What You Can Do Right Now

to Solve the Industry's Cyber Skills Shortage

NYOTRON

SECURING THE WORLD

What You Can Do Right Now to Solve the Cyber Security Industry's Skills Shortage

The statistics on the cybersecurity skills shortage seem dire. Many organizations cannot find the skilled personnel that they need to properly secure their IT systems and protect sensitive information. The prevailing belief is that the industry has inflicted this skills shortage on itself, but whatever the cause, it must be addressed.

To a large extent, the problem exists because organizations want to hire a skilled person for a security position. That makes perfect sense, assuming you have a plentiful applicant pool of skilled personnel to hire from. The trouble is, this is not the case, and that won't change in 2020.

This is not a universal problem across the entire IT industry. There are some regions where you can place an ad to fill non-security openings, and get more than enough qualified applicants. For example, if you want a Splunk analyst in the San Francisco Bay area, you have a potential applicant pool of hundreds, if not thousands.

These other fields have figured out how to overcome issues, so why can't security? The answer is that too many organizations fail to understand that if they want to have, they acknowledge the limitations of the current applicant pool, then determine how to overcome the issues.

What follows are a variety of tactics any organization can use to address the cybersecurity skills shortage. While it is true that you might not be able to hire an expert with the specific skills you need within a week, you should be able to develop a strategy to find people who can quickly acquire those skills you need.

Hiring Tactics

We are very specific with our use of the words "tactics" versus "strategies". A strategy involves a variety of tactics used in concert. For example, tanks, ships, airplanes, and soldiers are all tactical assets. They have to be used in a coordinated way - as part of a strategy - to be effective. Similarly, none of the tactics described below can solve your staffing problems on their own. You will have to incorporate them all into your recruiting, hiring and retaining strategy, depending upon a variety of factors specific to your circumstances.

Some tactics may be familiar to you, others may not. We “borrowed” many from other disciplines that have solved their skilled personnel shortages that can also apply to the security profession. It is also important to note that some tactics will not provide immediate results, so they may not be practical for your organization to pursue if your needs are immediate.

Competitive Compensation

While all organizations like to say that they value their people, including their security teams, many do not pay an adequate wage for cybersecurity personnel. There are countless stories of organizations advertising for skilled cybersecurity personnel with entry-level salaries. Likewise, many organizations do not want to adequately pay the security staff that they already have. It goes without saying that if you adopt this approach, you will have limited success in hiring and retaining qualified staff.

High Quality Management

There is a saying, “Employees don’t leave a job; they leave a manager.” Managers need to treat their employees with respect and ensure acceptable working conditions. Those factors can even be more important to employees than a higher salary.

People like to feel both valued and valuable. They want to believe that they are working on a bigger mission to grow the company, and even make the world a better, safer place. Entering the security field gives them the opportunity to battle the “bad guys”. Organizations should provide a clear mission statement and articulate how security personnel play a vital role in securing and protecting the organization, the other employees, customers, etc.

High quality management requires the organization to invest in its people. Many cybersecurity personnel want to advance their skills. They want to attend training, attend conferences, network with peers and receive support for pursuing a higher education. We’ve heard of organizations who hire people who regularly speak at conferences, and are excited to get someone on board who is perceived to be a security expert. Then once the person is hired, the company refuses to pay for conference attendance, and even require the employee use vacation time to go speak at the event. Of course, the employee’s tenure tends to be short.

Effective Recruiting

Write job opening ads that do not unnecessarily limit your applicant pool. Don't write job descriptions that are looking for "unicorns" with all the experience and skill-sets you need (and more) - that creature doesn't exist. You want to identify your minimum requirements for the position and advertise those.

For example, if you need a network security administrator, be open to hiring someone who administered a smaller network than yours. Writing your job description to allow for "acceptable" candidates allows you to attract a wider range of candidates.

Employee Referrals

Your employees likely know some of the most qualified candidates for your openings. Allow your security staff to network in the broader security community. They will likely meet other competent and qualified security personnel and refer them to you.

In the ideal world, you provide monetary incentives for your staff recruiting a new team member. For example, in Silicon Valley those referral bonuses can be as high as $10,000. This only makes sense, because using an outside recruiter will likely cost you over $20,000 per hire. However, if you provide a good working environment, your employees will be happy to tout your organization and help fill vacancies. In many ways, this can be the most fruitful recruitment tools that you have.

Events and Associations

While employee networking is useful, smart organizations network themselves. Hiring managers and organizations as a whole that are interested in improving their cybersecurity capabilities, make it a point to participate in groups and events where security professionals congregate. Such events might include meetings of local chapters of **ISACA**, **ISSA**, **(ISC)2**, and other professional associations.

There are also a variety of local and national conferences that attract cybersecurity professionals. These events include large events, such as RSA Conference, DEF CON and Black Hat. There are also regional events like **BSides** and one-day conferences held by professional associations. Private organizations such as DataConnectors also hold vendor sponsored events. They are typically free or inexpensive to attend.

While you should encourage all of your cybersecurity staff to attend these events, you could attend as an organization as well. Sponsoring events is a great way to establish visibility and reputation as a champion of the field. This generates goodwill among the community and, most importantly, qualified candidates who will seek you out.

Finally, organizations with strong security teams may consider organizing a MeetUp group that hosts events featuring guest speakers on a regular basis.

Transitioning Employees From Other Disciplines

While there are college curriculums dedicated to cybersecurity, it is significantly easier for an experienced IT professional to make the transition to a cybersecurity position than it is to train a recent cybersecurity graduate to perform basic functions.

One organization we are familiar with wanted to create a security business unit. The lead person responsible sent out a broad internal solicitation, asking for anyone who would consider transitioning to the cybersecurity field. This was not just limited to IT personnel. Customer service staff applied. They were trained as Level 1 Help Desk Analysts given their experience answering calls and walking callers through basic functions. Systems analysts were trained for more senior security positions. They did have a core team of security experts oversee the program, but the core of the program was matching individuals with the job functions that best met their skills and providing the appropriate training to overcome any gaps.

Also, look to military veterans returning from active duty. A number of government agencies such as the Department of Homeland Security have launched cybersecurity skills training and certification **programs** for veterans to help government and the private sector address the skills shortage. Some companies like **Cisco** have launched scholarship programs to attract veterans to ease the financial commitment to pursuing a cybersecurity career.

Chances are that you do not have to create an entire security function. However, you can still adopt this philosophy to filling a small number of open positions. Likewise, you don’t have to limit your transitioning from other disciplines to your own employees. There are a large number of people who hear the hype of the cybersecurity profession and want to enter it. If you are willing to find high quality talent and be willing to aid in the enhancement of already skilled personnel, you can both attract great people, while ensuring their loyalty.

Youth Outreach

Consider creating or sponsoring youth programs, but keep your expectations modest. You are not going to solve your immediate staffing shortages by supporting high school cybersecurity competitions. Youth outreach is usually reserved for large organizations who can sponsor and support sustained activities. Sometimes, it is supported by industry and training organizations.

Potential outreach include Capture the Flag competitions, robotics clubs, tutoring in schools, presenting at career days, presenting cybersecurity awareness presentations at schools, among other events and activities that promote cybersecurity as a potential career field.

It is always great to support the profession and encourage people to learn more about it. We do need to attract more people for the future. At the same time, these events are great for networking purposes and finding potential, qualified applicants, who are also helping with the events. It is also possible to find some outstanding talent at Capture the Flag events, who demonstrate better than entry level skills and abilities.

Diversity

While this topic should not have to be addressed, you need to ensure that you are not unknowingly limiting your potential talent pool by driving good people away.
This can take many forms. In your hiring programs, are you intentionally or unintentionally limiting qualified people from applying? Does your organization have policies or practices that make the organization uncomfortable for different types of people? Is there a culture that is supportive of all individuals?

Ironically, while referrals are a great source of employees, they can also potentially limit your efforts to foster diversity. In general, your employees' networks are populated with people who have similar backgrounds and interests. This may result in an overly homogeneous environment that limits innovation.

	Short-term	Mid-term	Long-term
Compensation	✕		
Management	✕		
Job description	✕		
Employee Referrals	✕		
Internal Transition		✕	
Events		✕	
Outreach			✕

Considering Outsourcing

Outsourcing may be appropriate, particularly in the short term. A Managed Security Services Provider (MSSP) that can fulfill one or more of your security functions, and do so in a way that is more effective and less expensive than you doing so yourself.

For example, MSSPs who provide monitoring and detection are able to automate and scale better than any individual organization can. They can conduct better reconnaissance and collect better intelligence. They can potentially perform better incident response, and have ready access to additional resources as required.

By outsourcing the appropriate security functions, you can use your cybersecurity experts for other functions. This means that you can hire fewer people, and reduce your staffing shortage while still immediately addressing your needs.

Creating a Strategy

The tactics you choose to employ will depend upon your immediate needs and your available resources. For example, if you do not have security expertise, it is much harder to attempt to hire someone who is transitioning into security.
But if you have a great security team in place, you can be more open to hiring someone with great technical ability, but limited hands-on security experience.

You also need to determine how active you want to be with the broader security community. Your activity can be casual, or it can involve sponsorship of different activities and allocating people to attend and/or support events.