CYBERSECURITY CENTRE of EXCELLENCE

A joint initiative of DSCI & Government of Telangana

Why is Cybersecurity today more important than ever?

The practice of defending various computers, mobile, networks, electronic systems, servers, and data from malicious attacks is called as cybersecurity. It is also known as information technology security or electronic information security. Cyber-security is a broader term which can be subcategorized into the following;

- **NETWORK SECURITY** is a practice of keeping intruders away from the computer whether it is targeted attack or opportunistic malware.
- **APPLICATION SECURITY** that keeps software and devices free of threats.
- **INFORMATION SECURITY** protects the integrity and privacy of data, both in storage and in transit.
- **OPERATIONAL SECURITY** is about the process and decisions for handling as well as protecting data assets.
- **DISASTER RECOVERY AND BUSINESS CONTINUITY** defines how an organization responds to a cyber-security incident or other events that cause the loss of operations or data.

The scale of cybersecurity

Every year, budgets have a different allocation for cybersecurity expenditure. They are designed by keeping in mind the requirement and contingencies of the country or nation. Cybersecurity and related expenditures are highly focused upon by the government as well as organizations.
Due to threats from neighboring countries and escalation of ATM/debit card data breaches, development in cybersecurity is being set up. It will be

administered by a high-power committee headed by National Security Advisor. Identifying the scale of cybersecurity, India has proposed to set up national cyber coordination (NCC) center. IT Department is also upgrading the Standardisation of Testing and Quality Certification (STQC) program, which audits government software and hardware for loopholes.

Taking into consideration recent cyber-attacks like ransomware, the Ministry of Information and Technology (MeitY) has recommended all ministries to spend 10% of their IT budgets on cybersecurity. Apart from this, it has also proposed the appointment of Chief Information Security Officers (CISOs) in every ministry to monitor and safeguard the IT infrastructure of the government bodies.

According to a study by DSCI, India faces the second–highest number of cyberattacks across the globe most of which are targeted towards healthcare, finance and critical sectors such as defense and nuclear power. With rising risks, more and more companies are opting for cyber insurance policies. In 2018 alone there were 350 cyber insurance policies sold – which were a whopping 40% increase from those in 2017.

Threats to cybersecurity

Viruses, worms, spyware, trojan, and ransomware are common methods attackers use to gain control of computers. Whereas spyware and trojans are often used for data collections of various kinds. Ransomware waits for an opportunity to encrypt all the user's information and demands payment to return access to the user.

All industries, regardless of their size or turnover are positively affected by the adoption of cybersecurity. Healthcare, manufacturing, finance, and government are reported to be most affected by the dangers of cybercrime. Today cybersecurity is more important than ever, especially when a large volume of data belonging to important industries and individuals are at stake – as they lie just a breach away from dangerous hackers. Hackers collect financial and medical data from the most appealing sectors and sell them on the darknet for a handsome amount of money. All the businesses that use networks can be targeted for customer data, customer attacks, corporate espionages, etc.

End-user protection

So, how does cybersecurity work to protect the system and users from hackers and cybercriminals? Cybersecurity works mostly on cryptographic protocols to

encrypt communication and data, e. g. password authentication, emails, files, and other critical data. It guards against loss or theft along with protecting information in transit. In addition to that, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. It is designed to encrypt or wipe data whereas security programs can even detect and remove malicious code which is hidden in Master Boot Record (MBR).

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 to analyze 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.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them.