Ali Abdelhamid

Cyber Security Careers

12/12/2022

Coursework

Table of Contents

Abstract

What is Cybersecurity? It is the action of protecting programs, networks, and systems from cyber-attacks, usually, the attacks are with a malicious aim, whether changing, deleting or just accessing crucial information. These attacks vary from Trojans, and ransomware, to even adware. Furthermore, Cybersecurity contains a lot of branches put in place to disperse the load among people with knowledge in each domain of Cybersecurity, resulting in a high variety of jobs (What Is Cybersecurity?, 2022). How is the Cybersecurity job market in Egypt? And what are the efforts being made to improve it even more? According to research, I made on my own, the market job in Egypt is not in its best state right now, job postings lack professionalism, important specifications, and salaries which are a very important part of the job selection process; there is an advantage, however, which is the lack of Cybersecurity specialists, this doesn’t exclude certain domains. This proves as an advantage to me and all other applicants, due to the low supply the demand is much higher. Other nations have not yet reacted to such low supply therefore you’ll find that most workers are Egyptians. I found minuscule efforts done by the government to improve the market due to the low supply, even though, Cybersecurity is on the rise and is going to be one of the most crucial jobs of the future due to the entire world heading towards computerizing everything.

Introduction

Why should a person consider joining the Cybersecurity field? Starting with the most motivating reason, is the salaries, according to the office of the Press Secretary (*FACT SHEET: President Obama Launches New TechHire Initiative*, 2016) jobs that require high IT skills pay around 50% higher than the average private-sector job in America, these statistics were provided on the USA due to the lack of market research in Egypt. In 2016 the average median pay for all non-cybersecurity jobs was 37,000$ per year, and for Cybersecurity, the average pay was 92,000$ annually. Another reason to consider joining Cybersecurity is the diversity of industries that require certain Cybersecurity specialists. Another reason that might tempt a lot of people to start looking for a Cybersecurity job is the density of job postings, due to the constantly growing nature of the field, there is an ever-growing need for Cybersecurity jobs. According to (Hatton, 2022) the largest labor market research pioneers, starting from 2007 leading to 2013 Cybersecurity job postings grew by a whopping 74%. Another research done by the Bureau of Labor Statistics; the employment rate is expected to grow exponentially, more specifically by 18% from 2014 to 2024. In other words, there are a lot of opportunities that need to be taken and jobs to be filled. (Krakoff, 2019)

Changing subjects, let’s talk about real-life examples that have shown multiple times the importance of the Cybersecurity field. Due to the transition of all fields to computerization, hackers all over the world have taken notice of this and have started exploiting everyone and everything they can find whether for pure malicious intent or financial payments. During 2020 multiple significant attacks took place varying from phishing, data leaks, breaches, ransomware, and even supply chain attacks. On March 31, 2020, the Marriott International, a large hotel establishment, suffered a huge data breach. According to a statement released by Marriott, 5.2 million guests' info was easily accessed using the acquired login info belonging to 2 staff members working on the establishment. According to the statement "We believe this activity started in mid-January 2020", it is also stated that "Upon discovery, we confirmed that the login credentials were disabled, immediately began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests" (Scroxton, 2020); but of course, it was too late, the information was already leaked, and the attackers could have already sold it to bidders or even worse. The information contained very sensitive information such as bank account passwords and PIN s, credit card information, passports, as well as personal IDs. Without the help of Cybersecurity specialists this scenario could have been way worse, as, in this instance, specialists are the ones leading the investigations, as well as trying to recover the stolen information. (Waldman, 2021)

With a more recent attack, on June 1, 2022, google received the largest DDoS attack ever recorded, by largest, it means the requests were sent at once since DDoS attacks consist of sending multiple packets all at once to cause a total denial of service. As stated by Google this attack has reached a peak of 46 million requests per second, which is unimaginable. According to a blog post by Emil Kiner, senior product manager at Google, the attack lasted for 69 minutes with 5,256 source IPs scattered around 132 countries (Kiner & Konduru, 2022). However, Cybersecurity specialists working at google have successfully blocked the attack which prevented the failure of service. (Powell, 2022)

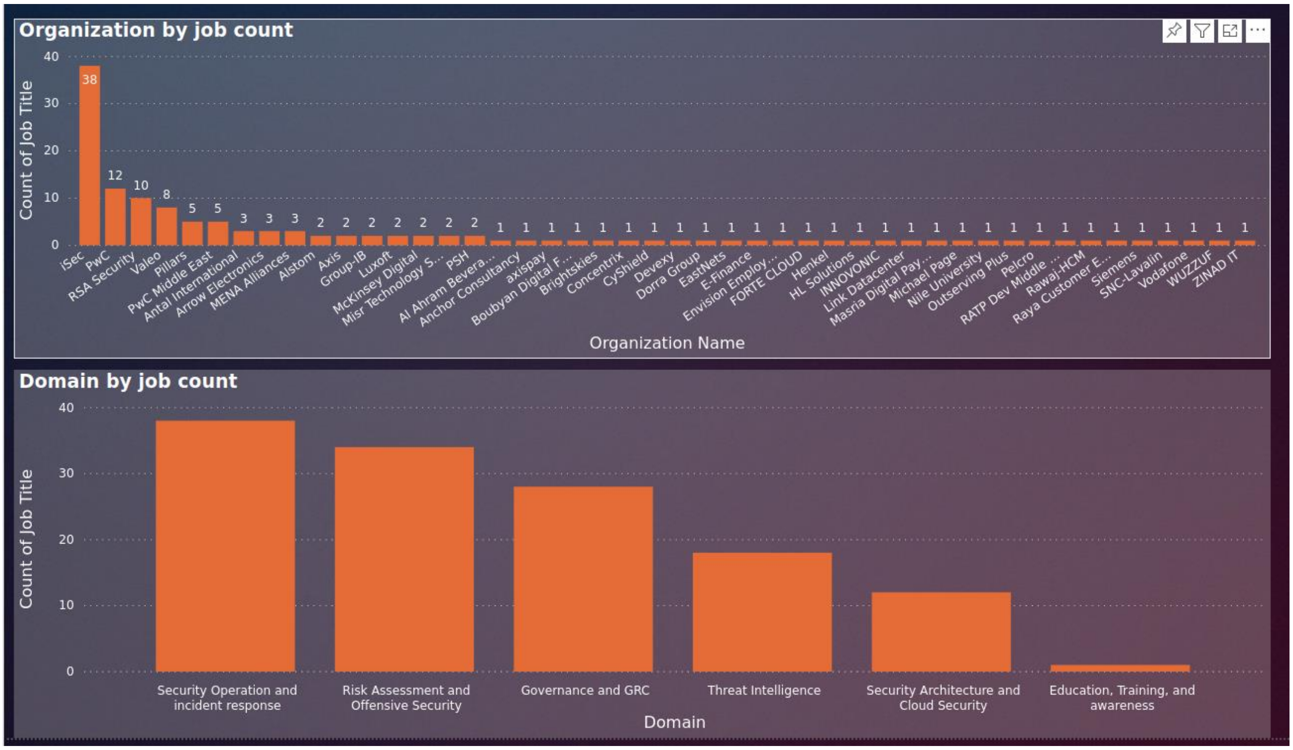
Furthermore, some random market statistics on cybersecurity, the total damages in 2022 have reached around $6 trillion according to dataprot, there is a cyber attack around every 39 seconds, and a ransomware attack happens every 14 seconds. (Jovanovic, 2022)

Filling Cybersecurity Career Gap

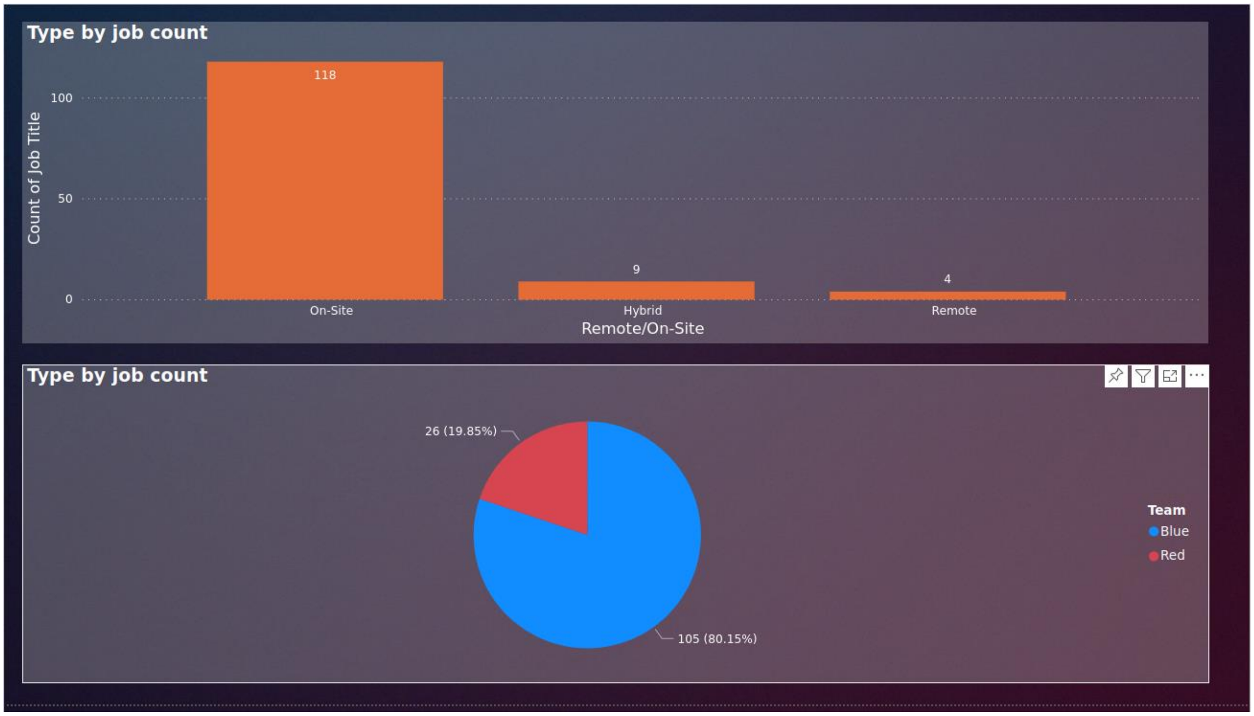
What actions can Egypt take to increase cybersecurity specialists as well as close the talent gap and provide organizations with educated workers? The cybersecurity skill gap is globally acknowledged. According to Cyberseek global security heat map, there are more than 600,000 identifiable cybersecurity job openings in the United States only (*Cybersecurity Supply and Demand Heat Map*, n.d.), what are they doing to mitigate such issues? The first step is building a cyber security competency model, organizations need to start defining the cyber skills needed for each job posting, by posting the education level as well as the skills the employee will need to succeed in the role. The employees can measure their skill level in multiple ways, for example, cybersecurity skills assessments, using a simple checklist assessment to determine if they have the skills needed; another method could be performance reviews, such as including questions about the worker's professional development goals and what employees consider to be their strong points. Another simple way is to collect work samples to assess the employee's technical level. (Monthie, 2022)

Cybersecurity jobs in Egypt

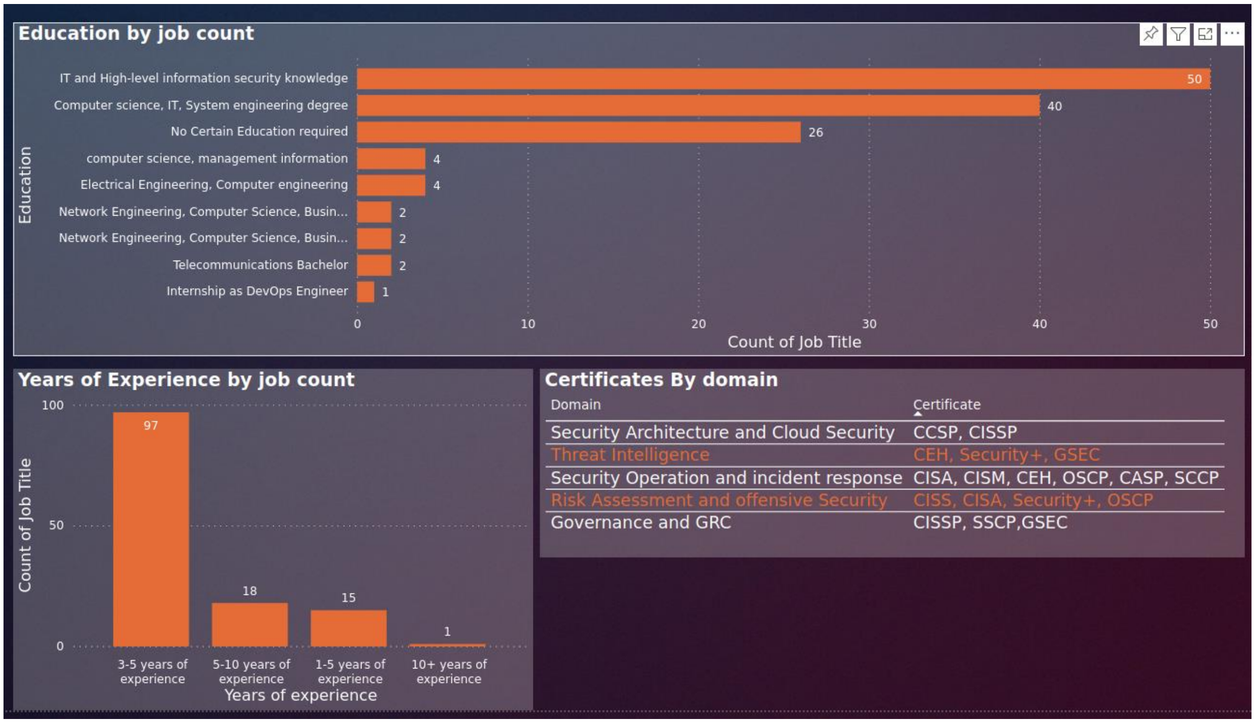
Based on personal research I found out a lot about the cybersecurity job market in Egypt and based upon that made statistical analogies and graphs describing my findings. I scoured the internet and job listing websites such as Glassdoor and LinkedIn looking for cybersecurity jobs in Egypt, I've also used applications such as Octoparse and ScrapStorm to make the process smoother and faster.



As seen from this first panel, the organization with the most job listings was Isec, generating around 38 jobs, followed by PwC scoring only 12 jobs, both huge cybersecurity-oriented companies. The remaining companies only had an average of one job listing. The graph below shows the number of jobs that are scattered across all the domains, with security operations and incident response having 35+ jobs, risk assessment and offensive security having around 33 jobs, on the other hand, education, training, and awareness have only 1 job, this raises the issue that there is a need for education jobs.



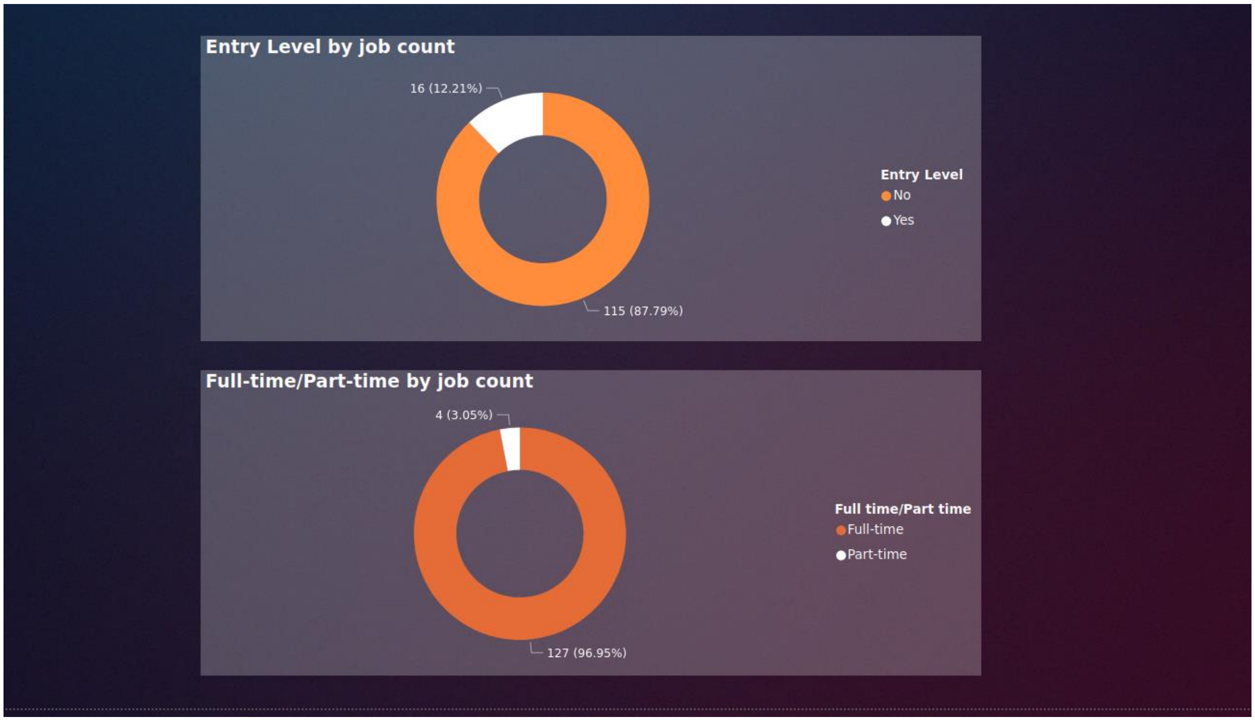
The following 2 graphs describe the job type by place and the team by job count, the top graph describes that the majority of the jobs were on-site and only 4 were remote. This is natural due to the high sensitivity of the job type and the need to decrease risks by having the employees on site. Most of the jobs were blue team as seen on this pie chart, and only 26 jobs were red team. Red team is more on the offensive side while blue team is on the defensive side of cybersecurity.


Education by job count
IT and High-level information security knowledge
Computer science, IT, System engineering degree
No Certain Education required
computer science, management information
Electrical Engineering, Computer engineering
Network Engineering, Computer Science, Busin...
Network Engineering, Computer Science, Busin...
Telecommunications Bachelor
Internship as DevOps Engineer
Education
50
40
26
4
4
2
2
2
1
0
10
20
30
40
50
Count of Job Title
Years of Experience by job count
100
50
0
Count of Job Title
97
18
15
1
3-5 years of experience
5-10 years of experience
1-5 years of experience
10+ years of experience
Years of experience

Certificates By domain

Domain	Certificate
Security Architecture and Cloud Security	CCSP, CISSP
Threat Intelligence	CEH, Security+, GSEC
Security Operation and incident response	CISA, CISM, CEH, OSCP, CASP, SCCP
Risk Assessment and offensive Security	CISS, CISA, Security+, OSCP
Governance and GRC	CISSP, SSCP,GSEC

The most education type that was required was ironically wasn't a degree, this is probably a mistake by the job posters, which is not explicitly describing certain education that they require, it was only described as IT and High-level information security knowledge, followed by some job postings that did it correctly, with 40 jobs having Computer science degree as the requirement. Most jobs required 3-5 years of experience to apply, this is not considered entry-level, I only considered 1-5 years of experience as entry-level; with only one job requiring 10+ years of experience. The certificates by domain mean which certificates were most common by each domain.



The following donut charts describe the number of jobs that were entry-level by percent and the percentage of full-time/part-time jobs, around 88% of jobs were not entry-level, and 12% were entry-level, the entry-level jobs are the jobs that required only 1-5 years of experience to apply. 97% of the jobs were full time as mentioned before, and 3% were part-time.

Road map to my dream job

Due to the ginormous variety of cyber security career options and domains, It was a vigorous process of research and decision-making and personal questions to decide which career path is the most suitable for me to follow. Practical Penetration Testing, I've set a full timeline from the start of college till after my master's degree, first I've researched all the certificates I'll need to reach my goal, CSSP, SSCP, PenTest +, Security+, ITIL, CES, CAC, A+; this is a simple list. During my college studying years, I plan on taking multiple courses that would eventually lead me to take OSCP certification which in my opinion is one of the hardest certificates to achieve, during my winter break as well as the summer break I plan on participating in multiple cybersecurity internships, although it is not a requirement that they be pen testing as any internship in the cybersecurity field would benefit me greatly. After finishing college, I plan on completing my master's degree in cybersecurity abroad. Finally, after finishing my master's I will start the process of job searching using the same methods I've used to complete this coursework.

I've acknowledged my strengths and weaknesses which I think is very important in this field since you need to know yourself very well before starting to know the field and getting technical. I think outside the box which is much needed in the pen testing field due to the much-changing nature and the variety of problems I could find. I'm a team player, this will be of great benefit due to the high probability of me working in a team once I am accepted into a new job. I am a solid and confident writer, since submitting a pen testing report to seniors is a major part of the job. On the other hand, my weaknesses, I require more practical practice, I plan on taking much more CTFs to fix that weak point, I also need more work and internship experience in the field due to the scarcity of it. I've yet to decide on a target company therefore I've not researched any companies and their specific requirements yet.

Conclusion

To conclude, based on my research and the research forums I've visited, I've concluded that the cybersecurity job market in Egypt is not in its best form right now and has a lot of room for improvement. My recommendations are that the job posters need to start describing the jobs better in their postings and start including the salary as well as describing the knowledge and skills needed. Many potential opportunities are available, especially in Isec and PwC due to the high rate of posting, they opened the opportunity for much more fresh graduates and new workers. My advice on how to penetrate the Cyber security market is, to begin with, a self-assessment checklist, find out your strong points as well as your weak points; discover your passion, research all the job positions available in your area, research every position to discover their roles and responsibilities, after doing all that you'll certainly discover what you like and don't like. Following that start collecting raw data sheets of all the jobs and create graphs to see the information right in front of you for it to become easier to decide. In my opinion, just working in the cybersecurity field whether blue or red teaming, part-time or full-time, all provide the opportunity of giving back to the community and the people around you. Protection of people's information and personal data is in itself a form of giving back and helping people.

submissions

References

1- *Cybersecurity Supply And Demand Heat Map*. (n.d.). https://www.cyberseek.org/heatmap.html

2- *FACT SHEET: President Obama Launches New TechHire Initiative*. (2016, March 3). whitehouse.gov. https://obamawhitehouse.archives.gov/the-press-office/2015/03/09/fact-sheet-president-obama-launches-new-techhire-initiative

3- Hatton, T. (2022, December 12). *Launching Career Pathways*. Lightcast. https://lightcast.io/resources/blog/career-pathways-launch

4- Jovanovic, B. (2022, November 2). *Better Safe Than Sorry: Cyber Security Statistics and Trends for 2022*. Dataprot. https://dataprot.net/statistics/cyber-security-statistics/

5- Kiner, E., & Konduru, S. (2022, August 18). *How Google Cloud blocked largest Layer 7 DDoS attack yet, 46 million rps*. Google Cloud Blog. https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

6- Krakoff, S. (2019, November 22). *The Top 5 Reasons You Should Consider a Career in Cybersecurity*. https://online.champlain.edu/blog/top-reasons-to-consider-cybersecurity-career

7- *Marriott International Notifies Guests of Property System Incident*. (2020, March 31). Marriott International Newscenter (US). https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

8- Monthie, H. O. S. (2022, July 4). *4 steps to closing the cybersecurity skills gap in your organization*. VentureBeat. https://venturebeat.com/datadecisionmakers/4-steps-to-closing-the-cybersecurity-skills-gap-in-your-organization/

9- Powell, O. (2022, December 2). *The top 10 hacks and cyber security threats of 2022*. Cyber Security Hub. https://www.cshub.com/attacks/news/the-top-10-hacks-and-cyber-security-threats-of-2022

10- Scroxton, A. (2020, March 31). *Marriott International hotel chain in second data breach*. ComputerWeekly.com. https://www.computerweekly.com/news/252480903/Marriott-International-hotel-chain-in-second-data-breach?

11- Waldman, A. (2021, January 5). *10 of the biggest cyber attacks of 2020*. Security. https://www.techtarget.com/searchsecurity/news/252494362/10-of-the-biggest-cyber-attacks

12- *What Is Cybersecurity?* (2022, October 10). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

LinkedIn: https://www.linkedin.com/in/ali-abdelhamid-b456a81a9/