SMIC offers Cyber security course in B.Tech

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.
In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-security framework. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources.
The importance of system monitoring is echoed in the "10 steps to cyber security", guidance provided by the U.K. government's National Cyber Security Centre. In Australia, The Australian Cyber Security Centre (ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.
Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record (MBR) and are designed to encrypt or wipe data from computer's hard drive.
Electronic security protocols also focus on real-time malware detection. Many use heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

While other types of IT jobs like network administrators or software developers are more common and well-known, cyber security jobs are smaller in number but fast increasing in importance. As our global economy has led to more Internet-based computing and connectivity the world over, organizations have grown ever more vulnerable to hacking and cyber-attacks. And just as a business might hire security even when there's a local police force, so must a business hire cyber security staff. It is ultimately the duty of the organization to protect their proprietary data as well as any customer information they are privy to.

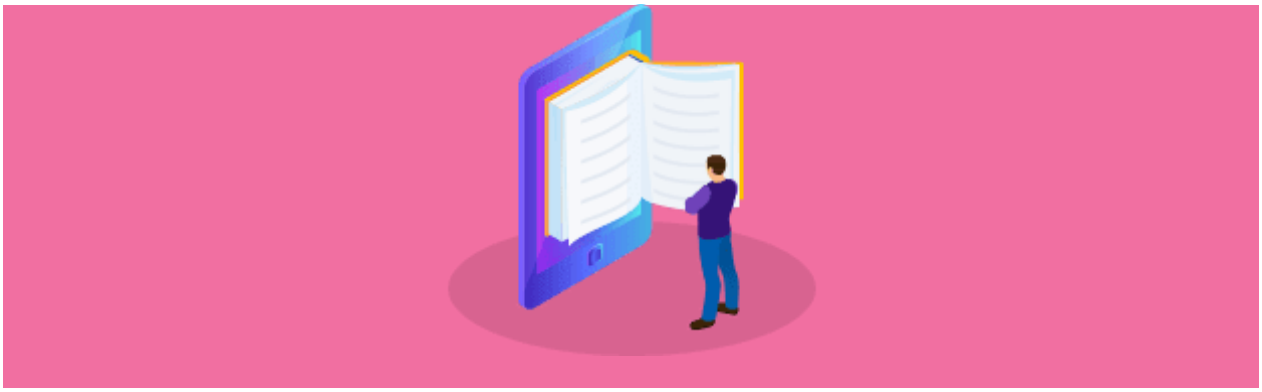
These cyber security professionals are in short supply, however. Last year, NASSCOM reported that India alone would need 1 million cyber security professionals by 2020, while job portal Indeed reported a spike of 150 percent in cyber security roles between January 2017 and March 2018. Companies like KPMG have doubled the size of their cyber security teams in recent years.

The recent overwhelming need for cyber security is the result of several factors:

Digital India and demonetization: According to Ashok Pamidi, the senior director of NASSCOM, while the government's initiatives such as Digital India and demonetization have pushed companies towards digital transformation, doing so has also made them vulnerable to cyber-attacks. In turn, this has led to a demand for cyber security professionals who can help companies achieve digital transformation without compromising security.

General Data Protection Regulation (GDPR): Although the GDPR didn't go into effect until late in May 2018, companies across the world have been preparing to safeguard their database from cyber crimes and comply with GDPR rules. This has driven a need for cyber security experts.

Aftermath of WannaCry ransomware: A year ago, in May 2017, government agencies and organizations across the world fell prey to the WannaCry ransomware, which infected over 200,000 computers in 150 countries within just three days. According to the latest numbers, it led to damage estimated up to hundreds of billions of dollars! The attack launched a debate on the vulnerability of data and the pressing need for stronger cyber laws and security systems. It has also caused many organizations to be more aware of the perils of cyber security loopholes and take steps to safeguard their organization from future attacks.



What does this mean for IT professionals?

Regardless of the reasons for the increase in demand, the pressing problem is a shortage of people trained and capable enough to fill the growing number of cyber security roles. NASSCOM reports that despite having the largest IT talent pool in the world, India simply lacks skilled cyber security professionals. In fact, the need for experienced professionals is so high that companies are willing to pay a premium salary of over Rs 1.5 to 4 crore to top talent. This has increased the cyber security budget by 71% as observed by PwC in its 2016 report.

The jobs that are seeing this sharp increase in pay include the following five cyber security roles:

1. Network Security Engineer

The network security engineer is a critical position within every organization. This person ensures the security systems are implemented within the organization to counter and stop threats. Their main responsibilities include maintaining systems, identifying vulnerabilities, and improving automation. They also oversee the maintenance of firewalls, routers, switches, various network monitoring tools and VPNs (virtual private networks).

The minimum salary of a network security engineer begins at Rs 4 lakhs and can go up to 8 lakhs per annum.

2. Cyber Security Analyst

A cyber security 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 cyber security 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.

The salary of a cyber security analyst begins at Rs 6 lakhs per annum.

3. 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 their company's employees should use the security systems and decide on the punitive action in case of lapses.

The average pay of a security architect begins at Rs 17 lakhs per annum.

4. Cyber Security Manager

Cyber security managers are responsible for the maintenance of security protocols throughout the organization. They create strategies 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 cyber security manager also frequently reviews the existing security policies and ensures the policies are currently based on new

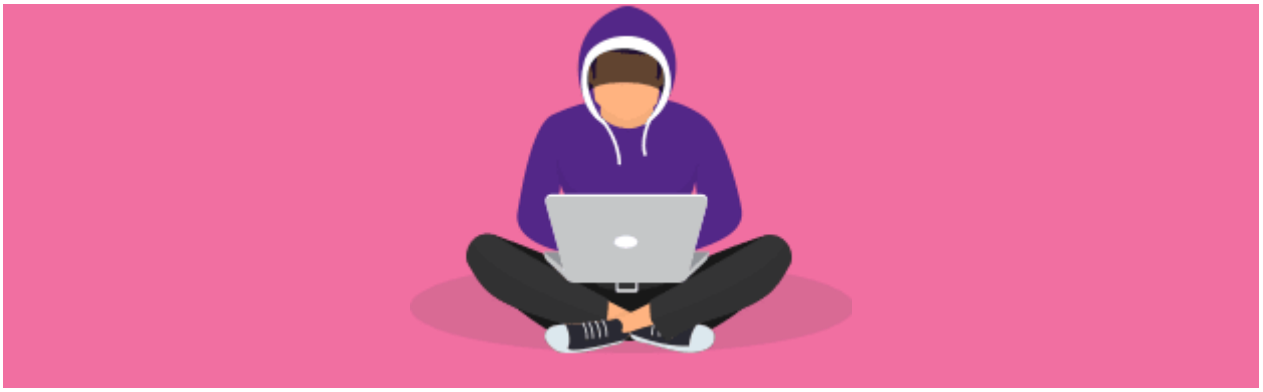
threats. They also perform regular checks on all servers, switches, routers and other connected devices to make sure there are no loopholes in the security.

The average salary of a cyber security manager begins at Rs 12 lakhs per annum.

5. Chief Information Security Officer (CISO)

According to a report by PWC, over 80 percent of companies now have a CISO on the management team. This trend shows that companies have grown aware of the threats of cyber crimes and the potential damage such attacks can cause. The CISO is a senior-level executive within an organization that ensures that the cyber security plan is aligned with the business's vision, operations and technologies. The CISO works with the staff to identify, develop, implement and maintain processes across the organization to ensure there are no security breaches. They respond to incidents and set up appropriate standards and controls to mitigate security risks without causing any interruption to the business. They are also responsible for overseeing the implementation of security policies and procedures within the organization.

The average salary for top CISOs is anywhere between Rs 2 crores to 4 crores.



Those are the top five cyber security jobs in India today, but plenty of other roles exist and go unfilled, including information risk auditors, firewalls, and security device development professionals, security analysts, intrusion detection specialists, computer security incident responders, cryptologists, and vulnerability assessors.