INVESTIGATION ON CYBER CRIMES

| Authored By : Ms. Amarpreet Kaur Virdi |

With the advancement of technology, every individual person has accessed to internet. The internet thus has become the largest and richest source of information there ever was, with even more systematic and highly refined search engines being developed, getting information (even though it may be restricted) has become easier than it ever was. This increase in the availability of the internet and has also seen a proportional rise in the amount as well as the magnitude of internet related crimes. Therefore, this bring us to the topic Cyber Crime Investigation.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cyber Crimes in India has been evolving rapidly in the 21st century. Technical support scams, along with impersonation of the IRS, are among the most common forms of confidence tricks used in order to receive money from unsuspecting victims.

Unfortunately, with technology on the rise, there's more room for cyber crime in 2019. According to the Cyber Security Breaches Survey 2018, 43% of businesses were a victim of a cyber security breach in the last 12 months. In the 2017 Official Annual Cybercrime Report, it's estimated that Cyber Crime will cost $6 trillion (42,46,86,00,00,00,000.06 Indian Rupee) annually by 2021. In 2015, that figure was $3 trillion (21,23,25,00,00,00,000.03 Indian Rupee).

It usually transgress geographical boundaries. With the increase in the domain of the internet, it is possible for a person sitting in Colombia hack into someone's account in Afghanistan. Therefore, to combat Cyber Crimes, the CBI has created a specialized structure. This includes:

- Cyber Crimes Research and Development Unit (CCRDU)
- Cyber Crimes Investigation Cell (CCIC)
- Cyber Forensics Laboratory
- Network Monitoring Center

6.1. Cyber Crimes Research and Development

The cyber crimes research and development unit has given the responsibility of keeping track of the deployments and changes that take places in this ever-changing area. This involves-

- Ensuring cooperation and ties-ups with the State Police Forces.
- Collection of information about cases of Cyber Crimes reported to the police investigation.

- It ties up with Software Experts to locate and identify areas where the attention of state police is required.
- It entails the collection of information relating to cases that happened in other countries and preparation of a monthly Cyber Crimes Digest.

6.2. Cyber Crime Investigation Cell

The CCIC was established in the month of September 1999. However, it came into action only from March 2000. It acts as a part of the economic offences division and has an all India jurisdiction.

Thus, it can investigate Cyber Crimes under the Investigation Technology Act 2000. It is also a round-the-clock nodal point of contract for Interpol to report cyber crimes in India and is also a member of "Cyber Crime Technology Information Network System" Japan.

6.3. Cyber Forensics Laboratory

The CBL was established in the month of November 2003 and it takes care of the following functions:

- Providing media analysis in support of the criminal investigations by CBI and other Law Enforcement Agencies.
- Providing on-site assistance for computer search and seizure upon request.
- Providing experts testimony.
- Providing adequate Research and Development In Cyber Forensics.

The information so collected is to be used as evidence in court.

The purpose of CBL is to police the internet to ensure that certain Cyber Crimes can be stopped before their commission. For this Network Monitoring Center has been provided with a Network Monitoring Tool, developed by I.L.T. Kanpur. It is also used to allow similar tools to achieve such a purpose.

Today with the growing arms of cyber space the territory boundaries seem to disappear and the concept of territorial jurisdiction as envisaged under Section16 of Criminal Procedure Code (Courts of Metropolitan Magistrate) and Section 2 of the Indian Penal Code (Punishments of Offences Committed Within India) will have to give way to alternative method to dispute resolution.

Karnataka was the first to establish a dedicated police station to handle digital crime 15 years ago. Other states including Uttar Pradesh and Maharashtra, have stepped up police training, including seeking out experts from industry.

Recently, On October 2, 2018, the SBM had issued a statement confirming that its India operations had been hit by a cyber fraud with a potential loss of around $14 million (99,09,76,000.00Indian Rupee). It had said that some unknown persons hacked into the bank's servers to illegally access various accounts and managed to transfer the monies to multiple accounts outside the country. It was the second major cyberattack on a bank in Maharashtra in the past couple of months.

In two cyberattacks on August 9 and 11,2018, the Cosmos Bank Pvt Ltd, Pune, lost a total of Rs 94.24 crore to an international group of operatives working in tandem in several countries.

The Ministry of Electronics And Information Technology (MEITY) has collaborated with The Data Security Council Of India (DSCI) to set up cyber forensic labs in all metro cities for training and building awareness of cybercrime investigation. Kunal Kumar, chief technology officer at Digital Task Force, a cyber-security company, said, "Policemen are regularly upskilled and updated about emerging technologies. States such as Maharashtra and Delhi have good infrastructure, but it still falls short when compared to the technology industry."

The following measures are being taken by the government to tackle Cyber Crimes:

- The Ministry of Home Affairs has issued an advisory to the State Governments and Union Territory Administrations on Cyber Crime, to build adequate technical capacity in handling Cyber Crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of Cyber Crimes.
- A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Courts.
- Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
- Cyber Forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.
- In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber Crimes for judicial officers.
- Government has decided to provide a centralized citizen portal through Crime and Criminal Tracking Network and Systems (CCTNS) for registering online Cyber Crime complaints.
- The Ministry of Home Affairs has also in-principle approved to set up an Indian Cyber Crime Coordination Centre (I4C) to fight against Cyber Crime in the country and establish an open platform for victims to raise cybercrime complaints with the protocol for resolution such as online crime reporting, to support and coordinate electronic investigations of cybercrime, assist the law enforcement agencies in criminal investigation etc.
- The cyber space is being closely monitored by the Government in respect of the situation of radicalization attempts. The Government has also directed the intelligence agencies to identify potential recruits and keep them under surveillance.

Though not all people are victims to Cybercrimes, they are still at risk. Crimes by computer vary, and they don't always occur behind the computer, but they executed by computer. The hacker's identity is ranged between 12 years young to 67years old. The hacker could live three continents away from its victim, and they wouldn't even know they were being hacked. Crimes done behind the computer are the 21st century's problem.

With the technology increasing, criminals don't have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren't guns anymore; they attack with mouse cursors and passwords.