# Cyber Security in India: Threats and Challenges

– **Subodh K Kesharwani**
Associate Professor, SOMS, IGNOU, skesharwani@ignou.ac.in

– **Madhulika P. Sarkar**
Reader, SOMS, IGNOU, madhulikalal@gmail.com

– **Shelly Oberoi**
Research Scholar, SOMS, IGNOU, shellyoberoi83@gmail.com

With the advent of information age, technology has evolved at a lightning speed, but there has been incredible growth in cyber world both in its prevalence as well as disruptive way. At present, there has been rise in problem of security in cyber domain mainly in digital privacy and governance structure. With the digital privacy norms and cyber governance framework, it is getting harder to pace with cybercrimes even after rigorous cyber security. Cyber-attacks continue at appear as global threat; hence, organizations need to establish innovative methods in cyber digital world to cater cyber-attacks.

## Introduction

After USA and China, India ranks 3rd in terms of highest number of internet users in the world, as the number of internet users have grown 6 fold since 2012. It also secures rank among top 10 spam sending countries in the world. According to the report by online security firm 'Symantec Corp', Indian is ranked among top five countries to be affected by cybercrime. The threat from professional cyber criminals is growing worldwide which forms a direct threat to the economy interests and national security of the countries. Numerous attacks are being done on the digital infrastructure of the economies which poses more danger to the economy as a whole. Government of various countries has framed development cells to strengthen the cyber security infrastructure of their countries to protect their interests. Such attacks pose great threat to the national initiatives of the countries like smart India, E-governance etc. Military organizations and Government store and process large volume of relevant data and transmit regularly across networks, which increase their exposure to cyber threats. Such potential damages put national security at risk when critical information is targeted by hackers. As we know, India is seen as a preferred outsourcing destination globally and is currently rolling out its largest ICT Programme 'Digital India', which mainly focuses on governance, health sector, logistics, digital currency etc to open India to digital age. Digital landscape in India has seen unbelievable transformation in short span of time, but Cyber security is also a great threat for India.

The present manuscript attempts to emphasis on the cyber industry in India and to highlight the threats and challenges of cyber security. The article also aims to highlight the various government initiatives in regards to Cyber security.

## Cyber security trends and Industry in India

Cyber landscape has become increasingly complex, consequently the cyber security industry too. There are basically three evolutionary phases of cyber security i.e. Virus Protection, It and network security and Cyber security. At first stage, the cyber security mainly focused on protecting computers from Vital Information resources under siege (VIRUS) attacks, which resulted in development of Anti-virus softwares. Second stage was focused on the network security which emphasized

on the protection of the devices and the information assets passing through networks by installation of firewalls and security softwares. Third phase is the current evolution, where threats have become more complex. According to the data security council of India (DSCI), the size of the global cyber security industry is USD 80 Billion which is estimated to grow to USD 190 Billion by 2025. At present, the businesses are keenly looking for innovative tools to save themselves from cyber-attacks. Recently, the Supreme Court of India has limited the use of data, with the draft of personal data protection bill, the aim of which is to protect the privacy and personal data. By 2020, Machine learning and Artificial intelligence in cyber security will mature and become the integral part of SoC (Security Operation Centres).the main focus across various organizations and the government would be on securing IoT structure by 2020 to achieve automation and efficiency. In This year only, attacks on cloud shared security model will mount manifold to protect infrastructure by authorizing on personal access. This will involve the adoption of technologies like Cloud Access security broker (CASB) for additional security controls. In digital economy, the organizations that have fear of fraud, blockchain will show them silver lining to prevent data theft.

## Cyber Security threats and challenges

To implement Cyber security, there are many challenges to be faced; some of them are given below:

***Lack of architecture for cyber security-*** Public sector and private sectors in India, have their own norms and protocols to protect their infrastructure from cyber-attacks. Similarly, Armed forces too have their own agencies for cyber security. Hence, in India, there is no national security architecture which unifies the efforts taken by both public and private sectors to tackle cyber threats effectively in coordinated fashion.

***Lack of uniformity in Internet access devices-*** In India, not everyone can afford sophisticated mobile phones with higher security norms, which makes it impossible for legal and technical standards to be set by regulators for data protection.

***Lack of awareness-*** there is lack of awareness about cyber laws and regulations at individual as well as corporate level in India. There is also lack of national regulatory policy in India for cyber security and supervised legal framework.

***Shortage of trained workforce-*** India has young workforce with extensive IT prowess, but still there is a dearth of talent in specific niches like cyber security. The demand and supply of talented and skilled labour in cyber security is lacking and with the market poised to grow in future substantially, this gap will widen further, creating more problems in the economy.

## Government initiatives in respect of cyber security in India

India is heading towards a Digital Society, with the recent government push towards a digital economy, which is increasing more dependency on technologies demanding a secure cyber space in country. Hence, Indian Goveremnt has aimed to secure country's cyber space by preventing cyber-attacks and by reducing national vulnerability to cyber-attacks. The Indian government has mainly focused on threats to national security, critical information, information security awareness, training and research etc. Lot of initiatives is undertaken by the Government of India (GOI) to tackle the cyber security challenges like establishment of national agency of Indian Computer Emergency Response Team (CERT) in 2004 which is actively involved in mitigating cybercrimes. GOI has also enacted the Information Technology (Amendment) Act, 2008 to address the needs of national cyber security regime. In 2013, National Cyber Policy also came into existence to integrate all the initiatives in area of Cyber security. The government has also formulated National Crisis Management Plan to tackle cyber Terrorism and also several other agencies like National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC) etc has been created to implement the cyber security policies. Security auditors have also been empanelled by both government and private companies for conducting security audits in the country.

## Conclusion

With the digital era and increased use of technologies in the country, cyber security has become an important issue to deal with, especially when the users are novices as afar as security practices are concerned. Although the GOI has set up many agencies and passed many laws to cater cybercrimes, still there is an urgent need for all the states to take up initiatives to ensure safe cyber space. All the Indian states need to

adopt a dynamic approach to create a safer cyber space through effective polices like States of Telangana and Karnataka in the field of cyber security.

## References


- DSCI (2010), "Data security council of India", available at: www.dsci.com.in (accessed February 2010).
- Gupta, M.P. (2010), "Tracking the evolution of E-Governance in India", International Journal of Electronic Governance Research, Vol. 6 No. 1, pp. 46-58.
- Chaturvedi et al., (2014),"Analyses of issues of information security in Indian context", Transforming Government: People, Process and Policy, Vol. 8, No. 3, pp. 374 – 39
- National Cyber Security Policy (2011), "India's national cyber security policy draft v1.0", 26 March, available at: www.mit.gov.in (accessed August 2011).
- Rajesh (2015), "Importance of cyber security", International Journal of Computer Applications, Vol. 111, No. 7, pp. 14-17
- https://www.pwc.in/consulting/cyber-security/blogs/seven-cyber-security-trends-that-india-will-witness-in-2019.html
- https://niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
- https://www.forcepoint.com/sites/default/files/resources/files/report-2019-cybersecurity-predictions-en.pdf


**Dr. Subodh Kesharwani** is an academician with a bronze medal in his post graduate and Doctorate in ERP System in 2002 from Allahabad University. He is one of the researchers who had concentrated his research on Total Cost of Ownership [TCO] & Critically evaluate ERP vendors including SAP. Dr. Kesharwani is presently an Associate Professor, School of Management Studies with a total 20 years of hardcore teaching and research in Information System and its linkages with various domains of management at Indira Gandhi National Open University, New Delhi.

skesharwani@ignou.ac.in

**Dr. Madhulika P. Sarkar** is currently Reader at SOMS, IGNOU (PhD LLB). She has a 15 year teaching experience with IGNOU. Her Area of interest is Taxation, Economics and Law. She has been part of various Seminars, Paper Presentations, and numerous Research Papers published in various National and International Journals. She is also a lifetime member of Indian Commerce Association.

madhulikalal@gmail.com

**Ms. Shelly Oberoi** Research Scholar,SOMS, IGNOU (BCom, University of Delhi, MCom, PGDBM, MPhil, and UGC Net) has worked with University of Delhi, IP University and Bhartiye Vidhyapeeth as Assistant Professor. She hasbeen part of various Seminars, Paper Presentations, and numerous Research papers published in various National and International Journals. She is also a lifetime member of Indian Commerce Association (Gold Medalist, Manubhai Shah Memorial Award, 2018). She has displayed vast success in continuously acquiring new knowledge and applying innovative pedagogies and has always aimed to be an Effective Educator and have a global outlook which is the need of today.

shellyoberoi83@gmail.com