Cyber Security Recruitment in 2015

Hosted by:

in-house RECRUITMENT network

Official Partner:

CyberSecurity Jobsite.com

INTRODUCTION

The UK cyber security sector alone is worth over £8 billion and employs around 50,000 people. With the ever increasing cyber security threat to organisations on a global scale, the need to build a robust cyber security team has never been more important.

This paper was created as a follow up to a recent specialist breakfast event for In-house Recruiters organised by The In-house Recruitment Network and officially partnered by CyberSecurityJobsite.com.

SPECIAL GUEST SPEAKER

Nigel Harrison, MBE – Director of Business Engagement, Cyber Security Challenge UK and Professional Secretary, Royal Signals Institution

With over 30 years in the military, almost 3 years in the Cabinet Office helping to shape Government cyber security policy and, most recently, 5 years on the board of Cyber Security Challenge UK, Nigel enlightened, inspired and helped motivate the audience of cyber security recruiters. He examined the current state of the cyber security profession, the complex array of qualifications and awarding bodies, the diverse profiles of those seeking to enter this sector and the potential barriers to them achieving their ambitions.

CHALLENGES & SOLUTIONS

Candidate shortage

This specifically refers to job-ready candidates with practical experience. With many companies recruiting up to 300+ cyber security professionals per year, the demand hugely outweighs the supply.

Solution:
There will always be a candidate shortage and unfortunately there is no single service, resource or strategy that will solve the problem. You quite simply need to use every available resource as part of an integrated recruitment strategy. This includes: events, advertising, profile searching, referrals, head hunting, networking, sponsorship and recruitment agencies.

Declined offers

By the time a candidate reaches the employment offer stage, they will typically have multiple offers to consider.

Solution:
Understand why the offer is being declined and don't always assume it's down to money. We heard from several self professed 'deep pocketed' recruiters who said in most cases an increased financial offer fell on deaf ears. Very often it's the whole package which includes; job challenge, career prospects, quality of life, location, company mindset, company reputation and hiring manager mindset to name but a few.

Safe passage from offer to start

Once an offer has been accepted, this does not mean you have a new employee. Notice periods, restrictive covenants and relocations can all create a volatile time frame that can regularly encourage counter offers from existing employers, recently turned down employers and of course new offers.

Solution:
Communication and engagement. In its simplest terms, picking up the phone and speaking to your new hire will provide an opportunity to counter any possible new objections as well as reaffirming that your company cares about their employees. Who exactly is responsible for this is on a company by company basis however the hiring manager should absolutely be part of this process. Clearly there are far more sophisticated onboarding solutions that dramatically reduce fallout. We recommend you take a look at PathMotion for engagement and SilkRoad for a complete onboarding solution.

Employee retention

Keeping hold of your employees is one thing, keeping hold of the best employees is another thing all together. The risk of poaching due to better offers, under appreciation, under challenge etc is always there. One recruiter remarked, "churn is sometimes a good thing, but why does it always have to be the best ones that go?"

Solution:

This is obviously a huge area that warrants its own paper however employee retention in almost all cases is down to communication, understanding your employee and putting preventative measures in place. As we're talking about cyber security professionals, we know they are clearly in demand and they thrive on challenges. Shape your retention strategy around these key points but also understand that sometimes there's just nothing you can do about it.

Knowing where to look for candidates

Contrary to popular belief, Cyber Security professionals do not just hang out on Linkedin with an up to date and perfectly badged profile saying 'Cyber Security Professional Ready for Hire'.

Solution:

Again, there is no single cyber haven. The definitive answer will come from the cyber security professionals themselves however the recruiters we spoke to indicated they have most success

searching the communities and profiles on Google+, Linkedin, StackOverflow, GitHub. And the CV databases on sites such as CyberSecurityJobsite.com.

Knowing what to search for

It's almost as though they don't want to be found. Cyber Security candidates will very often opt for a generic title of 'IT Professional' or similar and often don't detail their skills.

Solution:

Looking at enough profiles and CV's will give you a definitive list keywords to search for, and there are many. In conjunction with prolific security conscious organisations will again provide yet more searches. However it's more where the profile or CV is found that should give away the cyber security professional's true skill set. Take this Cyber Security Linkedin group for example. After around 10 mins of searching we found dozens of 'IT professionals' which upon closer inspection were the very candidates we were looking for but otherwise would not have found.

Lack of credible qualifications

It was recently remarked by a leading cyber authority that the qualifications for cyber security professionals are, "not worth the paper they are written on." This makes the recruiter search and testing all the more difficult.

Solution:

As you will read from this government article, a great deal of investment is going into the next generation of cyber security professionals and qualifications are very much part of the process. The known qualifications today include:

- CompTIA Security+
- CompTIA Advanced Security Practitioner
- Cloud Computing Security Knowledge CCSK
- CISM (Certified Information Security Manager)
- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Systems Auditor)

Getting hiring managers to sell the benefits

The recruiter has done the hard part in locating and creating candidate interest. Too often we see this hard work undone by hiring manager that cannot seem to understand that not every candidate is desperate to work for their team.

Solution:

Education, communication and senior management buy-in. By their very nature, cyber security hiring managers are not sales people however, they are clearly extremely intelligent and will therefore understand the key role they need to play in a successful hire. Spend one-on-one time explaining how and why the 'selling benefits strategy' is so important and result yielding.

Getting senior management to understand the challenges

There is clearly a disconnect between what senior management wants and what is realistic.

Solution:
Good luck! Yes you'll need lots of that but seriously, this is about making a case armed with facts and figures to back up. Worst case, you'll be covering your backside when you have the 'told you so' moment. It's equally important for you to truly understand why the business' stance is what it is. Sorry, not much help on this one as each case is so unique.

Diversity

Recruitment diversity policy is a good thing however it makes the recruiter's job infinitely more difficult to find candidate's that tick all the boxes

Solution:

There is no magic wand to quickly achieve your business' goals so it's simply down to an awful lot of leg work, additional resource and persistence.

Motivating employees to refer

Employees won't refer if they; a) are considering leaving themselves, b) don't feel the challenge is up to it c) feel that they don't know the referee well enough to ensure they are suitable d) don't need the supposed negative backlash/reputation tarnish for a candidate that doesn't hit the mark. And that's just some of them.

Solution:

Firstly, it's not about the money, it rarely is. It's about literally sitting down with the employee and saying, who do you know, what are their names and don't worry about your name being mentioned, it won't be! But to reiterate, this isn't over email, or through the intranet, it's face to face and personal. One recruiter explained how she had worked extremely hard over the last 18 months to develop a successful employee referral pipeline by simply plotting up at their desks and extracting the names. And then doing it again and again and again.

Getting the outside world to know your business has a great need for cyber professionals

If they don't know you're looking, how can you attract candidates you're not reaching out to through direct approaches?

Solution:

The word 'exposed' is not one you'd usually associate with cyber security but in the case of finding talent, it's essential. You need to let the cyber world know you're hiring and you can do this through sites like CyberSecurityJobSite.com which boasts a reach of circa 10,000, with 250+ jobs advertised daily. But it's not just advertising, you can blast your content through highly targeted mail shots too.

Reducing agency spend

Every company's mandate (when investing in an In-house recruitment function) is to reduce agency spend. But cutting off this valuable option might not actually provide a cost saving at all.

Solution:

Yes it's immensely satisfying to have not used a recruiter however what is the true cost of not using one? Obviously this depends on your business and the resources at your disposal however, recruitment agencies will always play a key role in supporting an in-house recruitment function especially within cyber security.

Understanding and maximising events

Which events? Where? What approach is best? How can you ensure your valuable time is put to best use?

Solution:

Again, a huge topic and one that needs its own whitepaper. However we heard from one recruiter saying he was literally boo'd when he announced his profession at an industry event. But don't let that put you off, a simple round of drinks purchased and/or sponsor place secured can soon turn those boos into cheers and hopefully candidates. Here are a number of events you can visit, gain exposure at and network at.

http://www.cybersecurityexpo.co.uk/

http://cybersecuritysummit.co.uk/

http://cyber2015.psbeevents.co.uk/

http://www.cybersec-expo.com/

http://www.cdans.org/

http://www.cto.int/events/upcoming-events/commonwealth-cybersecurity-forum-2015/

http://cybersecuritychallenge.org.uk/?post_type=tribe_events&eventDisplay=month

http://www.smi-online.co.uk/utility/uk/conference/european-smart-grid-cyber-security

http://www.insidegovernment.co.uk/event-details/cyber-crime-security/468

http://44con.com/

http://www.yourgx.com/pay360/pay360-cyber-security/

Time and demand

In most cases, time is every recruiters No.1 enemy and it's because they are very often under resourced compared to the demands of the business.

Solution:

There's no real quick fire solution. Knowledge, efficiency, understanding and additional resources are all components that will help you to regain that precious time.

Location

Clearly on a case by case basis however we heard from many recruiters saying location gave that extra, unwanted challenge.

Solution:

Many recruiters sighed as we discussed location however the conversation turned on its head as one recruiter remarked how the draw of the South Coast was his ace card. The point is, location is always going to narrow the options however it can also widen them if the lure is strong enough.

ADDITIONAL OBSERVATIONS

Money isn't really the issue

Interestingly, 90% of the recruiters we spoke to agreed that money alone did not a key motivator. So long as the salary package was reasonable and accompanied by job challenge, company mindset, location etc, the level of influence was noteworthy.

Mindset is more important than qualifications

Candidates with the right mindset are of more interest and likely to result in a successful hire than those with qualifications.

New talent is on the way

Significant investment is being made to create opportunities for candidates with transferable skills to enter the cyber security workforce. Cyber Security Challenge for example run numerous competitions in a bid to discover previously untapped talent.

Cyber security people communicate differently

One recruiter walked in to their office, said 'morning' to everyone and not one said 'good morning' back. Until she got to her desk to find IMs saying 'morning'!

Use the phone

One recruiter from a leading Investment Bank commented, "So long as you have a name, the phone is your most powerful weapon. Too many people hide behind electronic communications."

The need to be proactive

Every one of the recruiters we spoke to demonstrated an almost tireless campaign of activity. One recruiter said "It's a numbers game, simple as that."

Most in demand candidates

The hardest people to find are experienced hires (2+ years/2nd Jobbers).

Contract / Permanent

Defence companies seem to be more contract orientated due to clearance levels, private sector is more perm within Cyber.

Education

Masters degrees are more recognised in the market that the many B.Sc. Hons degrees. Also, GCSE are to be introduced into schools which is more cyber centric in the next 2 years.

Cyber security stats

- In 2013 the UK cyber security sector was worth over £6bn and employed around 40,000 people
- 1 in 6 businesses are not confident they'll have sufficient security skills to manage their risks in the next year
- 81% of large organisations had an information security breach in the past year
- 60% of small businesses had an information security breach in the past year

- £600k - £1.15m is the average cost to a large organisation of its worst security breach of the year (up from £450k - £850k a year ago)
- £65k - £115k is the average cost to a small business of its worst security breach of the year (up from £35k - £65k a year ago)

CONCLUSUION

Cyber security recruitment is amongst the most challenging sectors to recruit within. It seems that everything is against you from the start however as you explore all the resources, strategies and opportunities, you will see chinks of light at the end of the tunnel. This, coupled with the momentum gathered by public and private sector investment, is a recruitment sector that will get 'slightly' easier to recruit within and only slowed by the ever increasing demand for cyber security talent.