Hiding in plain sight — 4 places to find cybersecurity talent in your own organization

radware.com/newsevents/mediacoverage/2017/cyber-security-talent-in-your-own-organization

Simeon Holloway wanted to parlay his 13 years of IT experience into a cybersecurity position. He thought that it would be a relatively easy transition considering the global shortage of cybersecurity professionals and his eagerness to learn.

The information security department at the federal agency where he worked in Atlanta was an obvious place to start. Perhaps he could shadow a security professional there or fill an empty position and learn on the job, he thought. But the reception he received was cooler than he had expected.

“I consulted and got advice from them. I applied for some positions there, but it just didn’t pan out,” says Holloway, who applied for jobs as an IT specialist in infosec and as a cybersecurity engineer. “I think my lack of experience and a CISSP certification” had something to do with being turned down, he says. “They wanted experience with reporting and conducting risk assessments.”

His experience thus far had focused on network and desktop support, and systems administration. Holloway went on to get certifications and training on his own, studying nights and weekends, and later he left the agency and is now an information assurance analyst for the Georgia Lottery.

For Holloway’s former employer – perhaps an opportunity lost.

Companies are scrambling to fill cybersecurity positions. Some 41 percent of CIOs surveyed by recruiting firm Robert Half Technology say that cybersecurity skills are in the greatest demand in their organizations. The non-profit organization (ISC)2, which provides information security education and certifications, predicts a worldwide shortfall of 1.8 million cybersecurity workers by 2022, 20 percent more than was predicted in 2015.

Complicating the talent search further, many organizations are shooting beyond the stars in their job requirements – demanding that candidates have levels of security experience, education or broad skill sets that are exceedingly hard to find in one mere mortal, according to Gartner. How many people really have eight to 10 years of solid cybersecurity experience?

As a result, organizations are missing opportunities to cultivate inside talent who may lack experience but already know the business and have the fundamental skills to succeed in cybersecurity.

Of course, cybersecurity experience and expertise are required in management positions – but 27 percent of security experts surveyed in Radware's latest global security report say that a shortage of manpower is their biggest obstacle in countering cyber attacks.

"It's about being a little more realistic about the availability of talent in the marketplace," says Mark Coleman, research director at Gartner. "You don't have to create perfection. What we need is a huge number of people that are a good deal better than they are today." By looking at cybersecurity positions through a new lens, he says, companies can find budding cyber pros in their own organizations.

First, lower expectations

Organizations have become overly ambitious in their job descriptions that profile the ideal candidate, Coleman says. Companies must "free up your demands, talk to your HR department and unplug some of the requirements, such as [requiring] a degree in computer science or x number of years of information security experience," Coleman says. Alternatively, "take a look at people in the process of achieving qualifications," he says.

To fill cybersecurity positions, "You have to be creative and find some good folks who are willing to learn," says John Masserini, CISO at MIAX Options Exchange. IT workers at the equity derivatives market who want to make the jump to security got a leg up recently when the information security department modified some of its requirements for security experience from "mandatory" to "desired." This gave IT staff a chance to apply for the roles, and then be trained in the desired or missing skills.

"Bringing a Unix admin onboard and getting them up to speed on the security side might be a whole lot easier than holding out for someone with a couple years of security experience," Masserini says.

Another benefit -- "Those folks who want to make the jump can understand how their day-to-day responsibilities work right now, and how they can apply them to the security side. We've definitely seen an increase in the number of resumes and potential candidates," though he wouldn't reveal how many resumes he's received from inside candidates.

Mid- and late- career employees

"There are many mid- and late-career IT pros who are not considered for redevelopment into cyber roles simply because they've been around too long," Coleman says. In reality, their depth and breadth of experience could translate well into a security role.

One IT veteran, who did not want to be identified, says, "I have been in IT for 30 years and cybersecurity in various capacities for about 20 of those years. I find now that IT has become very siloed, almost impossible for IT folks to progress up to learn new skills. There may be a

shortage of cybersecurity professionals, but what could businesses be doing differently to promote from within providing a path for those interested and help to fill the void?"

Coleman says companies need to look more inclusively at all ages and genders in the company for suitable talent.

Research firm Forrester sees a trend where large organizations are creating their own contingent labor pools using alumna or company retirees. Nike, for instance, has already adopted a self-sourcing model for temporary IT workers, says Andrew Bartels, vice president and principal analyst at Forrester. The concept of self-sourcing is not new, but companies are developing larger self-sourced talent networks and automating workflows to identify and procure the talent.

Bartels hasn't seen companies fill cybersecurity positions specifically with this model yet, "but it may help companies address the skills shortage using people who are already attracted to their brand," Bartels says.

One Gartner client who was desperately seeking a security architect went outside his own company and was able to lure a retiree from a different firm back to work, according to the research firm. The man had grown bored in retirement and started looking for project work. He was eventually hired full-time. The company found his work to be high-quality and drama-free compared to some younger workers, and customers and staff valued his broad experience and humble demeanor.

Women

Women represent only 11 percent of the global information security workforce today, according to a global study by (ISC)2, and they represent a large and talented labor pool for cybersecurity positions. Women in cybersecurity today enter the profession with higher education levels than men. Half of women in the profession have master's degree or higher, compared to 45 percent of men. Globally, 42 percent of the women have undergraduate degrees in computer and information sciences compared to 48 percent of men. Among Millennials, 52 percent of women younger than 29 have computer science undergraduate degrees. The study recommends that more professional support, sponsorships and mentorships are needed for women in security and risk management.

Most companies offer IT internships for soon-to-be college grads, but interns with an interest in or aptitude for cybersecurity skills should be sought out early and courted, says Michael Eisenberg, vice president in the Office of the CISO at Optiv Technologies.

When Eisenberg served as global CISO at AON plc from 2008-2014, he remembers an "extremely smart and sharp" IT intern who he thought would be a good fit for the security team. "I talked to him about how information security would be different from IT because

it's a different role," he recalls. "He seemed very excited about it." His team gave the intern on-the-job training and enrolled him in some SANS courses, he says. "He worked as part of our team as a junior. We were throwing him into regular projects doing some lower-level tasks. We knew he was going to be able to take things over." That intern still works at AON today as a senior program management specialist on the global information security team.

Eisenberg cautions, "You don't want to bring somebody over [to a security role] if they don't have an interest in security. It's a different animal" from IT, he says. "Finding the right person and the right fit, and getting them excited about what their career could be, is an important aspect. If a year down the road they're not happy, you're going to lose them."