



National Conference of CIRC On Corporate laws-

Ghaziabad, 20th & 21st Dec 2008

Cybercrimes and legal enforcement in
India...

Karnika Seth
Cyber-lawyer & IP Expert

Partner,
SETH ASSOCIATES

ADVOCATES AND LEGAL CONSULTANTS

© copyrighted Seth Associates Dec 2008

Introduction to Cyber Crime

- **Computer Crime, E-Crime, Hi-Tech Crime or Electronic Crime** is where a computer is the target of a crime or is the means adopted to commit a crime.
- Most of these crimes are not new. Criminals simply devise different ways to undertake standard criminal activities such as fraud, theft, blackmail, forgery, and embezzlement using the new medium, often involving the Internet



Computer vulnerability

- **Computers store huge amounts of data in small spaces**
- Ease of access
- Complexity of technology
- Human error
- One of the key elements that keeps most members of any society honest is fear of being caught — the deterrence factor. Cyberspace changes two of those rules. First, it offers the criminal an opportunity of attacking his victims from the remoteness of a different continent and secondly, the results of the crime are not immediately apparent.
- Need new laws and upgraded technology to combat cyber crimes



CYBERCRIME UP BY 368% IN 2 YEARS

Mostly Women At The Receiving End Of Cyberbullying

Times News Network

Ahmedabad: It's not financial frauds alone but there has been a rise in the number of cases involving cyberbullying, threats and posting obscene sexual materials against women, which are being noticed by the state police over the last five years. In 2022, there were 5,238 cases involving social media accounts and in most cases more than 75% to 80% cases involved women.

According to the National Crime Research Bureau (NCRB), in Gujarat the most significant period for reporting such cases was between 2017 and 2020 where cases rose from 94 to 277 in 2020 — mainly involving cyber blackmailing, threatening, cyberbullying and posting of obscene contents pertaining to the victims. In all, 761 cases involving women victims were reported by the state police till 2020.

In 2021 and 2022, quite significantly cyber trafficking cases were reported where perpetrators fake a romantic relationship with the victims on social media to ex-



plot them. The cases reported by the CID crime were 32 and 46 cases respectively for the two years.

Post-pandemic, which is between two years, 2021 and 2022, cybercrime complaints have risen

368% — from 17,227 cases in 2021 to 70,183 in 2022. This stupendous rise in overall cybercrime cases is because of a 536% rise in just online financial fraud cases — from

11,133 cases in 2021 to 70,183 in 2022.

SBI cybercrime, Subodh Oshwara adds, "The biggest trap for victims of cyber fraud is the customer care numbers that appear against any services you search on Google, Be it banks, airline services, hospitals and other such services. One has to verify first whether it is a genuine site. We have been updating various search engines of these fraud numbers that appear on the first page."

CID crime Cybercell, DySP B M Tank told TOL, "Cybercriminals feed on the victim's greed, fears and laziness to con them. They use the same social engineering template — whether it be online shopping, electricity bill fraud or loan apps — of engaging them in a talk and then nudging them to click a link, or share their OTPs. Gujarat has witnessed a steep rise in such complaints since the Covid pandemic."

Crypto crimes double in a year in Guj

Cybercrimes Complaints Zoom From 17,000 in 2021 To 80,000 In 2022

Paul.John@timesgroup.com

Ahmedabad: A city-based trader was in shock when he got to know that his digital wallet used for his cryptocurrency peer-to-peer (p2p) trading was frozen by authorities. The wallet came under the scanner when it got payment for a batch of crypto sale from an unverified account from the dark web. Along with losing his legitimate cryptocurrency, the trader also came under the scanner of the cyber watchdogs.

This is just one of the 192 applications received by the national cybercrime helpline (1930) from the state in 2022. A rough calculation indicates that the state recorded one case every two days. The total



number had doubled from just 79 in 2021. City-based cybercrime experts said that in several of these cases, it's either greed or gullibility. Sunny Vaghela, a city-based cybersecurity expert, said that many just take to cryptocurrency with the lure of making quick bucks. "But when it comes to safety fe-

atures including use of escrow accounts or third-party apps, they are often not in place. The hackers exploit the vulnerabilities and target such transactions - in some cases, large sums are transferred within seconds," he said, adding that the complaints are still less due to possible involvement of

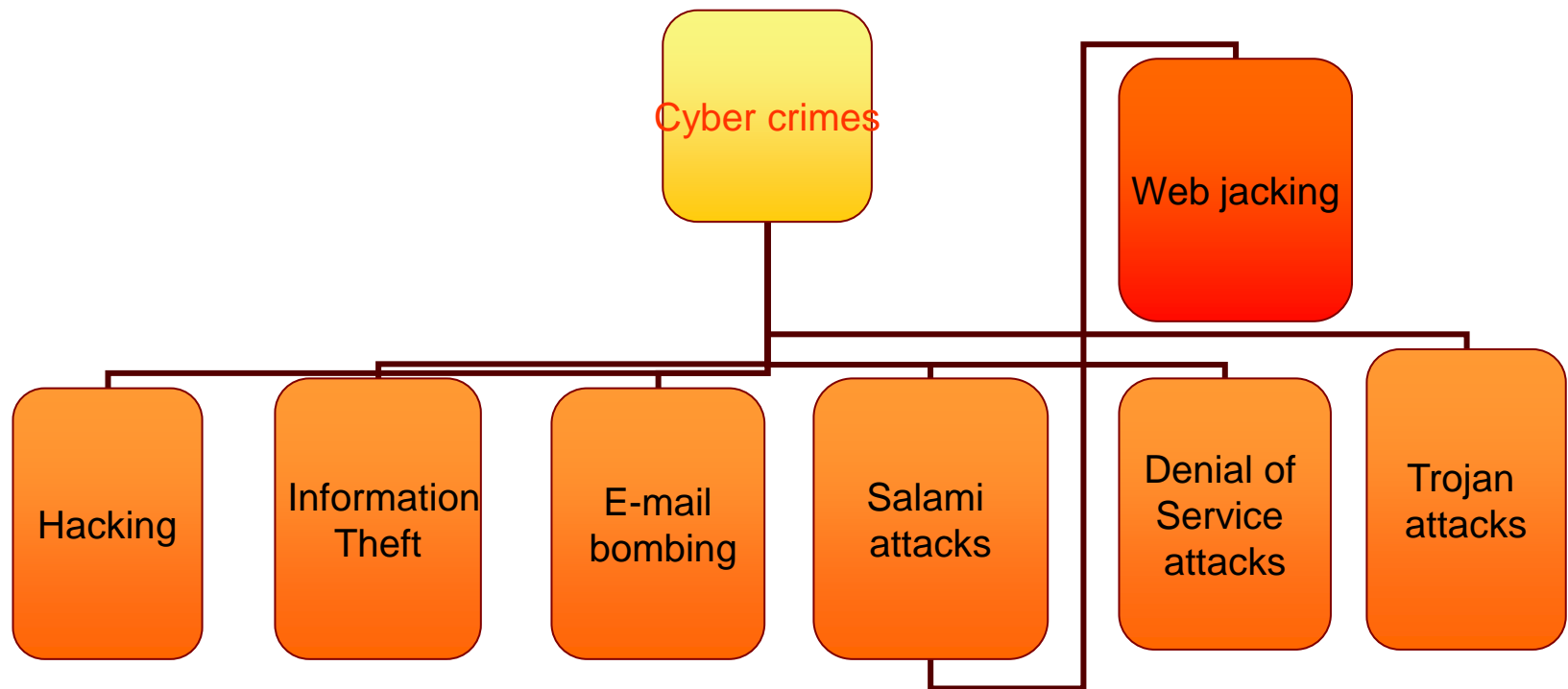
unaccounted cash.

But it's not just crypto - the trend of high number of frauds, cheating, extortion, gaming and even hacking that started in Covid years due to high dependency on digital devices continued in 2022. According to the state-based coordinators of National Cyber Crime Reporting Portal (NCCRP), the annual cases skyrocketed from 17,337 in 2021 to 80,681 in 2022. In simpler terms, the calls for help or applications of complaint rose from 47 to 221 daily on an average.

Among major categories, financial fraud accounted for 87% of the total complaints at 70,183, followed by social media-related crimes at 5,188.

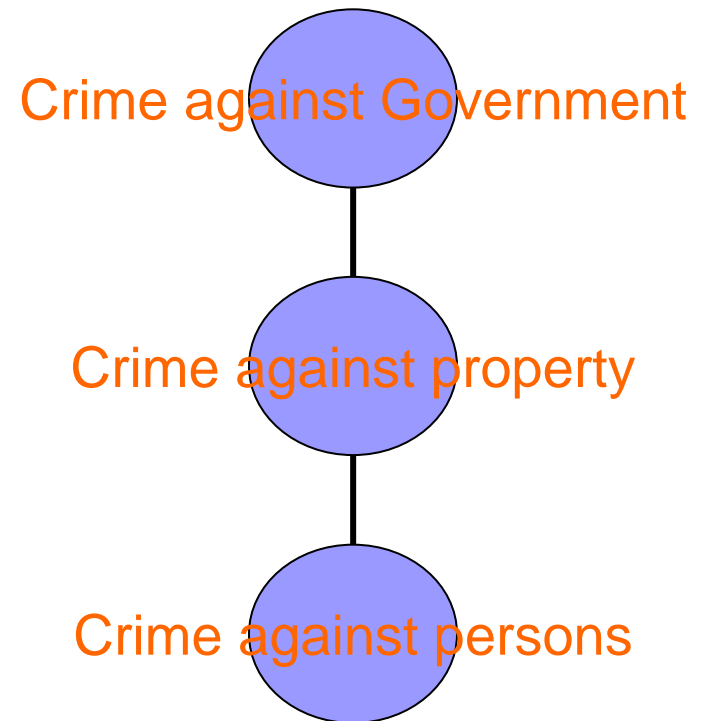
► Continued on P 2

Different Types of Cybercrimes



Types of Cyber crimes

- Credit card frauds
- Cyber pornography
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Defamation
- Cyber stalking (section 509 IPC)
- Phising
- Cyber terrorism





TYPES OF CYBER CRIMES

E-Mail bombing: Email bombing refers to sending a large amount of e-mails to the victim resulting in interruption in the victims' e-mail account or mail servers.

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

Salami attacks: These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer

Denial of Service: This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.



Some common cybercrimes...

- **Phishing, the mass distribution of “spoofed” e-mail messages, which appear to come from banks, insurance agencies, retailers or credit card companies and are designed to fool recipients into divulging personal data such as account names, passwords, or credit card numbers.**
- **“Carding,” which entails using stolen credentials (and can include package reshipping, money moving, and identity theft schemes)**
- **Compromised servers or “bots,” which may be launching cyber attacks or sending Spam**

Cyber Crime Data In Regional Context

■ Carding:-

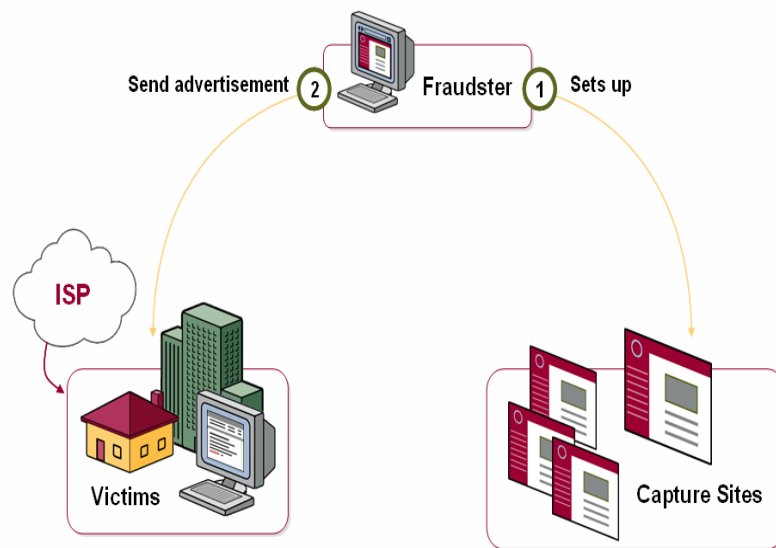
Carding is a serious threat to India, as it does not require a high degree of sophistication and is considered particularly pernicious by international financial institutions and e-commerce providers.

■ Bots:-

Bots, compromised servers that may be launching cyber attacks or sending Spam, were detected in the India IP space, including servers with the domain name.

■ Phishing:-

ISPs were able to point to a few examples of phishing capture sites being located on their servers, one targeting eBay (a frequent attack point for phishers).





Computer Viruses

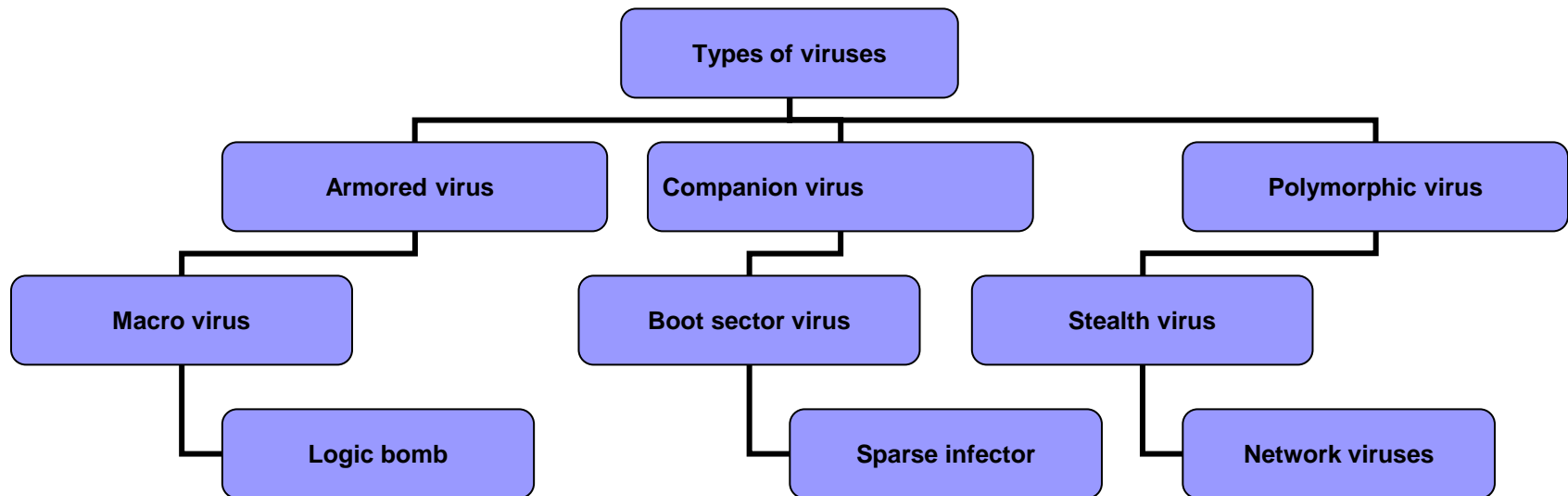
- **Viruses**
- **A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Note that a program does not have to perform outright damage (such as deleting or corrupting files) in order to be called a "virus".**
- **A computer virus is a program that can copy itself and infect a computer without permission or knowledge of the user.**



Why Do people Create These Viruses?

- To distribute political message.
- To attack the products of specific companies.
- Some consider their creations to be works of art, and see as a creative hobby.
- Financial gain from identity theft

Types of Viruses



Cyber Threats

Cyber Threats

- **Cyber threats to a control system refer to persons who attempt unauthorised access to a control system device and network using a data communications pathway.**
- **Main threats to cyber crime is Hacking.**
Hacking involves gaining unauthorised access to a computer and altering the system in such a way as to permit continued access, along with changing the configuration, purpose, or operation of the target machine, all without the knowledge or approval of the systems owners.



absents

- 84
- 88
- 127
- 208
- vivek



New Internet Threats

- **All computers need internet security**

Home users can lose valuable personal data with one click to the wrong website. Children trading games also exchange viruses unknowingly. You receive an email requesting an update to your payment details, and a hacker gains access to your bank account. A backdoor is installed on your machine, and your PC becomes a zombie, spewing out spam.

- **New technologies - new anti-malware solutions**

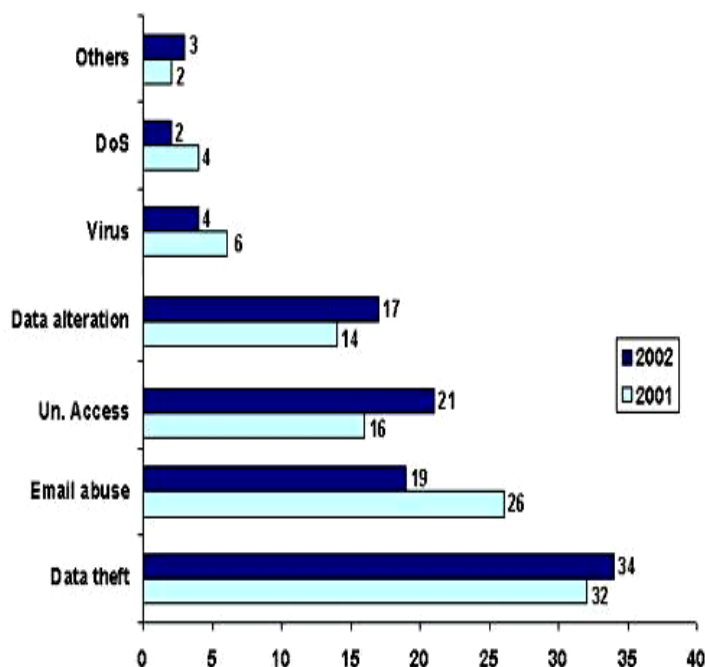
As cyber threats have evolved, so has software to deflect such threats. Sophisticated antispyware and antivirus solutions capable of detecting the most complex new viruses are now available.

What Is Spam

- Spam is the equivalent of physical junk mail and unsolicited telemarketing phone calls. It has become one of the largest nuisances to computer users for both home and business users.
- There are two main types of spam, and they have different effects on Internet users. Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at "lurkers", people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.
- Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.

Frequency of incidents of Cyber crimes in India

INCIDENT WISE BREAK UP



Denial of Service: Section 43

Virus: Section: 66, 43

Data Alteration: Sec. 66

U/A Access: Section 43

Email Abuse: Sec. 67,
500, Other IPC Sections

Data Theft: Sec 66, 65

Source: Survey conducted by ASCL

Frequency of reporting Cyber crimes in India

- During the year 2005, 179 cases were registered under IT Act as compared to 68 cases during 2004. 21.2% cases reported from Karnataka, followed by Maharashtra(26) , Tamil Nadu(22) and Chhattisgarh and Rajasthan (18 each) out of 179 cases, 50% were related to Section 67 IT Act., 125 persons were arrested. 74 cases of hacking were reported wherein 41 were arrested.

Combating cyber crimes

- **Technological measures-** Public key cryptography, Digital signatures ,Firewalls, honey pots
- **Cyber investigation-** Computer forensics is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in courts of law.
- These rules of evidence include admissibility (in courts), authenticity (relation to incident), completeness, reliability and believability.
- **Legal framework-laws & enforcement**



Combating Cyber crime-Indian legal framework

- Information Technology Act, 2000-came into force on 17 October 2000. Information technology Act 2000 consists of 94 sections segregated into 13 chapters. Four schedules form part of the Act.
- Extends to whole of India and also applies to any offence or contravention there under committed outside India by any person {section 1 (2)} read with Section 75- Act applies to offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India
- Section 2 (1) (a) –"Access" means gaining entry into ,instructing or communicating with the logical, arithmetic or memory function resources of a computer, computer resource or network
- IT Act confers legal recognition to electronic records and digital signatures (section 4,5 of the IT Act,2000)

Civil Wrongs under IT Act

- Chapter IX of IT Act, Section 43
- Whoever without permission of owner of the computer
 - Secures access (mere U/A access)
 - Not necessarily through a network
 - Downloads, copies, extracts any data
 - Introduces or causes to be introduced any viruses or contaminant
 - Damages or causes to be damaged any computer resource
 - Destroy, alter, delete, add, modify or rearrange
 - Change the format of a file
 - Disrupts or causes disruption of any computer resource
 - Preventing normal continuance of computer

Civil Wrongs under IT Act (Contd.)

- ☐ Denies or causes denial of access by any means
 - Denial of service attacks
- ☐ Assists any person to do any thing above
 - Rogue Websites, Search Engines, Insiders providing vulnerabilities
- ☐ Charges the services availed by a person to the account of another person by tampering or manipulating any computer resource
 - Credit card frauds, Internet time thefts
- ☐ Liable to pay damages not exceeding Rs. One crore to the affected party
- ☐ Investigation by
- ☐ ADJUDICATING OFFICER
- ☐ Powers of a civil court

Data diddling: changing data prior or during input into a computer

- Section 66 and 43(d) of the I.T. Act covers the offence of data diddling
- Penalty: Not exceeding Rs. 1 crore

Case in point :

NDMC Electricity Billing Fraud Case: A private contractor who was to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in his bank who misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Section 46 IT Act

- *Section 46* of the IT Act states that an adjudicating officer shall be adjudging whether a person has committed a contravention of any of the provisions of the said Act, by holding an inquiry. Principles of Audi alterum partum and natural justice are enshrined in the said section which stipulates that a reasonable opportunity of making a representation shall be granted to the concerned person who is alleged to have violated the provisions of the IT Act. The said Act stipulates that the inquiry will be carried out in the manner as prescribed by the Central Government
- All proceedings before him are deemed to be judicial proceedings, every Adjudicating Officer has all powers conferred on civil courts
- Appeal to cyber Appellate Tribunal- from decision of Controller, Adjudicating Officer {section 57 IT act}

Section 47, IT Act

- Section 47 of the Act lays down that while adjudging the quantum of compensation under this Act, the adjudicating officer shall have due regard to the following factors, namely-
- (a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- (b) the amount of loss caused to any person as a result of the default;
- (c) the repetitive nature of the default

Cybercrime provisions under IT Act,2000

Offence

Relevant Section under IT Act

Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

Section 65: Source Code

- Most important asset of software companies
- “Computer Source Code” means the listing of programmes, computer commands, design and layout
- Ingredients
 - Knowledge or intention
 - Concealment, destruction, alteration
 - computer source code required to be kept or maintained by law
- Punishment
 - imprisonment up to three years and / or
 - fine up to Rs. 2 lakh

Section 66: Hacking

- **Ingredients**
 - Intention or Knowledge to cause wrongful loss or damage to the public or any person
 - Destruction, deletion, alteration, diminishing value or utility or injuriously affecting information residing in a computer resource
- **Punishment**
 - imprisonment up to three years, and / or
 - fine up to Rs. 2 lakh
- **Cognizable, Non Bailable,**

Section 66 covers data theft aswell as data alteration

Sec. 67. Pornography

- Ingredients
 - ☐ Publishing or transmitting or causing to be published
 - ☐ in the electronic form,
 - ☐ Obscene material
- Punishment
 - ☐ On first conviction
 - imprisonment of either description up to five years and
 - fine up to Rs. 10 lakh
 - ☐ On subsequent conviction
 - imprisonment of either description up to seven years and
 - fine up to Rs. 10 lakh
- Section covers
 - ☐ Internet Service Providers,
 - ☐ Search engines,
 - ☐ Pornographic websites
- Cognizable, Non-Bailable, JMFC/ Court of Sessions

Computer Related Crimes under IPC and Special Laws

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act
Web - Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

Some more offences dealt with under IPC...

- Criminal breach of trust/Fraud- Sec. 405,406,408,409 IPC
- Destruction of electronic evidence- Sec.204,477 IPC
- False electronic evidence-Sec.193 IPC
- Offences by or against public servant- Sec.167,172,173,175 IPC

Email spoofing:

- Pranab Mitra , former executive of Gujarat Ambuja Cement posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe an Abu Dhabi businessmen . After long cyber relationship and emotional messages Mitra sent an e-mail that “she would commit suicide” if Ninawe ended the relationship. He also gave him “another friend Ruchira Sengupta’s” e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died and police is searching Ninawe. Mitra extorted few lacs Rupees as advocate fees etc. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.



Legal provisions to counter identity theft

- The IT Act 2000 in its present form does not have any specific provision to deal with identity theft. However, the Expert Committee on Amendments to the IT Act 2000 (whose report is presently under consideration by the government for adoption) has recommended amending the Indian Penal Code (IPC) by inserting in it two new sections:
- section 417A which prescribes punishment of up to 3 years imprisonment and fine for 'cheating by using any unique identification feature of any other person'; and
- section 419A that prescribes punishment of up to 5 years imprisonment and fine for 'cheating by impersonation' using a network or computer resource.

Forgery

■ Andhra Pradesh Tax Case

In the explanation of the Rs. 22 Crore which was recovered from the house of the owner of a plastic firm by the sleuths of vigilance department, the accused person submitted 6000 vouchers to legitimize the amount recovered, but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted . All vouchers were fake computerized vouchers.

Cyber stalking

- Ritu Kohli (first lady to register the cyber stalking case) is a victim of cyber-stalking. A friend of her husband gave her phone number and name on a chat site for immoral purposes. A computer expert, Kohli was able to trace the culprit. Now, the latter is being tried for "outraging the modesty of a woman", under Section 509 of IPC.

Cyber defamation

- ***SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra***: India's first case of cyber defamation was reported when a company's employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company.

The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Online gambling: virtual casinos, Cases of money laundering

- **Cyber lotto case:** In Andhra Pradesh one Kola Mohan created a website and an email address on the Internet with the address 'eurolottery@usa.net.' which shows his own name as beneficiary of 12.5 million pound in Euro lottery. After getting confirmation with the email address a telugu newspaper published this as news. He gathered huge sums from the public as well as from some banks. The fraud came to light only when a cheque amounting Rs 1.73 million discounted by him with Andhra bank got dishonored.



FIR NO 76/02 PS PARLIAMENT STREET

- **Mrs. SONIA GANDHI RECEIVED THREATING E-MAILS**
- **E- MAIL FROM**
 - missionrevenge84@khalsa.com
 - missionrevenge84@hotmail.com
- **THE CASE WAS REFERRED**
- **ACCUSED PERSON LOST HIS PARENTS DURING 1984 RIOTS**

Cyber Crime Online Challenges

Brand exploitation

Unauthorized use of trademarks

**Increased difficulty in managing
online distribution channel**

Sale of counterfeit goods





Current online Environment

- **Easy to “hide in plain sight”**
- **Easy to confuse customers due to the high quality of digital copies**
- **Difficult to track infringements**
- **Easy to establish a professional-looking website**



Common Forms of Online Threats

Trademark and Brand Infringement

Domain Name

- Commercial sites (e.g., offensive content or competing companies)
- Domain name monetization (e.g., click-through advertising)
- Unhappy consumer sites (e.g., xxx-sucks. COM) (generally, protected)
- Sale of Counterfeit Goods in Auction Sites
- Logo, Text, and Meta Tag Use in Commercial Sites
- Stopping unauthorized parties from using your trademarks
- Managing partners use of logos and trademarks
- Protecting against “Google bombing”

Domain theft

- **Domain theft** is an aggressive form of domain hijacking that usually involves an illegal act. In most cases, identity theft is used to trick the domain registrar into allowing the hijacker to change the registration information to steal control of a domain from the legitimate owner.
- Some registrars are quick to set things right when these cases are discovered. However, it is well documented that some registrars will admit no fault in accepting the forged credentials and will refuse to correct the record until forced by legal action. In many of these cases, justice is not done and the hijacker retains control of the domain.



Challenges of Cyber Security

The Environment

- **Explosion of computer and broadband internet availability (over a billion internet users today).**
- **Low priority of security for software developers.**
- **Challenge of timely patching vulnerabilities on all systems.**
- **Graphical user interface (GUI) based tools that exploit known software vulnerabilities.**

Electronic World

- Electronic document produced by a computer. Stored in digital form, and cannot be perceived without using a computer
 - It can be deleted, modified and rewritten without leaving a mark
 - Integrity of an electronic document is “genetically” impossible to verify
 - A copy is indistinguishable from the original
 - It can't be sealed in the traditional way, where the author affixes his signature
- The functions of identification, declaration, proof of electronic documents carried out using a digital signature based on cryptography.





Electronic World

- Digital signatures created and verified using cryptography
- Public key System based on Asymmetric keys
 - An algorithm generates two different and related keys
 - Public key
 - Private Key
 - Private key used to digitally sign.
 - Public key used to verify.



Public Key Infrastructure

- Allow parties to have free access to the signer's public key
- This assures that the public key corresponds to the signer's private key
 - Trust between parties as if they know one another
- Parties with no trading partner agreements, operating on open networks, need to have highest level of trust in one another

Role of the Government

- Government has to provide the definition of
 - the structure of PKI
 - the number of levels of authority and their juridical form (public or private certification)
 - which authorities are allowed to issue key pairs
 - the extent to which the use of cryptography should be authorised for confidentiality purposes
 - whether the Central Authority should have access to the encrypted information; when and how
 - the key length, its security standard and its time validity



Section 3 Defines Digital Signatures

- The authentication to be affected by use of asymmetric crypto system and hash function
- The private key and the public key are unique to the subscriber and constitute functioning key pair
- Verification of electronic record possible

Secure digital signature-S.15

- If by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was:
 - (a) unique to the subscriber affixing it;
 - (b) capable of identifying such subscriber;
 - (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated,then such digital signature shall be deemed to be a secure digital signature



IT Act –overview of other relevant provisions

- Section 16- Central Government to prescribe security procedures
- Sec 17 to 34- Appointment and Regulation of Controller and certifying authority
- Sec 35 to 39- Obtaining DSC
- Sec 40 to 42- Duties of Subscriber of DSC- exercise due care to retain the private key



Threats to cyber security- Methods Used To Penetrate Victim Machines

- Trojan droppers and downloaders injected into pirate software which is distributed via file sharing p2p networks (kazaa, eDonkey etc.)
- Exploiting vulnerabilities in MS Windows and popular applications such as IE & Outlook.
- Email worms



Password Authentication protocol

- Password authentication protocol, sometimes abbreviated PAP, is a simple authentication protocol used to a network access server used for example by internet service provider. PAP is used by point to point protocol. Authentication is a process of validating a user before allowing them access to server resources. Almost all network operating system remote servers support PAP.



10 Ways To Wireless Security

- **Use encryption - chances are bad guys won't bother breaking it.**
- **Use strong encryption - in case they are trying to break it, make it harder for them.**
- **Change the default admin password - avoid using 'password as the password.**
- **Turn off SSID broadcasting - don't 'shout' to everybody in the neighborhood "come and try me."**
- **Turn off WAP when not in use - do you leave your TV on running when you are not at home?**



10 Ways To Wireless Security

- **Change your default SSID - yes, there are at least 50 other 'linksys' stations around, and they are easier to find.**
- **Use MAC filtering - you give keys to your home only to trusted people - do the same with the wireless network.**
- **Isolate the wireless LAN from the rest of the network - why did you think Titanic sank? Create levels of protection.**
- **Control the wireless signal - unless you want to power the whole city, there is no need to use signal amplifiers.**
- **Transmit on a different frequency - this is why we haven't intercepted the aliens yet**


Protection of Personal Information

- **Identifying Purposes:-** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
- **Accuracy:-** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
- **Safeguards:-** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- **Accountability:-** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
- **Openness:-** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.



Recommended cyber safety tips

- **Use antivirus softwares**
- **change passwords frequently**
- **insert firewalls**
- **Adopt regular scanning against spyware**
- **install software patches**
- **uninstall unnecessary software**
- **separate user accounts**
- **maintain backup**
- **check security settings**
- **Perform IT audits**



In case you have any queries ...please feel
free to write in at
Karnika@sethassociates.com

SETH ASSOCIATES

ADVOCATES AND LEGAL CONSULTANTS

Corporate Law Office:

B-10, Sector 40, NOIDA-201301, N.C.R, India

Tel: +91 (120) 4352846, +91 9810155766

Fax: +91 (120) 4331304

E-mail: mail@sethassociates.com