sector is currently doing in terms of recruiting and retaining cybersecurity talent. We’ve also looked at all of the federal personnel transformations since the 70s for lessons learned.”

The project represents a transformation of how DHS thinks about roles in civil service and has already begun to more closely match cybersecurity professionals to positions that suit them.

“We’re taking a hard look at how long we want individuals to be on board, what type of work we want them to contribute to the mission, and how we measure that,” Hoadley explained.
Challenges For All

While these strategies should help to close the workforce gap in the public sector, they also need to coordinate on innovative solutions to recruiting talent, especially in the long term.

“I see so many pockets of innovation,” Cook said, referring to efforts like the Cyber Reskilling Academy, which is currently training its second cohort. “But there needs to be some coordination. The more diffuse it is, the less effective it is. It’s challenging for the agencies that we work with to have their finger on the pulse of everything that’s going on.”

“Coordination is the keyword,” Hoadley agreed. “I’m not sure that a singular strategy will work for every agency in this space — I think there are some differences in terms of work and mission orientation, depending on which department we’re talking about — but I think there are some common things that should be organized around, and there should be better information sharing.” Some of those common threads, he said, include the onboarding process and the “pre-hiring stage” including assessment and background investigations.

"I think aptitude might be a space where agencies can collaborate," he said. "It’s not really about the specificity of work, but the common skills that might be useful across the federal space.”