BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG681: Cyber Security
Lecture No: 09

Introduction to Cyber Crime

Agenda

- Cyber crime definition
- Cyber crime and information security
- Classification of cyber crime
- Cyber crime and Indian ITA 2000
- Global perspective on cyber crime

Introduction

- The internet is growing rapidly.
- It has given rise to new opportunities in every field one can think of - be it entertainment, business, sports or education.
- Internet also has its own disadvantages.
- Cyber crime is an illegal activity committed on the internet

Cyber Crime: What is it?

- Crime committed using a computer and internet to steal data or information.
  - Illegal activities: Actions carried out
  - Malicious programs: Software tools
- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
- Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
- Any financial fraud that takes place using a computer.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.

Cyber Crime: Definition

- **"Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them".**
- Cybercrime is also called as *computer-related crime, computer crime, E-crime, Internet crime, High-tech crime* *etc.*

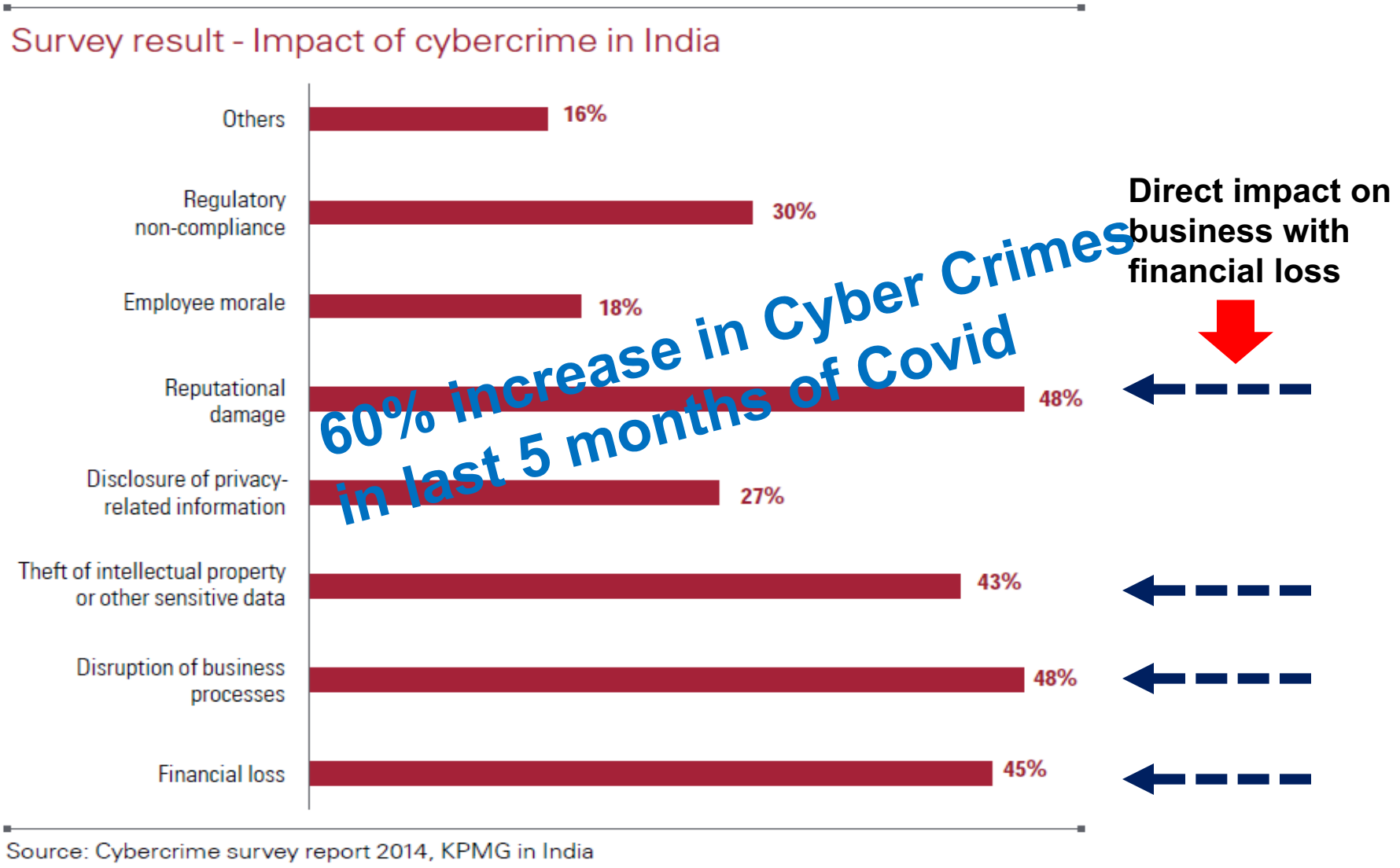
Cyber Crime: Alternate Definition

- A crime committed using a computer and the internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
- Any illegal activity through the Internet or on the computer.
- All criminal activities carried out using the medium of computers, the Internet, cyberspace and the www.

Cyber Crime Attack Types

- **Techno-crime: Active attack**
  - Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno Crime is usually pre-meditated and results in the *deletion, corruption, alteration, theft or copying of data on an organization's systems*.
  - Techno Criminals will usually probe their target system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.
- **Techno–vandalism: Passive attack**
  - Techno Vandalism is a term used to describe *a hacker or cracker* who breaks into a computer system with the *sole intent of defacing and or destroying its contents*.
  - Techno Vandals deploy *'sniffers'* on the Internet to locate insecure targets and then execute a range of commands using a variety of protocols towards a range of ports. The best weapon against such attacks is a firewall to hide and disguise your presence on the Internet.

Impact of Cyber Crime in India



60% increase in Cyber Crimes in last 5 months of Covid

Direct impact on business with financial loss

Challenges for Securing Data

- Cyber crimes occupy an important space in information security due to their impact
- Unwillingness of organizations to segregate the cost of computer security incidents into their accounting
- Difficulty in attaching a quantifiable monetary value to the corporate data
- Financial loses may not be detected by the victimized organization in case of insider attacks i.e. someone leaking customer data

Who are Cyber Criminals?

- Those who conduct acts such as:
  - Credit card fraud
  - Cyber stalking
  - Child pornography
  - Defaming someone online
  - Gaining unauthorized access to computer systems
  - Ignoring copyrights
  - Software licensing and trademark violation
  - Overriding encryption to make illegal copies
  - Software piracy
  - Stealing another's identity to perform criminal acts
  - etc…etc

Categories of Cyber Criminals

- Hungry for recognition
- Not interested in recognition
- The Insiders

Hungry for Recognition

- **Hobby hackers:** A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/software
- **Ethical hackers:** Person with no financial or other motives, helps improve security
- **Political hackers:** Supports objectives of individuals, groups or nations for causes such as anti-globalization, transnational conflicts, global warming etc.
- **Terrorist organizations**
  - Cyber terrorism
  - Internet attacks as part of terrorist activity
  - Large scale disruption of computer networks and personal computers attached to internet via viruses

Not Interested in Recognition

- **Psychological perverts**
  - Express sexual desires, deviates from normal behavior
- **Financially motivated hackers**
  - Make money from cyber attacks
  - Bots-for-hire: fraud through phishing, information theft, spam and extortion
- **State-sponsored hacking**
  - Hacktivists
  - Extremely professional groups working for governments
  - Have ability to worm into the networks of the media, major corporations, defense departments etc

The Insiders

- Disgruntled current or former employees seeking revenge
- Competing companies using employees to gain economic advantage through damage and/or theft
- Internally competing employees

Motives for Cyber Crime

- Money
- Gain power
- Publicity
- Revenge
- Sense of adventure
- Thrill to access forbidden information
- Destructive mindset
- Sell security services

Classification of Cyber Crimes

- Against an individual
- Against property
- Against organization
- Against society
- Crimes emanating from Usenet newsgroup

Cyber Crimes: Against an Individual

- Electronic mail spoofing and other online frauds
- Phishing, spear phishing
- Spamming
- Cyber defamation
- Cyber stalking and harassment
- Computer sabotage
- Pornographic offenses
- Password sniffing

Cyber Crimes: Against Property

- Credit card frauds
- Intellectual property (IP) crimes
- Internet time theft

Cyber Crimes: Against Organization

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack/dissemination of viruses
- E-Mail bombing/mail bombs
- Salami attack/Salami technique
- Logic bomb
- Trojan horse
- Data diddling
- Industrial spying or industrial espionage
- Computer network intrusions
- Software piracy

Cyber Crimes: Against Society

- Forgery
- Cyber terrorism
- Web jacking

Cyber Crimes: Emanating from Usenet Newsgroup

- Usenet groups may carry very offensive, harmful, inaccurate material
- Postings that have been mislabeled or are deceptive in another way
- These should be taken in with a considered view

E-Mail Spoofing

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- **Example:** senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency.
- Most spoofed e-mails fall into the "nuisance" category and require little action other than deletion; the more malicious varieties can cause serious problems and security risks.
- Spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information - any of which can be used for a variety of criminal purposes.
- Bank of America, eBay, and Wells Fargo are among the companies who were spoofed in mass spam mailings.
- One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

Spamming

- **Spam** is abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. People creating spam are called **spammers**
- Spamming may be:
  - E-Mail Spam
  - Instant messaging spam
  - Usenet group spam
  - Web search engine spam
  - Blogs or wiki spam
  - Online classified ads spam
  - Mobile phone messaging spam
  - Internet forum spam
  - Junk fax spam
  - Social networking spam
- Spamming is difficult to control because:
  - spammers have no operating costs beyond the management of their mailing lists
  - difficult to hold senders accountable for their mass mailings

Search Engine Spamming

- Alteration or creation of a document with the intent to deceive an electronic catalog or a filing system
- Some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- **Remedy:** Permanently exclude from the search index

Web Publishing Techniques to Avoid

- Repeating keywords
- Use of keywords that do not relate to the content on the site
- Use of fast meta refresh i.e. change to the new page in few seconds.
- Redirection
- IP cloaking i.e. including related links, information, and terms.
- Use of colored text on the same color background
- Tiny text usage
- Duplication of pages with different URLs
- Hidden links

Cyber Defamation

- An act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyberspace.
- **Example**: Someone publishes defamatory matter about someone on a website or sends an e-mail containing defamatory information to all friends of that person.

What Amount to Defamation?

- If imputation to a deceased person would harm the reputation of that person, and is intended to be hurtful to the feelings of his family or other near relatives
- An imputation is made concerning a company or an association or collection of people as such.
- An imputation in the form of an alternative or expressed ironically
- An imputation that directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person.

Types of Defamation

- **Libel:** written defamation
- **Slander:** oral defamation
- The plaintiff must have to show that the defamatory statements were unlawful and would indeed injure the person's or organization's reputation.
  - If failed to prove, the person who made the allegations may still be held responsible for defamation.

Cyber Defamation Case Examples

- First case of cyber defamation in India (14-Dec-2009),
  - An employee of a corporate defamed its reputation. He was sending derogatory and defamatory emails against the company and its managing director
  - A Delhi Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails.
  - The court passed as important ex-parte injunction.
- In another case, accused posted obscene, defamatory and annoying message about a divorcee woman and sent emails to the victim.
  - Offender was traced and was held guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000.
- Other defamation cases:
  - A malicious customer review by a competitor could destroy a small business.
  - A false accusation of adultery on a social networking site could destroy a marriage.
  - An allegation that someone is a “crook” could be read by a potential employer or business partner

Internet Time Theft

- An unauthorized person uses the Internet hours paid for by another person
- Comes under hacking
- The person get access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means
- Uses the internet without the other person's knowledge
- This theft can be identified when Internet time is recharged often, despite infrequent usage.
- This comes under "identity theft"

Salami Attack / Salami Technique

- Salami are used for committing financial crimes.
- Attackers makes alterations so insignificant that in a single case it would go completely unnoticed.
- **Example:** a bank employee inserts a program, into the bank's server, that deduces a small amount from the account of every customer every month,
  - The unauthorized debit goes unnoticed by the customers, but the employee will make a sizable amount every month.
- Examples:
  - Small "shavings" for Big gains!
  - The petrol pump fraud: delivering a few milli-liter less fuel than actual

Data Diddling

- Data diddling involves changing data input to a computer.
- Information is changed from the way it should be entered by a person typing in the data.
  - data changed by a virus
  - programmer changes database or application to change data
- **Example:** a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.
- To deal with this type of crime, a company must implement policies and internal controls.
- Performing regular audits, using software with built-in features to combat such problems, and supervising employees.
- **Example:** Electricity board in India have been victims to data diddling programs inserted when private parties computerized their systems.

Forgery

- The act of forging something, especially the unlawful act of counterfeiting a document or object for the purposes of fraud or deception.
- Something that has been forged, especially a document that has been copied or remade to look like the original.
- Counterfeit currency notes, postage, revenue stamps, marksheets etc. can be forged using sophisticated computers, printers and scanners.
- **Stamp Paper Scam:** a racket that flourished on loopholes in the system
  - Abdul Karim Telgi, the mastermind of the multi-crore counterfeiting, printed fake stamp papers worth thousands of crores of rupees using printing machines purchased illegally with the help of some conniving officials of the Central Govt.'s Security Printing Press (India Security Press) located in Nasik.
  - These fake stamp papers penetrated in more than 12 states through a widespread network of vendors who sold the counterfeits without any fear and earned hefty commissions.
  - **Amount swindled** Rs. 172 crores

Hacking

- Act committed toward breaking into a computer and/or network is hacking.
- Purpose
  - Greed
  - Power
  - Publicity
  - Revenge
  - Adventure
  - Desire to access forbidden information
  - Destructive mindset

History of Hacking

- Hacking is any technical effort to manipulate the normal behavior of network connections and connected systems.
- A hacker is any person engaged in hacking.
- The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems.
- M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking.
- The so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.
- Later, outside of M.I.T., others began applying the term to less honorable pursuits. for example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.
- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

Hacking V/S Cracking

- Malicious attacks on computer networks are officially known as cracking
- Hacking truly applies only to activities having good intentions
- Most non-technical people fail to make this distinction
- Outside of academia, its extremely common to see the term "hack" misused and be applied to cracks as well

Types of Hackers

- **Black Hats:** Criminal Hackers.
  - Possess desire to destruction
  - Hack for personal monetary gains : Stealing credit card information, transferring money from various bank accounts to their own account, extort money from corporate giant by threatening.
- **White Hats:** Ethical Hackers.
  - Network Security Specialist.
- **Grey Hats:** Deals in both of the above (jack of all trades, master of none).

Case Study 1: NASA Site Hacked thru SQL Injection (2009)

- Two NASA sites recently were hacked by an individual wanting to demonstrate that the sites are susceptible to SQL injection.
- The websites for NASA's Instrument Systems and Technology Division and Software Engineering Division were accessed by a researcher, who posted to his blog screen shots taken during the hack.
- A researcher, using alias "c0de.breaker," used SQL injection to hijack the sites.
- SQL injection is an attack process where a hacker adds additional SQL code commands to a page request and the web server then tries to execute those commands within the backend database
- The NASA hack yielded the credentials of some 25 administrator accounts.
- The researcher also gained access to a web portal used for managing and editing those websites.
- In this particular case, the researcher found the vulnerabilities, made NASA aware of them, then published findings after the websites had been fixed.
- An attacker, however, could have tried to use that web server as an entry point into other systems NASA might control or edit the content of the sites and use them for drive-by downloads.

Case Study 2: Nadia Suleman's Site Hacked (2009)

Case Study 2: Nadia Suleman's Site Hacked (2009) – The Story

- **LOS ANGELES, CA:** Octuplet mom Nadya Suleman launched a website to solicit donations, but it was immediately hacked by a group of vigilante mothers!
- The website originally featured photos of all eight octuplets, a "thank you" note from Suleman, images of children's toys and a large donation button for viewers to send money through. Suleman also provided an address where people can send baby use items.
- The site was hacked and brought down within hours. The original homepage was left up but defaced, as seen in the screenshot.
- The site was tagged by famous hacker group MOD (Mothers of Disappointment). The group has a history of attacking personal sites they disapprove of, including Britney Spears when she hung dry her sons on a clothes after a bath.
- Reporters received a short note from an anonymous e-mail address:
  - *MOD will not tolerate the selfish acts of bad parenting, we will remain true to our mission despite any setbacks viva la maternity (call your mother, she misses you)*
- Site was restored with extra security measures to guard against future attacks.

How do Pedophiles Operate?

- Pedophiles use false identity to trap the children/teenagers.
- Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
- Befriend the child/teen and extract personal information from the child/teen by winning his confidence.
- Get the e-mail address of the child/teen and start making contacts on the victims e-mail address as well.
- Start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him/her is normal and that everybody does it.
- Extract personal information from child/teen.
- At the end of it, the pedophile set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

Software Piracy

- Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
- End-user copying
- Hard disk loading with illicit means
- Counterfeiting
- Illegal downloads from internet

Pirated Software Has a Lot to Loose

- Getting untested software that may have been copied thousands of times
- Potentially may contain hard-ware infecting viruses
- No technical support in case of software failure
- No warranty protection
- No legal right to use the product

Computer Sabotage

- Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage or facilitating criminal conspiracies.
  - Through viruses, worms, logic bombs
- Chernobyl virus
  - The Chernobyl virus is a computer virus with a potentially devastating payload that destroys all computer data when an infected file is executed
- Y2K virus
  - **Y2K bug** also called Year 2000 bug or Millennium Bug is a problem in the coding of computerized systems that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000

E-Mail Bombing / Mail Bombs

- An ***email bomb*** is a form of net abuse consisting of sending huge volume of *emails* to an address in an attempt to overflow the mailbox or overwhelm the server where the *email* address is hosted in a denial-of-service attack.
- Configures a computer to repeatedly send emails to a specified person's email address.
- It overwhelm the recipient's personal account and potentially can shut down the entire system.

Network Intrusion

- An intrusion to computer network from any where in the world and steal data, plant viruses, create backdoors, insert trojan horse or change passwords and user names.
- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- Use of strong password, well configured firewalls and dedicated IDS safeguard against Network Intrusion.

Password Sniffing

- Password sniffers are programs that monitor and record the authentication details (name and password) of network users as they login, jeopardizing security at a site.
- Once authentication details are found out (using sniffers), one can impersonate an authorized user and access restricted systems/information.

Credit Card Frauds

- **Credit card fraud** is a term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying or to obtain unauthorized funds from an account.
- Credit card fraud is also an adjunct to identity theft.

Identity Theft

- Identity theft is a fraud involving another person's identity for an illicit purpose.
- The criminal uses someone else's identity for his/ her own illegal purposes.
- Phishing and identity theft are related offenses
- Examples:
  - Fraudulently obtaining credit
  - Stealing money from victim's bank account
  - Using victim's credit card number
  - Establishing accounts with utility companies
  - Renting an apartment
  - Filing bankruptcy using the victim's name

Identity Theft: Real Cases

- **Dr. Gerald Barnes**
  Gerald Barnbaum lost his pharmacist license after committing Medicaid fraud. He stole the identity of Dr. Gerald Barnes and practiced medicine under his name. A type 1 diabetic died under his care. “Dr. Barnes” even worked as a staff physician for a center that gave exams to FBI agents. He’s was prisoned for this.
- **Andrea Harris-Frazier**
  Margot Somerville lost her wallet on a trolley. Andrea Harris-Frazier had defrauded several banks - using Somerville’s identity - out of tens of thousands of dollars. Two years later she was arrested.
- **Abraham Abdallah**
  A busboy named Abraham Abdallah got into the bank accounts of Steven Spielberg and other famous people after tricking his victims via computer, getting sufficient data to fake being their financial advisors - then calling their banks…and you know the rest.

Cyber Crime: Legal Perspective

- Cybercrime possess a mammoth challenge
- Computer crime: Criminal Justice Resource Manual (1979)
  - Any illegal act for which knowledge of computer technology is essential for a successful prosecution.
- International legal aspects of computer crimes were studied in 1983
  - Encompasses any illegal act for which the knowledge of computer technology is essential for its perpetration

Cyber Crime: Legal Perspective…

- The network context of cyber crime make it one of the most globalized offenses of the present and most modernized threats of the future.
- Solution:
  - Divide information system into segments bordered by state boundaries. Not possible and unrealistic because of globalization
  - Incorporate the legal system into an integrated entity obliterating these state boundaries.

Cyber Crime: Indian Perspective

- India has the fourth highest number of internet users in the world.
- 350+ million internet users in India
- 37% - in cyber cafes
- 57% are between 18 and 35 years
- Information Technology (IT) Act, 2000, specifies the acts which are punishable. The primary objective of this Act is to create an enabling environment for commercial use of IT

Cyber Crime: Indian Perspective…

- 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006)
- Thereby reporting an increase of 52.8% in 2007 over 2006.
- 22.3% cases (49out of 217 cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

Incidence of Cyber Crime in Cities (2006 v/s 2007)

- 17 out of 35 mega cities did not report any case of Cyber Crime i.e, neither under the IT Act nor under IPC Sections) during the year 2007.
- 17 mega cities have reported 118 cases under IT Act and 7 megacities reported 180 cases under various section of IPC.
- There was an increase of 32.6% (from 89 cases in 2006 to 118 cases in 2007) in cases under IT Act as compared to previous year (2006),
- An increase of 26.8% (from 142 cases in 2006 to 180 cases in 2007) of cases registered under various section of IPC
- Bengaluru (40), Pune (14) and Delhi (10) cities have reported high incidence of cases (64 out of 118 cases) registered under IT Act, accounting for more than half of the cases (54.2%) reported under the Act.

Thank You