A CASE STUDY ON CYBER CRIME IN INDIA

K.Sridharan*1
Assistant Professor, 
Department of CS & Applications 
Sri Vidya Mandir Arts & Science College, Katteri, Uthangarai
Sridhar_svm@rediffmail.com

Saktheeswari
Assistant Professor 
Department of CS & Applications 
Sri Vidya Mandir Arts & Science College, Katteri, Uthangarai 
Saktheeswarisvmc5@gmail.com

ABSTRACT

“Cyber-crime,” which refers to any criminal activity committed with the aid of or in the arena of the Internet and similar telecommunications, is both a new incarnation of old crimes through a new medium, and a unique entity all its own. It differs from physical or “terrestrial” crime in four main ways: being easy to commit, requiring minimal resources for great potential damage, being committable in a jurisdiction in which the perpetrator is not physically present, and often, not being entirely clearly illegal. Virtually any crime, from vandalism to theft, extortion to copyright infringement, can become a cyber-crime. As new technology often does, cyber-crime also empowers criminals in new ways, such as allowing individuals like this Massachusetts teen to wreak havoc on entities like the telephone company which would previously have been considered far out of their league, but which now are just as vulnerable as anyone to an attacker with the right special abilities and motivation. At the same time, the increased digitalization of all aspects of modern life, from art to government to business, has led to vastly increased stakes and thus increased incentives for cyber-crime. This paper will examine cyber-crime from a variety of perspectives, starting with a brief history of cyber-crime attacks and corresponding defenses.

Keywords: Crime, Digitalization, copyright

1. 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 intercepted, lawfully or otherwise. An Australian nationwide survey conducted in 2006 found that two in three convicted cyber-criminals were between the ages of 15 and 26.

1.1 Classification of Computer Crime

Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (1) crimes that target computers directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device. Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Crimes that use computer networks or devices to advance other ends include:

- Cyber stalking
- Fraud and identity theft
- Information warfare
- Phishing scams
- Spam

1.2 The changing nature of cybercrime

New trends in cybercrime are emerging all the time, with costs to the global economy running to billions of dollars. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing criminal organizations working with criminally minded technology professionals to commit cybercrime, often to fund other illegal activities. Highly complex, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the
shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging.

1.3 Cyber-Forensics and Legal Procedures

The ubiquitous use of computers and other electronic devices is creating a rapidly rising wave of new and stored digital information. About 90% of corporate information currently exists in digital form. Companies generate about 17.5 trillion electronic documents a year. There is also more to this explosive growth than electronic documents. Additional forms of electronic data originate from

- Internet-based electronic commerce, online banking, and stock trading.
- Corporate use and storage of phone mail messages and electronic logs.
- Personal organizers like the palm pilot and pocket PC that sells about 40 million devices a year.
- Digital cameras.
- Corporate use and storage of graphic images, audio and video.

The information risks associated with these data are many. For corporations, the free flow of digital information means that the backdoor is potentially always open to loss. There are several factors as we have seen previously that increase the risk of litigation and loss of confidential corporate data and with this the importance of cyber-forensics grew.

In this information age the physical crimes are somewhat also associated with technology. Some traditional crimes especially those concerning finance and commerce continue to be upgraded technologically. Crimes associated with the theft and manipulation of data is detected daily. A serious and costly terrorist act could come from the internet instead of from a truck bomb. The diary of a serial killer may be recorded on a floppy disk or a hard drive rather than on a piece of paper or a notebook. So as we can see, criminal activity has to some extent converted from a physical dimension in which evidence and investigations are described in tangible terms to a cyber-dimension in which evidence exists only electronically and investigations are conducted online.

1.4 Goals of the forensic investigation

It is important in cyber-forensics to review the reasons why an investigation is needed and the plan of that investigation. It is important to determine the impact and feasibility of conducting an investigation. In some cases, if the cost of the investigations outweighs the benefits, there might not be a reason to conduct the investigation at all. There are many things (especially in a corporate environment) that might trigger an investigation and some of those are:

- Internet usage exceeds norm
- Using email inappropriately
- Using of internet, e-mail or PC in a non-work-related manner
- Theft of information
- Violation of security policies or procedures
- Intellectual property infractions
- Electronic tampering like fraud, mimicking someone or something, masking or masquerading as someone.
- Network Intrusion which potentially leads to compromising networked computers.

Some incidents regardless of their impact (financial or otherwise) would need to be investigated. Some items that cyber-forensics experts keep in mind when they determine the impact are:

- Benefits to pursuing such an investigation
- Liabilities for not pursuing an investigation
- Obligations to pursue or not to pursue (goodwill toward public, partners and other contracts)
- Resources available (time, people, finances, tools, etc)

Steps and Procedures

During an investigation, forensic investigators should be focused on the goal of gathering evidence for prosecution. They should become familiar with federal rules of evidence as well as local and state laws pertaining to the admissibility of evidence and what is required to provide “expert witness” testimony, should that become necessary. Investigators usually work on

- isolation of equipment,
- isolation of files,
- tracking of web sites visited,
- tracking of log-on, durations and times and
- Tracking of illicit software installation and usage.

They then work on correlating all that evidence found. Isolation of equipment - Investigators gains approval from management to access the equipment. Once they have the PC or device in their possession they need to preserve the chain of evidence by making sure that neither they nor anyone else is left alone with the equipment. Logs are kept about the whereabouts of and actions taking place on such equipment. It is also important to backup any data under investigation and that the programs used to perform the backup should be independent and have integrity. One good program for such backup is SafeBack, which performs a bit-stream backup that helps in making exact partition backups.

Isolation of files - In order to prevent the suspects from tampering with any files, investigators need to disable their user IDs and not delete it. Once IDs are disabled all files they had access to should be copied to a backup media. Tracking of web sites visited - This happens through reviewing the following items on the isolated equipment (or in other words on the backup of the data on that isolated equipment:
• Cookies, as those take the investigator(s) to the web sites to which the user was visiting.
• Bookmarks where most of the favorite URLs are stored
• History Buffer - these have more information on the timing on which individuals were accessing the websites and could give insights on unapproved or unauthorized web sites.
• Cache from which the investigators can get the last set of instructions or data that was saved to the cache. This requires special programs because it tends to be tricky in many cases.
• Temporary Internet files - This has the advantage over any other items in that it should contain the address of the site, when was it last modified, last accessed, and last checked, and it helps a lot in cases of too much internet access or in appropriate internet access. Tracking of illicit software installation and use - This is a comparison between the list of programs that currently reside on the PC or device (discovered through inspecting the registry or the files on disk) and the list of what can be on any given PC that follows the corporate policy.

These techniques are usually known as System Review. In this the examiner also has to take care of discovering hidden files if any exists. Intrusion profiling for network intrusion - For network intrusion, it is a bit different than the above. The hacker could be from outside the company. The concept of criminal profiling with a few twists can also be applied for profiling computer / network intrusions. The process of creating the profile involves seeing the intrusion in context, relating the activities to the threat to business functions, and making educated guesses based on probability, experience, and clues. The profile can assist in tracking the intruder, in identifying future targets, signatures of the attack and possible past intrusion locations, and in assessing the risk or threat of the hacker. The profiling can also reveal possible motives, technical abilities and geographic locations of the hacker.

In order to create a good profile, investigators have to gather information about the time of the intrusion, source of the attack, list of systems penetrated, method of penetration, and list of all files accessed including all written/read and created files. Organizing and compiling such information helps in creating the proper profile that would bring the information together and create an organized picture of who the intruder might be.

**Correlating the evidence** - Computer evidence as seen from the various listed procedures almost never exists in isolation. It is a product of the data stored, the application used to create and store it, and the computer system that directed these activities. To a lesser extent it is also the product of the software tools used in the laboratory to extract it.

After capturing the file evidence and the data, the examiner can graph an access pattern or list the illegal software or when it was loaded. Next they need to check the access and download dates and times against the time sheets, surveillance and other witness accounts to ensure that the suspect under investigation had the opportunity to engage in unauthorized acts using the equipment in question. Investigators in reviewing such evidence have to show only the facts and nothing else. They can’t make any leap in their logic to connect point A to point B as this only show that they lack enough evidence. They also need to be able to adequately explain how the person under review was able to commit the offense, illegal act or unauthorized action and present evidence and proof of how it was done.

The figure points out to a three-level hierarchical model consisting of the following:

- An overarching concept of the principles of examination.
- Policies and practices
- Procedures and techniques

### 1.5 Internet Crime

Internet crime is crime committed on the Internet, using the Internet and by means of the Internet. Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes.

With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem in the United States. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.

The different types of Internet crime vary in their design and how easily they are able to be committed. Internet crimes can be separated into two different categories. There are crimes that are only committed while being on the Internet and are created exclusively because of the World Wide Web. The typical crimes in criminal history are now being brought to a whole different level of innovation and ingenuity. Such new crimes devoted to the Internet are email “phishing”, hijacking domain names, virus immision, and cyber vandalism. A couple of these crimes are activities that have been exposed and introduced into the world. People have been trying to solve virus problems by installing virus protection software and other software that can protect their computers. Other crimes
such as email “phishing” are not as known to the public until an individual receives one of these fraudulent emails. These emails are cover faced by the illusion that the email is from your bank or another bank. When a person reads the email he/she is informed of a problem with he/she personal account or another individual wants to send the person some of their money and deposit it directly into their account. The email asks for your personal account information and when a person gives this information away, they are financing the work of a criminal

Statistics: The statistics that have been obtained and reported about demonstrate the seriousness Internet crimes in the world. Just the "phishing" emails mentioned in a previous paragraph produce one billion dollars for their perpetrators (Dalton 1). In a FBI survey in early 2004, 90 percent of the 500 companies surveyed reported a security breach and 80 percent of those suffered a financial loss (Fisher 22). A national statistic in 2003 stated that four billion dollars in credit card fraud are lost each year. Only two percent of credit card transactions take place over the Internet but fifty percent of the four billion, mentioned before, are from the transaction online (Burden and Palmer 5). All these finding are just an illustration of the misuse of the Internet and a reason why Internet crime has to be slowed down.

Stopping the problem

The question about how to police these crimes has already been constructed, but this task is turning out to be an uphill battle. Since the first computer crime law, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the government has been trying to track down and stop online criminals. The FBI has tried many programs and investigations in order to deter Internet crime, like creating an online crime registry for employers (Metchik 29). The reality is that Internet criminals are rarely caught. One reason is that hackers will use one computer in one country to hack another computer in another country. Another eluding technique used is the changing of the emails, which are involved in virus attacks and “phishing” emails so that a pattern cannot be recognized. An individual can do their best to protect themselves simply by being cautious and careful. Internet users need to watch suspicious emails, use unique passwords, and run anti-virus and anti-spyware software. Do not open any email or run programs from unknown sources.

The most serious consequence is that crime is often done by identity theft experts who perform their task very meticulously and thus the charge of crime comes on victim, whose identity has been theft. There are two broad types to Identity Theft

- Account Takeover
- True Name Theft

Account Takeover is a kind of situation where the criminal uses the information which he has stolen in order to have the access of victim’s existing accounts. Then there may be further misuse using the existing accounts like changing the address so that bill does not reach to victim's place and criminal can enjoy shopping and purchases online through the credit cards the thief runs up.

True Name Theft, the thief by using the personal information of the victim opens new accounts. In this the thief can open new credit card, cellular phones number, check books of the existing account and may misuse all. Online facilities of banking and credit cards called net baking has made things very easy for these sort of thefts, where only passwords or codes are the keys to do anything and real verification has no role to play as such.

1.5 Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

* From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

* Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
* Digital signatures have been given legal validity and sanction in the Act.
* The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
* The Act now allows Government to issue notification on the web thus heralding e-governance.
* The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

* The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security
procedure, as stipulated by the Government at a later date.

* Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and cause loss.

2. Cyber Crime in India

Cyber crimes are increasing in India and we do not have a robust cyber law and cyber crime investigation infrastructure in India. Incidences like e-mail cracking, abuse at facebook, misuse of G-mail id, intellectual property thefts, etc have significantly increased in India due to absence of a techno legal framework.

So far Indian government had failed to ensure both the modernization of police force of India and formulation of regulations and guidelines for effective investigation of cyber crimes in India. Further, Indian government has yet to formulate a cyber crimes prevention strategy of India. Although the National Cyber Security Policy 2013 of India has been formulated yet it has not been implemented in India so far. As a result the cyber security in India is still in an abysmal state.

2.1 Cyber Crimes Investigation Training In India

Cyber crimes have significantly increased in India. The trends in this regard are not very promising. For instance, the cyber law, cyber security and cyber forensics trends in the year 2013 have showed poor performance of Indian government in these fields. This position has not changed in 2014 as well. For instance, the cyber forensics trends of India 2014 still show inability of India to deal with cyber forensics related issues. India is also clinging to outdated laws like cyber law and telegraphs law and is not investing effectively in the field of intelligence agencies and law enforcement technology for India.

In the absence of scientific approach towards digital evidence and cyber crime investigation, there are very few cyber crimes convictions in India. In fact, the Supreme Court of India is hearing many Public Interest Litigations (PILs) in this regard. In one such PIL the Supreme Court of India has issued notice to centre to seek its views in this regard. The Supreme Court has sought response from the centre on a PIL seeking its direction to the government to frame regulations and guidelines for effective investigation of cyber crimes in India.

Realizing the seriousness of the situation, Indian government has announced to formulate a cyber crimes prevention strategy of India. Cyber crimes investigation, however, requires sound techno legal expertise. Skills development through online training and skills development courses in urgently required for Indian law enforcement agencies. Cyber crimes investigation training in India is one such skills development activity that must be imparted to make law enforcement agencies of India modern and up-to-date.

Modernization of police force of India requires not only basic knowledge of information and communication technology (ICT) but also practical trainings in the areas like cyber law, cyber crimes investigation, cyber forensics, etc. Cyber crimes investigation capabilities in India are not up to the standards. Presently, most of the police stations and police officers find it difficult to deal with cyber law and cyber crimes related cases. Another area where India needs to work is to strengthen the cyber forensics investigation capabilities. There is a dire need to develop cyber forensics best practices in India as soon as possible. Police must also ensure cyber law skills development. Similarly, police in India also need to undertake cyber frauds detection trainings so that cyber frauds can be anticipated even before they are committed.

2.2 Intelligence Agencies and Law Enforcement Technology Forums in India

Technologies regarding intelligence and law enforcement agencies are not very frequently discussed. Thus, they remain outside the mainstream media and very few works are available that inform about these technologies.

We have been discussing intelligence and law enforcement related technologies and projects like National Counter Terrorism Centre (NCTC) of India, Aadhaar Project of India, Crime and Criminal Tracking Network and Systems (CCTNS) Project of India, Central Monitoring System (CMS) Project of India, Internet Spy System Network and Traffic Analysis System (NETRA) of India, National Intelligence Grid (Natgrid) Project of India, etc. While implementing the intelligence and e-surveillance related projects, Indian government has failed to cater the constitutional requirements like Parliamentary oversight, privacy and civil liberties protections, balancing national security and civil liberties protection, etc. Similarly, law enforcement and intelligence agencies of India are still not very comfortable with techno legal issues. For instance, cyber forensics is rarely applied by these agencies and our police are not well versed in cyber crime investigations. Modernization of police force of India is urgently needed where police personnel must be trained in various techno legal issues. Cyber security issues are also not managed properly by these agencies.

Cyber security in India is not in a good shape as reflected by the cyber security trends of India 2013. Critical infrastructure protection in India is still not taken seriously by Indian government. It has been suggested that NTRO should protect the critical ICT infrastructures of India.

The National Cyber Security Policy of India 2013 (NCSP 2013) was drafted in the year 2013. However, NCSP 2013 itself is suffering from many serious drawbacks. These include lack of privacy protection, absence of integration with the National Security Policy of India, absence of civil liberties protection in cyberspace, absence of balance
between civil liberties and national security requirements, non implementation of the policy, etc.

Indian government has also proposed setting up of National Cyber Coordination Centre (NCCC) of India in 2012. However, till 2014 it has not been established though some interest in this regard has been shown recently by the Narendra Modi government. This seems to be the continuance of Congress government’s commitment to expedite establishment of NCCC in India.

2.3 Cyber crime in Tamilnadu
In Tamil Nadu, in the year 2002, two Cyber Crime Cells were created; one is exclusively for Chennai Police and another at CB CID, having jurisdiction throughout State of Tamil Nadu. The role of this Cell is to detect, prevent and investigate Cyber crimes that come under the ambit of Information Technology Act 2000 and assist the other Law Enforcement in the investigation of crimes in which elements of Computer related crime exists.

The cases under I.T. Act 2000 have to be investigated by not below the rank of Dy. Superintendent of Police. The Cyber Crime Cell is functioning in the First floor, Block-3 Electronic Complex, SIDCO Industrial Estate, Guindy, Chennai-32.

Online Safety Tips
- What you put online will be there forever.
- Use a strong password (a combination of upper and lower case letters, symbols and numbers).
- Don’t post inappropriate or illegal content anywhere on the internet.
- Don’t open e-mail attachments or instant-message attachments unless you are completely sure they do not contain viruses.
- Don’t click on links inside e-mails or instant messages.
- Never give out personal information about yourself, your family, or your friends (such as your last name, address, phone numbers, city, the name of your school, photos of yourself or your family, PIN numbers for your bank, etc.).

Wi- Fi Security Tips
- Change Default Administrator Passwords (and Usernames) of the WiFi Router.
- Change Password after regular interval.
- Position the Router or Access Point Safely.
- Turn Off the Network / WiFi routers if it is not in use.

Online Banking Tips
- Never use unprotected PCs at cyber cafes for internet banking.
- Never keep your pin and cards together.
- Never leave the PC unattended when using internet banking in a public place.
- Register for Mobile SMS, Email Transaction Alerts.
- Never reply to emails asking for your password or pin.
- Visit banks website by typing the URL in the address bar.
- Log off and close your browser when you have finished using internet banking.
- Memorize your PIN. Never carry your PIN.
- Report lost or stolen card immediately.

10 steps that can protect you from loss
- Register for transaction alert s via SMS and E- Mail.
- If you change your mobile number, update with the bank.
- Reduce the limit on your credit card if you use it sparingly.
- Use virtul cards for online shopping.
- Make use of the virtual keyboard wherever possible.
- Instead of going to the banks website using the link in E-Mail, type the web address directly.
- Memorise 3 digits CVV number at the back of the card and scratch it out.
- Do not leave unwanted photocopies of essential documents at the photocopier.
- If you lose your phone, deactivate all banking services linked to that number.

3. Types of Cyber Crime
While the IT Act covers a broad area in Cyber crimes we can be more specific and list down the types of cyber crimes one encounters. These are:

1. Internet Password Thefts
2. Threatening e-mails
3. Cyber Stalking
4. Child Abuse/ Pornography
5. Economic Offences
6. Credit Card Number Theft
7. Denial of service attacks
8. Web page Hacking
9. Domain name disputes/ IPR disputes

3.1 Protection of civil rights wing functions
The important duties of PCR Cell are as follows:
1. PCR Cell is the nodal, monitoring, coordinating and advisory agency for the Police department, in so far as the enforcement of these Acts are concerned.
2. PCR Cell receives petitions from Government, National Commission for SCs / STs, State Commission for SCs / STs and also Public on various issues which will be sent to the Unit Officers for enquiry and obtain enquiry reports which in turn will be furnished to the concerned agencies. Where the enquiry is not to the satisfaction, instructions will be issued to the Unit Officers to conduct a proper enquiry. If necessary and basing on the importance,
the enquiries will be entrusted to the officers of CID also for re-enquiry.
3. PCR Cell conducts periodical reviews of the cases pending with the Local Police at Range Level.
4. Attends the meetings of Parliamentary Committee for SCs / STs, Cabinet Sub-Committee for SCs / STs, National Commission for SCs / STs, Government, State Commission for SCs / STs etc.
5. PCR Cell prepares the required data and material for the above meetings.
6. PCR Cell pursues with Local Police on proceedings / minutes of the above meetings and obtains action taken reports.
7. PCR Cell issues suitable instructions to all concerned on prevention, investigation and prosecution aspects. In this regard, a compendium of instructions was prepared containing all the Acts, Rules, Government Orders and Circulars issued by the DGP from time to time.
8. The advisory role of the PCR Cell is important, as several other departments are also charged with the responsibility of enforcement of PCR and SC, ST (Prevention of Atrocities) Acts.
9. The PCR Cell prepares standing instructions fixing procedures and responsibilities on prevention and investigation and issue guidelines from time to time.
10. PCR Cell prepares various returns, reports and statements to be sent to the National and State Agencies.
11. PCR Cell ensures implementation of recommendations of Justice Punnaiah Commission.
12. The PCR Cell is responsible as per the provisions of SC / ST (POA) Act, 1989 under Rule (8) for the following:
   a) To bring about awareness among daliths about their rights and legal remedies available to them.
   b) To identify the crime prone areas and take preventive steps to prevent atrocities on daliths.
   c) To secure data on crime against daliths, analyze it and draw a strategy to curb this menace.
   d) To study the legal provisions and propose amendments to make the law more practical and effective.
   e) Making enquiries about willful negligence by public servants.
   f) Making enquiries about the investigation and spot inspections conducted by various officers.
   g) Restoring the feeling of security amongst the members of SCs & STs.
   h) Making investigations about the probable causes leading to an offence under the Acts.
   i) Conducting survey of the identified areas.
13. The PCR Cell prepares and sends half-yearly reports for the half year ending 30th June and 31st December in each year to the Government giving district-wise details of all the cases registered under the Protection of Civil Rights Act 1955 and SC / ST (POA) Act, 1989.
14. An annual report also should be sent by the PCR Cell indicating the steps taken for proper implementation of various provisions of the Act. (Memo No.2112/SC&ST Cell.A2/76-77, SW Dept., dt.11-7-1977).
15. PCR Cell obtains periodical/monthly reports on various issues from Unit Officers in prescribed format and submits a report to Government with a critical review in respect of atrocities, violation of civil rights and other offences.

3.3 Mobile Devices and Cybercrime: You see them everywhere: people hunched over their smart phones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them. They play games, download email, go shopping or check their bank balances on the go. They might even access corporate networks and pull up a document or two on their mobile gadgets. But as wireless devices become increasingly ingrained into the daily lives of Americans, they open the door to heightened security risks. Not only do such devices become points of access for cybercriminals, but they also may be more easily breached than personal computers since many consumers do not secure their smart phones or tablets with antivirus software or take simple precautions such as enabling password protection.

Do’s and don’ts for mobile user

Don’ts
Please do not click photographs without permission by your mobile phones. You are invading the privacy.
- Do not send obscene/pornographic text, images. SMS.
- Do not send obscene/pornographic text, MMS (multimedia messaging service)
- Do not receive from or reply to sms/mms of strangers.
- Do not transmit obscene/ pornographic material, as it is an offence under Information Technology act –2000.punishment is 5 yrs imprisonment and 1lac rupees fine.
- Do not call to the unknown phone/mobile numbers you get while chatting or exhibited on various profiles on internet. Which you are not familiar with. If you do you may be causing harassment on behalf of other person.
- Do not keep your Blue tooth open to all; you may receive obscene/phornographic text, images and viruses.
- Do not give your mobile numbers while chatting on INTERNET to avoid “STALKING”.
- DO not handover your mobile phone to unauthorised service center, to avoid CLONING.

Do’s
- Note down your IMEI number.
- Security pin code should be used to avoid misuse of your mobile phones.
- mms/sms received should be checked before opening the message.
- Delete obscene/phornographic text, images. SMS/MMS from your mobile phones.
- Anti-virus software should be loaded in the mobile phone.
- Mobile phone keypad should be locked after every use.
- Use your mobile phone when necessary.
3.4 Examples of cyber-attacks

- Attack on South Korea’s banks and broadcasters, 2013. A suspected cyber-attack brought down systems and computers at some of South Korea’s major banks and broadcasters. As a result, the local equity market declined 1.0%.
- Operation High Roller. Orchestrated in 2012 the attack siphoned around $78 to $2.5 billion from bank accounts in Europe, the U.S. and Latin America. Targets were high-value commercial accounts, rich individuals, credit unions and large global banks and regional banks. The attack located a victim’s highest value account and transferred money to a prepaid debit card (which can be cashed in anonymously). The target’s bank statement was then altered to hide the theft.
- The Stuxnet attack on Iran’s nuclear program, 2010. A sophisticated virus infiltrated the machine controlling gas centrifuges tasked with separating Uranium-235 isotopes from U-238 isotopes at the Natanz plant. As a result, the spin of the centrifuges were slowed, stalled and in some cases self-destructed. The perpetrator has still not been identified.
- Cyber-attack against state-owned oil company Aramco. Over 30,000 computers at Saudi Arabian oil company Aramco were hit by a devastating virus in August 2012. The attack destroyed data and erased hard-drives of Computers and is thought to have been aimed at stopping the production of oil.
- The Flame virus, 2012. Thought to have been operating since 2010, the Flame virus was detected in 2012.
- The virus code is seen as some of the most sophisticated and largest malicious code to date. It infiltrated computers belonging to the Iranian Oil Ministry, the Iranian National Oil Company and other networks in Hungary, Lebanon, Austria, Russia, Hong Kong and the United Arab Emirates - stealing and deleting information from the systems. Part of the functionality of the virus including turning on microphones of computers to secretly record conversations, taking screen grabs of infected computers and stealing Credentials of high-level and administrative users.
- Red October cyber-attack, 2013. Targeting governmental and diplomatic organizations. The Red October attack was discovered in January of this year, but is believed to have been operating undetected for a Number of years. The attack effectively stole confidential and encrypted documents (including deleted ones)
- From embassies, nuclear research centres and oil and gas companies. Information targeted included geopolitically sensitive data and credentials to access protected computer systems. The malicious code was also able to detect when a USB stick was inserted into a networked computer and undelete and steal any files on the stick. The cyber-crime racket behind the attacks shut-down their operations after the attacks. Were made public and documented.
- The MiniDuke Cyber-attack on EU governmental organizations and operators of critical infrastructure.
- MiniDuke Cyber-attack exploited a flaw in Adobe’s Acrobat reader to enter computer networks and gather Information.

REFERENCES