Computer Age Crimes - Cyber Crime

Dr. Anubha Singh

Introduction:

The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause a breach of rule of law. Before evaluating the concept of cyber crime; it is crucial that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms highlighted.

Conventional crime:

Crime is a social and economic phenomenon and is as old as human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment." A crime may be said to be 'any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.'

Cyber crime:

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime".

A generalized definition of cyber crime may be; "Unlawful acts wherein the computer is either a tool or target or both". The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be a target for unlawful acts in the following cases-

unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Reasons for cyber crime:

We may say that computers are vulnerable and therefore the rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

1. Capacity to store data in comparatively small space - The computer has unique characteristic of storing data in a very small space. This makes it much easier to remove or derive information either through physical or virtual medium.
2. Easy to access - The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach; not due to human error but due to the complex technology. Secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
3. Complex - The computers work on operating systems and these operating systems in turn are composed of millions of codes.
4. Negligence - Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal access and control over the computer system.
5. Loss of evidence - Loss of evidence is a very common and obvious problem as all the data are routinely destroyed.

Mode and manner of commiting cyber crime:

1. Unauthorized access to computer systems or networks / hacking - This kind of offence is normally referred as hacking in the generic sense.

2. Theft of information contained in electronic form - This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

3. Email bombing - This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

4. Data diddling - This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

5. Salami attacks - This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.

6. Denial of Service attack - The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

7. Virus / worm attacks - Viruses are programmes that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

8. Logic bombs - These are event dependent programmes. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs.

9. Trojan attacks - This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorised programme. The most common form of installing a Trojan is through e-mail.

10. Internet time thefts - Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password.

11. Web jacking - This term is derived from the term hijacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money.

Classification:

The subject of cyber crime may be broadly classified under the following three groups. They are-

1. Against Individuals
   a. their person and
   b. their property of an individual

2. Against Organization
   a. Government
   c. Firm, Company, Group of Individuals.

3. Against Society at large.

The above mentioned offences may be discussed in brief as follows:

1. Harassment via e-mails - Harassment through e-mails is not a new concept. It is very similar to harassing through letters.

2. Cyber-stalking- Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes

threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

3. Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography) / Polluting through indecent exposure - Pornography on the net may take various forms. It may include the hosting of a web -site containing these prohibited materials, use of computers for producing these obscene materials, downloading through the Internet obscene materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

4. Defamation - It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium.

5. Unauthorized control/access over computer system- This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

6. E-mail spoofing - A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

7. Computer vandalism - Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to

the computer or by physically damaging a computer or its peripherals.

8. Intellectual Property crimes / Distribution of pirated software - Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence.

9. Cyber terrorism against the government organization - At this juncture, a query often arises as to the need to distinguish between cyber terrorism and cyber crime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives".

10. Trafficking - Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms.

11. Fraud & Cheating - Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

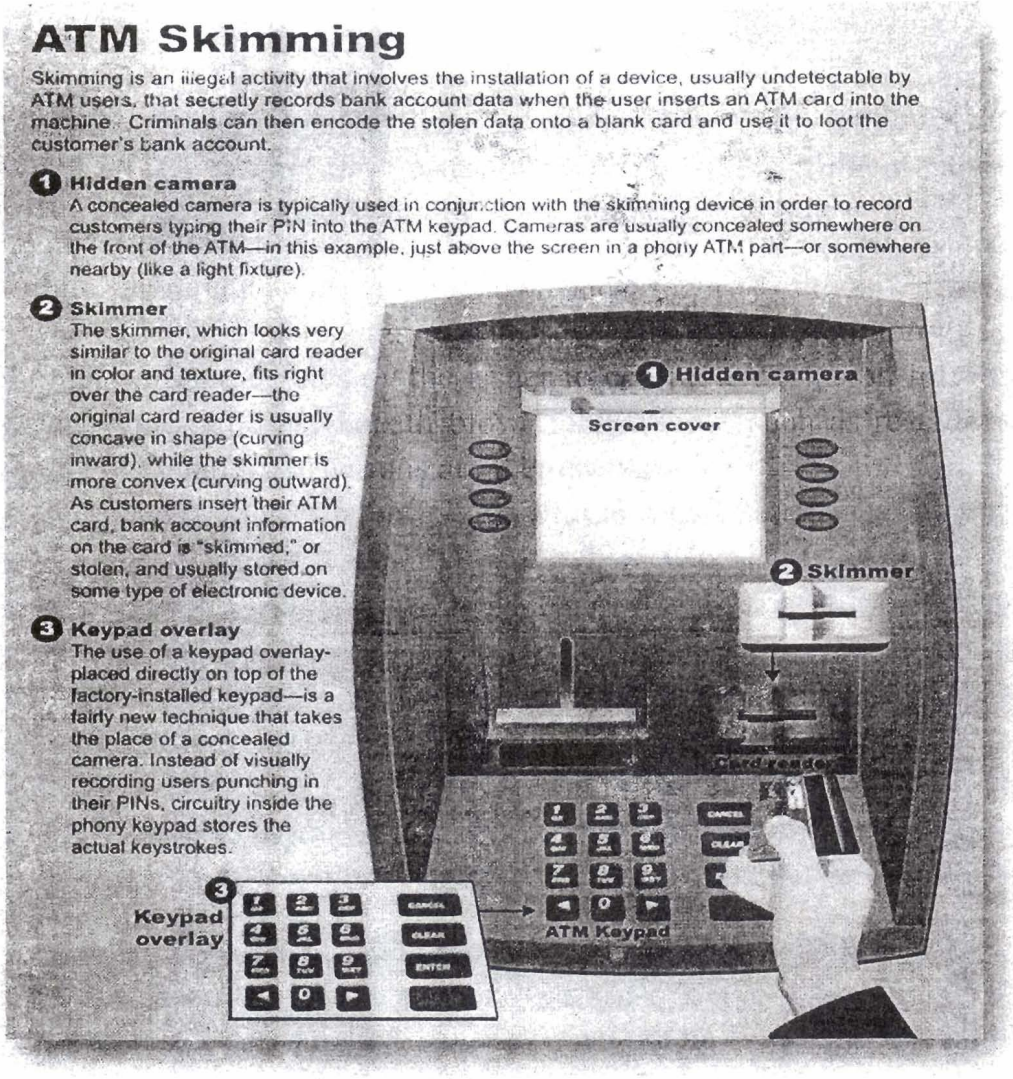
12. Skimming: An electronic method of capturing a victim's personal information used by identity thieves. The skimmer is a small device

> that scans a credit card and stores the information contained in the magnetic strip. Skimming can take place during a legitimate transaction at a business. Skimming is the theft of credit card information used in an otherwise legitimate transaction. The thief can procure a victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view.The thief may also use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip. Call centers are another area where skimming can easily occur. Skimming can also occur at merchants such as gas stations when a third-party card-reading device is installed either out-side or inside a fuel dispenser or other card-swiping terminal. This device allows a thief to capture a customer's cred-it and debit card information, including their PIN, with each card swipe.

Instances of skimming have been reported where the perpetrator has put a device over the card slot of an ATM (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a miniature camera (inconspicuously attached to the ATM) to read the user's PIN at the same time. Another technique used is a keypad overlay that matches up with the buttons of the legitimate keypad below it and presses them when operated, but records or wirelessly transmits the keylog of the PIN entered. The device or group of devices illicitly installed on an ATM are also colloquially known as a "skimmer". Recently-made ATMs now often run a picture of what the slot and keypad are supposed to look like as a background, so that consumers can identify foreign devices attached.

Skimming is difficult for the typical cardholder to detect, but given a large enough sample, it is fairly easy for the card issuer to detect. The issuer collects a list of all the cardholders who have complained about

fraudulent transactions, and then uses data mining to discover relationships among them and the merchants they use. For example, if many of the cardholders use a particular merchant, that merchant can be directly investigated. Sophisticated algorithms can also search for patterns of fraud. Merchants must ensure the physical security of their terminals, and penalties for merchants can be severe if they are compromised, ranging from large fines by the issuer to complete exclusion from the system, which can be a death blow to businesses such as restaurants where credit card transactions are the norm.



Prevention of cyber crime:

Prevention is always better than cure. It is always better to take certain precaution while operating the net. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.

A netizen should keep in mind the following -

1. To prevent cyber stalking avoid disclosing any information pertaining to oneself, as any information given is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photographs online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use the latest and up dated antivirus software to guard against virus attacks.
4. Always keep a back -up of one's data so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against fraud.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. 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.
8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.

10. Web servers running public sites must be physically separate and protected from internal corporate network.

Conclusion:

The capacity of the human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space but it is quite possible to check it. History is witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and making the application of laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world. There is no denial that there is an urgent and pressing need to bring changes in the Information Technology Act, to make it more effective to combat cyber crime. I would conclude with a word of caution for the pro-legislation school that should be kept in mind. The provisions of the cyber law need not be made so stringent that it may retard the growth of the industry and prove to be counter-productive.

References:

1. cybercellmumbai.gov.in/ý
2. http://www.fbi.gov/about-us/investigate/cyber/cyber
3. http://www.cybercitizenship.org/crime/crime.html
4. http://www.cybercrimeindia.org/