

# Your Career in Cybersecurity

Created by Jamie O'Hare

@TheHairyJ

March 2022



**Aim:** The aim of this exercise is to explore the various roles and career paths in the cybersecurity industry. Through extensive reading and reading online, this exercise hopes to make the reader more aware of the industry they may find themselves soon.

For this exercise, all you require is a web browser, however, a spreadsheet application may be beneficial.

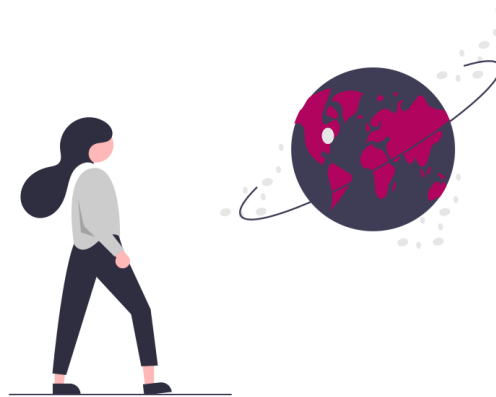
**Notes:** There is a tremendous amount of content in the exercise, this is intentional. You can tackle this content in as much depth as you wish. It is highly recommended you take your time to explore the content as thoroughly as possible on your first engagement. Although the document is worth revisiting down the line.

Wikipedia is used as reference material intentionally. These links are for generic introductions to a topic, they stay up to date, and they aren't likely to break. When writing reports don't reference Wikipedia as it is not seen as a credible source.

If any link does not work, please attempt to use the Wayback Machine (linked below) to view the content prior to its inaccessibility.

 **The Wayback Machine**  
<https://archive.org/web/>

## The Cybersecurity Skill Shortage



You'll hopefully be aware of the cybersecurity skill shortage, if you haven't, I'd be surprised. There has been no shortage in articles written about the matter, even as far back as 2010 (Muncaster, 2022)(Gjelten, 2010). However, if you somehow haven't heard of this "issue", then time for a quick explainer.

Hiring (and keeping) cybersecurity professionals has been an increasing issue for the best part of the last decade (Reese, 2021). In the UK, the estimated number of cybersecurity professionals is somewhere around 200,000 individuals, various estimates show a growing demand for these professionals at nearly 10% (Scroxtton, 2021). However, despite the rising number of graduates, apprenticeships, and a noteworthy number of workers retraining for cybersecurity roles, there is still a significant shortfall. As such there has been a concerted effort to attract more people to the industry, even if some of them have been ill-advised, see Figure 1.



Figure 1 - A poorly timed government advert concerning cybersecurity training.


**BBC Article about the Fallout Over the Fatima Advert**  
<https://www.bbc.co.uk/news/business-54505841>

In 2021, the UK Government’s Department for Digital, Culture, Media & Sport (DCMS) released research detailing skills needs and job vacancies across the UK cyber security sector (DCMS, 2021). These reports and the associated infographics provide greater insight than the flashy headlines, as seen in Figure 2. Take note of the reasons for hard-to-fill vacancies, we may come across the same language further on in this exercise.

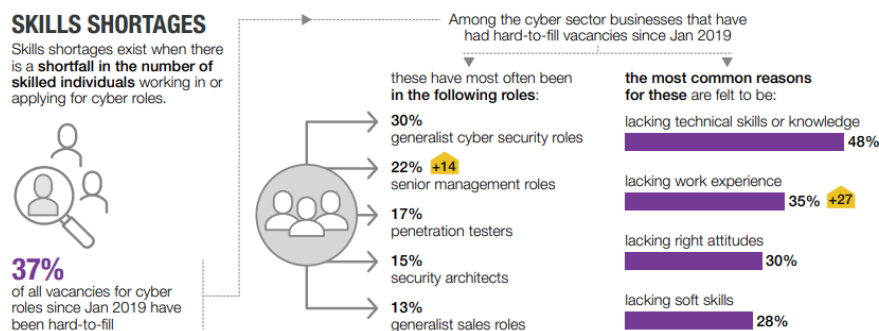


Figure 2 - Cybersecurity Skills Shortages in the UK in 2021 (DCMS, 2021)


**Cybersecurity skills in the UK labour market 2021**  
<https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021>

The same infographic provides some recruitment details, as seen in Figure 3.

## RECRUITMENT

**28%**  
have offered internships in  
cyber roles since Jan 2019



**47%**  
have had vacancies in  
cyber roles since Jan 2019

Among these 47%, the most common  
recruitment approaches are:

48% recruitment agencies

35% social media posts or ads

33% word-of-mouth or  
industry networks

**Figure 3 - Cybersecurity Recruitment Statistics in the UK in 2021 (DCMS, 2021)**

If you are up for some “light” reading, there is a further DCMS report, which goes into specific details about the makeup of workforce demographics. See the link below.



### **Understanding the cyber security recruitment pool**

<https://www.gov.uk/government/publications/understanding-the-cyber-security-recruitment-pool>

The cybersecurity skill shortage isn't just a UK issue, it's world-wide. An American academic, Ming Chow (@oxmchow on Twitter – who often streams his classes on Twitch) has been maintaining a page which documents articles detailing the skill shortage on his side of the pond. See the link below for more details.



### **Cybersecurity Skills Shortage**

<https://gist.github.com/mchow01/9569350f3b975ce84dad68f0d95c4579>

So, what does the cybersecurity skill shortage mean for you? Well, it does mean there are opportunities aplenty. However, if you expect to waltz into a job, I'm afraid you are sorely mistaken. As illustrated in the figures above, being able to demonstrate a high-level understanding of technical skills and knowledge, along with high-quality soft skills is a must. The specifics of these further requirements will differ depending on the role, so it's good to know what roles are out there...

## The Various Job Roles in Cybersecurity



As the cybersecurity domain has matured, more and more specialist roles have emerged. Many moons ago, I use to present a slide containing over 80 different jobs titles in the industry, as seen Figure 4. This was a great slide to show the diversity of opportunities open to a cybersecurity professional.



Figure 4 - Slide of 89 Job Roles in Cybersecurity


**80+ Job Roles in Cybersecurity**  
<https://www.inspiredcareers.org/browse-careers/cyber-security/>

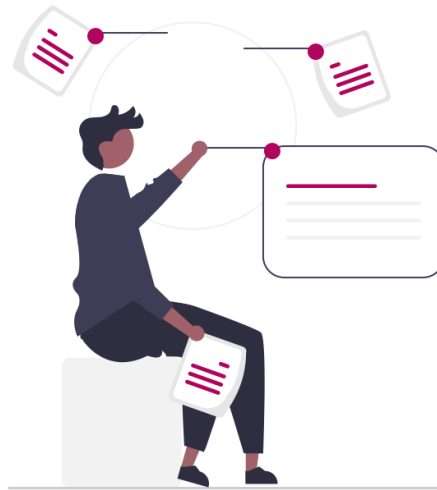
I've distilled this massive list down to some central roles and responsibilities. This is by no means an exhaustive list. I've merely selected some of the most

common role archetypes in the industry. Additionally, I've kept this list rather concentrated on rather junior positions. Naturally, there is a greater scope of senior and managerial positions as well as hybrid positions between cybersecurity and other business operations.

Look at the list below, select a few interesting roles and research what responsibilities someone with that role may have.

- Security Awareness Trainer
- Compliance Auditor
- Incident Responder
- Software Developer
- Cybersecurity Journalist
- Data Protection Officer
- Intrusion Analyst
- Malware Researcher
- Reverse Engineer
- Network Administrator
- PCI Consultant
- Penetration Tester
- Recruitment Consultant
- Risk & Regulatory Consultant
- Security Administrator
- Security Architect
- SOC Analyst
- Systems Administrator
- Targeted Attack Specialist
- Security Researcher
- Triage Coordinator
- Vulnerability Assessor
- Intrusion Analyst
- ISO27001 Auditor
- Forensics Analyst
- Database Administrator
- Access Control Administrator

## Start Thinking of Your Next Steps.



The previous sections may have sparked an interest in exploring the opportunities open to you in cybersecurity. Now is a good as time as any to consider what the next steps in your career will be.

Do you want to find an internship? Do you want to relocate? Would you want to work in cybersecurity in the public sector?... You are probably pondering questions like these, however, don't worry about being decisive in your answers, you've still got plenty of time to consider your options.

To help you in your decision making as well as expose you to the industry, the remainder of this exercise will explore and research the current job market to discover possible opportunities in the cybersecurity domain.

To keep track of your research, it is recommended you use a spreadsheet application such as Microsoft Excel or Google Sheets. The reason for the spreadsheet rather than a text document is to allow you to be as detailed as you want, while still catering towards comparisons. With a spreadsheet, the various employers and roles could be the rows, while the columns could be various aspects of the job role, such as location, requirements, benefits.

Once you've created your spreadsheet file, you'll need to populate it. The remainder of this exercise will show you how to do so comprehensively.



## Jamie's Job Discovery Methodology



In the sections above or perhaps in your own free time, you've likely Googled "Cybersecurity jobs" or something similar, while fruitful, this may not have returned all the vacancies you may be interested in. Have no fear! I've devised a methodology to help my students comprehensively discover opportunities in the cybersecurity job market.

This section will start out by outlining the methodology before, detailing each step chronologically.

### **Jamie's Job Discovery Methodology™**

1. Government, Military, Intergovernmental Organisations, NGOs etc.
2. The Big 4, FAANG, and other similar organisations.
3. Apps on your phone/computer.
4. The "High Street".
5. CREST-accredited companies.
6. Any sponsors of local conferences.
7. Contacts.

## Step 1 – The Public Sector and Beyond

The first step of Jamie’s Job Discovery Methodology is intergovernmental and non-governmental organisations. I’ve put these organisations first, as their recruitment process is likely to be the lengthiest and include the greatest obstacles to employment, some of which you may not be able to overcome.

Starting with the obvious, look at the various security services, and government agencies. In the UK, we have Government Communications Headquarters (GCHQ), National Cyber Security Centre (NCSC), National Crime Agency (NCA), The Security Service (MI5), Secret Intelligence Service (SIS). Have a look at the roles and vacancies for each of these agencies, looking at their requirements, both technical and non-technical.

If you hold dual nationality, or are not from the UK, go investigate your countries’ security services and see what they require. Additionally, the Government itself may require cybersecurity talent. As such, make sure to check out job posts and graduate schemes with the civil service.

Perhaps one of the most interesting “governmental” positions I have come across in my time was for the British royal household. See job posting linked below.

 **Cyber Security Engineer @ The Royal Household**  
<https://theroyalhousehold.tal.net/vx/lang-en-GB/mobile-0/appcentre-1/brand-3/xf-f2aaf105a1aa/candidate/so/pm/1/pl/4/opp/2380-Cyber-Security-Engineer>

Most if not all these organisations will require you to be a sole UK national, with a clean police record - these requirements are very strict. So, if you want to work for one of these agencies make sure to keep out of trouble! In addition to these stringent requirements, a successful applicant may be required to obtain appropriate security clearance via a rigorous vetting procedure. As such the application to successful job offer may take an extensive time, hence why these opportunities are positioned first on the methodology.

Now let’s consider larger intergovernmental organisations, and other. Depending on your world knowledge, you may not know many global organisations, therefore, I’ve compiled a list for you.

- United Nations
- European Union
- World Trade Organisation
- World Bank Group
- World Health Organisation
- Olympics

Perhaps unsurprisingly, Oxford University has many resources on trying to get a job at an international organisation, see link below for more detail.



**Oxford University's Career Service Advice for International Orgs.**

<https://www.careers.ox.ac.uk/international-organisations/>

The final consideration for this step is to consider roles that may require some uniform – the military and police. The massive impact technology has had over the past few decades has brought increasing demand on both the military and police to stay ahead of the new challenges they now face.

There has been a huge effort in recent years to expand the cybersecurity capabilities of the armed forces. One step toward modernisation was the creation of a new cyber regiment – 13<sup>th</sup> Signal Regiment (Sengupta, 2020). See the link below for more details. There are also cybersecurity roles in the Royal Air Force and the Royal Navy. If you are interested, look at their recruitment pages.



**Launch of Cyber Regiment in major modernisation.**

<https://www.gov.uk/government/news/armed-forces-announce-launch-of-first-cyber-regiment-in-major-modernisation>

If you hold dual nationality, or are not from the UK, go investigate your countries' armed forces' recruitment pages and see whether you could put your skills to use in uniform.

Alternatively, there are opportunities aplenty in the various forms of law enforcement. With cybercrime, and cyber-enabled crime on the rise, there are no shortage of cybersecurity work in the police force (O'Sullivan, 2021)(Roberts, 2021). In Scotland, the police force is centralised with Police Scotland, however, across the border in England, each geographic region has its own police force. Each police force may have its own cybersecurity division, in addition they may also have a digital forensics division. These forensic analysts work on the immense backlog of cybercrime and cyber-enabled crime investigations.

While on the topic of Digital Forensics, it may be worth dispelling the misconception that all digital forensics work is done in conjunction with police work. This is false. While there are private organisations which offer digital forensics services, namely for data recovery services, there is also work-place investigations in the scenario of an insider attack! Digital forensics skills can also be required in roles such as a SOC analyst, or incident responder.

Police work isn't typically as stringent as security agencies in terms of nationality requirements, so if you want to relocate, perhaps you can look at work in law enforcement elsewhere.



**Police Scotland Launches Cyber-Enabled Crime team in Northeast**

<https://www.scottishlegal.com/articles/police-scotland-launches-cyber-enabled-crime-team-in-north-east>

## Step 2 - The Big 4 and Big Tech

The second step of Jamie's Job Discovery Methodology involves looking at opportunities at some of the largest companies in the world. I've put this step second as the recruitment process is likely to be the lengthy, include numerous rounds and interview stages. Additionally, these openings will likely be the most competitive. This section will look focus on the "Big 4" as well as "Big Tech", however, it will also consider similar size enterprises.

Our first stop in surveying the largest companies in the world are the Big Four accounting firms, commonly called the Big 4. The members of this illustrious group are Deloitte, EY, KPMG, and PwC as seen in Figure 5 (and if that comes up in a pub quiz, I want credit). These large organisations have offices across the world, however, conveniently all have main offices based in London.



Figure 5 - The Big 4 Account Firms' logos

 **The Big Four Accounting Firms**  
[https://en.wikipedia.org/wiki/Big\\_Four\\_accounting\\_firms](https://en.wikipedia.org/wiki/Big_Four_accounting_firms)

Other firms outside the Big 4 do exist. Quite possibly the easiest way to identify such organisations is to rack your brains for businesses which appear on the side of buildings in business districts. Don't know what I am talking about? See Figure 6. Take time to consider, other related businesses. Perhaps Morgan Stanley, JP Morgan, Deutsche Bank etc.



**Figure 6 - Firms portraying their dominance by displaying their name on the side of large buildings**

The Big 4 and similar large financial institutions have very competitive graduate and internship positions. As such, they often require multiple rounds of interviews to whittle down the candidate list. Look up something similar Big 4 Graduate interviews on Google, and you'll be flooded with YouTube Videos, Blogs and Student Room forum posts all about the interview process. Going into detail about the interview process for all these different organisations is outwith the scope of the document, perhaps you can investigate it if you are interested.

On the Big Tech side, investors used the acronym FAANG to group Facebook, Apple, Amazon, Netflix, and Google. However, recently there has been suggestions of changing the acronym to MAMAA. This new acronym stands for Meta, Amazon, Microsoft, Apple, and Alphabet as seen in Figure 7. Reasons for change are four-fold, Google and Facebook's rebranding to Alphabet and Meta respectively, the inclusion of Microsoft, and the removal of Netflix (due to their market value not keeping pace with the others) (Stankiewicz, 2021).




Figure 7 - Logos of the MAMAA group

 **Big Tech**  
[https://en.wikipedia.org/wiki/Big\\_Tech](https://en.wikipedia.org/wiki/Big_Tech)

Like the discussion on the Big 4, other large technology firms do exist. After all Netflix was removed from FAANG when it transitioned to MAMAA. Think of organisations which might be included in MAMAA in years to come, then look up those businesses for any cybersecurity opportunities. Don't be too exhaustive for this section as the following methodology step should catch the rest.

Similar to the discussion regarding the Big 4, Big Tech have some very competitive graduate and internship positions. As such, a successful applicant may have to complete multiple rounds of interviews. Much of these processes are documented online, in fact you can actually watch real interviews on YouTube. Although mostly programming role focused have a look at some of the links below to see what an interview (and questions) may look like from a Big Tech organisation.

 **Python Interview with a Google Engineer**  
<https://www.youtube.com/watch?v=wyu6VRmtCmE>

 **Python Interview Qs from Google, Amazon, and more**  
<https://interviewing.io/python-interview-questions/>



**How To Solve Google's 25 Horses Interview Question**

<https://www.youtube.com/watch?v=i-xqRDwpilM>



### Step 3 – Those Familiar to You

The third step of the Methodology requires your phone (and or home computer). I've put this step third as these organisations can be quite diverse. Many may have lengthy interviews processes for a competitive graduate programme, or some may specialise in and or junior roles. Additionally, the companies are more likely to be international, so you may have to relocate.

For this step, open your phone and examine the apps you have installed. Use the apps you have in order to identify the companies that developed them. Avoid revisiting the same companies as the previous section (i.e., if you have Instagram, don't go back to Meta's career site).

If you are struggling to find anything, try these companies listed below.

- Snap Inc.
- Twitch
- Slack
- TikTok
- BBC
- Discord
- NHS
- Uber
- Spotify

This step also includes your various technology hobbies. Personally, I play too many video games. I therefore can use my collection of games to find companies who may require cybersecurity personnel and hopefully discover some unique opportunities. While some of the games I have were created by small indie developers, some of the bigger production houses, and publishers may have cyber teams.

Below I've listed some organisations you may want to look at, as well as a job which has caught my eye for some time.

- EA
- Valve
- Blizzard
- Ubisoft
- DICE
- Nintendo
- 2K
- Bethesda
- Riot


 **Cheat Software Analyst @ Rockstar North**  
<https://www.rockstargames.com/careers/openings/position/4351220003>

#### Step 4 - Those Down the Street

Despite what the senior generation may think, going out and handing in CVs around town, won't land you a job as it did back in there day. However, we can still use that idea to inform our job search. The fourth step of the Methodology is going to use your local high street(s) to identify possible employers. This is forth as while some employers may have lengthy interviews processes, most of these opportunities should be national, rather than spread around the globe.

For this step, either think back about your local high street and enumerate through each business to see if they have any opportunities.

Can't remember anything on the high street? Have a look via Google Maps Street View at Oxford Street in London or the new St James Quarter in Edinburgh, and/or look at those listed below.

 **Oxford Street in London**  
<https://www.google.com/maps/place/Oxford+St,+London/@51.5152543,-0.1442282,17z/>

 **St James Quarter in Edinburgh**  
<https://www.google.com/maps/place/St+James+Quarter/@55.9549869,-3.1911471,17z/>

- IKEA
- Tesco
- Asda
- Peloton
- ASOS
- M&S
- Lego
- Three
- Vodafone

While we're here, we might want to consider other atypical cybersecurity employers. More recently, large sports teams across various disciplines are hiring cybersecurity personnel. This includes Premier League football, F1 racing, NFL, etc. So, if you didn't make it at sports, you can still work for your dream team.

The transport sector has a few abnormalities which could lead to some interesting opportunities. Explore organisations such as Edinburgh Airport, Transport for London, Network Rail, Rolls Royce, and any more you can think of.

## Step 5 –The Cybersecurity Industry.

If you want to get some experience working in a cybersecurity company rather than a cybersecurity department, then using the fifth step of the Job Discovery Methodology may be the one for you. I've put this step fourth as it likely to be the most specific roles, and while most of the organisations are UK-based, there is some international organisations too.

For this step, we'll be using the CREST website. CREST is an international not-for-profit accreditation and certification body for the cybersecurity domain. Companies seek out these accreditations to be eligible and appeal to organisations which put contracts out for tender. What's great about the CREST website is that they list all accredited companies by the certification they've got. Meaning, you or I can examine the lists depending on what your interest.

 **CREST website**  
<https://www.crest-approved.org/>

Start by navigating to the accredited companies' menu found in Figure 8. Then select one of the "Accredited Services" filters on the right-hand side. Filter to your desire, then click on any company, and you'll be greeted with some information about this company – including their address and website. Additionally, you'll see phone numbers and email addresses, avoid reaching via these lines as it's for sales purposes – and one way to not get you an interview! Have a look through all the list and companies which pique your interest.



About Us ▾

Regions ▾

Membership ▾

Certifi

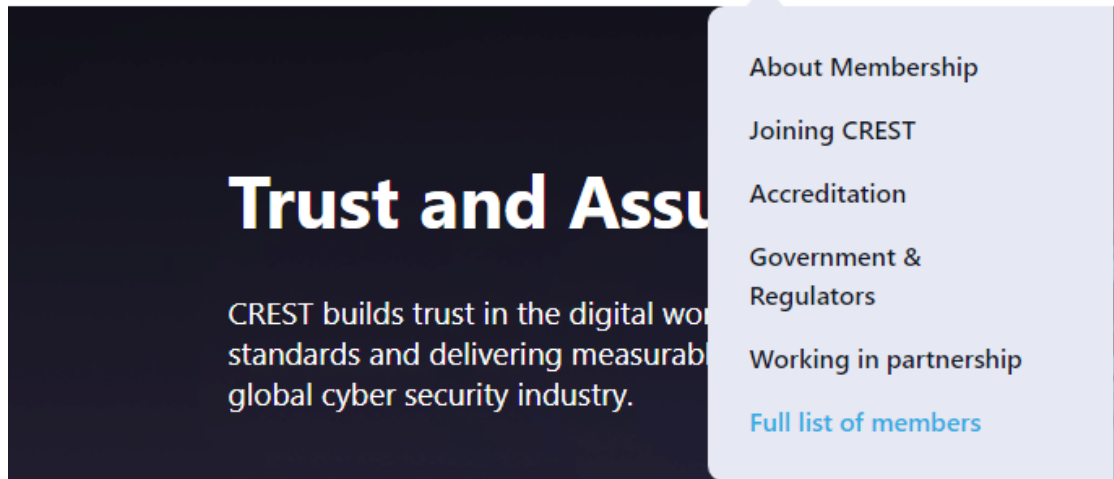




Figure 8 - Where to find CREST's Members Listing

Alternatively, a similar technique would be to look at the organisations operating bug bounty programmes on Hacker1 and Bugcrowd. Each of these bug bounty platforms include a handy list of all those operating programmes. See the links below for more possible job listings – don't forget to check Hacker1 and Bugcrowd themselves too.

-  **Hacker1 Directory**  
<https://hackerone.com/directory/programs>
-  **Bugcrowd Directory**  
<https://bugcrowd.com/programs>

## Step 6 – Local Friends

Cybersecurity professionals often attend conferences to see the latest research, and network with others in the industry. If you've never been to one of these I would highly recommend – even if just for the free swag. However, these conferences would not be possible without those companies who sponsor them. The penultimate step of this Methodology uses these local conferences to identify sponsors, who after all are spending the money for advertising purposes. This is the sixth step as organisations identified are likely those encountered in previous steps. However, this technique may uncover some small organisations who care about the community they find themselves in.

In Scotland you have multiple cybersecurity conferences, use the list below to identify conference sponsors. Then go look at their careers page, to see if there are any opportunities. You may wish to use the Wayback Machine, linked below, to view the sponsors of previous years to broaden your search.

- Securi-Tay
- Le Tour Du Hack
- G3C
- Scotsecure
- DIGITExpo
- Public Sector Cybersecurity Scotland
- BSides Scotland
- Scottish Cyber Awards



**The Wayback Machine**

<https://archive.org/web/>

Let's say you don't want to work in the UK and would like to move further afield. Well, you can still use this technique, all you must do is look up conferences in a place you'd like to relocate too. If you'd like to move to New Zealand, perhaps look at KiwiCon. If United States takes your fancy, there is DEFCON and BlackHat USA. Below are links to those respective conferences, along with the Security BSides conference page which contains a world map of all BSides conferences.

 **KiwiCon**  
<https://www.kiwicon.org/>

 **DEFCON**  
<https://defcon.org/>

 **BlackHat USA**  
<https://www.blackhat.com/us-21/index.html>

 **Security BSides Conferences**  
<http://www.securitybsides.com/w/page/12194156/FrontPage>

## **Step 7 – It’s Not What You Know, It’s Who.**

Finally, the last step of the Job Discovery Methodology is about your personal contacts. There is no nifty website, nor a sure-fire technique, this step is simply on you.

Throughout your life, you’ll meet, be introduced to, or bump into an innumerable number of people, some could be in cybersecurity, some in tangential fields.

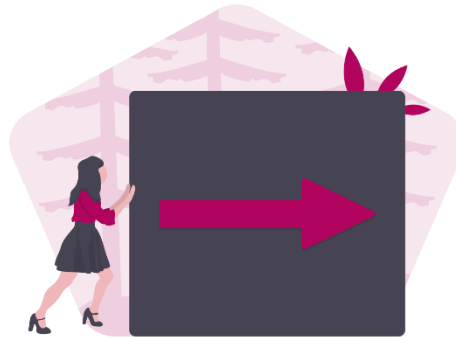
Each person you meet might have a vacancy in their team or know of someone else who does. On the flipside, you may be in the position to hire someone, and through connections know an acquaintance who is more than up to the task. Making these connections may lead your career down a path previously impossible, so it is important you make and maintain these relationships. Some may suggest having various social media accounts for this purpose, personally this is what I use my Twitter and LinkedIn for, however, it’s up to you.

### **Methodology Complete!**

Phew! We’re finally done. Hopefully by rigorously following the 7-step methodology you are now the proud owner of an extensive spreadsheet file containing a comprehensive compilation of cybersecurity opportunities. You may wish to keep maintaining this spreadsheet, this file should help you keep you focused on securing a the right position for you.



## The Next Steps



With your spreadsheet file at hand, come recruitment season you'll be well equipped to identify your ideal opportunity. However, just finding the job and applying for it, doesn't mean you'll get it. You'll not want your ideal opportunity to slip through your hands, therefore, you ought to make sure you stand out from the crowd of applicants to secure your dream job.

### Refining your CV



With a list of possible future employers squared away, next step would be work on your CV. I can't keep this document going on forever, so I am going to provide some quick tips, as well as some resources for further reading. The average employer spends less than 20 seconds looking at your CV, so better make sure it looks good!

- Save as a PDF, and with a meaningful filename (i.e., JOH CV Feb 22)
- Keep the length of the CV under 2 pages.



- At the top of the first page: name, location, phone number, professional email address.
- Below the details above, include a personal profile, which is a small paragraph detailing yourself.
- Be abstract about your education, school and grades.
- List your experience in chronological order (most recent first), with various achievements, responsibilities, transferable skills detailed with bullet pointed sentences.



### Harvard's Office of Career Services - Resume & Cover Letter's

[https://ocs.fas.harvard.edu/files/ocs/files/undergrad\\_resumes\\_and\\_cover\\_letters.pdf](https://ocs.fas.harvard.edu/files/ocs/files/undergrad_resumes_and_cover_letters.pdf)

## Interview Questions



A good CV can only get you so far (usually to an interview), so to get further in the recruitment process you'll need to refine your interviewee skills. Thankfully, there is a plenty of resources online to assist you in doing so. One of the resources I've linked is a comprehensive compilation of interview questions including a few I have faced myself.



### Cybersecurity Related Interview Question Bank

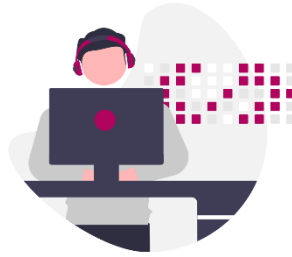
<https://hela-lucas.com/2020/03/12/cybersecurity-interview-question-bank/>



### 60 Cybersecurity Interview Questions

<https://danielmiessler.com/study/infosec-interview-questions/>

## Further Activities



It isn't necessary to invest more time into cybersecurity. However, as seen in the latter stages of the Methodology, there are known benefits from doing so. There is a whole host of online resources you can look at, interactive with, and learn from. The below lists just a few such resources.

Immersive Labs is an online cybersecurity learning platform, it includes a range of exercises from beginner to advanced cyber warrior. These activities focus on developing skills including ethical web hacking; ethical infrastructure hacking; reverse engineering; IoT/firmware security. It's free to sign up, just use your university email address. Additionally, the platform promotes graduate roles, some of which are limited to platform users.



### **Student Portal for Immersive Labs**

[dca.immersivelabs.online](https://dca.immersivelabs.online)

Hacker101 is a free online class focused on web security. There is multiple lecture series to watch, as well as a CTF to help you try out your knowledge in a practical environment.



### **Learn to Hack on Hacker101**

<https://www.hacker101.com/>

TryHackMe provides a mixture of instructional content and capture-the-flag challenges for both red and blue team cybersecurity content. The content is spread across a range of levels from complete beginner to intermediate/advanced and is largely free.



### **Learn Cybersecurity on TryHackMe**

<https://tryhackme.com>

PentesterLab is an online learning environment focused on penetration testing. Their environment provides vulnerable systems, based on common vulnerabilities that can be used to test and understand their exploitation. Unfortunately, it is a paid service, however, some labs can be accessed for free. Additionally, there is a PentesterLab Bootcamp with plenty of DIY practical exercises and reading.

 **Learn Penetration Testing on PentesterLab**  
<https://pentesterlab.com/>

The Web Security Academy is a free online training centre for web application security, including interactive labs. Ran by PortSwigger, those who make industry standard tool Burp Suite, the Academy is regularly updated.

 **The Web Security Academy**  
<https://portswigger.net/web-security>

If you are more inclined with traditional learning resources, then don't worry there is still plenty of them too! On the books front, No Starch Press have numerous fantastic books on a vast number of cybersecurity and computing topics. If you are looking for more computing focused books, the Head First series are highly recommended.

 **No Starch Press**  
<https://nostarch.com/>

 **Head First Books**  
[https://en.wikipedia.org/wiki/Head\\_First\\_\(book\\_series\)](https://en.wikipedia.org/wiki/Head_First_(book_series))

 **Humble Bundle**  
<https://www.humblebundle.com/>

Finally, keeping up with the constant involving domain, can be a time-consuming process, so let someone else do that for you! The tldr sec newsletter is one I personally subscribe to which has numerous links to interesting ongoings each week.

 **Tldr sec newsletter**  
<https://tldrsec.com/>

## References

DCMS, 2021. *Cyber security skills in the UK labour market 2021*. [Online] Available at: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021>

[Accessed 16 February 2022].

Gjeltén, T., 2010. *Cyberwarrior Shortage Threatens U.S. Security*. [Online] Available at: <https://www.npr.org/templates/story/story.php?storyId=128574055&t=1645021216992>

[Accessed 16 February 2022].

IDG, 2017. *2018 Global State of Information Security Survey*. [Online] Available at: <https://www.idg.com/tools-for-marketers/2018-global-state-information-security-survey/>

[Accessed 16 February 2022].

Leinster, T., 2014. *Mathematician Spies*. [Online] Available at: <https://slate.com/technology/2014/04/mathematicians-at-the-nsa-and-gchq-is-it-ethical-to-work-for-spy-agencies.html>

[Accessed 16 February 2022].

Muncaster, P., 2022. *90% of Security Leaders Warn of Skills Shortage*. [Online] Available at: <https://www.infosecurity-magazine.com/news/ninety-leaders-skills-shortage/>

[Accessed 16 February 2022].

O'Sullivan, K., 2021. *Cybercrime nearly doubles in single year as Covid forces criminals online*. [Online]

Available at: <https://futurescot.com/cybercrime-nearly-doubles-in-single-year-as-covid-forces-criminals-online/>

[Accessed 28 February 2022].

Reese, H., 2021. *The cybersecurity skills gap persists for the fifth year running*. [Online]

Available at: <https://www.techrepublic.com/article/the-cybersecurity-skills->

[gap-persists-for-the-fifth-year-running/](#)

[Accessed 16 February 2022].

Roberts, V., 2021. *Cybercrime Figures in Scotland Almost Double in the Last Year.*

[Online]

Available at: <https://www.digit.fyi/cybercrime-figures-in-scotland-almost-double-in-the-last-year/>

[Accessed 16 February 2022].

Scropton, A., 2021. *UK faces significant cyber talent shortfall.* [Online]

Available at: <https://www.computerweekly.com/news/252498337/UK-faces-significant-cyber-talent-shortfall>

[Accessed 16 February 2022].

Sengupta, K., 2020. *13th Signal Regiment: British military launches first dedicated cyber unit.* [Online]

Available at: <https://www.independent.co.uk/news/uk/home-news/13th-signal-regiment-cyber-attacks-uk-military-army-a9550021.html>

[Accessed 16 February 2020].

Stankiewicz, K., 2021. *'Bye-bye FAANG, hello MAMAA' – Cramer reveals a new acronym after Facebook's name change.* [Online]

Available at: <https://www.cnbc.com/2021/10/29/cramer-new-acronym-to-replace-faang-after-facebook-name-change-to-meta.html>

[Accessed 15 February 2022].