CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
CYBER WARNINGS

Smart Staffing Strategies To Support Cyber Defense-in-depth

By Robert W. Williams, CEO, Vector Technical Resources

June 2014

Defense-in-depth. That is the only way to defeat today's multi-directional, multi-dimensional threats against the network. Cyber defense-in-depth starts with an outer perimeter with a firewall, with intrusion detection and prevention systems forming an inner core of cyber protection.

What are the keys to finding the top technology talent needed to fortify your cyber defenses? Let me share the perspective I gained while serving, in the final duty post of my 30-year career in the U.S. Navy, as Director of Network Security and Chief Information Security Officer for the Navy-Marine Corps Internet (NMCI) Global Network Operations Center. In this capacity, I was in charge of information security and operational command and control for the Department of the Navy's $8 billion, 300,000-computer shore-based enterprise network in the continental United States and Hawaii.

Ever-Changing Threats Demand a Unique Skill Set

Just as the threats are ever-changing, so are the technology requirements in the cyber security field. Certainly "hard" firewall and other tech skills are important, as well as knowledge about what your protection devices are able to pick up and the ability to evaluate what is a real intrusion.

Also, you need people savvy enough to know when to disregard intrusive events that do not pose a serious threat to the network.

But don't overlook key "soft" skills. For example, you need people with sharp minds and the hunger to learn and to keep learning. It's also important for members of your cyber defense team to have the flexibility to adapt their job functions to keep up with what the bad guys are throwing at your network on a daily basis. The only way to size up these "soft" skills effectively is through the interview process.

Once you have identified the need and requirements for cyber security talent, these requirements must be clearly communicated to a tech talent acquisition specialist who could be in-house or with an outside staffing firm.

It is critically important for the tech talent acquisition specialist to have an A to Z understanding of what the company needs in a successful candidate for this position. At this stage, it is also advisable to establish what the position is worth in terms of salary and benefits.

Socializing the Talent Search

The hard reality in the staffing industry is that the best people aren't looking –they're working! That's why recruitment advertising is often a hit-or-miss proposition in a field such as cyber security, and why social media and referrals are often more productive in identifying top talent. This kind of "socialized" talent search can be conducted in-house, but it often makes sense to engage an outside staffing firm (i.e., a temp-to-perm or temporary services agency) that maintains a large professional network that includes social media channels.

(continued)

Here's another reason to outsource the cyber talent search: if your position is posted with several staffing firms, they will compete to offer the best candidates. Not only that, but they will also handle the clearance process.

Whether the talent search is conducted in-house or outsourced, a clear hiring process must be established that can be expedited if an ideal candidate is identified who needs to be brought on sooner rather than later. When a talent opportunity presents itself through the search process, the company must be ready to hire.

Narrowing the Field

You can see the skills listed by a candidate on his or her resume, but unless you talk to that person, preferably face to face, you will not be able to gauge whether or not they are a good fit with your team. Another advantage of using an outside staffing firm is that they will have done all the background checks, including criminal/financial screenings and verification of security clearances, so that you can concentrate on the interview process to determine the candidate with the best fit.

In fact, the biggest pitfall in finding top cyber security talent is hiring somebody off his or her resume. Not only must each candidate be thoroughly vetted, including reference and clearance checks, but if you're the hiring official you must talk to candidates! And you need to do more than ask the "standard" interview questions. Instead, asking open-ended questions is a better way to get a feel if the candidate is the right person.

If the person is being hired for a cleared position, the Facilities Security Officer (FSO) needs to verify his or her clearance. When all is said and done, everything on the candidate's resume should be up-to-date, verifiable and fully vetted.

Here is a cautionary note about background checks. If you are going the outsourcing route and are using a tech staffing firm, until you know who you are dealing with and trust their capabilities, it's wise to ask for documentation of background checks to confirm results of financial/criminal screenings and security clearance verification. After you have been dealing with the staffing firm for a while, your confidence level should increase.

Extending the Offer

After checking references and clearances, rank the top three candidates. Then offer the position verbally to the A (first choice) candidate. Give the A candidate 24 hours to make a decision. If he or she makes a verbal acceptance, send an offer letter immediately confirming the salary and benefits that were negotiated as well as the start date, working hours and whether the position is exempt or non-exempt from overtime.

The offer letter should have a signature line for the candidate to sign. The signed offer letter should be sent back within 24 hours.

Talent Acquisition for Cyber Defense: The Secret Weapon

What if you could find a turn-key solution that ensures a successful outcome in all stages of the cyber tech talent acquisition process described above? That's what an external IT staffing firm is all about. It's the cyber tech hiring manager's best friend – and secret weapon.

The sooner the decision to go with an external firm can be made after the cyber security position opens up and the firm decides to fill it, the better. The staffing firm should be contacted and an interview requested with an account manager experienced in cyber tech staffing.

(continued)

A good account manager is an attention-to-detail person who will not only ask the right questions – lots of questions – to get all the information about the job requirements, but will also be able to produce four to six candidates who have already been pre-screened and pre-qualified and are believed to be a strong fit for the position. A top-flight staffing firm is able to map candidates quickly to the specific requirements of any cyber tech position.

As noted earlier in this article, a key at this stage of the recruitment outsourcing process is to provide complete and detailed information about the position and the "hard" and "soft" skills needed for success. The more complete picture the staffing firm has, the quicker the search and the better the results.

Because external IT staffing firms are paid to find the A players, they make it their business to know who the top people are and how to find them.

The best staffing companies have their own proprietary applicant tracking systems using specialized database software to harvest cream-of-the-crop talent from many different sources. Not only that, but premier firms will offer a "try before you buy" guarantee that an applicant who doesn't work out within 30 days will be replaced.

Bottom Line Benefits

The reality in today's tech talent acquisition arena is that large businesses are using staffing firms. For small and mid-size companies, this approach can also pay dividends – literally – because a temp-to-hire agency will carry new hires on their payroll for as long as six months.

After you're sure that the new person has worked out, you can bring them on staff. This "test drive" approach to cyber tech staffing frees up capital that would otherwise go to salary and benefits. This means smaller firms often can grow faster by using a staffing firm.

What's the bottom line on finding top tech talent in the cyber security field? More often than not, a remarkable staffing company will find better quality candidates – and, in the long run, do it less expensively. The choice is to pay now for the right cyber tech talent solution, or pay later for talent that doesn't pan out and may cause a loss of competitive advantage.

Lately there has been a lot of talk about a "shortage" of IT professionals across all industries, not just in cyber security. The reality, as I see it, is that more and more young people – members of the Millennial Generation who grew up playing computer games and using mobile devices – are poised to enter the tech workforce. The issue is not a lack of talent, but a need to tap the supply of tech talent more effectively with support from professionals who make it their business to find the right people.

It's not an exact science to assemble a top-of-the-line cyber defense team. Nobody has a crystal ball, and not every single candidate will work out. But the right staffing firm, especially one with multiple layers of cyber security and IT expertise coupled with extensive network connections, can be an invaluable strategic – not to mention money-saving – asset.

About the Author

Robert W. Williams is Chief Executive Officer of Vector Technical Resources, an IT and staff augmentation company servicing the private, federal and state sectors. He has more than 30 years of experience successfully leading large geographically dispersed information technology (IT) organizations. For more information about Vector Technical Resources, please visit www.vectechresources.com.