CYBERSECURITY
CENTRE *of* EXCELLENCE
A joint initiative of DSCI & Government of Telangana

How Cybersecurity impacts the economy

Cybersecurity is a system of technologies, processes and practices that are designed to safeguard devices like computers, networks like Wi-Fi, programs and data from damage, unauthorized access or mainly against attack

Today, with cyber criminals lurking across the cyberspace, organisations need to rethink their cybersecurity measures. Various government, military, corporate, financial and medical organizations collect, process and store data on computers or other devices. A very huge proportion of this data can be considered as sensitive information for which unauthorized access or exposure could lead to devastating consequences.

An element of virtually every national security threat and crime problem is cyber-based or facilitated. They seek to strike our critical infrastructure and to harm our economy. – James Corney, Former Director of the FBI.

Today as cybercrimes continue to rise, governments, as well as corporations, are threatened. This situation makes it essential for organisations to stay aware of risks and practice the necessary precautions to avoid the damaging effects of cybercrime.

Cybersecurity and the economy

Cybersecurity plays a key role in securing not only Indian enterprises and their infrastructure, but also the safety and well-being of people all over the world, along with securing the prosperity of the global economy.

Between January and March 2019, the Indian manufacturing sector faced 27.56% of all the cybersecurity threats as reported by Quick Heal's enterprise, Seqrite. Other sectors that faced cybersecurity threats apart from manufacturing are professional services (22.59%) and educational sectors (14.64%).

Another startling revelation highlighted that about 3.13 lakh cybersecurity incidents have occurred across the country, including website hacking and phishing attacks, in October 2019. As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), 50,362 and 53,117 cybersecurity incidents were reported in 2016 and 2017, respectively. These numbers show there has been a steep rise of 523 per cent since 2016.

There was a surge in the cases regarding phishing, network scanning and probing, virus/malicious code and website hacking. There were around 2,08,456 cases in 2018 which further increased to 3,13,649 in October 2019. Cybersecurity experts state that this number is predicted to rise with the adoption of emerging technologies. As the Indian economy moves towards digitisation, the loss of privacy of vital data and financial capital associated with each threat encounter results in huge losses to the country's economy.

Cybercriminals devise novel ways to inflict their victims via attack vectors

Image source – Times of India; Source – Aegonlife, Feb 2019

An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload for malicious software or code. They enable hackers to exploit system vulnerabilities, including the human element. Web pages, email attachments, instant messages, viruses, chat rooms and deception are few of the easily available attack vectors.

Firewalls and anti-virus software can block attack vectors to some extent but there lies no protection method which is totally attack-proof. Hackers are constantly updating their attack vectors and hence the defence mechanisms which prove effective today may not remain so for long. Hackers are on the quest to seek and gain new unauthorized access to various computers and servers.

The right cybersecurity measures ensure that our economy stays protected

It has become important to take a step against today's cyber threats. By truly understanding the enemy and the threats, businesses that implement the right defences can not only protect their reputations but play a crucial role in disrupting the global tide of criminality.

As cybercrime establishes a strong foothold across the cyberspace, it is necessary for India to bring some new regulations and laws into the picture. The older laws are applicable to physical goods and people. They make it difficult to track cybercrimes, especially now when cybercriminals are coming up with novel attack vectors. As the boundaries between AR/VR and physical worlds blur, it is a necessity to keep abreast with the current scenario revisit the Indian cybersecurity laws.