The Cyber Security Skills Gap and Barriers to Entry – Practical Advice

Martha Tonks

June 2017
Introduction

The cyber security skills gap is certainly not unique to the industry, with many STEM companies struggling to meet their hiring needs, let alone a 40% quota of ethnical or gender minority within their team structures.

With many younger candidates now expecting a better balance of diversity within the companies they are working for; the pressure is on for end users to engage their prospective candidates into a technical security career path so as to be appearing progressive in managerial approach and not just operational outcome.

The reality however, is that career paths in cyber security are full of barriers to entry, with theoretical degrees and non-industry standard certifications muddying the waters of the talent pool.

The challenge for CISO's and hiring managers in finding and nurturing the right talent is a an increasing challenge as well – this report highlights some key findings found during a set of independent interviews with a group of UK based CISO's about their experience of hiring.

This report will look at the ways to improve the cyber security skills gap and the perceived barriers to entry from three view points; firstly, from a candidate perspective, secondly, from a hiring managers perspective and finally from a managerial perspective long term. The arguments made in this report come indirectly from a sample of the CISO responses that were interviewed by Acumin specifically for the purpose of this report.
For Candidates:

For those looking to enter into the cyber security industry, the prospect of making it through several interview stages to work for a large end user is certainly daunting. Especially for those without a technical security background or at an earlier point in their career path.

On behalf of Acumin Consulting, I conducted a survey with CISO’s from multiple organisations looking at what they value in prospective candidates when hiring, and also their own insecurities or concerns when hiring and managing teams of professionals.

The results were conclusive. Nearly all CISO’s agreed on several key issues that correlated to their hiring strategy which are outlined below. These fall into the following themes; Similar Experience, Certifications, interest and communication skills.

Similar Experience:

This is not something every candidate will be able to bring to the interview; but regardless of industry it's a sure way to be able to demonstrate an ability to perform the role requirements.

For those with experience in the industry; ensure you come prepared with examples of application and outcomes from your role responsibility relevant to the job requirement details.

For those who do not but are interested in starting a career utilising cyber security skills, consider trying to gain work experience or personal projects that demonstrate the technical ability that would be expected of you in the role.

Certifications:

Gaining certifications may seem like an obvious route for demonstrating your abilities. However, all CISO’s surveyed said that they do not put much stock behind the majority of cyber security industry certifications, the exception being CISSP.

The reason for this was that many certifications are based on theoretical knowledge that can be attained through revision – rather than experience in a post.

Gaining multiple certifications namely shows that the candidate is good at studying cyber security.

“Courses by their very nature are theoretical, which is not that helpful when looking for an individual with the experience to able to own the responsibility of the role. “

Moreover, more and more online certifications are up and running, the actual content of which the average CISO does not know.

The answer, less is more. Having the right certifications for the role is what the hiring manager is looking for. Do your research to know what is best and supplement your certifications with real experience.

Interest:

It is hardly a surprise that most CISO’s when asked said that they look for interest and passion in the role remit and the general cyber and technology industry.

The cyber security industry requires its participants to be constantly learning and researching new and potential threats and solutions, without a genuine drive to be a creative problem solver candidates might not last the distance.

“Passion for the topic, I look for energy. You can teach any skill.”
The idea that interest in the subject area is in some cases, more important than having a technical security background shows how much the cyber security skills gap is affecting organisations. CISO’s are now coming round to the idea that they will need to invest and train their workforce over longer periods of time rather than just hiring the finished article if they want to keep expanding their teams to their organisational needs.

So if you can demonstrate that you want to work within the industry long term and can demonstrate passion, you may just catch the interviewer’s attention.

**People Skills:**

What are the core skills you look for when hiring a cyber security professional?

*“People skills, it’s the first thing on my mind.”*

Said every CISO surveyed.

You can teach product knowledge or technical security but it is much harder to teach someone how to effectively communicate to team members and to those with a non technical security background.

It’s something that few people are lucky to have naturally, but come prepared to demonstrate how you have been a valuable leader when necessary, but also a team member that can be relied upon by your prospective manager and other team mates.

**Networking and Mentorship:**

If you are lacking experience in a corporate environment in technical security; your best strategy should be to get involved in the industry networking events as a way of demonstrating interest and communication and networking skills for your potential employer.

Sign up to conferences and awareness events and be active in your attendance on social media.

Whilst you’re there: It’s easy to forget that a lot of people are in a situation similar to you when going to these type events – not everyone knows each other. Whilst you might learn some valuable information from standing on the side-lines quietly, you are going to learn a lot more from talking to the speech makers and other attendees.

Networking at these events can lead to industry placements and finding a mentor from a company or job title you admire who can give you follow up advice on the route they took to making a successful career in cyber security.

You can also find mentors from online groups or industry forums and consortiums like ISC2.

Half of the CISO’s interviewed for this report said that networking events are crucial to the industry’s sharing culture and an easy way to get to grips with key trends that are affecting organisations.
For Hiring Managers:

For those with the responsibility of hiring strategy for the cyber security division within their organisation, the findings of this report will most likely echo past or current experiences when on the hunt for new staff.

From the CISO’s interviewed, the most common responses for why it was difficult to find a suitable candidate can be seen from Fig. 1.

**Fig. 1**

**ISSUES WHEN HIRING**

![DIAGRAM SHOWING ISSUES WHEN HIRING]

**CV Inaccuracy:**

The biggest contributor to why the hiring process could be timely or frustrating was down to how the candidates themselves were painting a picture of their relevant experiences.

*"You meet a lot of people with very good CV’S but nowhere near enough actual knowledge."*

During the interviewing stage for the research of this report, each CISO spoke at length at the problem of over-exaggeration on CV’s which were easily unpicked at interview stage.

The solve to this problem is difficult; it cannot be easily managed by the company who is recruiting but the responsibility falls to the individual applying. Recruitment Service providers can definitely help; if they have the technical knowledge to be able to unpick relevant skill sets for each role and pre-qualify candidates.

An overzealous CV from a potential candidate can be born out of several intentions. The obvious assumption that is made is that the person is overcompensating for the experience they do have. Most Hiring Managers expect that certain candidates might stretch the truth a little, and so dig a little to explore the truth of the situation. However, if the person conducting the interview has little technical security background, wheedling out weaker candidates from a first stage interview might not be so clear cut.
CV puffery can also arise from internal promotions from previous roles making actual role responsibilities unclear to the interviewer. For technical roles; this can be a real headache when hiring as previous grandiose job titles may relate little to managing complex security procedures day to day.

**Available Candidates:**

The second most important issue when hiring is the lack of talent pool available for roles, otherwise recognised as the cyber security skills gap itself.

Interestingly, some CISO’s had not noticed roles advertised getting little interest though this would likely correlate to the fact that the organisation itself has enough brand authority that roles are in high demand across all job titles.

It is also important to make the distinction between not having enough candidates applying for roles advertised, and not enough of the hiring managers ideal profile of candidate applying for the available roles.

Candidates with no technical security background; or a limited security background but with the commercial awareness to understand that the industry is growing on a growth period which is set to continue long term are making the strategic attempt to enter the industry.

This is understandable; and there are no illusions that the UK needs more people to be interested in training in cyber relates skills. For hiring managers without the ability to spend time to train recruits; this can provide a bit of a headache as CV’s with limited yet puffed up accounts of related experience can lead to skill vacuums within teams once too many people of this calibre get placed. However, Hiring Managers with the resources to train those with a genuine interest in the sector could obtain highly engaged new employees.

The way to tackle the lack of technical security background when faced with too few fully qualified candidates for the roles available; is to be looking for transferable skills that can work well within existing teams.

Hiring managers have placed good communication and influencing skills high on the agenda when hiring cyber professionals because of the understanding that there needs to be an improvement in the way security risks are judged in the boardroom.

Those looking at the consistent problem of too few candidates applying for roles need to assess whether they have the time to train those who can demonstrate good communication skills into such role to bridge the gap between technical and commercial viewpoints.

**Competitiveness:**

A final comment on the lack of suitable candidates that enter the hiring process is that the role on offer is not as inviting as a competitors. Improving diversity statistics within the STEM industries including cyber security musty come from getting the attention of women, and also of younger candidates who can positively affect the age imbalance of those currently within the industry.

The gender diversity gap is prevalent in all STEM industries but government initiatives and education-focused organisations are currently working towards improving the statistics of young women looking to enter such industries. The statistics related to women holding senior positions in STEM related industries is another topic; but it is certain that the way in which cyber roles are presented needs work to attract additional attention from women.

Comments on the idea that cyber remains a “dark art” and the public understanding of the breadth of roles and skills necessary to make a successful cyber security management process is limited.
Organisations would do well to focus less on technical qualifications and more on analytical, creative problem solving, and communication skills that are of equal importance when selecting an individual candidate – should they want to make a conscious effort to improve gender diversity statistics.

There is also the awareness that recent graduates or entry-level candidates are caught by consultancies and the Big 4. Firms wishing to hire junior roles with a mind to fostering their loyalty should consider advertising cyber focussed career progressions pathways or graduate schemes.

For Managing Long Term:

The cyber security skills gap and the associated barriers to entry for prospective candidates are set to continue. CISO’s need to be forthcoming with their hiring and staff retention strategy to drive results.

During the interviews undertaken to provide insight for this report, CISO’s were asked what actions they were undertaking to improve the processes of finding and retaining the right staff.

Fig. 2 reflects on the priorities of CISO’s interviews for their HR related activities in the upcoming months.

Fig 2.

HIRING PRIORITIES

<table>
<thead>
<tr>
<th>Retaining Staff</th>
<th>Improving Diversity</th>
<th>No Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiring More Staff</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Retaining Staff:

CISO’s or those with the responsibility of managing teams name retaining their current staff as a major priority.

Retaining effective staff is good both for team morale but also for business performance. Departments evolve and adapt to the organisational and external industry climate. Strategies and processes in the day-to-day running of departments are most often unstructured and the result of casual communication between staff.

A team that disbands or in the scenario of key team members leaving, information gets lost, and it is for the retained staff to bring to light the activities that were successful from the previous group dynamic’s strategy. Moreover, these learned nuances form a brain drain that can then be picked up by other organisations and even used as a competitive advantage.

Retaining staff depends on primarily how individuals are treated, or their investment in the company. Those with a genuine interest in cyber security practices and also with a desire to take on managerial responsibility are likely to be engaged employees with long term career aspirations. Appreciating each employee’s intrinsic incentives of being in their current role is paramount to keeping them engaged.
Understanding if someone is driven by salary incentives, or the need to be recognised for doing positive work through internal promotion or for the fact that the role works within their value set and lifestyle is key for managers so they can edit their communication approach.

A manager’s communication approach has a large effect on an internal company culture, which in turn drastically affects team productivity and attitude. Understanding what your staff are incentivised by and providing a culture in harmony with that is no easy feat – but imperative if you want to retain and grow.

The other point to mention is to focus on creating a company culture that supports individual development and learning. Companies that focus on training opportunities for staff are far more likely to foster good levels of employee engagement and loyalty.

**Increased Hiring:**

The need for effective cyber security solutions and management will continue to grow as companies and individuals become more and more interconnected with each other, and technology. This in turns makes cyber security a stable career path. But the need to get people interested and correctly trained is still proving an uphill struggle; much to the concern of hiring managers.

It is no doubt that the need for increased hiring in cyber security will hit most organisations in the UK and worldwide. CISO’s and managers need to think carefully about their selection process to ensure they are hiring the right people for their needs.

One approach would be to be more vigorous and try to only allow those with the technical ability to do the role reach interview stage.

“I use a Technical screening in the interview process, early on.”

Though this approach may be off-putting to some candidates, there is an argument that only candidates who are invested in becoming part of the company continue. It is also an impartial way of deciding who progresses to interview, if you are in the situation where lots of individuals apply.

Another approach is to be far more fluid with the selection process and to hire with a focus on getting the right transferable skills for the team the candidate will be part of. This reflects the interpretation of a lot of the CISO’s interviewed views on needing candidates with good analytical and communication skills, but finding relatively few with the exact technical experience as well.

If facing a severe issue keeping up with the demand for cyber security staff in your organisation, then this approach could prove effective.

This is also supported by the evidence shown in Fig 3. of candidates hired into technical security roles by CISO’s interviewed from different backgrounds. When asked if hiring outside a security background had been effective, most agreed that someone’s ability to do the job can only be truly explored once they are in the role and the lack of technical background had been of little disadvantage.

---

![Fig.3](image-url)
Improving Diversity:

Improving diversity is a heavy burden to place on the shoulders of a CISO. The diversity skills gap far outstrips the general issue not having enough trained and available security staff for the demand in the current UK market.

Whilst there are plenty of initiatives that are trying to support women and ethnic minorities who may be interested in working in cyber security in existence, the reality it the push is mainly in education at trying to encourage students to choose a career path in a STEM industry. This does little to solve the immediate problem that CISO’s and organisations have in terms of the cyber skills gap; though encouraging for the future.

A way in which CISO’s can manage their diversity hiring process alongside being more open to the technical security experience they are looking for; is by contributing to debunking stereotypes of the industry itself.

Marketing the flexibility of working conditions and focus on diversity initiatives is both positive PR for the organisation as a whole but also does much to encourage candidates who may have felt the environment would not have been a natural fit to consider a role.

The benefits of creating a more well-rounded team are manifold such as increasing innovation and agility as diversified teams represent different viewpoints and skills sets that come from different backgrounds and working styles.

Another way to increase the amount of candidates from minorities is to change the approach to role advertisements. Creating open, transferable skills based advertisements rather than a focussing on checklist of technical capabilities or certifications may make the industry seem more approachable to potentially successful candidates.

Rather than focussing on technical capabilities as must-haves that might alienate candidates who may have 8 out of 10 skills otherwise needed for the role, an alternative would be to champion the attributes the person would need to possess in order to do well.

Role advertisements that seem to have a holistic approach to candidate selection suggest a flexible and modern company ethos; which can be extremely attractive to people who value communication and openness.

Conclusions:

The reality of the cyber security industry is perhaps very different from how it might be perceived by those external to it. We know it as a collaborative and forward thinking entity that values those who can analyse, problem solve and effectively communicate, generally in that order.

Those with an interest to enter into the industry would do well to heed the advice or arming themselves with a passion to learn from industry experts rather than text books, and find technical experience wherever they can.

Hiring managers would also do well to keep focussed on the person they are hiring rather than just focusing on the skills they can demonstrate. Someone who can be a linchpin between technical staff and boardroom politics is a much have, and should be rewarded as such.

Those responsible for the company cyber security division long term would also do well to try and keep building flexibility into their hiring approach and continue with good intentions in terms of diversity and managerial flair – in the hope that the statistics will balance to industry expectations eventually.
About:

Acumin was one of the first Cyber and Information Security recruitment specialists to emerge back in 1998. Now we are an industry leading consultancy operating throughout EMEA as well as in the USA.

We work with world leading clients and provide our services to security vendors, end user organisations, systems integrators and consultancies.

Our unique understanding of the industry, and the specialist skills our candidates need to survive position our consultants to provide effective services across contract, permanent and retained search and managed services projects.

Acumin offer a bespoke service that works with the client to understand the processes and requirements and always deliver with organisational goals in mind.

Acumin work to produce interesting industry relevant content as a further supplement to our insider knowledge and sharing culture with our network in the cyber security industry.

About the Author:

Martha Tonks has nearly 3 years experience in marketing and content creation, and works directly for Acumin. Whilst maintaining the Acumin blog and other marketing duties Martha works to create whitepapers and larger report projects that highlight key industry issues and common experiences for those acting within the cyber security landscape.

If you would like to reach her directly, either about this report or for information about other content created for Acumin please email: mtonks@acumin.co.uk

Contact:

e-mail:

For Clients: vacancy@acumin.co.uk
For Candidates: careers@acumin.co.uk

phone -

0203 119 3333

web -

www.acumin.co.uk