Executive Summary

This paper introduces the problem that there are not enough people with the “right” skills in the cyber industry to meet the needs of the nation. Getting an entry level job in the industry is no small task. The requirements are typically a lot to stomach for someone looking to start fresh or sometimes even recent graduates. Many have gone about seeking a job in the traditional methods of reading job listings and applying for positions where they meet all of the qualifications and can perform the responsibilities. Some people even go as far as thinking that you have to hack the government to get a job with them. These are recipes for failure when it comes to cyber. This paper covers the following:

* Where to start
* The mindset
* Where to get a security clearance
* What to learn
* How to learn it
* Who to learn it for

Cyber Skills Gap? (Introduction)

A stack of books

Description automatically generated with medium confidenceMany in the cybersecurity community and technical talent acquisition industry are familiar with the cybersecurity skills gap. We see this gap in the statistics from cyberseek.org (2021) where it shows less than half the supply to demand ratio for cybersecurity jobs than for other jobs in Maryland. At 1.6 persons per position, this creates a large demand for the little supply and allows for the average salary of cyber professionals to go up. Owen Winn explains this gap well in an article on rackspace.com. To summarize the article “What’s Causing the Cybersecurity Skills Gap” (Winn, 2020), the current jobs needing to be filled require a unique combination of technical skills, soft skills and experience that are rare to find in candidates.

This very thing is the issue. Companies want to hire experienced professionals to guard their data and computer networks, but most importantly, their reputations. Nobody wants to risk becoming the next Equifax with a major public data breach or join the list of businesses decimated by ransomware. The problem then becomes, how does one get into the industry without prior cyber work experience or skills?

Common Misconceptions (Previous Approaches)

There are many wrong ways to go about solving this problem. Many people first learning about cybersecurity think that it is one job, when it is a whole field of careers. There are job careers that focus on the prevention of attacks, jobs that focus on recovery from attacks, and jobs that focus on simulating attacks to test security. There are even jobs for the government and military that involve covert operations where you may be authorized to hack into foreign networks and systems for the purpose of intelligence collection and reconnaissance. For the sake of brevity and concise direction, we will focus on the role of Cyber Operator as defined by the NICE (2021) framework at NICCS.CISA.gov:

Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations. (para 1)

A popular misconception is that in order to become a hacker working for the government, you have to hack a government agency to prove yourself. This is not only wrong, but it violates the Computer Fraud and Abuse Act of 1986 (Department of Justice, 2020) which prohibits “accessing systems without authorization or exceeding the level of access authorized”. In other words, not only will you upset your hiring manager, but you could also end up in jail.

It is also thought that you must meet all of the requirements in the job description to get the job. According to Cybersecurity Hiring Manager Aaron Katz, (2021) even if you don’t meet all of the criteria of the job including a degree, you should apply to at least get a dialogue with the hiring manager/s. This gets your foot in the door for them to fully evaluate you. The worst that can happen is you do not get the job you wouldn’t have had in the first place and the best thing that can happen is you get the job or another job at the company.

New Findings

We know how not to get into the industry, but what exactly does one need to do/be to become a cyber operator? Dr. Charles Clancy of Virginia Tech does a great job of getting the ball rolling on this question in his article (2018) “So You Want to Be an Elite Hacker? Finding your career in cyber operations”. He gives good starting points:

* Look for a school designated as a CAE-CO (Center of Academic Excellence in Cyber Operations).
* Get an internship with the NSA or CIA to obtain a security clearance.
* Consider a full-time career for the agencies or a defense contractor (which typically pays more) that staffs them.

These are great starting points, but there is more that can be gleaned elsewhere to further your chances of success and obtaining that first internship or entry role. Many in the industry look for people they describe as “hungry”. They are not talking about the sensation that tells you its time to eat again. They are talking about a hunger for knowledge. Hiring managers want their future employee to enjoy what they do enough to research trends in the industry and stay current even outside of work. This is crucial especially for cyber due to the constantly evolving threat/attack landscape. Almost daily, new bugs, vulnerabilities, attacks, and malware are announced or discovered and there is a lot to keep up on.

A picture containing text, electronics, indoor, monitor

Description automatically generated

A screenshot of a computer

Description automatically generated with low confidenceA very popular trend in the offensive/operations fields of cyber are home labs. With the popularization of virtual machines and containerization learning to hack has never been safer. You can use virtual machines and containers to test malware and exploits on vulnerabilities without as much of a threat towards your home network. I say “as much” because if configured incorrectly, they can function like normal computers on your network and propagate malware. If you are unfamiliar with setting up a home lab, the SANS Webcast: *Building Your Own Super Duper Home Lab* (2017) is a great resource that explains this in depth.

Another new trend is what is referred to as the gamification of cyber training. In the article “Game On: How Gamification Pragmatically Impacts The Future Of Cybersecurity Training”, Mike Moniz explains how people are creating challenges and competitions to put a game-like spin on solidifying materials taught. Gamified learning can be found in various forms for learning hacking and cyber skills. Following is a short list of examples:

* Hackthebox.eu
* Tryhackme.com
* Picoctf.com
* Ctftime.org
* Immersive Labs
* National Cyber League
* Mid Atlantic Collegiate Cyber Defense Competition

A picture containing text

Description automatically generatedAnother area that may be news to students especially in technology related majors, is that another essential is the ability to grow your social network and make a name for yourself. You can be a great cybersecurity wizard, but if nobody knows who you are, your job seeking efforts are fruitless. It is often said that it is not what you know, it is who you know. This is somewhat true. According to LinkedIn (2017), 35% of people have gotten their job starting with a casual conversation.

Graphical user interface, text, application

Description automatically generatedFinally, we can look at the job descriptions for current cyber operator positions at NSA and CIA. Looking at the job description for “Computer Network Analyst” which covers offensive and defensive positions in the application, we see that the minimum qualification is a Bachelor’s degree in a STEM related field for the entry level position.

Scrolling down, we can see preferred competencies in more niche focuses. This is where the home lab and self-educating comes in handy. Pick a few areas and research them. When you come across a term you don’t recognize, research that and keep following the rabbit holes until you understand what you are looking at and how it works. This may seem excessive. You don’t need to know what a PLC is to know that the Stuxnet worm physically destroyed Iranian nuclear machinery. However, understanding that a PLC is an interface that allows a program to spin a centrifuge at a specific speed can help you understand how the malware works and allow you to come up with a solution to prevent similar attacks on your organization or carry out reconnaissance without making as much noise on a network and getting caught.

Text

Description automatically generatedText

Description automatically generated

Looking at the requirements for the CIA’s version of this job, the Cyber Operations Office, we can see that their requirements are a bit stricter than NSA’s. It is also worth noting that both agencies have strict drug use policies and full scope Top Secret security clearances with Polygraphs are typically required for these roles, so if you have any issues in your life, try to clear them up a year in advance to applying for CIA or six months prior to applying for NSA.

Conclusion

Without guidance, becoming a cyber operator can be a daunting task at first. Some of the traditional job seeking strategies are ineffective or insufficient alone. With proper guidance and goal setting, one can achieve success in the field. It is still possible to become one with little to no background, however your chances of success go up if you can show that you have a spark for what you do, don’t have a lot of current/recent background issues, and are familiar with the job and at least some of the skills necessary. It is also worth noting that most people in the industry find the good opportunities through people they know or friends of friends, or even friends of friends of friends. Its never too late to start growing your social network and making a name for yourself in the industry.

References

Charles Clancy. (2018). So you want to be an elite hacker? finding your career in cyber operations. *XRDS: Crossroads, The ACM Magazine for Students - Pseudonimity and Anonymity*, *24*(4), 12–13. https://doi-org.ezproxy.umgc.edu/10.1145/3220665

Central Intelligence Agency. (2021). *Cyber operations officer*. Central Intelligence Agency - CIA. Retrieved May 6, 2021, from <https://www.cia.gov/careers/jobs/cyber-operations-officer/>

CTF Time, C. (2021). *Main Site*. CTFtime.org / All about CTF (Capture The Flag). <https://ctftime.org/>

Cybersecurity and Infrastructure Security Agency. (2021). *NICE framework work roles*. National Initiative for Cybersecurity Careers and Studies |. [https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Operator&id=All#](https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Operator&id=All)

CyberSeek. (2021). *Cybersecurity supply and demand heat map*. Cyberseek. Retrieved May 6, 2021, from <https://www.cyberseek.org/heatmap.html>

D5IQ. (2021, March 2). *Main Site*. GamifiedCyberlearning.com. <https://gamifiedcyberlearning.com/>

Department of Justice. (2020, January 29). *9-48.000 - Computer Fraud and Abuse Act*. U.S. Department of Justice. <https://www.justice.gov/jm/jm-9-48000-computer-fraud>

Hack The Box. (2021). *Main Site*. <https://www.hackthebox.eu/>

Katz, A. (2021, February 1). *How to get a cybersecurity job – Tips from a hiring manager*. freeCodeCamp.org. <https://www.freecodecamp.org/news/how-to-get-a-cybersecurity-job-tips-from-hiring-manager/>

LinkedIn. (2017, June 22). *Eighty-percent of professionals consider networking important to career success*. LinkedIn Newsroom | LinkedIn. <https://news.linkedin.com/2017/6/eighty-percent-of-professionals-consider-networking-important-to-career-success>

MACCDC. (2021, April 1). *Main Site*. <https://maccdc.org/>

Moniz, M. (2020, May 21). *Game On: How Gamification Pragmatically Impacts The Future Of Cybersecurity Training*. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2020/05/21/game-on-how-gamification-pragmatically-impacts-the-future-of-cybersecurity-training/?sh=1320eff33fe2>

National Security Agency. (2021). *IC candidate Portal*. IC Candidate Portal. Retrieved May 6, 2021, from <https://apply.intelligencecareers.gov/job-description/1160297>

Sans Offensive Operations. (2017, August 25). *SANS Webcast: Building Your Own Super Duper Home Lab* [Video]. YouTube. <https://www.youtube.com/watch?v=uzqwoufhwyk>

TryHackMe. (2021). *Main Site*. <https://tryhackme.com/>

Winn, O. (2020, September 30). *What’s causing the cybersecurity skills gap?* Rackspace Technology. <https://www.rackspace.com/solve/cybersecurity-skills-gap>