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 → Refer IT to Cyber domain mapping → Prepare a study plan → Enter the field → Find a mentor in Cybersecurity → Apply for jobs → Congrats! Mission Completed.

Keep doing your current job
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 are already working 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 fields there are in the security field.
Take each bullet point from that PDF and Google it. Ask the below questions to yourself:
1. What is that domain?
2. What kinds of roles company offer in that domain?
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. ***(Page 3)***

Understand what your position is, in which IT field you are working currently.

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 select domains that are closet to your IT role or maybe completely separately as you are willing to learn new things from scratch. Any approach would work here.

Prepare a study plan

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

1. **Read a book** – Time-consuming but can give you a very granular level basic to advance understanding of each thing.
2. **Study a complete course on YouTube** – Depending upon channel creators, their views, opinions, the study approach can be 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.
3. **Go for any certification and read official certification materials** – 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 towards achieving the goal. Some reputed certification authorities are ISC2, eLearnSecurity, SANS/GIAC, Offensive Security, CompTIA, ISACA, Mile2.
4. **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.
5. **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 that has 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 are going to teach in that book. Then Google each topic, read, and study. Watch practical/theory explanation videos from YouTube. Prepare your notes.

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

1. **Time management for work-life balance**
2. **Time allocation for your job, social life, learning security from above options (Prepare a daily, weekly schedule, Set targets)**

Go for certification post your preparation. It is vital to have relevant certifications to crack interviews.

Enter the field

Do company research before applying for a job.

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

1. Revenue
2. Company size (no. of employees)
3. Company's area of serving
4. Their client base
5. Glassdoor and other reviews, People reviews

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 areas 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
3. Daily routine/Job duties
4. Types of services they offer
5. Type of company (Small, Big, Product based, Consulting based, Research-based, etc.)
6. Type of Industry they serve (Banking/Financial, Retail, Gaming, Healthcare, etc.)
7. Boss/Senior management
8. Money
9. Learning opportunities

Create a killer LinkedIn profile (So many guidelines out there on YouTube and Google)

Add more security connections to your LinkedIn.

Volunteer in any cybersecurity conference.

Join a cybersecurity working group (LinkedIn).

Start a blog or YouTube channel.

Guest on a podcast.

Join a cybersecurity meetup or club in your local town.

Find a mentor in Cybersecurity

Finding the right mentor is a challenging task, 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 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 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, 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 are giving 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.

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 which 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:

1. Volunteering experience for any cybersecurity conference
2. Security certifications
3. Open-source contribution (Any tool created/contributed)
4. Any talk given at a conference

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 of business, management. Learn people, process and technology problem dealing.
3. **Know your competitions –** Competitions are everywhere; it is a good 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, 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, 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 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 few topics. Gain confidence in public speaking. Then advance to national level conferences and then international level. Meet more people, build relationships.
8. **Bad practices in Cybersecurity –** Nothing is perfect in this world. In Cybersecurity, even there are bad practices, loopholes, cheats. Ensure whatever small or big decision you take, you do all your sanity checks and don't get trapped into all of these.

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
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 modeling
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, 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 role in Cryptocurrency & Blockchain Industry
Blockchain Security
Assembly Programmer, Assembly Technician/Specialist
Malware analysis
Reverse Engineering

Master's Degree

Shall I go for a master's degree?
Shall I go for masters in your own country or foreign?
Is there any value of 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 masters 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 they have 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 in 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, 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 in job interviews are higher	It won't make any difference in job interviews; people with even CA or commerce field with cyber knowledge and skills can even 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 a master's in the first place. Is it so that you can progress in your career? Is it a requirement to pursuing 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 masters in your career, especially in Cybersecurity or any other field.

Advantages:

- If you do master, from a 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, local 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, and especially you 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 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 expectations by 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.

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.

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.

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 their security of people, process and technology estate.
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 compliance, 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

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.

They have to 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?
Just keep trying until you get one.

References:

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