WHERE HAVE ALL THE GOOD HIRES GONE?

Lysa Myers
ESET, USA

Lysa.Myers@eset.com

ABSTRACT

Much ink has been spilled about the difficulty that organizations are experiencing in hiring information security professionals. While the goal – more, and better qualified applicants – may be clear, the necessary steps for reaching that goal are anything but. Many people feel there are plenty of available applicants, but that they're being excluded due to systemic problems. Others believe that the only solution is to get many more people interested in a career in computer security. Regardless of which of these statements is more accurate, it greatly behooves us to proceed as if both statements are true.

When more people are educated about how best to make computers secure, the utility of the Internet as a whole is improved, regardless of whether those people ever go into a security-focused field. Investing time and effort into participating in outreach efforts that educate people about security concepts, or that enable them to seek either formal education or certification pays dividends – and not just in terms of potential future hires.

Examining your hiring processes and employee development will likewise provide benefits far beyond simply having an easier time filling your open headcount. Many companies create artificial barriers for potential employees, either unintentionally or with the goal of weeding people out. It's worth examining whether you're creating those barriers within your hiring process, and whether they deter unqualified applicants or if they're actually turning away qualified experts who have unconventional backgrounds.

UNIQUE PROBLEMS OF INFOSEC HIRING

When someone has a 'traditional' career, such as a doctor, fire fighter or lawyer, you can conjure up a pretty specific image of what that position entails, and what education it took for them to reach that point. When someone has a career in infosec, the image that comes to mind is either fairly nebulous or simply inaccurate. (I don't know about you, but I don't work in a dark room with my face hidden under a hooded sweatshirt, I've never 'hacked the Gibson' [1], and I don't have a computer science degree or an arcane list of certifications following my name.)

How does a hiring manager – especially one who's not a security professional – know what to ask for? It might be tempting to throw everything but the kitchen sink into the list of requirements for a position, and even security companies full of experts are guilty of this. Inaccurate and over-inflated requirements are a huge red flag to people with experience in this industry, especially when poorly conceived requirements are matched to underwhelming compensation packages. It's imperative that hiring managers ask and answer some specific questions about the company's needs and resources *before* they set about writing a position listing.

Don't worry if your organization can't offer sky-high salaries, free laundry service, catered meals, or other hip perks. There are plenty of experienced security professionals who are happy to work for companies that offer 'merely' reasonable salaries, benefits, and a healthy work-life balance, especially if your organization has other valuable things to offer prospective employees. Understand that this may mean that you need to be more creative in the recruiting phase by searching for candidates that higher-profile companies might miss, or by developing talent in your own backyard.

OUTREACH

The process of searching for prospective employees can – and likely should – begin long before someone is actively looking for employment in your company or before a position is actually available. Establishing your organization as a desirable place to work and an active participant in your local community can make the task of recruiting far less arduous.

The use of advertisements, plus sponsoring or participating in local and industry-specific events, are obvious ways to start. But there are other methods for getting involved in your community that make it clear to job seekers that your organization offers more than just a way to make a living, or that can even increase the number of people in your area who might be qualified to work for you.

- **Community education**
  Help organize events that educate students about your area of expertise, or in STEM or tech more generally, either through an existing group that's active in your area or by starting your own. Focusing on traditionally under-served populations can give a greater return on investment in terms of the number of people who might not otherwise be exposed to your company or the possibility of a career in this industry.
- **Interns or apprenticeships**
  If you have an existing security group, you can hire interns or create apprenticeship positions. Internships can help familiarize students with the realities of a career in this industry while they build skills. Even if you do not have a security group, hiring interns in other areas of your company can be a good way to build enthusiasm for your organization if they spread good word of mouth.

RECRUITING

It's important to get a realistic sense of what skills or education a position *actually requires* before beginning the process of recruiting. It can be a challenge even to know what name to give the position you're looking to fill, if you're starting from scratch with no in-house security experience.

- **Check the 'dictionary'**
  The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [2] provides a common language for speaking about security roles and

jobs, and helps define requirements for each specialty area. The CyberSeek Cybersecurity Career Pathway [3] tool can give you an idea what sorts of job titles you might want to look for in résumés you receive.

- **Supply and demand**
  The Security Supply/Demand Heat Map [4] can tell you what other organizations in your area are looking for and the number of available workers. If you are able to offer the option to work remotely, you may significantly increase the size of the pool of available applicants, especially if your organization is in an area of the country with a small to nonexistent pool of locally available security talent.

- **Mandatory versus preferred skills**
  If you're faced with a challenge in terms of location or budget, it is especially important to be realistic about what skills are mandatory before starting, as opposed to skills that are just 'nice to have' but not strictly essential, or that can be learned on the job. Speaking to someone who has already held this position either within your own company or in a different organization can be helpful. Understand that, just as the nature of threats evolves against your company's IT assets, your staff must grow and evolve to combat them. Continuing education is an essential part of being an effective security practitioner. Make sure that recruits know you will continue to invest in their education.

- **Certification after hiring**
  There are some skills that an applicant might be able to offer, but which may simply be more costly than a company can afford; if you have the leeway to hire someone who does not yet have all the desired experience but will agree to attend training and get certified in those areas within a set time frame, it can create a mutually beneficial situation for your organization and the employee. Once they have demonstrated the skills in practice, it's important that their remuneration be adjusted to reflect this additional value.

- **Creating a job listing**
  Make sure your requirements are accurate and reasonable (don't ask for more years of experience than a technology has existed). Avoid using superlatives or extreme modifiers (do you really need the 'world's best'? – someone who's 'very skilled' can usually get the job done at least as well). Start using more inclusive descriptors [5] (avoid using verbiage tied *only* to individualism and hierarchy; include words that emphasize community and cooperation).

  Keep in mind that recruiting is not *just* about asking applicants to prove themselves to you; especially in times of talent shortage, you must also be selling your company to them. Descriptions should be engaging, and should include how the candidate that you hire to fill this position can contribute to business objectives. You may also choose to discuss their potential for advancement. It is a good idea, either in the initial job listing or early in the interview process, to state the expected salary range for the position.

- **Placing your job listing**
  Once you've created a job listing, you'll need to consider where to place it. While it might be tempting to pick the biggest job recruitment site or a single recruiter and call it good, you might get better results by casting a wider net. You can also ask for recommendations from people already in your security group if you have one, or from people in the security community. Contacting tech or STEM groups that meet in your local area, or organizations that support under-served demographics in tech, will naturally give you access to a bigger subset of applicants. A word to the wise: if you host an on-line application form/process on your own website, please make sure it's set up with good security practices; there are few things that set a prospective security applicant's hair on end more quickly than submitting their personal information to a company that has demonstrated an inability to protect their data.

INTERVIEWING

Once you find enough interesting candidates to begin the interview process, you may feel you're in the clear, and that it's simply a matter of weeding out all but the best contender. Many companies take the choice out of their own hands at this stage by setting up unnecessary obstacles that dissuade or discourage otherwise excellent candidates. We've probably all heard horror stories of interviews 'gone wrong': a never-ending series of phone interviews, marathon in-person interviews with little opportunity for 'bio-breaks' [6], expecting candidates to meet at inappropriate off-site venues, asking brainteaser or trivia questions that have nothing to do with the job in question, etc.

- **Be considerate to your candidates**
  Understand that interviewees may have other commitments (such as an existing job!) that preclude them from being available for an interview when and where you would prefer. If you choose to meet at an off-site location, consider whether it might cause difficulties for someone with mobility or sensory challenges. Within reason, you should be accommodating their schedule and physical necessities. If you're interviewing people who would need to relocate, let them know if or when you'll cover expenses for their trip, and whether you'll cover the expenses in full.

- **Ask appropriate questions**
  When you start asking questions to ascertain candidates' suitability for the position (once you've refreshed your memory of which topics are legally acceptable or off-limits in your area) it's best to stick with qualities and skills that actually pertain to the day-to-day job responsibilities, as laid out in the job description. Even if you don't know much about security yourself, you can assess other important information such as a person's temperament and ability to communicate, as these are elements that are challenging to assess on a résumé or application form. Few people will have encyclopedic memories for minutiae, especially in a stressful environment with an audience. On the actual job, most of us will do an Internet search for obscure facts or tasks, or we'll have reference books to check.

- **Tie-breakers**
  If you find yourself in the enviable position of having two or more qualified candidates to decide between, consider going with the more 'non-traditional' candidate; someone

who doesn't fit the mold of a typical tech person. That could be someone who is part of a demographic that is underrepresented in tech, someone who came to their interest or career in infosec via an unusual educational trajectory, someone with a different socio-economic background, someone with skills or abilities other than just tech or security, etc. The most effective security teams are those that have a wide variety of people who bring a wealth of different perspectives from which to help spot potential problems before they become costly mistakes.

CARE AND NURTURING OF YOUR NEW SECURITY TALENT

Now that you've done all the work of hiring a security practitioner, it's a good idea to take reasonable steps to reduce replacement due to attrition.

- **Time and space to think**
  Security is a brain-intensive task, and security practitioners will need quiet time and space to do their jobs.
- **Continuing education and effectiveness**
  The reason many of us got into security is because it offers an almost unlimited learning opportunity. If we don't continue to learn about new threats and technologies, we become less effective over time. Make sure your researchers have time, funding and availability to participate in workshops or community events (e.g. conferences, seminars or webinars) to keep their knowledge fresh. It can also be helpful to make sure they have sufficient time to work on projects; having the ability to fix problems properly – rather than simply running around trying to deal with the metaphorical equivalent of 1,000 dripping faucets – can do a lot for our sanity.
- **Trust your expert**
  There are few things quite as wasteful and frustrating as hiring security practitioners only to completely disregard their suggestions, and yet this is a sadly common complaint. If you're hiring people to help secure your organization, trust their expertise and work with them to understand the business case for their recommendations.

Hiring outside your traditional area of expertise, and for such a new discipline, can certainly be fraught with anxiety. But as all of us need to be security-conversant to help secure our own personal data, as well as that of the companies for which we work, it can also be an excellent learning opportunity. You can help increase the size of the pipeline by increasing educational opportunities within your community. You can also help improve the robustness of the pipeline by implementing sane hiring practices, and providing a good working environment for your security practitioner.

REFERENCES

[1] Hackers (film). Wikipedia. https://en.wikipedia.org/wiki/Hackers_(film).

[2] NICE Cybersecurity Workforce Framework. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

[3] Cybersecurity Career Pathway. https://www.cyberseek.org/pathway.html.

[4] Cybersecurity Supply/Demand Heat Map. https://www.cyberseek.org/heatmap.html.

[5] Finley, K. New study exposes gender bias in tech job listings. Wired. 3 November 2013. https://www.wired.com/2013/03/hiring-women/.

[6] Bio Break. Merriam-Webster. https://www.merriam-webster.com/words-at-play/bio-break-meaning-and-origin.