CYBER SECURITY AS A CAREER

IT has engulfed our lives so much that most of our daily activities are dependent on it. And with so many people using it as part of their lives, it has also emerged as a means for criminal activities. It is not just an individual who is threatened by illegal activities in cyber space, but even an entire country's security could be at risk. For instance in 2008, there was news that the email system of the Indian Prime Minister's Office was affected by a computer virus for three months, and upon investigating it was revealed that its computers were being remotely controlled. One might also recall the 2006 train bombings in Mumbai, where terrorists used advanced techniques such as IP address masking for funds transfer and other communications.

Cyber Security is quickly becoming a hot issue. The term itself is relatively new. Many colleges and schools may still list their cyber security degree programs under more general terminology like network security, computer systems analyst, information security, IT or even criminal justice. We predict that CyberSecurity will be one of the biggest and fastest job growth areas in the coming decade. This high paying field is demanding and requires the security expert to constantly keep up with growing computer threats, attacks and changing technology. The great majority of companies have computer networks and must have cyber security personnel now to protect themselves.

Cybersecurity professionals protect data and systems in networks that are connected to the internet. Cybercriminals or hackers strike in various ways by virus attacks, which may erase your entire system or someone can steal confidential information

from your systems or even break into your systems and modify your files without your knowledge.
A computer hacker finds out the loopholes in a system and breaks into it, the information security professional, or an ethical hacker has a similar job. He needs to think like a hacker and find the loopholes in the system before a hacker can get to them. As per a website on smejobs the job nature of a cyber security expert is described as below:

Job Profile

The job of a cybersecurity professional includes:

- Ethical Hacking into a company's network to find out what security loopholes need to be fixed
- Creating security policy for an organisation
- 24×7 remote management of security products like firewall
- Security auditing, that is, compiling a report on a company's security system to see if it matches standards
- Cyber Forensics, that is, clinical investigation of computer crimes/frauds
- Training

Where are the Jobs?

Most of the cybersecurity jobs within government fall in the category of computer specialist, information technology officer, Information technology specialist, assistant chief security officer etc. These jobs are available with various government agencies and departments including Central Bureau of Investigation (FBI), Department of Transportation, Aviation and Defence. This means that cyber security careers will be available in local

law enforcement, federal law enforcement, the military, utility companies and homeland security. CyberSecurity careers will also be available in the corporate world with almost any kind of business you can think of. Medical records, ecommerce data, banking information and even small mom and pop businesses will all need cybersecurity workers.

Some of these positions will only require a minimal amount of training such as a certification or an Associate Degree. Others will require a Bachelors, Masters or Doctorate in Cyber Security. There will probably be a shortage of these types of workers for several years to come. That means qualified and trained people should be able to pick and choose the jobs with the best pay and the best working conditions. If you think this may be the career for you, start looking at colleges and exploring the various specializations of study this field has to offer.

Within businesses, the cybersecurity positions available are cybersecurity analyst, research scientist, engineer, senior information security specialist. Most of these jobs are available with government contractors, scientific research laboratories, security consulting firms and IT and security vendor companies. The common theme of most of these positions is to defend the nation through the development and utilization of cutting-edge systems, procedures, and technologies to prevent future terrorist attacks.

Career Path

1. **Entry Level -** IS Executive Manager (Role: to correlate broad security guidelines of the organisation with security operations.)

2. **Middle Level -** IS Manager (Role: Security program management, data security, ploicy creation/maintenance, business continuity/ disaster recovery)

3. **Senior & Top Level -** Chief IS Manager (Role: Design and development of information security policy. Regulatory compliance, information security governance)

4. **Senior & Top Level -** Security Advisors / Auditors (Role: Advisory services for information security, policy design, risk assessment, compliance to global/industry standards)

5. **Senior & Top Level -** Chief Information Officer (Role: Justifying the cost of ongoing and future investments to mitigate information risks, aligning business objectives with a concise security strategy)

Qualifications

Graduate in any discipline, but software engineers would have preference. A good knowledge of networks and understanding of hackers mind is essential. It is recommended that one does a course in Cyber Security. Such courses would help a erson learn the tricks of the trade, it does not help joining a course for a few days, but it is recommended that one joins reputed certificate programs and long term programs. Certifications like CISA (Certified Information System Auditor), CISM (Certified Information Security Management) and CISSP (Certified

Information Systems Security Professionals) would help a person to start a career in Cybersecurity. Other vendor specific certifications like CCSP (Cisco Certified Security Professional) and MCSE (Microsoft Certified Systems Engineer) also help.

Expected Renumeration

A person with an years experience can expect Rs.3 Lakh per annum. Those with 5 years can get upto 8-10 Lakhs. Those with certifications like CISM, CISSP and CISA can expect annual salaries of 100,000 Rs. abroad.

Cyber Forensics professionals

Cyber Forensics is a new and developing field, which can be described as the study of digital evidence resulting from an incidence of crime. According to pcquest, this science involves investigation and a computer to determine the potential of legal evidence. It helps create preventive intelligence and threat monitoring besides post incident investigations. The growing spectre e-commerce and web-based business transactions has changed the way white- collar crime is committed. Enterprises have become increasingly concerned about the use of computer networks for corporate spying and other similar threats. In addition, extraordinary risk factors such as terrorism in India are also witnessing a strategic change from an operational perspective. India, like elsewhere, is also witnessing an exponential rise in the number of frauds done through computers and IT systems.

From the government's perspective, cyber security has become as important a parameter for national security as physically safeguarding the nation's borders. In fact, there exists a critical dependence of various industries and business sectors on the

government-controlled IT infrastructure and networks. And if any vulnerability is attacked by terrorists, it can be disastrous for the country's corporates and businesses. For instance, the banking sector's inter-bank financial settlement process is based on a centralized IT infrastructure that's managed by RBI, and any disruption in the system can cause tremendous loss to the sector. Such high IT dependence is also present in national assets like oil and gas networks, national stock exchanges, railways, air traffic controls, etc. Such systems are prime targets for hackers as well as terror organizations to cause severe business and economic losses to the country. This has further escalated the need to have Cyber Forensics experts in India to preserve country's IT assets against operational and reputation risks. Thus, Cyber Forensics professionals are not just required by enterprises for their information security, but also by government agencies to keep track of nation's cyber security and preserve it from malicious attacks.

Opportunities in Cyber Forensics

A Cyber Forensics professional is required to gather electronic evidence of misuse of computer networks and provide evidence in a court of law to bring the culprits to justice. A Cyber Forensics pro is sought by both public as well as private sector. In the public sector, people are mostly absorbed in law enforcement agencies like cyber crime cells, state forensics departments and central agencies like the CBI. In the private sector, it's the information that is of paramount importance for the enterprises, and so they require professionals to safeguard their data from being stolen and misused and also preserve them from hackers. Additionally, there are specialist companies that

work on ethical hacking, Cyber Forensics and IT security. A budding Cyber Forensics expert can start his career as a cyber analyst or engineer for an enterprise after gaining experience and domain knowledge can proceed to niche areas in Cyber Forensics. Also, professionals can divert to freelancing and become independent security consultants.

Somapriya Sinha

Trainer & Public Relationship Manager

SAMARTH ED CELL

Contact No :- +91-9531019004

+91-8607281729

Email:-samarthedcell.sinha@yahoo.in