CASE STUDIES OF CYBERCRIMES IN INDIA

Amanpreet Kaur

Guru Nanak College for Girls, Sri Muktsar Sahib, Punjab, India.

Introduction to Cyber Crime

Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. Net crime is criminal exploitation of the Internet. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or tampered. In 2010, the top ten reported cybercrimes to the IC3 were 1. Non-delivery payment/merchandise—14.4 percent of the sellers/purchasers did not receive payment/merchandise.2. FBI-related scams—13.2percent of criminals pose as the FBI to defraud victims.3. Identity Theft—9.8 percent were unauthorized use of personal identifying information to commit crimes.4. Computer crimes—9.1 percent were crimes that target a computer or were facilitated by acomputer.5. Miscellaneous fraud—8.6percent of scams and fraud included sweepstakes and work from- home scams.6. Advance fee fraud—7.6 percent were the Nigerian letter scam.7. Spam—6.9 percent of users received unsolicited, mass produced bulk messages.8. Auction fraud—5.9 percent was fraudulent or misleading information in the context of an online auction site. 9. Credit card fraud—5.3 percent was fraudulent charging of goods and/or services to a victim's account. 10. Overpayment fraud—5.3 percent of victims deposited bad. Here are the few cases registered with the cybercrime.

CASE STUDIES OF CYBER CRIME The number of crimes is rising in the India, with maharashtra as a leading country. There are certain case studies with motives like Blackmailing, Credit card fraud, Hosting obscene profiles, illegal money transfer, Intellectual Property Theft, hacking and so on.

Case 1: Blackmailing

State	Maharashtra
City	Mumbai
Sections of Law	292, 389, 420, 465, 467, 468, 469, 471, 474 IPC
	r/w 67 of IT Act 2000.

Background

The accused posed to be a young girl living in Kolkata and lured a non-resident Indian (NRI) working in Dubai (the complainant) to enter into an e-mail correspondence. Subsequently, the accused began corresponding with the complainant using different e-mail IDs, under the guise of different female names which made the complainant believe that he was corresponding with different girls. Having won the confidence of the complainant, the accused asked him for money and gifts. The complainant complied with the requests in the hope of receiving sexual favours from the 'girls' he was corresponding with. However after a period of time, when these favours were not forthcoming the complainant stopped this correspondence. The accused then resorted to blackmailing the complainant by referring to the e-mail exchanges that had taken place earlier. In addition, the accused led the complainant to believe that one of the girls had committed suicide and that the complainant was responsible for it. The accused also sent fake copies of the letters from CBI, High Court of Calcutta, New York Police and Punjab University etc.

The complainant lived in constant fear of being arrested in connection with the suicide over a year and a half. He paid the accused a sum of INR 12.5 million ostensibly to bribe the officials that were supposedly investigating the suicide and to compensate the victim's family for the loss of her income. The complainant was continuously under the threat of being arrested by the police. Given the huge strain upon his financial resources as well as the mental agony faced by him, the complainant himself contemplated suicide.

Investigation

The complainant handed over all the e-mail correspondence to the police. Many of them had masked headers and therefore the police could not investigate them any further. Moreover there was no e-mail that could be traced to Kolkata where the accused was staying as per the complainant's version. However the investigating team was able to trace some of these e-mails to the corporate office of a large cement company and a residence in Mumbai. A raid was conducted at these premises. In the raid one computer, two laptops, seven mobile phones and a scanner were seized. The computer equipment that was recovered was sent to the office of the forensic examiner, who found all the evidences of e-mails, chatting details etc in the laptops and the computer. During the investigation, property worth INR 0.9 million was seized, along with cash worth INR 0.3 million. The total flow of the extorted money was traced from the bank in Dubai to the account of the accused person.

Case-2: Credit Card Fraud

State	Tamil Nadu
City	Chennai
Sections of Law	Section of Law: 66 of Information Technology Act
	2000 & 120(B), 420,467,468,471 IPC.

Background

The assistant manager (the complainant) with the fraud control unit of a large business process outsourcing (BPO) organization filed a complaint alleging that two of its employees had conspired with a credit card holder to manipulate the credit limit and as a result cheated the company of INR 0.72 million. The BPO facility had about 350 employees. Their primary function was to issue the bank's credit cards as well as attend to customer and merchant queries. Each employee was assigned to a specific task and was only allowed to access the computer system for that specific task. The employees were not allowed to make any changes in the credit-card holder's account unless they received specific approvals. Each of the employees was

given a unique individual password. In case they entered an incorrect password three consecutive times then their password would get blocked and they would be issued a temporary password.

The company suspected that its employees conspired with the son (holding an add-on card) of one of the credit card holders. The modus operandi suspected by the client is as follows.

The BPO employee deliberately keyed in the wrong password three consecutive times (so that his password would get blocked) and obtained a temporary password to access the computer system. He manually reversed the transactions of the card so that it appeared that payment for the transaction has taken place. The suspect also changed the credit card holder's address so that the statement of account would never be delivered to the primary card holder.

Investigation The investigating team visited the premises of the BPO and conducted detailed examination of various persons to understand the computer system used. They learnt that in certain situations the system allowed the user to increase the financial limits placed on a credit card. The system also allowed the user to change the customer's address, blocking and unblocking of the address, authorisations for cash transactions etc. The team analysed the attendance register which showed that the accused was present at all the times when the fraudulent entries had been entered in the system. They also analysed the system logs that showed that the accuser's ID had been used to make the changes in the system. The team also visited the merchant establishments from where some of the transactions had taken place. The owners of these establishments identified the holder of the add-on card.

Case-3: Hosting Obscene Profiles

State	Tamil Nadu
City	Chennai
Sections of Law	67 of Information Technology
	Act 2000 469, 509 of the Indian Penal code

Background

The complainant stated that some unknown person had created an e-mail ID using her name and had used this ID to post messages on five Web pages describing her as a call-girl along with her contact numbers. As a result she started receiving a lot of offending calls from men.

Investigation

After the complainant heard about the Web pages with her contact details, she created a username to access and view these pages. Using the same log-in details, the investigating team accessed the Web pages where these profiles were uploaded. The message had been posted on five groups, one of which was a public group. The investigating team obtained the access logs of the public group and the message to identify the IP addresses used to post the message. Two IP addresses were identified. The ISP was identified with the help of publicly available Internet sites. A request was made to the ISPs to provide the details of the computer with the IP addresses at the time the messages were posted. They provided the names and addresses of two cyber cafeslocated in Mumbai to the police. The investigating team scrutinised the registers maintained by the cyber cafes and found that in one case the complainant's name had been signed into the register. The team also cross-examined the complainant in great detail. During one of the meetings she revealed that she had refused a former college mate who had proposed marriage. In view of the above the former college mate became the prime suspect. Using this information the investigating team, with the help of Mumbai police, arrested the suspect and seized a mobile phone from him. After the forensic examination of the SIM card and the phone, it was observed that phone had the complainant’s telephone number that was posted on the internet. The owner of the cyber cafes also identified the suspect as the one who had visited the cyber cafes. Based on the facts available with the police and the sustained interrogation the suspect confessed to the crime.

Case - 4: Illegal money transfer

State	Maharashtra
City	Pune
Sections of Law	467,468, 471, 379,419, 420, 34 of IPC & 66 of IT ACT

Background

The accused in the case were working in a BPO, that was handling the business of a multinational bank. The accused, during the course of their work had obtained the personal identification numbers (PIN) and other confidential information of the bank's customers. Using these the accused and their accomplices, through different cyber cafes, transferred huge sums of money from the accounts of different customers to fake accounts.

Investigation

On receiving the complaint the entire business process of the complainant firm was studied and a systems analysis was conducted to establish the possible source of the data theft. The investigators were successful in arresting two people as they laid a trap in a local bank where the accused had fake accounts for illegally transferring money. During the investigation the system server logs of the BPO were collected. The IP addresses were traced to the Internet service provider and ultimately to the cyber cafes through which illegal transfers were made.

The registers maintained in cyber cafes and the owners of cyber cafes assisted in identifying the other accused in the case. The e-mail IDs and phone call print outs were also procured and studied to establish the identity of the accused. The e-mail accounts of the arrested accused were scanned which revealed vital information to identify the other accused. Some e-mail accounts of the accused contained swift codes, which were required for internet money transfer. All the 17 accused in the case were arrested in a short span of time. The charge sheet was submitted in the court within the stipulated time. In the entire wire transfer scam, an amount to the tune of about INR 19 million was transferred, out of this INR 9 million was blocked

in transit due to timely intimation by police, INR 2 million was held in balance in one of the bank accounts opened by the accused which was frozen. In addition the police recovered cash, ornaments, vehicles and other articles amounting to INR 3 million. During the investigation the investigating officer learned the process of wire transfer, the banking procedures and weakness in the system. The investigating officer suggested measures to rectify the weakness in the present security systems of the call centre. This has helped the local BPO industry in taking appropriate security measures.

Case-5: Intellectual Property Theft

State	:	Karnataka
City	:	Bangalore
Sections of Law	:	65 and 66 of the Information Technology Act 2000
		381, 420 of the Indian Penal Code

Background

The complainant (software company based in Bangalore) alleged that some of the company's former employees had accessed the company's IT system and tampered with the source code of the software under development.

Investigation The investigating team visited the complainant's premises and scanned the logs of e-mails. They identified the IP address and using tracing software traced the ISP and the address of the place where the e-mails had been sent. This address was of a Hyderabad based company. On visiting the company the investigating team found 13 computers and a server. Using specialised forensic tools the disks were imaged and analysed by the team. The analysis revealed that the original source code as well as its tampered version had been stored from these systems.

Case-6: Data Theft

State	Delhi
City	New Delhi
Sections of Law	420 / 408 / 120B IPC R/W 66 IT ACT

Background

The complainant filed a case of fraud and cheating alleging theft and sale of proprietary data. The complainant had a subsidiary company in the United States which did business with its US partner. The US partner provided mortgage loans to US residents for residential premises. The business of the complainant was providing leads to their US partner. The data included the details of the loan seekers along with their telephone numbers. The complainant generated leads through arrangements with call centres in India who called from their database and shortlisted home owners who were interested in availing refinance facility on their existing mortgage loans.

The complainant realised that there was a sudden drop in the productivity of the call centres and therefore the production of leads, although the inputs meant to be given to various call centres by the employees of the company had remained the same as before. The concerned officials of the company got alarmed and made an in house enquiry. On a careful and meticulous scrutiny it was revealed that one of the employees of the complainant (company), in connivance with some other officers, had been deceiving and causing wrongful loss to the company by selling the data purchased by the company and in effect wrongful gain for themselves.

Investigation

Preliminary investigations revealed that the accused was holding the post of the senior programme manager and was the team leader for data management. During employment the accused along with his father had opened a partnership firm. It was found that raw data was sent as attachments from the e-mail ID of this(accused) firm's Website domain. The Website was traced and the e-mail ID address and registration details were recovered by the investigating officer using specialised softwares. It was revealed that the accused had passed data bought by and belonging to the complainant firm to various call centres (as if the same belonged to his firm), to make the calls on their behalf for generating leads.

The entire business process of the complainant firm was studied and a systems analysis was conducted to establish the possible source of data theft. The accused had opened a foreign currency account in the name of his firm. An analysis of the printout revealed that payments had been made to two call centres. The call centres were contacted and the raw data sent as attachments were collected. The data was comprised of six separate files and it was compared with the data purchased by the complainant company in the US. This was done by writing and executing SQL queries.Analysis of the e-mail headers of the mails sent by the accused through his ID were carried out. The originating IP address was found and information was obtained from VSNL. Accordingly it was found that the range of IP was allotted to the complainant company. It was thus established that the accused has sent the stolen data from the office of the complainant company using the e-mail ID of his (accused) firm.

An analysis of the bank account of the accused showed that payments were being made to two people. It was found that they were also ex-employees of the complainant company who had resigned after the accused left the company. On interrogation he revealed that he had roped in two of his colleagues who actively assisted him in his clandestine activities. One of them, while still an employee of the complainant company, coordinated with various call centres on behalf of the accused. The other facilitated the installation of proprietary sequencing software in the personal computer of the accused. In order to have a clientele base in US, the accused had sought the assistance of one more person. The two accused were arrested.

The modus operandi has been diagrammatically explained below.

Case-7: Hacking

State	:	Karnataka
City	:	Bangalore
Sections of Law	:	66 & 67 of IT Act 2000.

Background

The complainant approached the police stating that she had been receiving obscene and pornographic material at her e-mail address and mobile phone. She stated that this person appeared to know a lot about her and her family and believed that her e-mail account had been hacked.

Investigation The investigating team using a different e-mail ID tried to chat with the accused using the complainant's e-mail ID. Subsequently the investigating team was able to identify the ISP address of the computer system being used and it was tracked to an organisation in Delhi. The investigating team visited the company and through its server logs was able to identify the system from which the obscene material was sent. Using forensic disk imaging and analysis tools the e-mails were retrieved from the system.

The residence of the accused was located and the hard disk of his personal computer was seized. On the basis of the evidence gathered the accused was arrested.

III.STASTICS OF CYBER CRIME IN INDIA : A total of 11,592 cases were registered under the cyber crimeswith increase of 20%. Uttar Pradesh has reported the highest number ,followed by Maharashtra (2,195 cases out of 11,592 cases) In these cases a total of 8,121 persons were arrested during 2015 in comparison to 5,752 persons arrested during the previous year (2014) registering 41.2% increase over the previous year

Table 1

Patterns of Cases Reported and Persons Arrested under IT Act during 2013 – 2015 and Percentage Variation during 2015 over 2014

SL	Crime heads under IT Act	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Tampering Computer Source Documents (Sec. 65 of IT Act)	137	89	88	-1.1	59	64	62	-3.1
2	Computer Related Offences(Sec. 66 to 66E of IT Act)	2,516	5,548	6,567	18.4	1,011	3,131	4,217	34.7
3	Cyber Terrorism@(Sec. 66F of IT Act)	-	5	13	160.0	-	0	3	-
4	Publication/Transmission of Obscene/Sexually Explicit Content(Sec. 67 to 67C of IT Act)	1203	758	816	7.7	737	491	555	13
5	Intentionally not Complying with the Order of Controller(Sec. 68 of IT Act)	13	3	2	-33.3	3	4	3	-25
6	Failure to Provide or Monitor or Intercept or Decrypt Information(Sec. 69 of IT Act)	6	2	0	-100	7	0	0	-
7	Failure to Block Access any Information Hosted etc.@ (Sec. 69A of IT Act)	-	1	0	-100	-	0	0	-
8	Not Providing Technical Assistance to Govt. to Enable Online Access@(Sec. 69B of IT Act)	-	0	3	-	-	0	0	-
9	Un-authorized Access/Attempt to Access to Protected Computer System(Sec. 70 of IT Act)	27	0	8	-	17	0	4	-
10	Misrepresentation/Suppression of Fact for Obtaining License etc. (Sec. 71 of IT Act)	12	5	4	-20	14	13	2	-84.6
11	Breach of Confidentiality/Privacy(Sec. 72 of IT Act)	93	16	20	25	30	13	6	-53.8
12	Disclosure of Information in Breach of Lawful Contract@(Sec. 72A of IT Act)	-	2	4	100	-	5	2	-60
13	Publishing/Making Available False Elect. Signature Certificate (Sec. 73 of IT Act)	4	0	3	-	8	0	0	-
14	Create/Publish/Make Available Electronic Signature Certificate for Unlawful Purpose(Sec. 74 of IT Act)	71	3	3	0	51	5	3	-40
15	Others	274	769	514	-33.2	161	520	245	-52.9
Total Offences under IT Act		**4,356**	**7,201**	**8,045**	**11.7**	**2,098**	**4,246**	**5,102**	**20.2**

Note: '-' implies sezo value in previous year. % Var. – refers the Percentage Variation during 2015 over 2014
"@ implies data collected in 2014 for the first time

. **IV. Cases Of Cyber Crime In Various Category Under It Act ,2000**

Information on the cases registered under the IT Act relating to cyber crimes at all-India level.

A total of 8,045 cases were registered under the IT Act during the year 2015 in comparison to 7,201 cases during the previous year (2014), showing an increase of 11.7% in 2015 over 2014. 81.6% (6,567 cases) of the total 8,045 cases under IT Act were related to computer related offences (under section 66 & 66A, 66B, 66C, 66D and 66E of IT Act) followed by 10.1% (816 out of 8,045 cases) under publication/transmission of obscene/sexually explicit content (under section 67 & 67A, 67B and 67C of IT Act). A total of 14,121 cases under IT Act including 6,268 cases pending from previous year were investigated during the year 2015 and at the end of the year 8,088 cases remained pending for investigation. A total of 2,396 cases were charge-sheeted during 2015. A total of 4,191 cases were pending for trial at the end of the year 2015, in which maximum number of cases were computer related offences (under section

66 & 66A, 66B to 66D of IT Act) (3,110 cases) during 2015. In 486 cases trials were completed, 193 cases ended in conviction. The total 62.8%(5,102 out of 8,121) of the persons arrested under cyber crimes was under the IT Act. Out of 5,102 persons arrested under the IT act., maximum were arrested under computer related offences (under section 66&66A, 66B to 66E of IT Act) (4,217 out of 5,102 persons) accounting for 82.6% followed by publication/transmission of obscene/sexually explicit content (under section 67 & 67A, 67B and 67C of IT Act) accounting for 10.9% (555 out of 5,102 persons) during the year 2015.

The age-wise profile of persons arrested in Cyber Crime cases under IT Act, 2000 showed that 62.5% of the offenders were in the age group 18 yrs. – below 30 years (3,188 out of 5,102 persons) and 30.8%(1,573 out of 5,102 persons) of the offenders were in the age group 30 yrs. – below 45 years. 98 juvenile offenders (below 18 years) were apprehended under IT Act during 2015. A total of 3,502 persons were charge-sheeted, 250 persons were convicted and 358 persons were acquitted under such cases of cyber crimes under IT Act during 2015

V. Incidence Of Cyber Crime Registered Under IPC

Information on the cases registered under various sections of IPC which were considered as cyber crimes at all-India level. A total of 3,422 cases were registered under various sections of IPC during the year 2015 as compared to 2,272 such cases during 2014, thus showing an increase of 50.6% over the previous year. 65.9% (2,255 cases) of the total 3,422 cases registered under different sections of IPC were related to cheating followed by 2.5% (84 cases out of 3,422 cases) under data theft. A total of 1,681 cases under different sections of IPC were pending for investigation from previous year out of total cases for investigation (5,094 cases) during 2015 and 3,605 cases remained pending for investigation at the end of the year. In 710 cases, charge-sheets were submitted during 2015. Forgery under IPC crimes show highest pendency rate (81.0%) followed by data theft (76.5%) during 2015. A total of 962 cases were pending for trial from previous year, in which maximum number of cases

were reported under cheating (306 cases) followed by forgery (29 cases) during 2015. In 53 cases trials were completed, 15 cases ended in conviction and 1,608 cases remained pending for trial at the end of the year 2015

Out of total persons arrested under the cyber crimes, 35.3%(2,867 out of 8,121) were arrested in connection with cases relating to different sections of IPC during 2015. Out of 2,867 persons arrested under IPC cases relating to cyber crimes, maximum persons have been arrested in cases of criminal breach of trust/fraud (1,292 out of 2,867 persons) accounting for 45.1% of total such persons arrested under IPC crimes followed by 754 persons arrested under cheating cases accounting for 26.3% during the year 2015. The age-wise profile of persons arrested in cyber crime cases under different sections of IPC showed that 55.2%(1,583 out of 2,867 persons) of the offenders were in the age group 18 – 30 years.

Preventive Measures to Avoid Cyber Crimes

Cyber Forensics can be use to detect cyber Evidence

- To make necessary amendments in Indian laws to control on Cyber Crimes
- There is strong need to harmonize some sections of IT act 2000 to curb cyber crimes and Individuals to prevent cyber stalking avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always use latest and up dateanti virus software to guard against virus attacks.
- always keep back up volumes so that one may not suffer data loss in case of virus contamination
- Never send your credit card number to any site that is not secured, to guard against frauds.

- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- Web servers running public sites must be physically separate protected from internal corporate network

CONCLUSION In this paper I have tries to discuss the case study of different crimes with their statistic analysis carried in the report of NCRB.I have also tried to discuss the effective measures to control the crime rate that can be taken care even by the general public.Asin order to deal with them the society the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can efficiently fight the cyber criminals.

REFERENCES

1. A Study on Cyber Crime and Security Scenario in indiaYougal Joshi, Anand Singh,
2. A CASE STUDY ON CYBER CRIME IN INDIA K.Sridharan, Saktheeswari
3. A report of National Crime Report Bureau.
4. http://ncrb.gov.in/