Cyber Security : Learning and Careers in Future
(By Prof. Prathamesh Churi)

B.Tech Program in cybersecurity from NMIMS University give graduates access to lucrative and rapidly expanding careers in the information management and technology industry. Cybersecurity professionals work behind the scenes to protect civilian, business, and government data from hackers.

The Cybersecurity program prepares students for employment in a variety of entry level careers in Cybersecurity with practical hands-on training, necessary to equip students with the skills employers expect.

In this program, students will learn to:

- Configure, troubleshoot and maintain computer systems, virtualised environments and secure network communications.
- Protect computer networks/systems against unauthorised access, modifications and/or destruction.
- Analyse and recommend counter measures to mitigate security threats to systems/networks.
- Develop scripts for automating configuration and management of system/access controls.

Job perspective in Cyber Security Course:
Cybersecurity professionals work in every size company and industry to protect organisations from data breaches and attacks. And the demand for cybersecurity professionals is growing at a breakneck speed. Job postings for cybersecurity positions have grown three times faster than openings for IT jobs overall. Here are ten career pathways you can pursue as a cyber-security professional.

a) Security Software Developer

Security Software Developers build security software and integrate security into applications software during the design and development process. Depending on the specific position and company, a security software developer might oversee a team of developers in the creation of secure software tools, develop a company-wide software security strategy, participate in the lifecycle development of software systems, support software deployments to customers, and test their work for vulnerabilities.

b) Security Architect Career Path

If you're enthusiastic about problem-solving and formulating big-picture strategies, the security architect career path is for you. A security architect is meant to create, build and execute network and computer security for an organisation. Security architects are responsible for developing complex security framework and ensuring that they function effectively. They design security systems to counter malware, hacking and DDoS attacks.

c) Security Consultant

A security consultant is a catch-all cybersecurity expert. They evaluate cybersecurity threats, risks, problems, and give possible solutions for different organisations and guide them in protecting and securing their physical capital and data. Security consultants must not be too rigid and must be tech-savvy — they deal with a wide range of variables when assessing security systems across diverse companies and industries.

d) Information Security Analyst

Information Security Analysts are the front-line defence of networks, Information Security Analysts put firewalls and encryption in order to protect breaches, constantly monitor and audit systems for unusual activities.

e) Ethical Hackers

Ethical hackers normally hold a CEH certificate and are given license by their employers to try and infiltrate the security of their system. The idea is that they use the same techniques as malicious black hat hackers to test existing security protocols; if they are successful, upgrades can then be developed and implemented.

f) Computer Forensics Analysts

Forensics analysts focus on cyber-crime, an ever-growing phenomenon. They work with law enforcement agencies in both public and private sector organisations and are asked to undertake a wide variety of tasks, including:

- Recovering deleted files
- Interpreting data linked to crime
- Analysing mobile phone records
- Pursuing data trails

Computer forensic analysts must keep a well — detailed records of their investigations, and often provide evidence in court.

g) Chief Information Security Officer

The Chief Information Security Officer is normally a mid-executive level position whose job is to manage the affairs operations of a company's or organisation's IT security division. CISOs are usually responsible for planning, coordinating and directing all computer, network and data security needs of their employers. CISOs work directly with the management to determine an organisations' custom cybersecurity demands. The CISOs are usually saddled with the responsibility of assembling an effective staff of security professionals, which means that the position requires an individual with a strong background in IT security architecture and strategy, as well as effective communication and human resource skills.

h) Penetration Tester

Penetration testing is the proactive authorised employment of testing procedures on the IT system to identify system flaws. A penetration tester usually attempts to (with permission) hack into a computer and network systems to pre-emptively discover operating system vulnerabilities, service and application problems, improper configurations and more, before an intruder cause real damage. Penetration testers must be highly skilled, often using testing tools of their own design, to "break into" the systems under watch. Penetration testers are required to keep accurate records of their activities and discovered vulnerabilities.

i) IT Security Consultant

IT security consultants meet with clients to advise them on how to protect their organizations' cybersecurity objectives best efficiently and cost-effectively. IT Security Consultants are often employed by smaller firms and agencies that cannot afford to handle their security issues in-house but are also employed by big corporation to supplement their security teams and provide an impartial outside perspective to current systems challenges.

j) Security Systems Administrator

A security systems administrator's responsibility is a bit similar to many cybersecurity jobs i.e., installing, administering, maintaining and troubleshooting computer, network and data security systems. The main distinction between security systems administrators and other cybersecurity professionals is that the security systems administrator is normally the person in charge of the daily operation of those security systems. The regular tasks include systems monitoring and running regular backups, and setting up, deleting and maintaining individual user accounts. Security systems administrators are usually often involved in developing organisational security procedures.

As you can see, there are endless paths your cybersecurity career can lead you down. But first, you have to start somewhere. Coder Academy's new Cyber Security Bootcamp course is a great accelerated education option for you to learn the essential skills, knowledge, and technologies you'll need to venture into any cybersecurity career you desire. Through our industry-led IT training from current cybersecurity professionals, Coder Academy will help you master sought-after skills and prepare you for a career in cybersecurity. Whether you're just getting your feet wet in the IT industry or wanting to take your IT career to the next level, Coder Academy offers hands-on technology courses you need to up-skill or change careers.