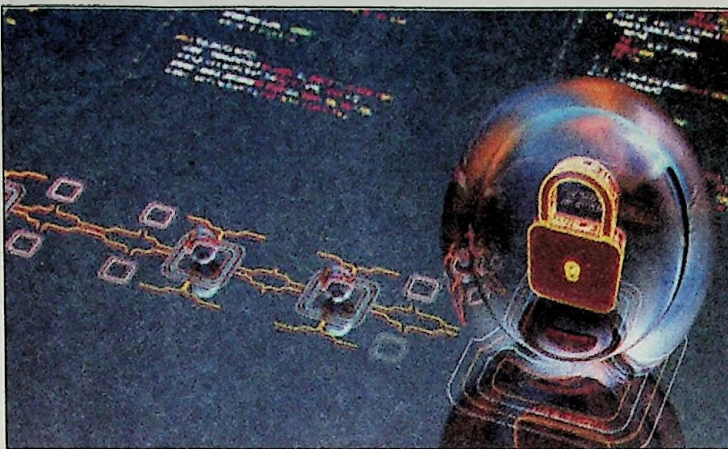# PURSUING A CAREER IN CYBERSECURITY

Nidhhi Prasaad

Information security dates back to when humans began keeping secrets. In the early days, physical files and documents were kept under physical lock and key. The advent of the internet changed everything, adding once-unimagined technological capabilities but also creating new vulnerabilities like reverse - engineering, hacking, phishing, etc; and giving rise to a critical new industry-Cybersecurity.

What is Cybersecurity?

Cybersecurity or Information Technology (IT) Security are the techniques of protecting computers, networks, programs, and data from unauthorized access or attacks that are aimed at exploitation. The world is increasingly turning into a virtual arena, with cyber attacks becoming a norm. As technology has become more intertwined with our daily lives, every day, we come across news of some kind of cyber attack or data breach. This has unleashed an ever increasing demand of professionals for pro-tecting data integrity and combating the threat of cybersecurity breaches. Cybersecurity has thus, become an absolute necessity for any enterprise, private or government, in protecting their digital infrastructure. There have been instances when not only individuals and businesses but also governments have fallen victim to online scams, ransomware, phishing, and hacking.

Demand for Cybersecurity Professionals

The escalating cyber threat landscape illustrates the urgent need to alter the approach to cybersecurity both in terms of Research and Development as well as training and availability of human resources. Presently, there is a huge gap in the demand and supply of cybersecurity experts. This has led to an unprecedented hike in the earnings of cybersecurity professionals, in both salaried jobs and freelancing.

According to a report published by Accenture titled 'State of Cybersecurity Resilience 2021', there has been a 125% year-over-year increase in the volume of cyber attacks across industries and geography and it has become a major cause for concern. By 2025, cybercrime is expected to cost the world \$10.5 trillion annually and the cybersecurity market is expected to reach a value of \$478.68 billion by the year 2030. Accenture is an Irish-American professional services company based in Dublin, specializing in information technology services and consulting.

Cybersecurity is therefore a booming career option today with a number of job roles available across different set ups.

PURSUING A CAREER IN CYBERSECURITY

Responsibilities of a Cybersecurity Professional

- Analyse and evaluate the suitability of hardware, software, and security measures against threats.
- Work with other departments to determine strategies for eliminating or containing cyber risks.
- Test new systems before they are deployed in order to prevent a security breach that could result in intellectual property loss or damage to an enterprise's reputation.

Educational Requirements

The Cybersecurity market of Asia Pacific is expected to register a growth of 18.3% CAGR during 2020-2025, but there is a talent shortage in the field. To bank upon this opportunity and to start a career in Cybersecurity you must first understand the basics of Cybersecurity and related skills. Invest time in advanced training programs that will help advance your knowledge.

While a Bachelor's or Master's degree in Computer Science or related fields like mathematics or engineering is incrementally helpful in making a career in cybersecurity, there are several specialized certifications available. Some of the most common qualifications/certifications required for a cyber-security career include:

- **Entry/Associate Level Requirement:** Comp TIA Security+, GIAC Security Essentials Certification (GSEC), Cisco Certified Network Associate (CCNA), Systems Security Certified Practitioner (SSCP).
- **Mid/Senior Level Requirement:** Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Comp-TIA Advanced Security Practitioner (CASP+).

The following are some of the most in-demand certifications:

- CEH -Certified Ethical Hacker.
- OSCP-Offensive Security Certified Professional.
- CISA - Certified Information Security Auditor.
- GCIH (GIAC Certified Incident Handler)
- CISSP - Certified Information Systems Security Professional.
- CISSP-ISSAP (Certified Information Systems Security Architecture Professional)
- CISSP-ISSEP Information Systems Security Engineering Professional.
- CISSP-ISSMP Information Systems Security Management Professional.

Personal Skills

Apart from a college degree and a training certificate, a few soft skills will help one grow in a cybersecurity career.

- **Strong analytical and problem-solving skills:** Cybersecurity issues are bound to create chaos in any setup as compromise in data security is huge. It involves the privacy of an individual and organization. It is the responsibility of the cyber-security professional to solve the cyber issue and safeguard the data. Your critical thinking power will help you shine as an instant responder.
- **Enthusiasm:** To get a better insight into the problems, one needs to draw inspiration from stories and incidences. If you are an enthusiast, then the job of a Penetration Tester will be suitable for you; if you are passionate about solving problems creatively.
- **Quick learning capability and familiarity with operating systems and networking hardware:** One has to have a curiosity for new technologies that are used in solving cybersecurity problems; learn about the tools that are developed to assist security professionals; be quick in understanding the problem and applying the right technique to solve it. You can have a bright career as a Security Architect because of your curiosity about

Job Roles/Positions

The following positions are the most in-demand and have the most growth and scope.

- **Network Security Engineer-** This is a critical role within every organization. This person ensures that security systems are implemented within the organization to counter and stop threats. The main responsibilities include maintaining systems, identifying vulnerabilities, and improving automation, oversee the maintenance of firewalls, routers, switches, various network monitoring tools, and VPNs (virtual private networks).
- **Cybersecurity Analyst-**If you have studied Information Technology, then a Cyber-security Analyst is a good career option. In today's times, every IT professional should have knowledge of basic security practices and techniques to protect computers from malicious attacks. Working as a Cybersecurity Analyst in an organization requires you to work very closely with the members of various departments like finance, sales, marketing, and operations. You will be responsible for securing the company's network against external and internal security threats. It is important for a Cybersecurity Analyst to be aware of the latest security vulnerabilities in the market so that he can make recommendations to mitigate them in time. Strong analytical skills are required to monitor potential attacks, evaluate systems, and map out penetration testing techniques. Organizations often hire these professionals as part of their information technology staff, or they may be hired as independent consultants. A Cybersecurity Analyst helps in planning, implementing, and upgrading security measures and controls. They continuously monitor security access and perform internal and external security audits to ensure there are no loopholes or evidence of security lapses. A Cybersecurity Analyst is also responsible for conducting vulnerability testing, risk analyses and security assessments, and for managing the network. In addition to these tasks, the analyst trains fellow employees in security awareness and procedures, so they are aware of the best practices to be followed to avoid security breaches.
- **Security Architect-** A Security Architect plays a crucial role in designing the network and computer security architecture for their company. The Security Architect helps in planning, researching, and designing elements of security. Without a Security Architect, a company's security system is vulnerable to attacks. The Security Architect first creates a design based on the needs of the company and then works together with the programming team to build the final structure. Besides building the architecture, they also develop company policies and procedures for how employees should use the security systems and decide on punitive action in case of lapses.
- **Cybersecurity Manager-** Cyber-security Managers are responsible for the maintenance of security protocols throughout the organization. They create strate-gies to increase network and Internet security related to different projects and manage a team of IT professionals to ensure the highest standards of data security. A Cybersecurity Manager also frequently reviews the existing security policies and ensures the policies are currently based on new threats. They also perform regular checks on all servers, switches, routers, and other connected devices to make sure there are no loopholes in the security.
- **Cybersecurity Engineer-** A Cybersecurity Engineer creates and executes secure network solutions. In order to strengthen technology initiatives and take them to the next level, Cybersecurity Engineers are an integral part of the system.
- **Cybersecurity Consultant-** A Cybersecurity Consultant works independently with businesses for resolving their cybersecurity issues. For this, you must have enough industry experience with professional certifications and showcase your potential to employers. Most companies usually hire Cybersecurity Con-sultants on a contract basis.
- **Digital Forensics Analyst-** Digital Forensics Analysts must have a comprehensive knowledge of computer hardware, operating systems, and software programs.
- **IT Security Administrator-** They are hired to plan, implement and troubleshoot information systems designed to protect the company from cyber-attacks and sophisticated security threats. They are normally assigned to computer networks, applications, and databases in order to ensure that they provide adequate protection.
- **IT Security and Consul-tant-** IT Security Consultants are hired to perform independent assess-ments of information systems in order to identify vulnerabilities and recommend the best ways to protect these systems.
- **Cybersecurity Investigator-** Cybersecurity Investigators are hired to examine how security incidents occurred and to recommend additional procedures that should be implemented in order to prevent these incidents from happening again.

(The author is a Counseling Psychologist & Career Consultant. She can be reached at nidhiprasadcs@gmail.com) Views expressed are personal.

RITES LIMITED
(A Govt. of India Enterprise)

Shikhar, Plot No. 1, Sector – 29, Gurgaon – 122001

Applications are invited from dynamic, sincere and hard working qualified professionals for following posts:

S No	VC No.	Post	Number of Vacancies					
			UR	EWS	OBC (NCL)	SC	ST	Total
1	56/22	Deputy General Manager (Legal)	1	-	-	-	-	1
2	57/22	Assistant Manager (Legal)	1	-	-	-	-	1

I. Minimum Educational Qualification and Experience criteria are as under:

Please refer the RITES website for detailed advertisement.

II. Relaxations & Concessions:

Reservation/ relaxation/ concessions to EWS/ SC/ST/OBC (NCL)/PWD/ Ex-SM/ J&K Domicile would be provided against reserved posts (where applicable) as per extant Govt. orders.

PWD candidates suffering from not less than 40% of the relevant disability shall only be eligible for the benefit of PWD. Such PWD candidates shall be eligible for relaxation of 10 years in upper age limit.

III. Details of fee to be paid for applying to the above posts are in the detailed advertisement uploaded on RITES website.

IV. Selection Process & Remuneration:

Please refer the RITES website for detailed advertisement.

V. How to Apply:

Please refer the RITES website for detailed advertisement.

VI. Important Dates:

S. No.	Particular	Date
1	Commencement of submission of online application and online payment of fees	Please Refer the detailed advertisement uploaded on RITES website for Important Dates
2	Last date of submission of online application and online payment of fees	
3	Last date of submission of document	
4	Tentative date of selection process	To be notified later

VII. For further details, candidates may see the detailed advertisement posted on RITES website www.rites.com under Career Section.

EN 28/60