Page 739 - 746 **DOI:** *http://doi.one/10.1732/IJLMH.25663*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 1

2021

Current Scenario of Cyber Crime in India

ANIMESH SINGH[1] AND ANKITA RATHI[2]

ABSTRACT

This research paper will provide a brief introduction about cyber crime in India, what constitutes a cyber crime and a general awareness about cyber crime around the globe. People of India are unaware of continuous initiatives taken by Indian government, law makers and executors to curb cyber crime. It will also help us to understand that with the increase in the use of internet, cyber crime has also been increasing, so what are the tactics these criminal used to hack into computers, identities of people, get the benefits by illegal means and are the laws and initiative been taken are enough or not to curb the cyber crime in India. It is important to research about the reasons of increasing cyber crime in India. According to reports, in 2019, 25% of FIR's in Bengaluru were filed for cyber crime. So, we need to identify what's wrong in the mindset of these criminals and how we can be safe from these crimes. This research is based to analyze the types of cyber crime and its punishments according to Indian laws, make people aware and give an overview of cyber security, cases that happened in past few years and initiatives taken by Indian government to curb the cyber crime. Further, the paper aims discuss about the recent Data Protection Bill, 2019 and the solution through which we can be aware and safe while using Internet and devices. Also it will help us to know what's missing in the laws and its implementation that the cybercrime has been increasing over the years and do India has enough of Technology and skilled people to curb the cyber crime.

I. INTRODUCTION

With the increase in use of internet globally, the crime associated with the internet is also increasing which is known as cyber crime. Cyber crime is usually committed by using computer as target or using computer to target or using computer as a minor tool in the target. The cyber crime is not only prevalent in India but is increasing globally. In India, the Information Technology Act, 2000 deals with the cyber crime. Information Technology Act, 2000 defines cyber crime as an act or omission of the act punishable under the Information Technology Act, 2000 but there are also certain crimes which are included in the definition of cyber crime like defamation, threatening emails, etc whose punishment is covered under Indian Penal Code.

[1] Author is a student at Bharati Vidyapeeth University, Pune, India.

[2] Author is a student at Bharati Vidyapeeth University, Pune, India.

From past few years, Indian government as well as law makers and executors are trying to curb the cyber crime from India but it has been increasing. Most of the people don't know about cyber crime and they have been becoming a victim of cyber crime. According to reports, in 2019, 25 % of Bengaluru's FIR's were of cyber crime. Most of the Indian rely on YouTube to gain knowledge which has no authentication and reliability. People have been watching about online fraud, ATM Pin leakage and many more which is doing nothing more than increasing their fear and making the process of digitalization slow in India. There are many cities like Delhi, Bengaluru, and Pune which have become a major city where most cyber crimes are being done and when a city come into the criminals limelight, then the government set-ups the cyber cell for that states.

The government is constantly taking initiatives to reduce cyber crime from India but is still lacking in doing so. The laws which dealt with crime at workplace like Sexual Harassment (prevention, prohibition and control) Act 2013 included the offences committed by the colleagues like stalking, defamation, harassment which are done online. The Information Technology Act, 2000 and Indian Penal Code clearly mention these punishments in various sections of the Act. Since the cyber crime has no boundary and can be committed by any means, we need to wake up and work for our safety at every place and every platform. Most of the people of India don't even know they have become a victim of cyber crime because they don't have adequate knowledge regarding cyber crime.

With the growing information in the society, serious threats are also emerging in a very fast pace. With the growth of internet users across the world, it is becoming a fertile ground for cyber criminals with so much of data and information of users at stake. Most of the cyber crime today is carried out by organized criminal enterprises. Sudden increase in the cyber threats are no less than a nightmare for the Indian government. Terrorist attacks are terrifying as it embarks on ambitious and high profile projects such as Digital India. According to Symantec's annual internet security report 2015 video, there has been an increase in targeted attacks on Industries dealing with critical infrastructure in India in 2014. Cyber threats can be differentiated into five subjects i.e cyber espionage, cyber terrorism, cyber warfare, cyber crime, using cyberspace to encourage real life attacks. Cyber crime is not only limited to user's data or an individual but it is also considered as internal security issue. We can see with the recent attack by the Israeli virus Pegasus which came into the phone of important persons in India such as politicians, lawyers, etc. but Israel denied of giving the correct information regarding this issue as to how this virus came to India decide in their official statement they never sold this virus to India and this is not only limited to India and In 2015, 650 million Euros gone missing after a gang used computer viruses to infect networks in more than hundred Financial Institutions worldwide. In October 2016, as many as 32 lakh debit cards were compromised in one of the biggest breaches of financial data in India. These are just some examples to show the damage which can be done by the cyber criminals to the Nation's security. Recently, the Twitter handle of Mr. Donald Trump(a well known politician of United States of America) was hacked. The Twitter handle of the (Former President of United States of America) Mr. Barrack Obama was hacked and the hacker tweeted for the donation of some money from their account but that was deleted after half an hour but the link he generated got many millions of donation in that half an hour. These are just some of the examples to show that how much important these threat are to the world where majority of the population are connected via Internet.

It's not only threat to the people of the country but also to the businesses. In this year of 2020, where Novel Corona virus disease (COVID-19) has changed the whole working scenario from office work to work from home, cyber crime is a major threat to the world as a whole. All the countries should unite globally and work together to curb the cyber crime. Cyber crime has also been prevalent in almost every country but with the increasing use of internet it has been increasing. In the initial stage it will be easier to take control on it. Government of every country is working on it to curb the crime but it will be effective if multiple country joins together to curb the crime.

II. Kinds of cyber crime

1. *Cyber crime against the persons*

It includes the offences like harassment through emails which is very common sent as attachments and letters. Harassment via the social media platforms like Facebook, Instagram, etc. are very common way of online harassment. Cyber stalking which take place online true text messages websites videos, etc. Transfer of malwares which is a software which can control the individuals computer and hacks it completely, Online defamation by sending messages, audio, video or even symbols to someone on their personal account in a vulgar language. Other than these there are various cyber offences committed through SMS spoofing, cracking, cheating and fraud, phishing, child pornography, etc.

2. *Crimes against the person's property*

It includes the cyber crime done on intellectual property consisting of the rights of an individual such as design, software piracy, Trademarks, etc. Other cyber crime against the persons personal property includes software piracy, cyber squatting, cyber vandalism, hacking through White-Hat hackers, Black-Hat hackers and Grey-Hat hackers. Action of viruses is also damage to personal property of a person.

3. *Cyber crime against government*

It includes cyber terrorism which includes the hate website and hate email circulated worldwide. Cyber terrorism is one of the dangerous crimes which endangers the unity and integrity of the nation. Other such crimes includes cyber warfare, use of internet and terrorist, distribution of softwares which are pirated, and position of unauthorized information.

4. *Cyber crime against Society at large*

It includes child pornography, online gambling, cyber trafficking, financial crimes and forgery. These are the crimes which are done against the society at large and harm the complete cyberspace.

III. Major cyber crime cases in India

1. Cosmos Bank cyber attack in Pune

In 2018, Cosmos Bank which is situated in Pune had to suffer from a cyber attack which was a shock on banking sector of India where hackers siphoned off INR 94.42 crores of money from Cooperative Bank Limited in Pune.

2. UIDAI Aadhar application hacked

There was a major data breach of personal record of 1.1 billion Indian Aadhar holder's. As per UIDAI, about 210 Indian Government’s websites were hacked causing breach of data of 1.1 Billion Indians.

3. Official Maharashtra government website hacked

In 2007, the official website of Maharashtra government got hacked where police of cyber crime division got involved in the case and tried to track down the hackers. In the result of hacking, the http:/www.maharashtragovernment.in website remained blocked for a day.

4. Official website of IRCTC hacked

The official website of IRCTC got hacked which resulted the risk to put personal information of 1 crores of customer at stake.

IV. What’s the solution?

To curb the cybercrime it is important to understand the causes of cyber crime and the motive of cybercriminals commit the crime. There are various criminals who are motivated for the sake of getting money from the innocent people through internet by fooling them, hacking into the computers or system, or even by threatening them. Money is the major source for them to commit the crime. There are many individual who turns into criminals because of their ideologies to hack or damage the systems, websites and even the working of national government. There are individual who gets motivation out of their personal agenda hacking into their partner’s personal space or a teenager who is not aware of the seriousness and effect of the damage.

V. AGENCIES DEALING WITH CYBER SECURITY IN INDIA

1. *National Security Council Secretariat*

It is an Apex agency looking into political economic and energy security concerns of India and acts as a secretariat to NIB.

2. *National Information Board*

It is an Apex body with representatives from relevant departments and Agencies that form part of the critical minimum information infrastructure in the country. And I be entrusted with the responsibility of enunciation national policy on information security and coordination on all aspects of information security governance in the country.

3. *National Cyber Coordination Centre*

It is a critical component of India cyber security against hackers and espionage as well as track terrorist activity online. NCCC will ensure you're near real-time threat assessment and situational awareness that will help in analysis and generation of timely alerts periodic reports. NCCC will be set up by CERT-In and will function under the NIB.

4. *Ministry of Home Affairs*

It issues security guidelines from time to time to secure physical infrastructure. The respective Central Administrative Ministries and Critical sector organizations are required to implement these guidelines for being strengthening security measures of the infrastructure.

5. *Department of Information Technology*

It is under ministry of communication and information technology and strives to make India a global leading player in information technology and at the same time take the benefits of information technology to Every Walk of life for developing and empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion and policies in electronics and IT. It also prepared as the National Cyber security policy.

6. Department *of Telecommunication*

It is under the ministry of Communications and information technology and is responsible to revaluation facility comprehensive testing of Information Technology security products as per international criteria for security testing standards.

VI. NATIONAL CYBER SECURITY POLICY 2013

The policy is aimed to secure the complete cyber space and to build an Information Technology which is free from any kind of cyber crime. The policy is also aiming to remove the cyber threats and it will also create a large of specialist who are expert in Information Technology and can beat the cyber criminal in their motive. The approach that will be put in place to achieve the different priorities of the cyber security policy. The policy also aims to establish a nodal agency at the national level to coordinate all cyber security issues in the country. As per international best practices, it will allow organizations to create their own security policies. The program would ensure that a clear budget is earmarked for all organizations to enforce their security strategies and initiatives. Regulation proposals are designed to provide different schemes and rewards to ensure that proactive security enforcement steps are taken.

VII. Initiatives by Indian Government

1. The CERT-In

The introduction of CERT-In (Indian Computer Emergency Response Team) is a national agency to tackle with the increasing cyber crime. It has helped in lowering the rate of cyber crime from India, CERT-In deals mainly with cyber attacks like hacking and phishing. it has been set up as a national agency Pratapgarh security incident response National watch and alert system team is working 24/7 and scanning the cyberspace in the country.

2. Cyber Swachhta Kendra

Cyber Swachhata Kendra is a part of digital India initiative which has come under Ministry of Electronics and information technology. It has also collaborated with department of Telecommunication, antivirus companies and internet service provider. Its main objective is to detect clean infected system in the country.

3. Crisis Management Plan

There are three ways to tackle the crises through a crisis management plan which includes Pre-Crisis, Crisis Response and Post-Crisis. The cyber crisis management plan includes guide to prepare and respond to the cyber attacks committed by the cyber attackers. Its main objective is to counter cyber attacks and cyber terrorism on the state and Central level.

4. National Critical Information Infrastructure Protection Centre

It is providing adversaries on Software Hardware vulnerabilities and alerts on cyber attacks are being issued regularly to Chief Information Security offices of critical information infrastructure organization.

VIII. Data protection bill, 2019

The shortcomings of IT Act, 2000 to provide the complete guide to curb the cyber crime attacks has resulted in the upcoming Data protection Bill, 2019 which will fulfill the needs as per the current cyber crime scenario in India with some stringent Laws. The main aim of the Bill is to provide the citizens of India their Right to Privacy which should be compromised by any means. It will create a sense of trust and build up the relationship between the user and the service provider while keeping the personal and sensitive data of individual private. The Bill is mainly focuses on the restriction of data that is circulated through online mode. Users unknowingly accept the terms and condition where they don't know what all information are being collected from their devices. The Bill will provide wide range of right to the users to know and be well aware of where their data and how their data has been processed. Consent will play a major role in this Bill as without consent, nothing can be used, processed or stored. There are various third party service providers who take up the data with just one click on the 'Accept button' and we don't get to know what data has been taken or stored with their system. The Bill is under its amendment stage. The amended draft of the Bill has been drafted after making 89 amendments in the Bill and it also added one new clause under the Bill.

There are also various exemptions given where the data may be processed without the consent of Individual i.e., in case of legal proceedings, in case of medical emergencies, in case of employment related terms and in case of fraud, merger & acquisition, etc.

IX. Solutions to tackle cyber crime

- Always beware about the types of cyber crime prevails in the society.
- The government of India needs to bring stringent punishment to curb this crime from India.
- We need more people working for cyber crime department of government having in depth knowledge of computer, internet, and hacking.
- Each State needs to have a complete mechanism and a cyber crime department consisting of specialized people like Software engineers, ethical hackers, lawyers, etc.
- Never believe anyone especially a stranger and don't share your personal information with them.
- With the increasing cyber crimes, the government has also set up cyber crime police station and cells which deals with cyber crimes only.
- The online portal for cyber complaint in India is available.
- There are various NGO's and institutions working with police departments to curb the cyber crime.
- There are various portals where we can know the procedures of complaints to cyber crime.

- There are various website which gives in depth knowledge about cyber crime in India.
- Always beware about whom you share your bank details with. Never entertain any calls in the name banks and never share any of your information related to the bank on telephonic conversation or on the internet.
- Beware of fraudulent website who takes your personal information like credit/debit card details, etc.
- There are several ways in the browser to retain control over data access so that it can be personalized.

X. Conclusion

We all know that with the increase in the use of internet services, the cyber crime has been increasing. There are various kinds of cyber crime which are used by different kinds of cyber attackers in different ways. Cyber crime is not only limited to India and has be increasing globally due to the high reliance on the internet services. Crime can’t be curbed completely from any country, but every country tries to keep their people safe as much as possible through the legal system of the country. India still does not have cyber crime cell in each and every state. These are being set up after a city of the state or the state itself comes into a limelight of a major cyber crime case. Indian government has been trying to work on to tackle cyber crime through various laws, initiatives and technology but the main question is that do we have enough of technology and skilled people to track down the cyber crime? And is Indian government investing enough on the advancement of technology and skilled people who can help in India’s cyber security?

If Indian government invests in the technology advancement and look for skilled people in technology at the right time then it would be great, otherwise the attacks which we looked in this research paper are nothing and there is a lot more to go. The Data Protection Bill, 2019 which came in the year 2019 will take more than one and a half year to be implemented as an Act. The Bill is under its amendment stage and yet to be finalized for the processing to make it an Act. The crime is increasing day by day and the government is taking initiatives at a very slow pace. We can help ourselves as well as others by being aware about our rights, past cyber attacks and upcoming cyber attacks so that we can be safe as much as possible.

*****