



# Winning Your Company's Battle for Top Cybersecurity Talent



# Winning Your Company's Battle for Top Cybersecurity Talent

BY CHANCE HOAG

If you are reading this article, you know how challenging it is to recruit Cyber Security talent during one of the most competitive landscapes for any profession in the past 30 years. You're in good company. But your organization and customers are looking to you to build a recruiting machine that attracts and retains top candidates. Despite the obstacles, you can achieve this goal if you are willing to implement some ideas that will require significant time and resources – but not nearly as much as missing a great hire or having a key person leave your Program.

I read plenty of White Papers and Research Reports on Cyber Security, and this one will be a little different. Overwhelming you with graphs and statistics on Cyber Security talent shortages, spending, and breach scare tactics isn't a good use of your time. But positioning your Security Program to win and retain the right candidates is. Let's take a top-down, or philosophical-to-tactical approach, to building your team.



# 1. Attracting Top Talent:

## HOW DOES THE COMMUNITY PERCEIVE YOUR SECURITY PROGRAM?

I talk to Security professionals all day, every day. The majority of them have deep insight into the Security Programs of companies in their local market. The current Security tribe is more insular than most other professions because the primary educational path for the industry was trying stuff that could lead to a rap sheet.

Security was an early hobby for many people now in the industry, so the need to gather, learn, and share knowledge was and is very important. Whether it be “Capture The Flag” events, Hackathons, meet-ups, or local chapters of the five or six top national Security associations, Security professionals tend to be “in the know” about local leadership, companies, and reputations of different Programs. What Security people say about their company’s Program, the consistency of their leadership, and the internal “feel” of the staff is critically important to building a solid team.

Good Security talent looks to build a career, not hop from job to job. To do this, they need stability within a Security Program. Does the company’s Board place a priority on Security? Does the company display a consistent commitment to the level of Security they espouse? Is the Security leader trusted and valued by the executive leadership team? Are learning, teamwork, and teachability just buzzwords or are they proven values within the Security Program?

To successfully recruit good people, your internal house must be in order. Good people are attracted to, stay in, and flourish in stable, progressive environments – and these types of environments are always the result of unified and clear leadership. Good people quickly attract good people. In Security, word gets around and becomes reality to the greater Security community, especially in the local market. How your program fits into and is respected by the company as a whole is a critical aspect to attracting good talent. If you are doing this well, then the next steps are fairly straightforward.

---

# 2. Recruiting & Hiring:

## ARE YOU ENGAGING CANDIDATES THROUGHOUT THE PROCESS?

Understand what you are up against. There is 0% unemployment in Cybersecurity. Zip, zero, nada. In IT, 10% of all job postings are in cyber and the growth rate is 2x faster than other IT jobs. There will be 1.5–2 million unfilled cyber jobs by 2019. Currently, cyber job postings take 24% longer to fill than other IT jobs and 35% longer to fill than all job postings. In a time when your company needs to balance speed with the right hires, the market is brutal and the competition is fierce. So how can you set your company up for success?



## ***Involve Your Security Department in Recruiting***

First, your Security Department should be more involved in hiring than other departments in your company. Recruiting an accountant is a walk in the park compared to what you are trying to accomplish. Security positions are highly specialized, somewhat new, and oftentimes exceed the network and time restraints of internal HR/Talent. Plus, Security Programs are notoriously tribal. You know your culture, so you are responsible for finding the right personality and skillset. It's important for you to have done the research on your competitive landscape, salaries, and what you can get for your money.

## ***Promote Your Job Openings Where Talent is Likely to See Them***

In recruiting, visuals are important and you should take the time to ask for extra love from Talent and HR. Oftentimes, there is a battle going on inside your company between departments for recruiting resources and you can make a great argument that your department needs focus. Ask for special recruiting sections on your company's website, and especially on LinkedIn. Google and Facebook have nothing on the target marketing you can do on LinkedIn for targeted articles and sponsored job recs. Use them to your advantage. Also, Google Adword buys can be a focused and inexpensive method to owning keyword searches.

## ***Invest Time in Perfecting the Job Description***

One of the biggest mistakes I see from companies is in defining the role. This sounds simple, but you will get a leg up over the competition by directing your team to spend a little more time in this area. Do this right and competent candidates will immediately know that you get it. A job description should read more like a story than a checklist of demands. Remember: THIS. IS. A. BUYERS. MARKET. You have to sell! Don't lose a great candidate in the reading of a job description just because you copied and pasted the requirements from your competitor.

## ***Cast a Wide Net and Be Willing to Teach***

As a Security department, you know that the top qualifications you're seeking are passion and an innovative mindset, so try not to constrain the role too much with an exhaustive laundry list of certifications and pie-in-the-sky experience expectations (like a demand for a young Analyst carrying a CISSP, or a Senior Security Engineer with patching responsibility). If you do this well, you might interview a candidate that's not right for the immediate posting but would be a great fit elsewhere. Or you might interview a candidate that is almost there but not quite. Maybe the team loves him/her and agrees that the added knowledge wouldn't be hard to teach. You don't want to waste your team's time with a cattle call but, in Security, you want to be in the position of turning a close-to-great candidate into exactly what you need.

## ***Optimize Your Interview Process***

Next is the interview process, which done right can continue to push your Security Program forward in the minds of Security candidates. Seventy-seven percent of candidates believe the interview process is important and speaks to the values of a company. You can use this to your advantage. First, to win in Security, you must interview with speed. This is tough because you must carve out valuable staff time weekly. If you find a good candidate or two but it takes a week to line up the right interviewers, you are dead. A well-defined and speedy interview process wins!

Most company interviews lack structure and metrics. They are too loose and personality-driven, making it difficult for the team to score and the candidate to feel like the right topics were given appropriate time. Yes, you need time to assess a candidate's personality and vibe with the team, but that's pointless if the candidate doesn't have the chops to do the job. The best assessments are provided when a candidate pool for a job meets with the same person or team and is asked the same questions. Also, it's important that a candidate's first touch is with a positive "yes" person. The guy most likely to make a colleague feel like an idiot for opening a dangerous spam email should not conduct the first interview! The goal is to ratchet up the expectations in an interview process, not nuke your candidate base early.



### **Navigate the Job Offer and Negotiation Stage**

With Security talent, the job offer stage is usually more freewheeling than in other professions. Payscales within Security positions, even in similar markets, are harder to define because they are based on three factors: current salary (which can have more moving parts in the way of bonuses), what the competition is willing to pay, and your company's pay structure. When approaching offer stage, a company must be quick, decisive, and as armed as possible with the knowledge of what that can make a deal go bad. I believe that any successful negotiation results when both parties don't get exactly what they want. It sounds negative but, if your interview process is strong, candidates understand that there is give and take in every situation. At offer stage, both parties have invested a lot of time, and the candidate has placed him/herself in that role. Be open to the negotiation and close quickly.

### **Respect All Candidates – Not Just the One You Choose**

One of the best ways to build a good reputation is to treat rejected candidates with respect. Always call the candidate to give a no, thank them, and provide clear and truthful feedback. The candidate may disagree, but they will appreciate it because that experience will be different and will set you apart. Plus, the candidate might be a prime target for you in a few years and a good experience will keep the door open.

I believe that a Security Program is hitting on all cylinders when they are employing multiple methods to acquire and retain talent. Since I own a recruiting firm, I want to mention the benefits of a good recruiter for specific roles. Good recruiters are worth the money if they can do several key things that are not attainable with other methods.

- 1. First, you must find a recruiter that knows your market and focuses exclusively in Security. This type of knowledge results in speed of hire. Time, as they say, is money.**
- 2. Second, a good recruiter can save a ton of grief when it's time to close. At offer stage, a good recruiter has been working to bring both sides together, which eliminates unwelcome surprises at the altar.**
- 3. Third, a good recruiter knows that an accepted job offer is never a done deal. Candidates, especially Security candidates, should be hand-held through the process of resigning his/her current position through onboarding and the first critical months at the new job.**

---

## **3. Retaining Employees:**

### **ARE YOU SETTING NEW HIRES UP FOR SUCCESS?**

Let's say your Security Program's perception is excellent and your recruiting and hiring process is effective. Did you know that 80% of new hires decide within the first six months whether they will stay at a company? Plus, it's estimated that replacing an executive or serious tech employee can run up to 215% of their salary. Know that you didn't win the battle the morning that new hire walks in the door. Execute on the ideas below and you will retain your best employees.



## ***Master the Art of Onboarding***

Onboarding can be trickier in Security than in other departments in your company. You probably don't have all the resources you need, the pressure is high, and it's natural to need an immediate return on a new employee. So, Security Programs tend to throw their new hires right into the work – but restraint is the wiser decision. It's so important to clearly explain and execute a defined runway for an incoming employee. They know the pressure is coming. The salaries demand results. You can help by beginning the onboarding process long before the new hire's first day. Put the new hire in the loop early with what's going on within the department. Let him/her get an initial feel of the pace and lingo. Ask a few people in the department who have not met the new hire to reach out and introduce themselves. Also, personal gestures go a long way. Stocking a new hire's workspace with the stuff they need buys a ton of loyalty.

## ***Encourage and Empower Professional Development***

Good Security people crave learning and opportunities to interact with their peers. I've seen first-rate companies commit up to \$10K in outside learning and conference money to Security employees per year. Continuing education and

training for your staff – done right – is going to be expensive, unless you consider that it's going to cost you 10 times that to hire someone new. If you want to attract new hires, send some of your people to Vegas for a big conference, let them share their fun experiences on Instagram while their colleagues at other companies in your market sit in the office and work. It will move the needle.

## ***Develop and Maintain Mentorship Programs***

Lastly, there is only upside to mentoring. It is a big deal for retention, future leadership, learning, operating margins, and almost every other positive thing in your company. People are 77% more likely to stay in a job if they have a mentoring relationship. Plus, any statistics you find with regard to mentoring jump even higher when it comes to females and minority workers. This is something you desperately need, want, and should foster at every opportunity. And it turns out mentoring works both ways: younger people, especially Millennials, are rubbing off on their Mentors, which is a necessary thing for companies. The exchange of ideas and help offered to younger staff by Mentors can set them up for a long haul in leadership. Plus, if you broker mentoring relationships for your Security staff outside of the Security Program, it usually helps sell Security ideas throughout the company.

---

# Conclusion

At Talon Placement, we focus exclusively on recruiting in Cyber and Information Security. We are focused, fast, and fun. We also believe in a holistic approach to acquiring the talent you need to set your Security Program apart. We hope this paper gives you a few ideas to better your perception, recruiting and hiring process, and retention efforts. Contact me at [talonplacement.com](http://talonplacement.com) or on ***LinkedIn*** or ***Twitter*** and let's continue the conversation.

