Finding a talented cybersecurity workforce is a continuing challenge

Cybersecurity and the challenges in finding a talented workforce to fill thousands of positions is a continuing problem. There's debate on the qualifications to fill these roles — whether that's a four-year degree, certifications, years of experience or even on-the-job training.

Alex Orfinger, market president and publisher of the Washington Business Journal, recently spoke with cybersecurity experts to dive deeper into the workforce problem. The discussion was sponsored by the George Washington University College of Professional Studies, which offers an array of cybersecurity programs from workforce development to bachelor's and master's degrees as well as executive education. Panelists represented a cross-section of industry sectors to include enterprise, government, and academia.

Participants included Liesl Riddle, Dean, George Washington University College of Professional Studies; Connie Uthoff, Director, Cybersecurity Strategy and Information Management Master's Program, George Washington University College of Professional Studies; Scott Smith, Government & Public Sector Cyber Lead, Ernst & Young (EY); Mike Baker, IT CISO, DXC Technology; P.J. Ross, CFO, HITT Contracting; Andrew Kim, Civilian Cyber Lead & Cyber Strategy Lead, Accenture Federal Services; Dr. Pape Cisse, Former CIO AmeriCorps; Peter Romness, Cybersecurity Principal, CISO Advisor's Office, Cisco.

Following are excerpts from the discussion, which have been edited for publication.

Orfinger: What you are looking for when recruiting people at all levels?

CISSE: Along with the technology, there's a critical human piece — training, education certification, expertise, experience. You're trying to hire people with different expertise levels from the privacy, technology, policy and operations sides. But there are restrictions because the core, especially in metro Washington, is small. The pool is so small because there's not enough people from the education pool we can draw from, because all the entry level positions require four years of experience. You get four years of college, but it's not experience, it's education. It's theoretical, without having a practical aspect.

KIM: I agree soft skills are critically important, especially if you want to cultivate someone over the longer term. But in the consulting industry, especially when you have government clients, you're beholden to contract requirements. You can't just look at someone who has the best soft skills. We're often held to requirements, like this person needs this certification, this new person needs X years of skills in a certain technology.

Orfinger: How can Washington have a shortage of staff versus the rest of the country?

ROMNESS: There's 750,000 open jobs in the US right now.

BAKER: We've had very low unemployment in this area for a while now. There's a lot of opportunities to choose from, so there's a bigger talent gap here. As an employer, I look for soft skills and the intangibles. I look for hunger and passion. I don't necessarily look for technical stuff but that depends on the role. We need to invest in cyber apprenticeship models. We need the patience to hire people and train them for two to five years to really mature their skills. I feel we have an opportunity gap over a skills gap. We have a lot of people that want to break in, but a lot of people try to hire only specific unicorn candidates to fill positions for a current need. We need to realize we probably can't fill that. We owe it to the workforce and industry to train people from the ground up.

ROMNESS: It's not necessarily their STEM skills, it's also their people skills. Creativity and problem solving is huge. You can train somebody on a tool, but you can't train them to be inquisitive or to be able to solve problems. We've started working with early in the career of up-and-coming CISOs and offer them leadership development classes so they can learn how to talk to the board, identify their goals, develop their mission statement and manage people better by looking for clues in their personality. It highlights the fact that cybersecurity leadership is not only technical anymore. It's people skills, but you must have the technical chops.

ROSS: I like to hire people who are curious, who see a challenge and want to get to the root cause. When you ask somebody for a piece of information, they don't just give you exactly what you ask for, they go that extra step to figure out what the real problem is.

Orfinger: What's the retention strategy?

BAKER: We have a flexible, virtual work environment. We have a lot of opportunities to take greater responsibility in your job because we embrace an agile opportunity-led environment that is based on outcomes. However, the meaning of opportunity is different for each individual, so we really lean in to understand that for each employee.

Orfinger: How important are credentials? A four-year career?

KIM: At a recent cyber workforce seminar, most speakers advocated for skills-based hiring over education or certification requirements. But there's a lag. Credentials therefore remain critically important to get the people you need for government support.

RIDDLE: That's why in our curriculum, I would much rather design a program where you could get the base skills and have them do actual practice work for credit. Have them toggle between learning and applying it on the job for six months in an organization. It would give employers a chance to try on talent, because you could always turn that co-op student into an FTE and they can still finish their program at night.

BAKER: When you bring in a good IT talent into cyber, it's an amazing crossover and magic happens. They can thrive in that environment given the proper support. I'm looking for hunger for that opportunity. Certifications are great, but they're not everything everyone makes them out to be. The ability for someone, on their own time, to get certifications is indicative of the curiosity I'm looking for, but the certification itself doesn't mean they'll be successful in the role.

ROSS: The certifications, college experience and the degree shows the ability to learn and put effort in and finish something. There's definitely value in it, but I don't know if it always matches the full price tag and not every position requires it. We've created a similar program where we have people who want experience in the construction industry. College might not be an option for them or might not have been their first choice. We have a new program that allows people to learn while they earn. They're paid for 40 hours a week. They work on the job site 24 hours and spend the other 16 hours studying and doing their schoolwork. They're pursuing an associate's degree but are paid full time.

KIM: We're pursuing a program focused on entry level applicants called Cyber Million. We've partnered with Immersive Labs, a cyber training platform, to offer a skills-based interview format where people looking for entry level jobs, regardless of their experience, can take a series of labs - if they get through those labs, the platform provides access to relevant job opportunities. The goal of this program is to help fill more than one million cyber jobs in the next decade.

SMITH: When it comes to the ongoing challenge of building a cyber workforce, we need to recognize that there is a talent shortage and take the responsibility to train our teams. We can do this by creating cyber-specific 'bootcamps' focused on cyber competency areas like identity and access management or the risk management framework. For this to work at scale, we need to partner with the government to focus on cyber outcomes as opposed to specific role descriptions. In cases when specific labor categories are required, we need to expand the description to account for different experiences and backgrounds. In addition, we also need to open the recruiting aperture and tap into different groups of talent, which includes the veteran community and neurodiverse candidates.

UTHOFF: At the RSA conference, the CEO of RSA mentioned that AI is probably going to change cybersecurity work, the jobs people do and how they do them. We are talking about training people for today's cybersecurity roles, but we also need to prepare people for new jobs as they evolve. As AI shifts cybersecurity jobs, we need to consider how to prepare the workforce. There are a lot of unknowns right now.

BAKER: AI is going to provide amazing opportunities for our field. We will be able to put someone with no coding skills directly into a technical role like threat hunting. All you need is an inquisitive mind, a person that works great on a team, good soft skills, but you wont necessarily need the technical coding skills. Generative AI will be the coding language of the future, and we have that now. When this hits, it's going to offer a lot more opportunities to bring people rapidly into the field.

ROMNESS: We're building AI into our tools. Right now, you can program your network using normal language. A network manager can say 'please allow access for this person to these resources' and the built-in AI will do it for you. We are using AI and automation to upscale the job of a defender. We're prioritizing threats and correlating events. That first-level defender is now a second- or third-level person.

Orfinger: There's a lot of vacancies in a lot of industries in Greater Washington. What is the overall game plan for filling these vacancies?

UTHOFF: The National Cybersecurity Workforce and Education Strategy is being implemented to address cybersecurity workforce needs. The Department of Defense also updated and released their cybersecurity workforce strategy, which includes new AI specializations. And at the College of Professional Studies, our cybersecurity boot camp, bachelor's, and master's programs aim to strengthen the cyber workforce.

ROMNESS: We, and many of our competitors, are providing curriculum. Ours is called Network Academy, which concludes with a certification. It includes classes that start in middle and high schools and continue into community colleges and universities. Google also has a program that provides certifications. We've trained over 10 million people around the world. As part of the presidential incentive, we've committed to training a large number of people - much of that is providing curriculum, tests and certifications.

ROSS: I wonder what percentage of those open positions will be filled by Mike's team, which will result in other open positions. You take 250,000 open positions, fill them with 250,000 people in the workforce and you still have 250,000 open positions, which is where you're looking to fill with junior analysts and junior associates.

Orfinger: We're recruiting all these people, but at the same time, somebody like HITT is also recruiting from the same group. There's a limited number of people.

CISSE: There may be a need for a feeder program, a cybercorps, to train across all needs, both private and public, and still offer the credentials and the choice, for instance, do they want to stay technical, or do they want the managerial and policy side? Or do they want to create the things we can't think about today, but would be needed in 10 or 15 years? How do you create that pipeline? Part of that conversation starts through STEM. How do you create a space where academia, private industry and local and federal government are harnessing that?

Orfinger: I hear a lot of optimism that we're on the path to solve this challenge. How are you feeling good about?

BAKER: Here's why I'm positive cyber is attracting more talent than ever. People want to get into it. It's a great time to be in cyber to learn a lot of cool stuff and work on hard problems to are growing exponentially. We're at or should be a boardroom concern now pretty much universally across companies. In general, the discipline has been significantly elevated over the last couple of years so we are attracting a lot of new and diverse talent.

RIDDLE: We've been talking about the cyber workforce and how we can fill the numbers gap. But there was no conversation here about finding a diverse workforce. When speaking about cybersecurity, people usually mention this issue of the lack of diversity within the industry.

ROMNESS: That's part of the reason it's important to think of cybersecurity as not just a STEM issue. There are a lot of disciplines in cybersecurity and hopefully we'll get more women into STEM. I'm pretty sure each of our companies has programs to do that. If you diversify what you're looking for, you get a more diverse pool.

KIM: It can't be solved overnight. Why aren't we thinking about cybersecurity as a subject that's included in elementary school education? People talk about personal finance as something that needs to be instilled early, I think cybersecurity should be too. In terms of diversity, it's important to generate interest at an early age.

BAKER: It goes back to the opportunity led perspective. If you have tunnel vision for a minute skillset right now you will only be hiring for that specific problem. If you open your aperture and allow growth in the role, there is a diverse candidate pool that is hungry and ready to become the next industry leaders.

UTHOFF: Yes, while there may be immediate tactical challenges related to filling workforce gaps, there are also strategic, long-term requirements that need to be considered.

The George Washington University College of Professional Studies is an accelerator for career transformation in cybersecurity. To learn more, go to: https://cps.gwu.edu/cybersecurity.