13 Pursuing a cyber security career

Two questions I am commonly asked are ‘How did you get started in cyber security?’ and ‘How can I get started in cyber security?’ I was very lucky to find myself working in this industry and I consider it a huge blessing that I found something I am hugely passionate about. It was not a career I had even considered – I was barely aware of it – until I was headhunted by a start-up consultancy. On top of that, the little I knew about the industry gave me the impression that it was an exclusively technical discipline, and this did not seem accessible to me. And my story isn't that uncommon; many people of my age and stage in cyber security stumbled into it. Cyber security was not taught when I was at school – we were only in the early stages of having the internet – nor when I was at university. This is why my husband (who is also my business partner) and I are such big advocates of outreach work with schools and universities: we want young people to know that there is a big, fun, diverse cyber security industry that is full of opportunities which they may love.

Since I started in the sector, I have seen cyber security being taught in schools; university degrees in subjects such as ethical hacking and cyber psychology; and many great initiatives set up to develop people's skills in cyber security and raise awareness of careers in the industry. However, this does not mean that pathways into a cyber security career are clearly defined. There are lots of ways into a cyber security job, but no *one* way. This has many benefits, but can feel overwhelming if you're looking to get a foot in the door.

Qualifications and certifications

In the UK, there are now many universities offering cyber security degrees. The National Cyber Security Centre has granted 19 universities the status of Academic Centres of Excellence; if you're keen to get a degree, looking at these would be a great place to start. There are also many certifications you can take to gain recognition for your cyber security knowledge and skills. At the beginner level, these include: CompTIA Security+; and the EC-Council's Certified Ethical Hacker (CEH). As your career progresses, certifications for more experienced professionals include: (ISC)2's Certified Information Systems Security Professional (CISSP); and Offensive Security Certified Professional (OSCP).

Let's have a look at a few of these in a little more detail.

Security+

The aim of Security+ is to equip someone with a foundational understanding of risk management, cryptography and security vulnerabilities. Emphasising practical skills and knowledge, passing Security+ requires demonstrating an understanding of:

- vulnerabilities, attacks and threats;
- identity and access management;
- network architecture;
- cryptography;
- risk management.

The Security+ certification covers the junior IT auditor/penetration tester job role, systems administrator, network administrator, and security administrator.

There is more information on CompTIA's website: www.comptia.org

Certified Ethical Hacker

CEH was designed to equip individuals with an ethical hacking methodology to be used in penetration testing. It is aimed at security professionals and anyone interested in understanding the integrity of network infrastructure and penetration testing. The certification covers scanning networks, vulnerability analysis, malware threats, social engineering, cryptography and much more.

To undertake the CEH exam, an individual must have at least two years' experience in information security, or they must complete official EC-Council training.

Find out more about CEH via EC-Council's website: www.eccouncil.org

Certified Information Systems Security Professional

CISSP is aimed at experienced security professionals who can demonstrate that they can design, implement and manage a security programme at the organizational level. The CISSP exam evaluates across eight areas of security:

- security and risk management;
- asset security;
- security architecture and engineering;
- communication and network security;
- identity and access management;
- security assessment and testing;
- security operations;
- software development security.

To qualify for the certification, an individual must have at least five years of cumulative, paid work experience in two or more of the eight domains above. It is aimed at people in positions such as security manager, security analyst, IT manager, director of security and chief information security officer.

Find out more about CISSP via (ISC)2's website: www.isc2.org

Offensive Security Certified Professional

OSCP is an advanced certification focused on penetration testing. Those taking the certification are expected to have a good understanding of TCP/IP networking, a fair understanding of Linux, and are advised that familiarity with Bash scripting with basic Python or Perl would be beneficial. The certification is aimed at penetration testers, security professionals and network administrators. The OSCP is a 24-hour lab-based exam with a written element, aimed at testing an individual's time management skills as well as their technical expertise. Passing the exam involves exploiting machines in the lab, documenting your work and submitting a final report.

There is more information on Offensive Security's website: www.offensive-security.com

University study

Given that I took an academic route up to and including PhD level, it would be remiss of me not to mention the benefits of university study. Completing a degree teaches you not only about the subject of study, but also equips you with transferable skills that include time management, written and oral communication skills, how to conduct research, team working experience, self-study discipline and more. If you want to pursue a cyber security career, undertaking a degree in the subject would give you a chance to learn some of the foundational subjects, explore the discipline and perhaps uncover those particular areas that interest you the most, demonstrate your interest in the field and make valuable contacts. There are benefits to going to university and benefits to focusing your studies on cyber security.

'Real world' experience

However, there are also benefits to *not* going to university, not least that you can potentially start working in the field sooner, gaining experience and contacts and getting 'real world' insight into what it means to work in cyber security. My university studies did not include cyber security and that is true for all professionals of my generation (unless they went to university recently); the degrees were not there to be studied and so we learned in different ways, on the job and with self-study. Whether you go to university or not, whether you study (or have studied) cyber security or not – these are personal choices that come down very much to individual circumstances and preferences.

What do employers want?

For many of us running companies and hiring individuals, we are not looking for a specific degree, qualification or certification. Of course, if it is something you are motivated and inspired to do then that's great, and hopefully you'll have seen some of the benefits outlined in the sections above; but if someone tells you that you need a piece of paper to work in cyber security, they are the wrong person to be speaking to. There are many of us working in cyber security who believe that personal attributes are most important when it comes to working in this field. Some of the most important attributes include:

- *Your ethical and moral code*: Working in cyber security, you are often in a position of trust and so it is important that those working in the industry have a strong professional set of ethics. We are often exposed to confidential, personal and sensitive information and it is imperative that we treat that with respect and afford it the privacy and security necessary. Cyber security professionals operate in highly trusted roles, seeing where organizations and individuals are vulnerable, and so you need to be trusted not to take advantage. For example, an ethical hacker performing a penetration test on a banking website may discover a vulnerability that could, technically, allow them to siphon off some money; this individual cannot profit from that discovery outside of their legal contract.

- *Curiosity*: It is often the case that the best way to identify a vulnerability is to be curious. This spans across all areas of cyber security, from technical ('I wonder what happens when I type this code there?') to physical ('This CCTV camera looks a bit off. Does it actually cover the safe door?') to human ('No one is using the right procedure to email confidential information. I wonder if it's too complicated or we haven't communicated it as well as we could?'). Being curious about the way things work, or don't work, is a great personality trait for a cyber security professional.
- *A desire to learn*: This does not have to be learning in any kind of formal way (I don't mean you need to love textbooks!), but as the field of cyber security is constantly shifting with new technology, new vulnerabilities and new forms of attack and defence, it is beneficial if you enjoy staying informed and, even more so, if you have a knack for putting together information from different places or disciplines.
- *An acceptance that you don't know everything* (and that's ok): At the same time as having a desire to learn and drive to acquire more knowledge, you will benefit from acknowledging that you don't have all the answers when it comes to security, that it is a very wide field and people from different areas of security will have knowledge that can inform and enhance your understanding. An open mind is *crucial* in cyber security, so that you can see problems from other people's points of view and consider solutions that might not have been immediately obvious to you. It is easy to get overwhelmed in security and to believe that everyone else knows more than you and you never know enough, because the field is so wide and fast-paced. At the other end of the scale, there is a danger that people become entrenched

in their own narrow area of expertise and over-estimate their value compared to other people. Develop resilience in the face of this: seek more knowledge and refine your skills but stay open-minded to learn from other perspectives. Resist the Dunning-Kruger effect, the cognitive bias in which people overestimate their intelligence to be higher than it actually is. Cyber security is a multi-faceted problem, which requires input from different people and areas of expertise.

- *Empathy*: Cyber security is about listening and understanding, putting yourself into someone else's shoes. For example, this can be listening to people in a business to understand what their most valuable information is, how they work and why some security rules might be really difficult for them to follow. It might also be listening to people about their personal cyber security and understanding that the 'perfect' technical solution is not going to work for them, and that you need to find them a solution they will actually engage with. As a cyber security professional, I would love it if everyone would use a password manager, but I need to understand that they might not be accessible enough for some people.

These personality traits can all be developed, and demonstrating them will be appealing to prospective employers. There are other skills you can hone, too:

- *Situational awareness*: This is a baseline for anyone wanting to enhance their level of security. Situational awareness often comes down to observational skills, having an understanding of what is happening around you and the potential impact of that. Ask yourself questions such as: Has my company identity pass been swiped from my bag? Am I speaking about confidential information in a public place? Is someone tailgating behind me when I enter the office?
- *Spotting patterns*: As a cyber security professional, you will often have to identify what 'bad' or 'unusual' looks like, which means knowing what 'good' or 'normal' looks like. Noticing

patterns is a skill that benefits those working in offensive security (for example, if you are going to simulate an attack on an organization, being able to spot some abnormal code or a break in their physical perimeter is going to be crucial to your success) and those working in defensive security (for example, if you are analysing internet traffic coming into an organization's network, identifying unusual traffic is a must).

- *Communication skills*: Whatever role you have in cyber security, it is likely that you will need a level of communication skills. This will vary from the skills needed to communicate well with your team members about the project you are working on, needing to explain technical issues in a report that is going to people that don't have the same level of technical knowledge as you, to needing to explain to colleagues why some security rules are important and not just there to be a blocker or something they seek to work around.

What can you do to get a job in the industry?

This really depends on your personal circumstances. If you are at school or university, see if there is a cyber or hacking club or society that you can join. If not, set one up! Look into some of the amazing initiatives for young people that may be available to you.

If you are already in the workplace and there is a cyber security or information security team in your organization, why not approach them and see if you could learn more about what they do? You may find that there is a champion or ambassador programme in your organization, in which people in non-security roles volunteer to represent security in their department, in the same way that we have health and safety representatives or fire wardens. If so, these initiatives are often great ways to increase your understanding of the field, get some experience and training and boost your CV.

There are many cyber security community conferences, events and meet-ups happening all around the world, and these are often free or low-cost to attend.

DEFCON groups

DEFCON groups (DCGs) grew out of the annual DEFCON conference in Las Vegas, which began in 1993 as a place for people interested in hacking to meet. As stated on the DEFCON website:

> DCG meetings are open to anyone, regardless of their skill, age, job, gender, etc. DCGs are designed to help you learn new things, meet new people, mentor others in areas you may be strong in, and provide some cohesion within the hacker culture and its members.[1]

At the time of writing, there are 270 DCGs worldwide, covering half of the United States and in over 20 countries around the world, from Algeria to Zimbabwe. DCGs are usually informal, local, monthly meet-ups where you can meet people interested in hacking and cyber security and perhaps listen to a talk or take part in a workshop. They are often a great place to get to know people in your local security community, so it is worth discovering if there is a group near you, or, if there is not, consider setting up your own. There is more information on the DEFCON Groups website: https://defcongroups.org

BSides

BSides are security community events, aimed at enabling people in the community to meet, present their ideas and research and listen to others sharing their knowledge. BSides are run by local community teams and so they vary, but they are most often an annual conference with a call for presentations (CFP) in advance of the event, to which people can submit a topic they would like to speak about, which is then voted on by the community. Many BSides also run rookie tracks, in which people new to the industry or new to speaking can present in a smaller room with the support of a mentor, as well as lightning tracks, which offer shorter speaking slots that you sign up for on the day of the event.

Jack Daniel, BSides co-founder

I'm a displaced mechanic who landed in automotive management where I had to learn to work with computers and soon took over computer operations and administration. If you did systems and network admin in the 1990s, you learned about security whether you wanted to or not. I liked it and gradually shifted focus to security. As I was thrown into tech, I discovered local user groups and learned much from them. When I had something to share, I shared it – that started my long involvement in community engagement. When I saw the US auto industry decline on the horizon, I joined the vendor side, first at Astaro, and later at Tenable, where I have been for over eight years. Both companies have been incredibly supportive of my community engagement work.

In 2009 many in the hacker and security communities had come together on Twitter, and when people started discussing the talks that were turned down at the bigger conferences a few of us looked and saw some interesting ideas so we made a place for people to share their presentations and discussions. Although there had been some discussions on how to make conferences better, we didn't intend to create a series, and certainly never expected to launch a global movement, but people wanted more, and the BSides idea took off. As we discussed the keys to BSides' success and growth, we found four core ideas, each building on the others. First was content – interesting ideas are shared. Second was conversation – since the events are smaller and more informal, the presentations are usually more conversational, ideas are shared and discussed. Third is community – if you share ideas and spark conversation, people build and strengthen the local (and often global) hacker and infosec communities. Last, but not least, is career – if you share and discuss ideas in a healthy and growing community, people will naturally progress in their careers as they see what topics are hot, what companies are hiring and who has what expertise.

Capture the flags

'Capture the flags' competitions often run at events and conferences like BSides, and they also run online. They usually run within a set timeframe and consist of a series of challenges that participants solve using different skills, and when you complete a challenge, you are awarded a flag and earn points. People complete capture the flags (CTFs) on their own or in teams. The more you take part in CTFs, the more you learn how they work and what you can do to maximize points.

CTFs generally include challenges that cover lots of different skillsets, including open source intelligence, programming, cyptography, hacking, networks, forensics and more. This makes them very democratic: obviously, the more skilled you are, the more likely you are to get points, but whether you are experienced or not, or technical or not, you are likely to get a flag or two if you have a go and persevere. Working as a team can be beneficial because of the variety of challenges, but also because it enables you to practise team-working skills, become known for what you are good at and build up your connections.

Sophia McCall, Captain of Team UK at the European Cyber Security Challenge

I have always been interested in computers and technology from a young age. From as early as primary school I would excel in subjects such as IT. This continued through my secondary school years and eventually the completion of my BTEC Extended Diploma in Software Development. Originally I wanted to be a programmer, but during the completion of my BTEC at college I soon discovered that breaking things was a lot more fun than building them! And that sparked my interest in cyber security. From college I then went on to pursue a degree in cyber security management, which provided me with the essential knowledge of business management and policy decisions in a security context. In addition to this, I built up my technical skills, which then allowed me to pursue the dream job of a technical security consultancy role after university.

CTF competitions helped me grow and hone my technical skills in addition to the managerial skills I was learning from my cyber security management degree. At first, I used CTFs as a way to pursue additional security topics outside of my scheduled university hours – but it soon turned from a hobby to a passion, and I am grateful that I got involved early on in my degree. Everything technical, I originally learned from CTFs – they prove an exemplary learning tool to teach the basics of ethical hacking. As President of the Computing and Security Society at my university in my final year, I gravitated towards using CTFs to teach our members (most of whom had limited to no security experience) the fundamentals of ethical hacking and cyber security technical skills. When I first started at university, I struggled with being ‘technical’ – I struggled, a lot! But through perseverance and completion of an array of competitions and labs I saw myself go from ‘zero to hero’ – going from a novice CTFer that struggled to get a single flag, to Captain of Team UK at the European Cyber Security Challenge in a short span of two years. I can't thank the existence of such competitions enough, and I encourage anyone and everyone of all abilities to get involved when they can.

As the budding security professional I am today, I thank organizations like Cyber Security Challenge UK for providing the stepping stones for individuals like myself to enter the security industry and field. Completing their competitions and boot camps and attending their community events allowed me to expand my network, create a name for myself and exercise my security skills in a healthily competitive and fun environment. Organizations such as the Challenge provided the foundations of my career, and I am very grateful for the opportunities the Challenge provided me to create the personal brand that I have today.

Bug bounties

Many organizations run bug bounty programmes, in which they set specific guidelines to reward people who find 'bugs' (vulnerabilities) in their websites, software or applications can win. This enables the organization to crowd-source the finding of vulnerabilities, with the aim of increasing their chances of identifying and fixing them before they are found and exploited by cyber criminals or result in a data breach due to data leakage. There are organizations, such as Bugcrowd and HackerOne, which manage bug bounties on behalf of organizations, acting as a bridge between the organizations running bug bounties and the hackers looking for bugs.

Develop your network

In an industry based on trust, networking is important. Getting to know people, and them to know you, can really help you move ahead in your career. This doesn't have to be in person – engage in conversations on Twitter, look for some of the cyber security discord groups to join, or set up your own blog. People sometimes worry that they don't know enough to write a blog, but you don't have to be an 'expert' to share your learnings or your passion for a subject. As long as you don't claim to have knowledge or experience that you don't possess, then blog posts can cover subjects you are just learning about, a technology that you have just started applying or a project that you completed.

There is a lot to learn when it comes to cyber security, and while you should definitely not feel that you need to know it all in great depth (that would be impossible!), it is important to develop knowledge and skills in the area you pursue (for example, that might be forensics, penetration testing, organizational cyber security culture or one of the many other areas). This will be true throughout your career, as new technology is developed and new vulnerabilities are found. There is a wealth of information out there and much of it is freely accessible. There are of course many excellent books you can read, but there are also podcasts, video tutorials, blog sites, email newsletters and much more you can engage with to learn and stay in the know.

Note

[1] DEFCON Groups (2019) The latest, https://defcongroups.org (archived at https://perma.cc/KY4W-VM3F)