How to successfully break into Cyber security?

You are a successful experienced IT professional (non-cyber) or a beginner who wants to enter Cybersecurity field. How can you do? What things to be considered? Are there any best approach or steps for this process? In this guide I am going to share an approach you can follow to successfully break into cybersecurity.

Chintan Gurjar (@iamthefrogy)
Email: chintangurjar@outlook.com
LinkedIn: https://www.linkedin.com/in/chintangurjar/

There are 3 main components of this approach.

1. Understand the scale of the spectrum

2. Create & meet your requirements/ needs

3. Plan & execute it

8 Steps of the Approach

Keep doing your current job	Research various Cybersecurity domains	Prepare a study plan	Enter the field	Find a mentor in Cybersecurity	Apply for jobs	Congrats! Mission Completed.

Keep doing your current job (If you are not doing a job, skip to the next part)

It is vital to keep earning with your current job until and unless you have successfully entered the Cybersecurity field with a full-time job. Your family might be dependent on you.

Do not take a break for specific study/course/certifications/masters if you already work in the non-cyber-IT field.

Research various Cybersecurity domains

Refer to SANS CISO mind map. https://www.sans.org/posters/ciso-mind-map-and-vulnerability-management-maturity-model/

Understand how many various domains there are in the security field.

Take each bullet point from that PDF and Google it. Ask the below questions yourself:

1. What is that domain?

2. What kinds of roles does the company offer in that domain?

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

3.	What tools/commercial solutions do people use?
4.	What daily routines do people have in that job role?
5.	Is it demanding or not?
6.	Which reputable organizations provide certifications in that domain?
7.	Look for the course syllabus of that cert to understand what can be covered?
8.	Does that fancy you?
9.	Which roles can you start within that domain as a beginner, and where can you reach maximum?
10.	What will be the future of that domain?

Refer IT to Cyber domain mapping

Refer to the IT to Cyber mapping table. *(Appendix 1)*

Understand your position in which and the IT field you are currently working in.

Understand what possible options/areas you can start your journey with within cybersecurity.

If you are an absolute beginner with no IT experience, you can select any field you are interested in. Maybe you would choose domains close to your IT role or possibly completely separate as you are willing to learn new things from scratch. Any approach would work here.

Study Option	Why	Pros	Cons	Resources/How-to
Read a book	-	- Structured learning from basic to advance. Granular level understand.	- Time consuming - Paid	1. Go to Amazon 2. Seach your interested domain in Amazon. 3. Filter the result by 'Publication date'. 4. Order book. 5. Read. **Review:** - Author history - Starts of the book - Table of contents
Complete course on YouTube	-	- Easy way to grasp topic. - Free & easy access.	- Depending upon channel creators' views and opinions, the study approach can vary. No. of topic coverage & in-depth content may also vary. So, you will require to do a lot of research before selecting any particular course on YouTube as they are free.	1. Search for a topic on YouTube. 2. Use YouTube's filter section. 3. Select 2 filters. 1) Type – Playlist 2) Sort by – Upload Date. This will provide you the entire playlist on that topic but sorted by latest uploaded on the YouTube.

Official Certification	Some people feel that they can't feel motivated if they don't have any goals/challenges. Hence, they go for paid certifications as once they spend money, they will require to study and crack the exam in a limited timeframe. This keeps them motivated and focused on achieving the goal. Some reputed certification authorities are ISC2, eLearnSecurity, SANS/GIAC, Offensive Security, CompTIA, ISACA, and Mile2.	- Demanded in job descriptions. - Later or sooner you will have to go for that.	- Limited time to complete lab/cert - Expiration dates for some certs. - Paid	Refer to the Which certifications should I go for? Section in order to decide which certification you should go for.
Study a complete course on Pluralsight/Udemy/Coursera/Oreilly	These are some popular portals for studying the entire course of any security domain. Trainers on these platforms are well experienced, and these portal owners also review course content. Ensure you check the ratings of the course before you select and start.	- Courses you may not find on YouTube directly, can be found on these training portals.	- Some courses are overrated - Some authors are overrated. - Quality content might be paid.	Login and search for the free course. Enroll and learn. **Review:** - Author and course rating but do your own research
Freeform well-structured self-study via Google & YouTube	Manier times, you cannot or don't want to spend money on material as it can be found via Google. So, you can follow this approach. Before starting self-study, all you need to do is select a particular field. Find a famous book on Amazon with good ratings and is not older than a maximum of 6 years. Find a table of contents of that book. E.g., You found a book on Amazon.com. Refer to its table of contents what all they will teach in that book. Then Google each topic, read, and study. Watch practical/theory explanation videos from YouTube. Prepare your notes.	- You can become more proactive in terms of grasping different knowledge but filtering the best information to your brain.	- Can be time consuming - Will be hard to different author's knowledge when you search them on various portals each week.	Explained in the Why section.

Prepare a plan that works best for you. Things to consider:

Identify what learning options you have. There are various learning options for any IT or Cyber field. There are pros and cons to every option, which I have illustrated.

1. **Time management for work-life balance**

2. **Time allocation for your job, social life, and learning security from the above options (Prepare a daily, weekly schedule, Set targets)**

Enter the field

Perform a thorough **company research** before applying for a job.

Talking about reviewing a company, I would personally consider all factors before choosing my next company:

1. **Revenue –** To identify whether company is financially doing good or not.

2. **Company size –** To identify whether no. of employees are increasing or not. If increasing, company is doing great.

3. **Company's area of serving –** So you can predict what core values you would be serving to the company's wider level goal/business.

4. **Their client base –** So that you can understand who will be your most of the stakeholders with whom you will work on regular basis.

5. **Glassdoor and other reviews, People reviews –** Does not really matter, but may give you some indication of work culture especially the one with anonymous bad reviews and then you can ask around in your network to have better view of it before joining.

I believe below are the foremost common factors one should consider before selecting a company or applying for a role:

There **can never be** any company which would fulfil all your below needs. *(You will need to prioritize a minimum of 2 maximum 3 factors you would assess in your next company. So, if the first 2/3 of your needs are completed, you can select that company.)*
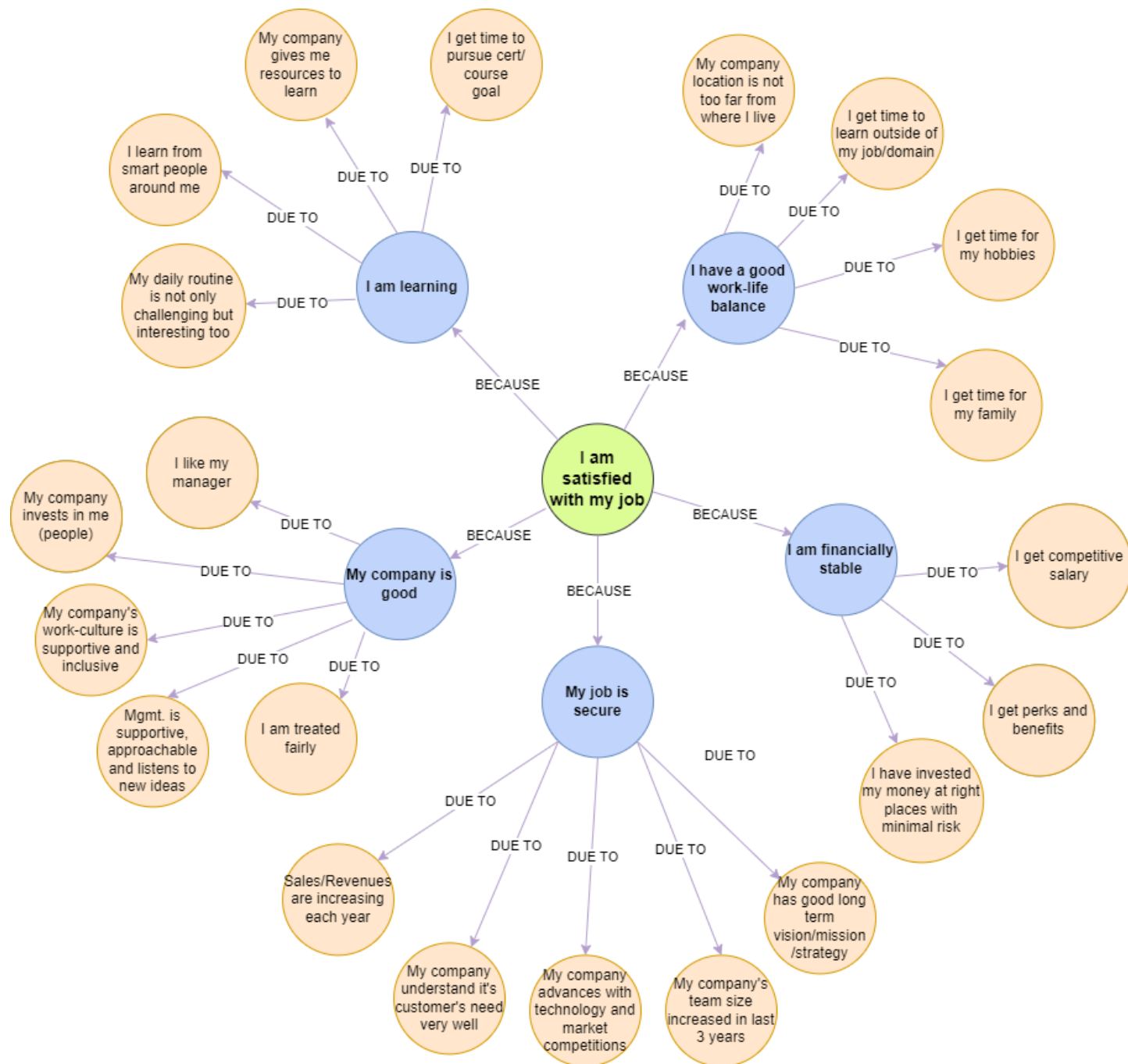
1. Location

2. Flexibility/Flexible working facility

3. Career advancement/Challenging work/Learning and development opportunities

4. Types of services they offer

5. Type of company (Small, Big, Product based, Consulting based, Research based, etc.) /Reputation/Brand

6. Type of Industry they serve (Banking/Financial, Retail, Gaming, Healthcare, etc.) /Reputation/Brand

7. Team/People/Boss/Management/Colleagues

8. Base Pay/Salary/Bonus/Benefits

Find a quality mentor in cybersecurity

Finding the right mentor is challenging, especially for beginners in the security field. There are DOs and DON'Ts to consider before selecting the right mentor for yourself:

1. Don't just get attracted by no. of certifications those mentors have.

2. Don't select mentors just based on their online presence/appearance/how famous they are in the industry.

3. Don't select mentors just based on the total no. of experience they have.

4. Don't select mentors just based on their super technical hacking skills.

5. Don't select mentors just based on the number of achievements they possess.

6. Select a mentor who is down to earth, willing to learn from you as well while also coaching you.

7. Select a mentor who just not only solves your tech queries but gives you a perfect vision/direction for what you need to do to become XYZ down the line in the next 2-5 years and so on.

8. Select a mentor who is regularly contributing and giving back to the community.

9. Select a mentor with the right attitude not only the right knowledge.

10. Give time for your research, talk to them regularly, and talk to many regularly before you select them as your mentor.

11. Most notably, in the above list, ensure all or the majority of the points give a green signal to select your mentor and don't just evaluate anyone based on one or a few DOs or DON'Ts. Remember, no one is perfect in this world.

When can you be satisfied with your job

I am satisfied with my job

BECAUSE → **I am learning**
- DUE TO → My company gives me resources to learn
- DUE TO → I get time to pursue cert/course goal
- DUE TO → I learn from smart people around me
- DUE TO → My daily routine is not only challenging but interesting too

BECAUSE → **I have a good work-life balance**
- DUE TO → My company location is not too far from where I live
- DUE TO → I get time to learn outside of my job/domain
- DUE TO → I get time for my hobbies
- DUE TO → I get time for my family

BECAUSE → **My company is good**
- DUE TO → I like my manager
- DUE TO → My company invests in me (people)
- DUE TO → My company's work-culture is supportive and inclusive
- DUE TO → Mgmt. is supportive, approachable and listens to new ideas
- DUE TO → I am treated fairly

BECAUSE → **I am financially stable**
- DUE TO → I get competitive salary
- DUE TO → I get perks and benefits
- DUE TO → I have invested my money at right places with minimal risk

BECAUSE → **My job is secure**
- DUE TO → Sales/Revenues are increasing each year
- DUE TO → My company understand it's customer's need very well
- DUE TO → My company advances with technology and market competitions
- DUE TO → My company's team size increased in last 3 years
- DUE TO → My company has good long term vision/mission/strategy

Apply for jobs

If you are an experienced IT professional, you will need to tweak your resume to make it sound more of a cybersecurity one than just an IT.

If you are a beginner, you will require to create a professional resume to apply for a job. There are plenty of cybersecurity resume templates on Google that you can refer to.

If you have no professional experience in IT or Cybersecurity, you can add below things in your resume as a beginner. Kindly refer to the Resume writing – How not to blunder section.

Select any portal to apply for jobs but do not forget to use LinkedIn for the same. LinkedIn jobs are best, according to my viewpoint compared to other specific job-hunting portals.

You can contact specific cybersecurity recruitment companies who fill positions for big companies.

You can add cybersecurity specific HRs to your LinkedIn to build relations and ask them to take an interest in your profile.

Prepare for interviews based on job descriptions. Whatever roles/responsibilities are mentioned in the JD, most likely, you will be asked questions from those areas only + the things you have mentioned in your resume.

Congratulations! Mission Completed.

It is not over yet. You have just entered the cybersecurity world. There are things you will need to continue doing for better survival and better growth.

1. **Learn more things –** Learn those things in your company which you cannot simply learn by Google and YouTube. E.g., One can learn how to hack a website by sitting at home, but cannot learn, how to design a new secure architecture diagram for application development within the DevSecOps project based on their company's infrastructure. That is the real experience.

2. **Advancing to management –** See what else you would require learning apart from tech skills to advance your career to the management level. Learn more soft skills in business, and management. Learn people, process and technology problem dealing.

3. **Know your competitions –** Competitions are everywhere; it is an excellent way to keep yourself motivated and learn more things that others are learning in your network.

4. **Know the market –** Understand how the market is shifting in cybersecurity, know various new vendors coming into the market, and launching their products to tackle large enterprise problems. Understand what problems are being discussed in the community through conference panel discussions, YouTube podcasts, or other sources. Understand the market when you started your career, how rapidly it is changing, and where it is going. You can determine your future roles and opportunities and can set goals accordingly.

5. **Do not get demotivated –** Cybersecurity is a very competitive field. You will meet many people in your life who might know more things than you. Don't get demotivated by that. If they know 2 things, you know 1; if they share 1 extra thing with you, now you both know 2 things. So always keep +ve attitude of learning from them and don't get demotivated by your position of learning.

6. **Make StackOverflow & Google your besties –** It is not important what you don't know; it is crucial to how quickly can you learn. Google and StackOverflow are the best sources for your doubts (tech or non-tech). Keep them at your fingertips. It is ok to ask stupid questions, so keep asking around.

7. **Community appearance –** You should attend/present at well-known conferences. Start with your local town conference/meetups. Present on a few topics. Gain confidence in public speaking. Then advance to national level conferences and then international level. Meet more people and build relationships.

8. **Bad practices in Cybersecurity –** Nothing is perfect in this world. In cybersecurity, even there are bad practices, loopholes, and cheats. Ensure whatever small or big decision you take; you do all your sanity checks and don't get training to all of these.

Things to learn before starting your career in the Cybersecurity

Networking & Fundamentals	OSI Model	Packets & Frames	Ports & Protocols	DNS in detail	HTTP in detail	Windows fundamentals	Linux Fundamentals

Roles and Responsibilities *(Source: TryHackMe)*

Role	Description	Responsibilities
Security Analyst *(Responsible for maintaining the security of an organization's data)*	Security analysts are integral to constructing security measures across organizations to protect the company from attacks. Analysts explore and evaluate company networks to uncover actionable data and recommendations for engineers to develop preventative measures. This job role requires working with various stakeholders to gain an understanding of security requirements and the security landscape.	• Working with various stakeholders to analyze the cyber security throughout the company • Compile ongoing reports about the safety of networks, documenting security issues and measures taken in response • Develop security plans, incorporating research on new attack tools and trends, and measures needed across teams to maintain data security.
Security Engineer *(Design, monitor and maintain security controls, networks, and systems to help prevent cyberattacks)*	Security engineers develop and implement security solutions using threats and vulnerability data - often sourced from members of the security workforce. Security engineers work across circumventing a breadth of attacks, including web application attacks, network threats, and evolving trends and tactics. The ultimate goal is to retain and adopt security measures to mitigate the risk of attack and data loss.	• Testing and screening security measures across software • Monitor networks and reports to update systems and mitigate vulnerabilities • Identify and implement systems needed for optimal security
Incident Responder/Digital Forensics *(Identifies and mitigates attacks whilst an attacker's operations are still unfolding)*	Incident responders respond productively and efficiently to security breaches. Responsibilities include creating plans, policies, and protocols for organisations to enact during and following incidents. This is often a highly pressurized position with assessments and responses required in real-time, as attacks are unfolding. Incident response metrics include MTTD, MTTA, and MTTR - the meantime to detect, acknowledge, and recover (from attacks.) The aim is to achieve a swift and effective response, retain financial standing and avoid negative breach implications. Ultimately, incident responders protect the company's data, reputation, and financial standing from cyber-attacks. If you like to play detective, this might be the perfect job. If you are working as part of a law-enforcement department, you would be focused on collecting and analysing evidence to help solve crimes: charging the guilty and exonerating the innocent. On the other hand, if your work falls under defending a company's network, you will be using your forensic skills to analyse incidents, such as policy violations.	• Developing and adopting a thorough, actionable incident response plan • Maintaining strong security best practices and supporting incident response measures • Post-incident reporting and preparation for future attacks, considering learnings and adaptations to take from incidents • Collect digital evidence while observing legal procedures • Analyse digital evidence to find answers related to the case • Document your findings and report on the case
Malware Analyst *(Analyses all types of malwares to learn more about how they work and what they do)*	A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings. A malware analyst is sometimes called a reverse-engineer as their core task revolves around converting compiled programs from machine language to readable code, usually in a low-level language. This work requires the malware analyst to have a strong programming background, especially in low-level languages such as assembly language	• Carry out static analysis of malicious programs, which entails reverse-engineering • Conduct dynamic analysis of malware samples by observing their activities in a controlled environment • Document and report all the findings

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

	and C language. The ultimate goal is to learn about all the activities that a malicious program carries out, find out how to detect it and report it.	
Penetration Tester *(Responsible for testing technology products for security loopholes)*	You may see penetration testing referred to as Pentesting and ethical hacking. A penetration tester's job role is to test the security of the systems and software within a company - this is achieved through attempts to uncover flaws and vulnerabilities through systemised hacking. Penetration testers exploit these vulnerabilities to evaluate the risk in each instance. The company can then take these insights to rectify issues to prevent a real-world cyberattack.	• Conduct tests on computer systems, networks, and web-based applications • Perform security assessments, audits, and analyse policies • Evaluate and report on insights, recommending actions for attack prevention
Red Teamer *(Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective)*	Red teamers share similarities to penetration testers, with a more targeted job role. Penetration testers look to uncover many vulnerabilities across systems to keep cyber-defense in good standing, whilst red teamers are enacted to test the company's detection and response capabilities. This job role requires imitating cyber criminals' actions, emulating malicious attacks, retaining access, and avoiding detection. Red team assessments can run for up to a month, typically by a team external to the company. They are often best suited to organisations with mature security programs in place.	• Emulate the role of a threat actor to uncover exploitable vulnerabilities, maintain access and avoid detection • Assess organizations' security controls, threat intelligence, and incident response procedures • Evaluate and report on insights, with actionable data for companies to avoid real-world instances
Security Analyst (SOC – Tier 1) *(Triage)*	A Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring a company's network and systems 24 hours a day, seven days a week. Their purpose of monitoring is to: • Find vulnerabilities on the network • Detect unauthorized activity • Discover policy violations • Detect intrusions	As Tier 1 analyst in the SOC, your duties will involve • Monitor network traffic, logs, events, alerts • Work on tickets and close, triage alerts • Perform basic investigation & mitigation,
Security Analyst (SOC – Tier 2) *(Incident Responder)*	A Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring a company's network and systems 24 hours a day, seven days a week. Their purpose of monitoring is to: • Find vulnerabilities on the network • Detect unauthorized activity • Discover policy violations • Detect intrusions	As Tier 2 analyst in the SOC, your duties will involve • Focus on the deeper investigation, analysis and remediation. • Proactively hunt for adversaries • Monitor and resolve more complex alerts • Prepare weekly/monthly reporting
Security Analyst (SOC – Tier 3) *(Threat Hunter)*	A Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring a company's network and systems 24 hours a day, seven days a week. Their purpose of monitoring is to: • Find vulnerabilities on the network • Detect unauthorized activity • Discover policy violation • Detect intrusions	As Tier 3 analyst in the SOC, your duties will involve • Works on more advance investigations & remediation • Perform advance threat hunting and adversary research by consuming threat intel data • Malware analysis and possible reversing • Developing new adversary detection signatures through SIEM

Master's Degree

Shall I go for a master's degree?
Shall I go for master's in your own country or foreign?

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

Is there any value in a master's degree?

Let me start answering this section with myths and realities.

Myths	Reality
A Master's degree in cybersecurity is not required.	It is true but not 100%. There are some intermediate benefits of having a master's degree on your resume. Those benefits are not just limited to your technical and academic knowledge of cybersecurity but also related to your people networking and other soft skills such as team building, project management, strategic planning, communication, business communication writing, etc.
A Master's degree in cybersecurity is helpful to get more salary or a quick job.	There won't be any difference in your starting salary as a fresher in cybersecurity even though you have a masters from any country. There is an exception to this. If your university is super famous and has quality placements, then based on grad assessments, they can give you a good package as a starter compared to someone who just passed out from university and is trying to find a job via LinkedIn and other portals.
Cybersecurity requires skills, and masters, they don't teach practical knowledge; they only teach basic skills and primarily theoretical.	It is not true, and it is based on the university to university and country to country. What you see people doing in the community is knowledge of working in corporate & doing professional research. Don't expect the university will provide you with that level of knowledge. Master's programs are designed to develop your cyber foundation and let you know how many different fields there in cybersecurity are rather than teaching you very professional stuff that is being used in the corporate world. They expect you to clear your fundamentals, communication, and consulting skills. Also, if you are a university pass out, companies understand your level of knowledge, so they will not even expect you to showcase your skills that match their company's requirements.
If I have masters in cybersecurity, my chances of getting selected for job interviews are higher	It won't make any difference in job interviews; people with even CA or commerce with cyber knowledge and skills can get a job instead of you. This field demands skills and knowledge and not your solid academic background only.

The first thing to consider is why you want to study for a master's in the first place. Is it so that you can progress in your career? Is it a requirement to pursue a particular field? Or are you just doing it for the sake of learning? Whatever the reason, it can help you to narrow down your options. Don't be tempted to pick a degree just because you feel it might look good on your CV, either.

This question is very hypothetical, and there is not a single answer. There are 50-50% advantages and disadvantages of doing and not doing a master's in your career, especially in cybersecurity or any other field.

Advantages:
- If you do a master's degree in foreign country, you will get good local exposure to that country; you will be studying and spending time with different people from various countries.
- Your communication will be improved.
- You will be doing many projects with your classmates together, which will teach you how professional project management can be done, including planning, execution, communication, & presentation.
- You will be able to travel to a new country to meet new people, get exposure to the local cybersecurity market of that country, regional security conferences, etc.

Disadvantages:
- A Master's degree will not give you real-life knowledge of security that is being done in corporates. However, this is not a big disadvantage, as those programs are designed to build a foundation only.
- A Master's degree takes 2/3 years of your life. So, if you want to skip it, you can have 2/3 years of corporate experience instead of doing masters.
- Masters will not give you a higher salary.
- Masters will not make you different in job interviews.
- Course fees are very high, especially you if are going for a master's degree in western countries.
- **Important:** You may or may not get a post-study work visa. In most countries, once you study, there are very tiny chances of finding a company that can sponsor you, so you may have to come back to your original country after studying there. Work visa sponsorships are very, very, very rare for Indian students.

So, it really depends on you. If you have TIME and MONEY and want to get some foreign exposure, you can do master; else, you can prefer doing it from your own country. If you don't have time and money, you can skip it and get a job directly after your bachelor's.

Things to consider before choosing any master's degree program
Post-study work visa options/Chances of sponsorship
Course syllabus and topics of study
Professor's background and credentials
University's global rank and national rank
University's partnership with leading security firms/government agencies
Internship opportunities are included or not
Post-study placement opportunities are included or not
Access to the career services department has been in helping you prepare for interviews and search for internships and full-time jobs
Consider course fees
Consider course duration/length
The job market in the country you are planning to do masters

Internship

Shall I go for an internship in any company after my study?
Will it be helpful in my career?
What kind of internship do companies provide?
Is it necessary to do it from a renowned company or any company?

The answer to this question is too broad. It depends on many factors such as:

- Which company is providing Internship (Product based company, security consulting company, Big4 etc.?)
- What are their requirements for internship programs?
- What will be the job roles and responsibilities during the internship?
- What are the expectations from an employer?

There are very few; I would say only a handful of companies that provide quality internships where you would learn valuable things. Most of the money-making companies are running CEH (Certified ethical hacker – Which is the official certification from EC-Council, a well-reputed cybersecurity certification authority) and related courses on the name of an internship. For example, if my company's name is Prakash, then I will provide my own CEH certification in the name of "PCEH – Prakash Certified Ethical Hacker" and so on.

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

So, I have prepared 'DO' and 'DON'T' for selecting a company for your internship.

DO
Understand the nature of a company (consulting, product-based, small, big, etc.).
Ask them about your daily responsibilities, tasks, and job routines.
Ask them what the learning options are they can provide to you during your internship.
Ask them what their expectations from you during the duration of the internship will be.
Ask more and more people around for the reviews of those companies you are evaluating for internships.
Identify your career interests. This could be done by self-reflection, speaking with a Career Counsellor or your mentor
Ask the company about paid or unpaid Internships. You can go for any as far as other criteria are matched.
Start searching for an internship at least 6 months prior.
If you are interested in any company and can't find any internship opportunity, you can check their website and social media. Connect to their HRs via LinkedIn and ask the same.
Better understand and research who they are, what they do, their strengths and weaknesses
Perform at least 5 mock interviews with your career counsellor or mentor before going for an internship interview.

DON'T
Don't select a company that just provides course teaching, coaching.
Don't select a company that do not serve any clients or serve any handful of clients only with simple projects.
Don't select a company that asks you to teach their students via their coaching, training programs.
Don't get attracted by any company's marketing & PR success.
Don't get attracted by their company's reputation through magazines, press, awards from random conferences or panels.
Don't select a company where only 4/5 people are working; all are Founders, Co-Founders, Directors. If you do, please check their professional background. Check whether they obtained these titles without having any prior corporate experience or started their start-ups after having at least 8 years of experience in the industry.

Which certifications should I go for?

This is a debatable question, and there is definitely not a single answer for this. Before planning for the certifications, it is best to know what the factors are to consider before choosing/going for any certification.

Things to consider before choosing any cybersecurity certification
Certification must be from well-known authorities
Cybersecurity-specific cert provider authorities - ISC2, eLearnSecurity, Offensive Security, ISACA, EC-Council, CompTIA, CREST, SANS, GIAC, etc.
These are vendor product-specific cert provider authorities – Amazon (AWS), Google (GCP), Microsoft (Azure), Cisco, Checkpoint, etc. There can be others as well.
Are these certs requiring in the market? Search LinkedIn jobs where those JDs require these certs for the jobs. If they are not required, no need to go for that cert

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

Are you going for a beginner level cert in your particular domain or going for a management/high-level cert directly? Know what the starting point vs is ending point

Are you going to obtain multiple certs from the same cert provider or choose different cert providers every time? It is good to have different cert providers' certificates on your resume.

Are you taking cert for the sake of job only? Or for knowledge?

If the job only then is, you are spending a huge amount of money without having any job confirmation even?

What will be the future of this cert after 5 years? Can it be obsolete? Will people still feel its value?

E.g., the Overtime value of CEH has dropped, companies still recommend it, but anyone who has CEH is not that regarded compared to OSCP, OSCE, GPEN, etc.

E.g., Regardless of the time period, the value of CISSP, Security+ have always been there in any company. It has never decreased.

Are your career goals aligned with the certificate you are going to obtain?

If possible, it is recommended to obtain a certificate in technical and managerial areas of your cybersecurity domain.

Types of companies

How many types of different companies are there?
Which types of companies to choose in the initial career?

Legends	Consulting (Big4 & Other Big companies)	Small Consulting Firms	Product-based Firms	Security Vendor Firms
Size	They are giants, thousands of employees	Small and Medium Enterprises	It can be any small, medium, large Enterprises	It can be any small, medium, large Enterprises
Reputation	Well-reputed	Maybe reputed in their region (State or city) Sometimes famous within the country but not internationally reputable and known	Can be well-reputed within a country or internationally recognizable.	Can be well-reputed within a country or internationally recognizable.
Example	KPMG, Deloitte, EY, PwC, Accenture, etc.	Your local security consulting firms.	Google, Microsoft, Apple, Amazon, Tesla, Walmart, etc. Your local product-based companies are smaller than the above giants.	All cybersecurity vendors: CrowdStrike, Whitehat, Rapid7, Qualys, Tenable, RSA, Trustwave, Imperva, etc.
Client-base	Serves clients all over the world	Limited based on their presence, areas of services they provide due to expertise	Big giants serve the entire world. Small companies are limited to serve their local clients.	Big giants serve the entire world. Small companies are limited to serve their local clients.
Project type	Executes various types of projects (Projects vary from technical to management all areas of cybersecurity)	Depends on the areas of services they master. They will provide services in limited cybersecurity areas based on their expertise. Some only provide technical, some provide tech + management, etc.	You will be doing anything and everything to secure the products of these companies from external attackers.	Two types of roles: 1. Serve clients by solving their queries on your security products OR 2. Work with the engineering team to enhance product algorithm, engine, features, signatures.

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

Learning opportunity	Good learning opportunities in consulting & technical both areas. Their own global network cross-country learning opportunities	Limited (From your peers and surroundings) Mostly, you will be a self-learner	Massive as you work within a company to secure their infrastructure. So, you have the advantage of knowing the company better than external attackers.	Limited based on the area you work in for that firm.
Your role	Jack of all trades	Jack of all trades but limited to one domain of cyber. If Pentesting, then all Pentesting areas only.	You will be required to work within 1 or 2 domains of cybersecurity within that company, and there will be other security domains. You work closely with every team to secure your company's products.	Master of one (You will be working in a limited cyber domain, but you will be master of that domain)
Salary	Competitive salaries	It depends on the size and revenue of the organization	Competitive salaries (depends on the size of the company)	Competitive salaries (depends on the size of the company)

Types of high-level job roles & responsibilities

Technical Consulting (External – Red team)	Technical Consulting (Internal – Blue team)	Compliance (Management/Leadership)
Work as a security consultant, security analyst, penetration tester.	Work as a threat hunter, threat intelligence analyst, vulnerability management specialist within a company to secure your own company. You are a part of the blue team and not required to consult external clients. You do your own security.	It is a non- or semi-technical cybersecurity field to get in where you work for a company to maintain its overall 360-degree security posture by auditing and reviewing people, processes, and technology estate security.
You will be given targets to hack. Those targets are of your clients, and it could be website, software, network, IoT device or anything. You hack it. You write a report on how you hack it. You present and explain the report to the client.	Your task depends on which area of the blue team you work in. The goal is still the same – secure your organization.	Fewer quality people are in the compliance field at the beginning of their career, at least, so it's a good chance to start a career. For these job roles, the company provides higher designations in their organization. Direct reporting to the senior leadership of the organization.
The most typical job in every company, so easy to switch at every location you prefer. You get an overall good knowledge of every field within cybersecurity, such as web security, mobile security, wi-fi security, IoT security, malware research, compliance etc. You can earn good money in companies and do freelancing stuff to support your financial situation.	Technical + Managerial job role	It is a less technical job. You will be required to work more on audits, reviews, reporting than technical security.
High competition	Intermediate competition	Less competition

Resume writing – How not to blunder

Do you want to break into cybersecurity but don't have the experience to show on your resume?

No worries.

Here are ten great resume-building activities that will make you stand out from the competition: (Thanks to Naomi Buckwalter for compiling this list - https://www.linkedin.com/in/naomi-buckwalter/)

1. Volunteer with a cybersecurity conference
2. Teach a cybersecurity class
3. Mentor a student
4. Join a cybersecurity working group
5. Contribute to an open-source project
6. Build a home lab
7. Start a blog
8. Guest on a podcast
9. Lead a study group

10. Start a cybersecurity meetup or club
11. Get a basic CEH, Security+ or equivalent cert
12. AWS, Azure, GCP, etc. certifications
13. Find a vulnerability in a reputed website (bug bounty)
14. Find zero-day and get a CVE id

Once you do the majority of these, you would have a good number of things to showcase in your resume and your Interview.

Below are some common resume blunders I have seen over the years. Try to avoid it.
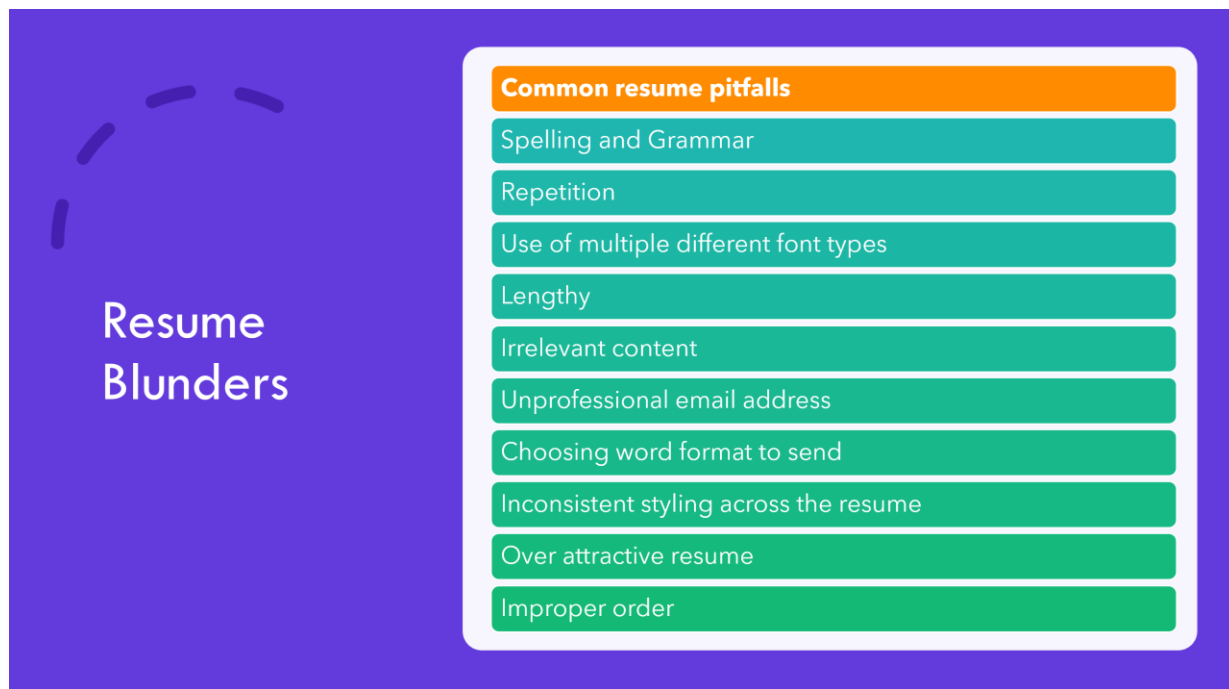
LinkedIn – Why create a quality profile

One question to you, do you want to get noticed by reputable persons in your industry? Then it is a must to create a killer LinkedIn profile. Here are the steps to create and maintain a perfect LinkedIn profile.

How to create a killer LinkedIn profile	
Profile pic	Your profile picture matters a lot to many. It's not about to look, but it's about professionalism. We have social media like Facebook, Instagram, etc., to share our photos in whichever way we want. But on LinkedIn, many HRs or professionals would want to see you as a professional. Posting a professional profile pic shows your attitude, how seriously you take a LinkedIn platform, and professionalism. Not that it's going to affect you a lot in your next Interview round, but something to consider in order to mature your LinkedIn profile from all 360 degrees.
Things you share and like	Things you share and like describe your personality. This is a very common issue among all. People share and like a random post. People use LinkedIn from their perspective but not from the other's (HR and big company's CEO or manager) perspective. Ask yourself if you are HR and if you want to find a candidate to work in your company, and you are visiting his or her profile. You find more stuff regarding other general things such as jokes, politics, random debates, inspirational quotes etc. How would you know that the person is good at his domain or not? Does that profile sound good? If you are a cybersecurity person and visit my profile, there should be some

	takeaway for you in terms of my knowledge sharing through my profile. So, you visit my profile, and you will find more articles, links, etc., about cybersecurity that may interest you. Because this is a professional network, and you should try to share and like stuff related to your profession only. So, the point is only talking about shares and likes related to your field, not random things.
Writing a post on your wall	Writing a post also matters a lot. Do not write stuff out of your field, portraits discrimination, hate rate, bad things about a specific community, cast, religion, etc. Your post must be crystal clear and should be understood by all types of audiences who read it. Don't do bulk sharing. You shared a post today; wait for 5 days at least to write another post. Let people read, react like and share your existing work. Don't act like a spammer or unprofessional enthusiast who just keep on sharing things to increase your reachability.
Write relevant posts	Only write posts that are not discussed before yet not explored a lot. Well, I would never talk about cybersecurity, why it is essential, what is website hacking, etc. Numerous amounts of the stuff are there on the internet. I would only discuss specific things within the topic only, which can take the interest of others. If I sound unique, people may create an impression that I am a researcher/explorer, not just a techie guy who works on cybersecurity. Writing a post can be your own work, discussion topic, research, tutorial, literature review and debate outcomes. Always before writing, think that do I sound negative? Can many people dislike this, or do I have a negative view of this topic compared to others? Do not share such things at all. You must be neutral on each topic. Be neutral, be unique, add more specific and detailed things to explain your writing, give a clear message do not sound confused that whether you are asking or telling or just sharing or what you want, avoid using short forms and F words or any lame and abusing words.
Be polite and gentle	Be gentle all the time. When someone adds you give these two lines to them. Thanks for adding me to your professional network. I am glad to connect with you. How are you? No need to use sir, mam; no one likes that on LinkedIn. If you share something and people give negative comments, then gently accept, or share your further argument. Do not fight. Choose your words carefully.
Contact information	Keep your LinkedIn profile up to date with your contact info, email id, phone number and other details. For your every job, also mention what your key role in that company was. Also, mention if any awards or recognition you got in that company or not. For this, you can visit my profile and check yourself how I highlighted my work in each former company.
Introduction Paragraph	Write your introduction paragraph carefully, mention three things. What are you? No. of experience and what are you looking for in your future (means where you want to move your career ahead, what you want to learn, what type of challenging roles you are looking for)
Achievements	Mention the relevant achievements in your profile only. I have plenty of national-level prizes in drawing competitions but does it relevant to my profile. HR is visiting my profile to see what kind of tech expertise I have. How does it matter to them? Even within IT, I hold web and graphics designing certification from Aren animation. Still, I work on cybersecurity, so I don't see a reason to share this even in my profile. So only share relevant things.
Profile title	Add the best profile title. 2 liner title. Whoever visits your profile, he/she should have your impression just by looking at your profile title only. For this, visit my profile and see how and what I wrote under my name.
Upload documents	Add images or documents to your experience. Did you know that you can add media files to your experience? It is a great way to create a visual portfolio along with your standard resume information.
Ask for recommendations	Endorsements are great, but recommendations are the currency of the realm on LinkedIn. Reach out to past colleagues, managers, and associates and ask that they write you a recommendation.

Finding a job in a foreign country

How to get a job in a foreign country?

It is hard to get a job in a foreign country sitting in your own country. Why because of Visa sponsorship.

Visa sponsorship – It is commonly believed that visa sponsorship is just a single sponsorship letter for a company to give you. So why do not they give it? It is not like that. Visa sponsorship for a company is really a massive pain. It requires them to hire a lawyer, immigration officer for you to do the process. It requires them to fill different lengthy forms to convince the government legitimately that they tried to hire people from locally within their own country. Still, they could not find the right talent compared to the one they intend to hire from overseas.

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

They must answer a lot of questions on paper, such as:

- How many interviews have they taken for that post in their own country?
- How many were rejected?
- Why were they rejected?
- Why do they want to hire someone from overseas only and not any other country?
- How skillset of yours differing from those previous guys whose Interview was taken in their country?

Even after all these headaches, there is a 50-50 chance that the government will be convinced to grant permission to that company to hire you.
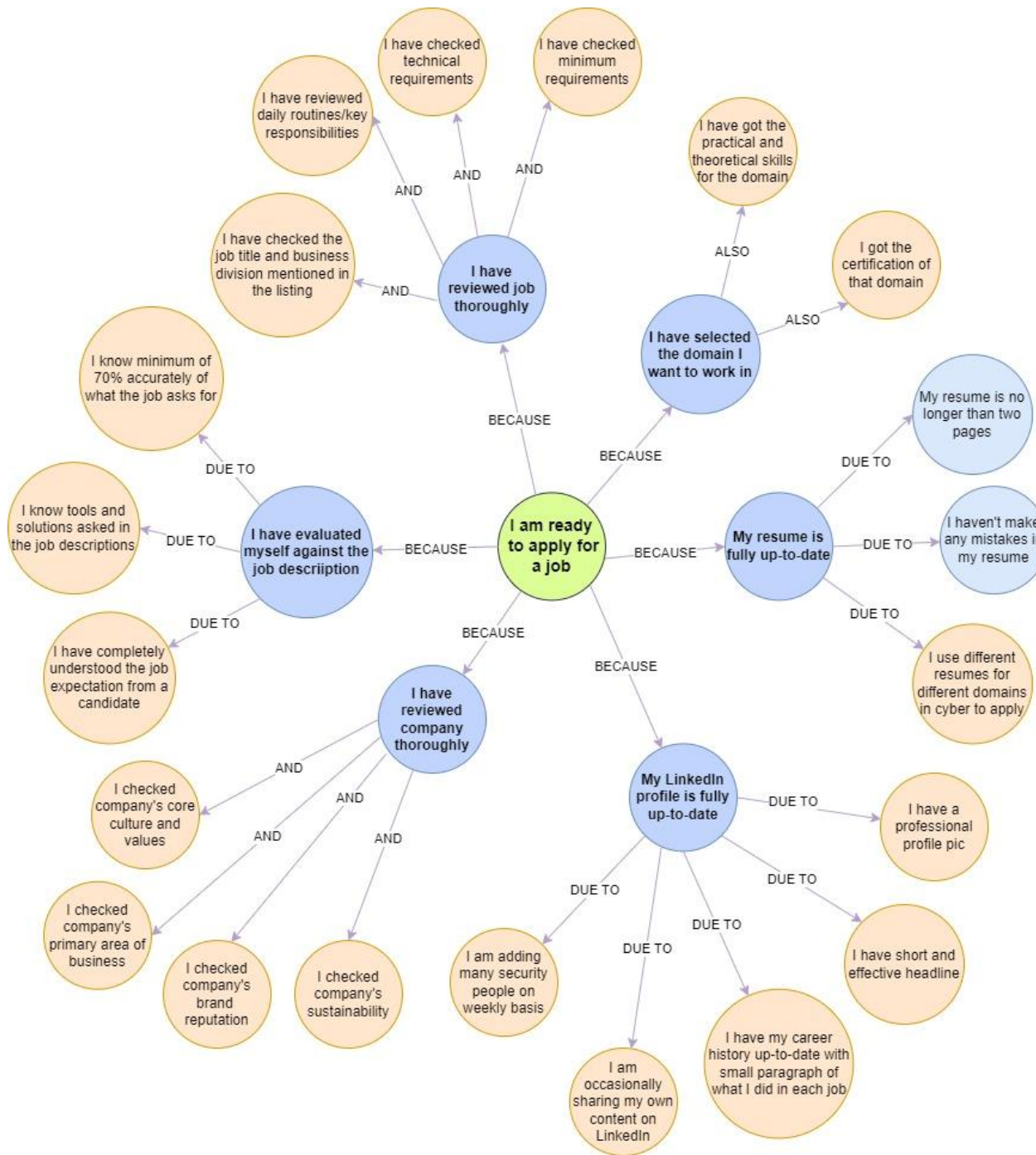
None of the methods is accurate and achievable. Because getting a job in abroad company depends on so many factors such as:

- Target country's strict immigration rules
- If a company is willing to take the headache of visa sponsorship or intend to wait and hire someone locally
- A unique skill set requirement of the job in that company
- Skill shortage in that country, specifically in your field
- Your luck

What is the approach to apply?

Step-by-Step guide you can follow	
Countries	1. Create a list of countries you are interested in working in.
Job titles	2. Create a list of job roles/titles/positions you are interested in or relevant to your area of domains.
LinkedIn Job Filter (Country)	3. Go to LinkedIn jobs. Filter country with one of your dream countries. Give a single job title.
LinkedIn Job Filters (Date)	4. Filter results by latest jobs first through advanced filters of LinkedIn.
Apply for jobs	5. Apply for every single job you think are worth it for you to have.
Create alerts	6. Once you have applied to all the jobs of the last 30 days, create job alerts on LinkedIn for any new job posts that come out in that country. Apply it straightaway.
Change country	7. Repeat the entire process with another country in next week. Keep shuffling countries and repeat the same steps.
Add security people	8. Add 10 cybersecurity practitioners every day in your LinkedIn from the country you want to go in who work in the same area of security as you.
Add security HRs	9. Add 5 cybersecurity HR every day in your LinkedIn from the country you want to go in.
Share knowledge	10. After increasing your network in the local region of your dream country, you need to do create unique, valuable research and start posting regular content on LinkedIn. Let people know who you are, what you can do, what your interests, etc. If they know you more, there are good chances they might want to work with you, or they see you as a potential candidate for their company, etc. *This is important even if you are not looking for a job.*

Job search approach

I have checked technical requirements

I have checked minimum requirements

I have reviewed daily routines/key responsibilities

I have got the practical and theoretical skills for the domain

AND — AND — AND

I have checked the job title and business division mentioned in the listing

AND

I have reviewed job thoroughly

I got the certification of that domain

ALSO

I have selected the domain I want to work in

ALSO

I know minimum of 70% accurately of what the job asks for

DUE TO

BECAUSE

BECAUSE

My resume is no longer than two pages

DUE TO

I know tools and solutions asked in the job descriptions

DUE TO

I have evaluated myself against the job descriiption

BECAUSE

I am ready to apply for a job

BECAUSE

My resume is fully up-to-date

DUE TO

I haven't make any mistakes in my resume

DUE TO

I have completely understood the job expectation from a candidate

DUE TO

BECAUSE

BECAUSE

I use different resumes for different domains in cyber to apply

DUE TO

I have reviewed company thoroughly

BECAUSE

My LinkedIn profile is fully up-to-date

DUE TO

I have a professional profile pic

AND

I checked company's core culture and values

AND

AND

AND

DUE TO

DUE TO

I checked company's primary area of business

I checked company's brand reputation

I checked company's sustainability

I am adding many security people on weekly basis

DUE TO

DUE TO

I have short and effective headline

I am occasionally sharing my own content on LinkedIn

I have my career history up-to-date with small paragraph of what I did in each job

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

General DOs and DON'Ts in Cybersecurity

Apart from all the things we have discussed so far, there are still plenty of things you should and shouldn't do in the cybersecurity industry. The following table illustrates DOs and DON'Ts of the cybersecurity industry.

DO
Ask lots and lots of questions to yourself. Such as • Why this • Why not that • How it is happening • Why it can't work in another way • How can I learn this? • etc.
If you develop more curiosity, you will learn a lot, which is the only way to succeed in our industry.
Keep a target of two years and ask yourself where you want to see yourself in the next two years. Keep achieving this target and then set a new target after two years.
• Share knowledge. Don't just keep it with you. If you share, you will: (Source: https://github.com/s0md3v/be-a-hacker) • Be appreciated and it will motivate you to share more. • Any mistakes or improvements to be made in your content will be pointed out so the overall quality of it will increase. • You can only explain something if you understand it well which can be a self-check to see if you actually know enough about a topic. • Exposure is a great thing. It will bring you opportunities and the power to influence people for good.
It is good to work in different areas of cybersecurity; maybe some of the areas might not be relevant after some years; at that time, if you would have knowledge and skills in other areas of cybersecurity, you would be able to survive and find a new job. It would be easier for you to switch from one domain to another at that time.
Respect gender diversity and give the same amount of respect to all men and women.
Maintain healthy relationships with everyone in cybersecurity because the security industry is very small, and you would meet the same people wherever you go.

DON'T
Do not waste money blindly.
Do not go for the paid courses which are already available freely on the internet
Do not get attracted by fame and money game after bug bounty industry
Do not apply any shortcuts in the industry, whether it's for certification or getting a job.
Try to learn from your seniors but as well as from juniors.
do not defame others
Do not leak sensitive data which are copyright protected.
A rockstar is a person who might be skilled but isn't a very good person to work/talk with. They often have a big ego; they like to work alone because they know* everything and they often look down on people. It doesn't essentially mean that they are bad people because this behaviour can be both intentional and unintentional. The point is, they look bad doing so and more importantly, make others feel bad.

To be honest, this is a common problem and I too once started to slip into this zone due to depression, it was not fun, that's why I have included it.

Don't be some egoistic genius sitting in a room. (Source: https://github.com/s0md3v/be-a-hacker)

Challenges for beginners

I think below are the challenges beginners face in any industry when they step into the corporate world. Not only I have shared the challenges, but I also shared how you can overcome them.

Area	Challenges	Solution
Communication fear	• Don't understand how to communicate with new professionals in the market. • Don't understand what business and corporate communication vs friendly college/social life communication is • Don't know how to start talking with new professionals • Don't know what to talk what not to talk about until you make a healthy relationship with the new professional	There are plenty of videos on YouTube specifically for business and corporate communication skills improvisation. It is essential to go through it and stand different from your fellow beginners in the market as a beginner. You can use the below keywords to go through YouTube videos. • Professional communication skills • Business communication skills • LinkedIn communication skills • Business communication
Unprofessional communication	Below are some examples of unprofessional communication. • Asking straightaway for reference and jobs • Asking questions for which you can easily get answers from Google • Chasing people often as they might be busy • Writing long intro email until and unless someone asked you • Giving your resume straightaway as you add people • Not checking your tone of the message	Simple, don't do things mentioned in the left column. • Keep patience • Start with simple, small • Build slow healthy relations • Ask experienced people around you to help you • Ask your mentor • Observe how to experience people talk to you when you are talking with them • Adapt different professional people's talking/writing styles to improvise yourself.
Lack of patience	Beginners are very much desperate to get something, whether it's material, an answer to a question, suggestion or even a reply from HR after applying for a job. They send chaser emails, call them, and find ways to communicate with them faster via phone, social media, etc.	Remember, what's essential for you can or cannot be important for others. So, it is wise to keep patience. Keep patience as there are always other ways, different alternatives for your needs. Give them reasonable sufficient time. Don't chase people often as you want things to move desperately. Especially for jobs, if HR does not reply after you apply for the job, maybe your resume is not selected. No HR in the world just receives a resume and send it to the dustbin without looking at it.
Writing blunders (Resume, LinkedIn, Email)	Beginners make a lot of mistakes in resumes, LinkedIn profiles and emails to any professional.	I have described all the resumes and LinkedIn blunders in a detailed section of this article.
Lack of industry/corporate understanding	Beginners assume things in their own way, but they are not well-versed with the reality of how corporate works. What you think outside is not the same case as how a company works within the inside. **For example,** submitting 1 bug (vulnerability) to a company, you think why the company has not responded for 4/5 days even as it's just a straightforward bug. What you don't know is, any single bug/vulnerability related comms that come from outside will go through a proper VDP program inside for which app team, infra team, incident management, vulnerability management and SOC team would be a part of. They all are responsible for doing one or many things with that report. Such as: • VM team will communicate that vulnerability to the app team • Infra team will see if an app can be protected by FW/IP based restrictions or not • SOC would see if there were any alerts/incidents or not	Some tips for you: • Unless and until you work in the industry, you cannot understand how it operates from outside • Don't assume ask around • Keep patience • Keep seeking advice of your mentors

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

	- App team will fix the bug - VM also checks severity, a risk to business (Risk to business is not only the CVSS you submitted, but what is an actual risk is to business can be only known by the internal blue team) - Management involvement in order to decide how much to pay a researcher - Document all evidence of bug, fix, payment, researcher name, email comms. - Identifying how many similar types of bugs companies know - Checking with traditional vulnerability scanners is why they could not detect those as companies pay for those scanners. - App/Infra/Network team gather and identify the root cause problem business-wide for all similar types of bugs and how they can fix it rather than point fixes. - VM team to identify how they can increase their coverage for those out-of-box vulnerabilities. - Management to ask questions and check in their app pentest/red-team partners why they could not detect the vulnerabilities you submitted. **Another example is submitting your resume to HR of a company and expecting** a response in 5/6 days. Assume if you are the HR of a large company, how many resumes in a day you would get? Also, you are not only filling 1 position but many positions from various divisions of the company. You would be flooded with tons of resumes for all different departments. You will have to go through each one of them, filter them, talk, and discuss CVs with those division leaders in your company, filter candidates, send them emails one by one, keep track of records of emails and candidates, organizing interview rounds, including phase 1 phase 2 and all, aligning candidate's time with the interviewer's free slot, and many other responsibilities. Again, not just for the 1 position you are filling but many in the same company. Hence, when you apply, you should not expect a quick response.	
Poor grades	Some beginners will have poor grades in their education, and they are hesitant to show them on their resumes.	You don't need to write grades or show them to any company unless and if they ask you. Just mention what study you have completed. In the cybersecurity world, skills and practical knowledge weigh more than grades. If some companies, ask for grades and also questions you why poor grades you can answer them below: - You were interested more in practical knowledge during your education; hence you focused on real skills than theoretical knowledge. - Maybe you might genuinely have some social or other responsibilities or any other reason you got poor grades; you can transparently explain those. - Maybe you are preparing for the cybersecurity certification. So, you don't need to fear even if you have poor grades. You can still transparently show your education stuff on your resume.
Lack of self-learning	I have seen beginners asking many simple questions for which answers are readily available on Google. Self-learning is really required in the cybersecurity industry.	I think the YouTube industry has created so many videos on YouTube which lets you know from very simple things to very complex things; on top of that, you can search all the things easily on Reddit and Google. You should only ask other questions if you cannot find answers easily from Google or any other sources on the internet.
Don't know which companies to go for	Often beginners don't know which company they should apply for a job, whether it's a product base, consulting, or a good security company.	I have covered this challenge & it's solution in-depth within this article.
Feeling demotivation,	there are two types of demotivation. 1. knowledge and skills demotivation 2. Experience demotivation	I have covered both of them in detail within this article, along with the possible solutions.

How to stay up to date with the latest knowledge in the security field

If you Google this, there are plenty of methods to stay up to date in the security field. The best way I found is by using more and more hashtags (#). Individuals and companies both love hashtags. If there are any latest news, people tweet it using hashtags. If you follow any blog, YouTube channel, or any single resource, you will not have other domain knowledge than those creators put out there. If you start visiting many links, you will not be able to keep a bookmark of all URLs, and management would be difficult. All you can do is collection of more and more hashtags.

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning
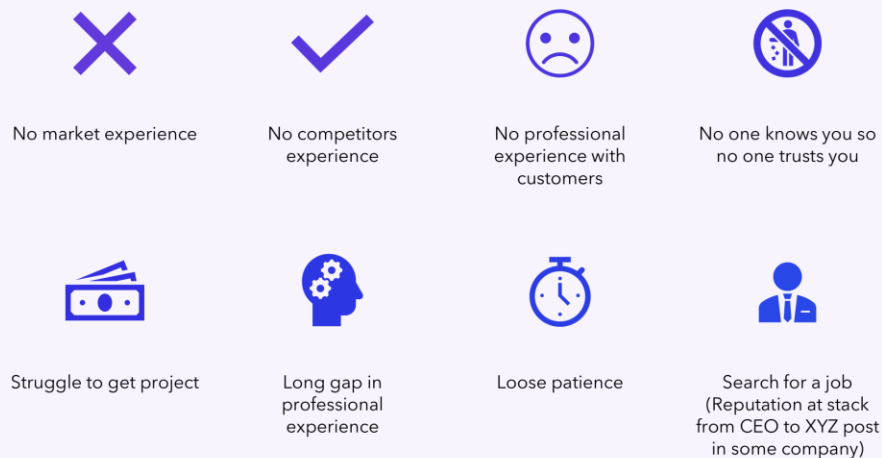
What you need to do:

DO
Know what your area of the domain is specifically (E.g., SOC, Pentest, Cloud Security)
Start listing all possible hashtags in those areas. Ensure you think of a wide variety of stuff while creating hashtags, such as methodologies being used, most common tools being used, other relevant tags being used with that, etc.
Go to Twitter, LinkedIn, search content with those hashtags
Filter noise of data by looking at the latest (last 24 hours, last week) contents only.
Read it
Take notes if required
Repeat the cycle
Create a weekly schedule on reading on 1 topic every day; then follow the cycle.

DON'T
Don't add irrelevant hashtags for which people don't often put any content (simply because they don't use those hashtags even)
Don't add a very long hashtag for which chances of finding content are tiny

Sample hashtag database for you to start with *(you can create your own like this)*	
General security	#cyber #cybersecurity #cyberattack #cyberattacks #cybersécurité #cyberrisk #securitymanagement #securityawareness #securityprofessionals #infosecurity #informationsecurity #infosec #security
Threat intelligence and threat hunting	#threathunting #threatintel #threatintelligence
Penetration testing & security assessment	#pentest #pentesting #penetrationtesting #testing #networksecurity #Redteam
Application security	#bugbounty #bugcrowd #bughunting #appsec #applicationsecurity #apis #webapplicationsecurity #web #webdevelopment #mobileappdevelopment #owasp
Cloud security	#cloudcomputing #cloud #cloudsecurity #aws #azure #gcp

Don't become a CEO/Founder directly without having any corporate experience

Pitfalls of becoming a quick CEO

- ✗ No market experience
- ✓ No competitors experience
- ☹ No professional experience with customers
- 🚫 No one knows you so no one trusts you
- 💵 Struggle to get project
- ⚙ Long gap in professional experience
- ⏱ Loose patience
- 👔 Search for a job (Reputation at stack from CEO to XYZ post in some company)

I have found this scenario that many college/university pass-outs become CEO/Founder/Co-Founder straight after graduation. Some think that having a founder/co-founder/CEO on a profile makes a difference, and it looks cool. I am not saying no one should become an entrepreneur, but my point is without having any proper corporate experience, you should not jump straight into entrepreneurship.

One should not become an entrepreneur in cybersecurity without having any of the **single things** from below:

Solid Product	Unique Service	Solid Funding
When I say solid product means, you created something that is unique and solves a significant amount of problems for an enterprise. There are no products in the market such as you. You have all the features in your product to meet any large enterprise's need.	When I say, unique service means no common services such as pentest, code review, risk management assessment etc. If your approach to providing these services is unique, if you can create a difference and give value to your customers, then it is ok to provide the same services. You need to ensure to provide a great quality of services compared to other competitors in the market. If you are not the one who can make a difference, don't become a CEO at an early age.	Many people might be rich already; if you don't have a great idea or unique service, you can invest your money to create an exceptional service or product with the help of the right mindsets in your team. Even you can invest money into experienced BDMs (Business Development Managers) who already have established contacts in the market who can bring projects for you.

Without any of the single thing from above, there is no way you can survive in the market, and I guarantee you.

Approach to create a solid product:

1. Do a lot of literature review

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

2. Do a lot of market review
3. Understand what gaps there are in the industry and what kinds of products are not available
4. Evaluate whether you can create something that can fulfil the market's need?
5. How much time/money/efforts would be required for not just making a product but also running its post-build operations
6. How much time it can have to be successful by doing marketing, customers purchase it, and revenue is generated afterwards
7. Which are your target industry and country
8. (A lot of things go in this thought process; these are some really basic before you start)

Post this analysis, create a product, and sell in the market as an entrepreneur.

Since you will be a young, dynamic aspirant, if you go with this all analysis, you will still be excited to work on something as you want to become a CEO, don't rush, the market is very dynamic, almost there are every solution in the market, and they are good even. So do proper research else, don't even think about this.

I have seen plenty of people who started their company without having any of the above and then:
- Not able to serve client properly as they don't understand how big corporate works internally
- Not able to beat their competitors as they don't know what they are up against
- Not able to know how the market industry works as no experience of working in corporate at all
- Struggle to get a project as they don't have good funding to invest, unique service or unique product.
- No one knows about you as you are an absolute fresher with no credible experience or achievements.
- You lose patience after a few years of trying to run your company, and when you close it, search for a good job with a stable income in any big company.

How not get demotivated in cybersecurity?

Demotivation in cybersecurity is not a new thing. Due to the high amount of competition in security, things such as attitude, knowledge monopoly, marketing of experience and knowledge is common. A lot of youngsters who get demotivated when:
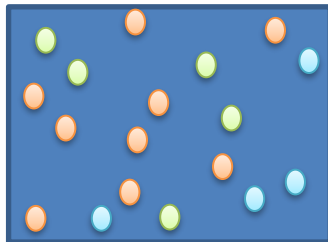
- They see other's success
- They are not treated well by others (in or outside of the company)
- They can't find a way to get success
- They see money and fame games on all social media about bug-bounty and other stuff
- Any other reason…

What you really need to know is this:
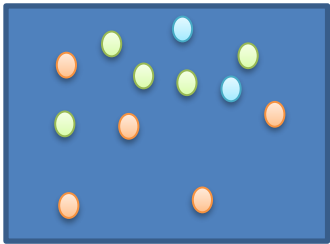
Knowledge/Skills Demotivation
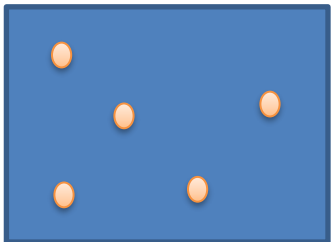
       You know   **They know**
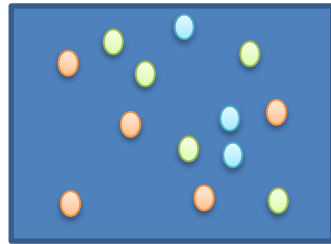
**You learn**

Now

You know   SAME as   They know

You need to take this as a positive approach and keep constant learning without getting demotivated. If another person knows 5 things, you learn them from YouTube, Blogs, Courses, and Free materials. Now you and they both have the same knowledge, so there is no need to get demotivated in security if you don't know things.

Be grateful that you met that person through whom you came to know what else you needed to learn. Make a not, learn it. Have the same knowledge as they now. Mission accomplished.

Experience Demotivation

If you get demotivated by someone's massive experience in cybersecurity, always believe in the below diagram 😊
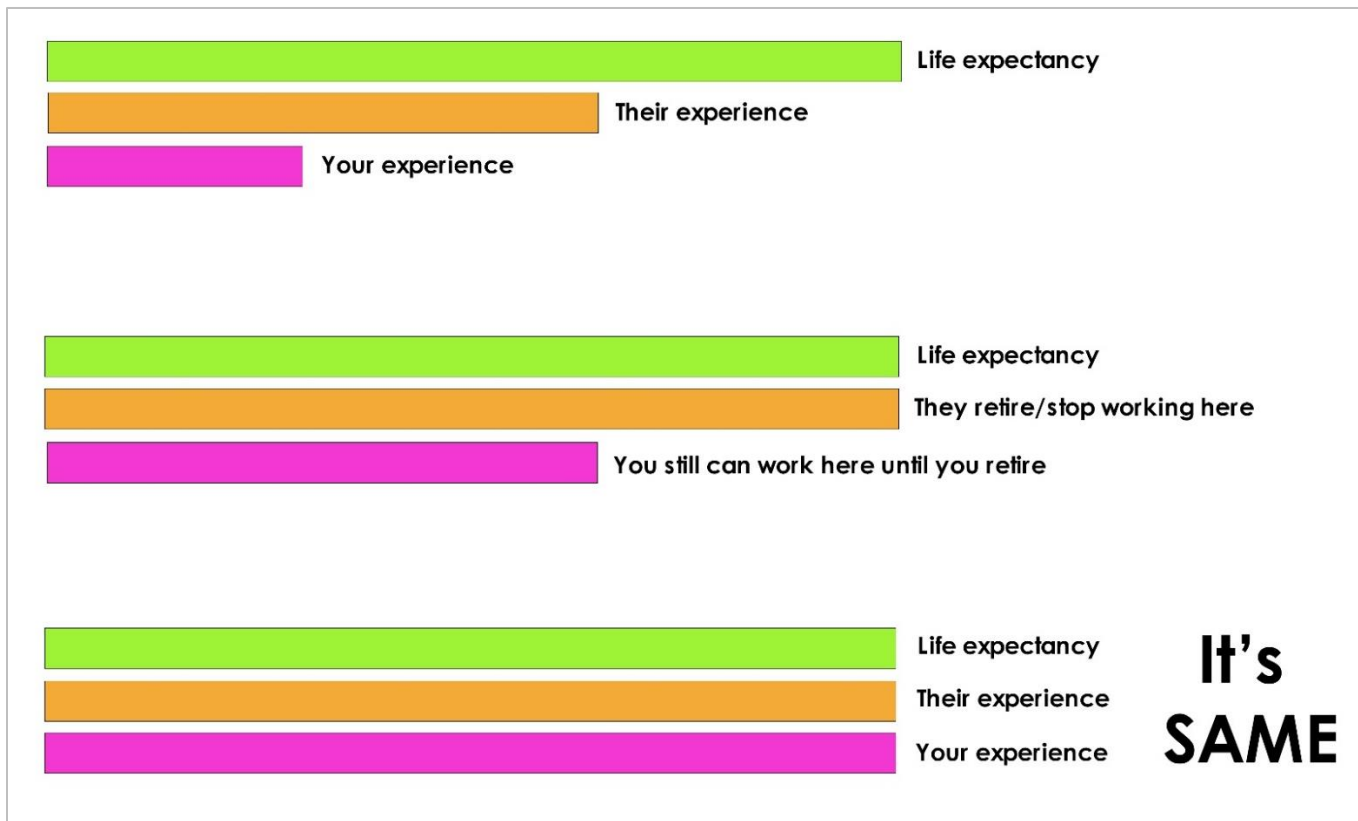
So at the end we all are same. In fact younger generation (pink bar) has slight advantage in this case where they can learn new technology and advance their last couple of years of career when older generation (orange bar) has already retired by that time.

Appendix 1 - IT to Cyber domain/role mapping

It is not a 100% mapping of all IT roles to all Cyber, just a heads-up.

Network Engineer, Network Administrator, Network Architect
Network security
Firewall, IDS, IPS proxy
Filtering
VPN
DDOS protection

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

CIS benchmarks for networking devices
Infrastructure VAPT
Security Log management and analysis
DevOps, Web Developer, Software Developer, Development Manager, Project Development Manager (Agile/Scrum Master), Project Manager, Database Administrator, Database Engineer, Quality Tester, QA Engineer
Threat modelling
DevSecOps
Design review
Secure coding
Static Analysis
Bug bounty
VAPT
Application security testing (Web, Android, iOS, thick/thin client app testing)
SAST
DAST
WAF
RASP
CIS benchmarks for anything in application security
Windows Administrator, Server Administrator, Linux Administrator, System Administrator, Windows/Linux Engineer, IT analyst, IT Helpdesk Analyst, Helpdesk Technician, Technical Support Engineer/Specialist, Programmer
Endpoint security
Anti-virus/anti-malware
EDR solutions
HIDS/HIPS
App whitelisting
Patch and Image management
Vulnerability and patch management
Infrastructure VAPT
Secure configurations
CIS benchmarks for OS

Auditor, Reviewer, Compliance Manager, Financial Auditor/Reviewer, Legal and Regulatory and any Senior Leadership within IT role

Compliance (PCI, SOX, HIPPA, NIST, FedRAMP)

Privacy and GDPR

ISO, SOC1, and SOC2 audit and review

Lawsuit Risk

Risk management

Security strategies

Identity and access management

Business impact analysis

Vulnerability Management

Risk assessment

Security awareness

Vendor risk management

DR/BRP

Policies, Procedures, Frameworks

Cloud Architect, Cloud Consultant, Cloud Service Developer, Cloud Administrator, Cloud System Engineer

Cloud infrastructure security

Cloud penetration testing

Cloud security architect

Cloud security monitoring and detection

Cloud automation in DevSecOps

Containers & Kubernetes security

Incident Manager, Incident Handler, Investigation Specialist/Officer, Crisis Management

Incident response

Breach investigation

Forensics analysis

Breach communication

Crisis Management

All DevOps roles in Cryptocurrency & Blockchain Industry
Blockchain Security

Assembly Programmer, Assembly Technician/Specialist
Malware analysis
Reverse Engineering

References:

- https://www.careeraddict.com/choose-master-degree