Cyber Crimes &

Law dealing with Cyber Crimes

By Neeraj Aarora

Advocate, Supreme Court
CISSP, CISA, FCMA, CEH, CFCE

Learning Objectives

- Recent Challenges of Cyber Crimes
- Regulatory Framework of IT Act
- Cyber Contravention / Cyber Offences
- Privacy of Data
- Liability of ISP
- Liabilities of Company

Ransomware- Cyber Laundering

- Mails along with pdf are being sent.
- Virus, Cryptowall encrypts the hard drive.
- Also encrypt the external or shared drives.
- Hackers demand money in BitCoin
- Layering to misappropriate
- Difficult to decrypt the data.

Cryptolocker

Denial-of-Service - Estonia's Hack Attack

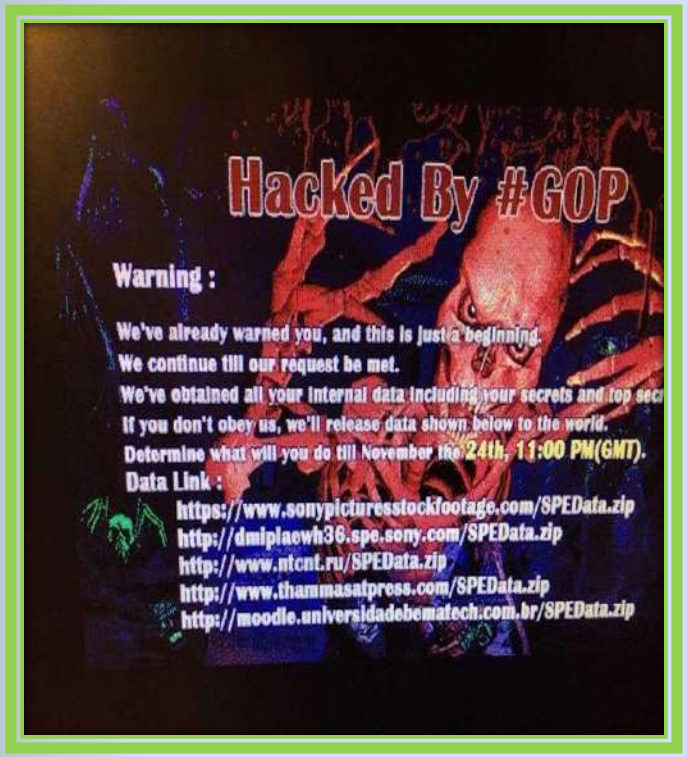
- DDOs Attacks against Estonian Websites.
- First Accessed other People's Computers through Zombie Applications.
- Estonian Attack relied on vast Botnets to send Coordinated Crash-inducing Data to Web Servers.
- Freezed complete infrastructure

Virus Live Case – Stuxnet

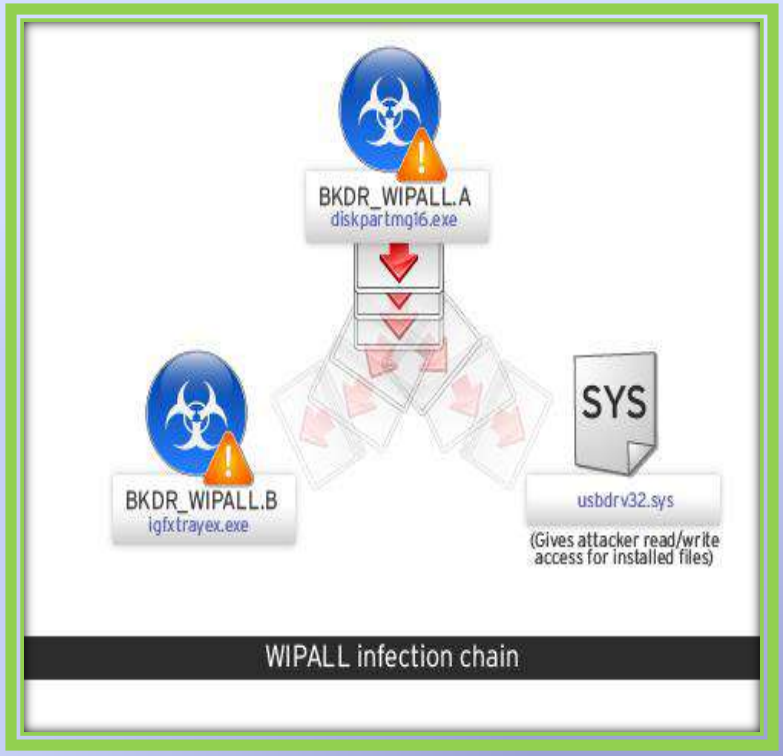
- **Very Effective, Size: 500 KiloByte.**
- **Attacked in Three Phases**
  - it targets Microsoft Windows Machines and Networks.
  - Sought Out Siemens Step7 software (Windows-based used to Program Industrial Control Systems that Operate Equipment, such as Centrifuges).
  - Compromised Programmable Logic Controllers.
- **Spy on Industrial Systems and even Cause Fast-Spinning Centrifuges to Tear themselves apart.**
- **Can Spread Stealthily Between Computers running Windows.**
- **Can Spread through USB thumb Drive.**

Sony Hack Case

Employee Computer Desktop



Wiper Malware…



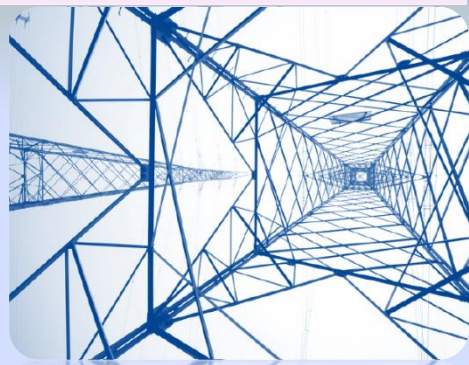
Hackers Hit J.P. Morgan- Cyber Laundering

- Russian hackers attacked the U.S. financial system in mid-August, infiltrating and stealing data from JP Morgan Chase & Co.
- Theft of sensitive data belonging to customer of JP Morgan.
- Attack was done using a malware.
- Misappropriate money converted to legal through layering.

'iCloud' Naked Celebrity Photo Leak

Jennifer Lawrence

Hack of Ukraine's Powergrid



- Send spyware to employees and asked to click on micros
- Hackers used a program called BlackEnergy3
- Infected their machines and opened a backdoor to the hackers.
- Hackers harvested worker credentials for VPNs which was used to remotely log in to the SCADA network.

Hack of Ukraine's Powergrid

- Reconfigured uninterruptible power supply to control centers.
- Replace malicious firmware on serial-to-Ethernet converters at substations.
- Entered SCADA networks through hijacked VPNs and disable UPS systems.
- Launched Telephone Denial-of-Service attack against customer call centers to prevent reporting for outrage.
- Used malware 'KillDisk' to wipe files from operator stations.

Blackout

Digital Certificates Breaches

- Comodo Attack
- DigiNotar Attack
- Stuxnet Attack
- NIC CA Attack
- ANSSI Attack

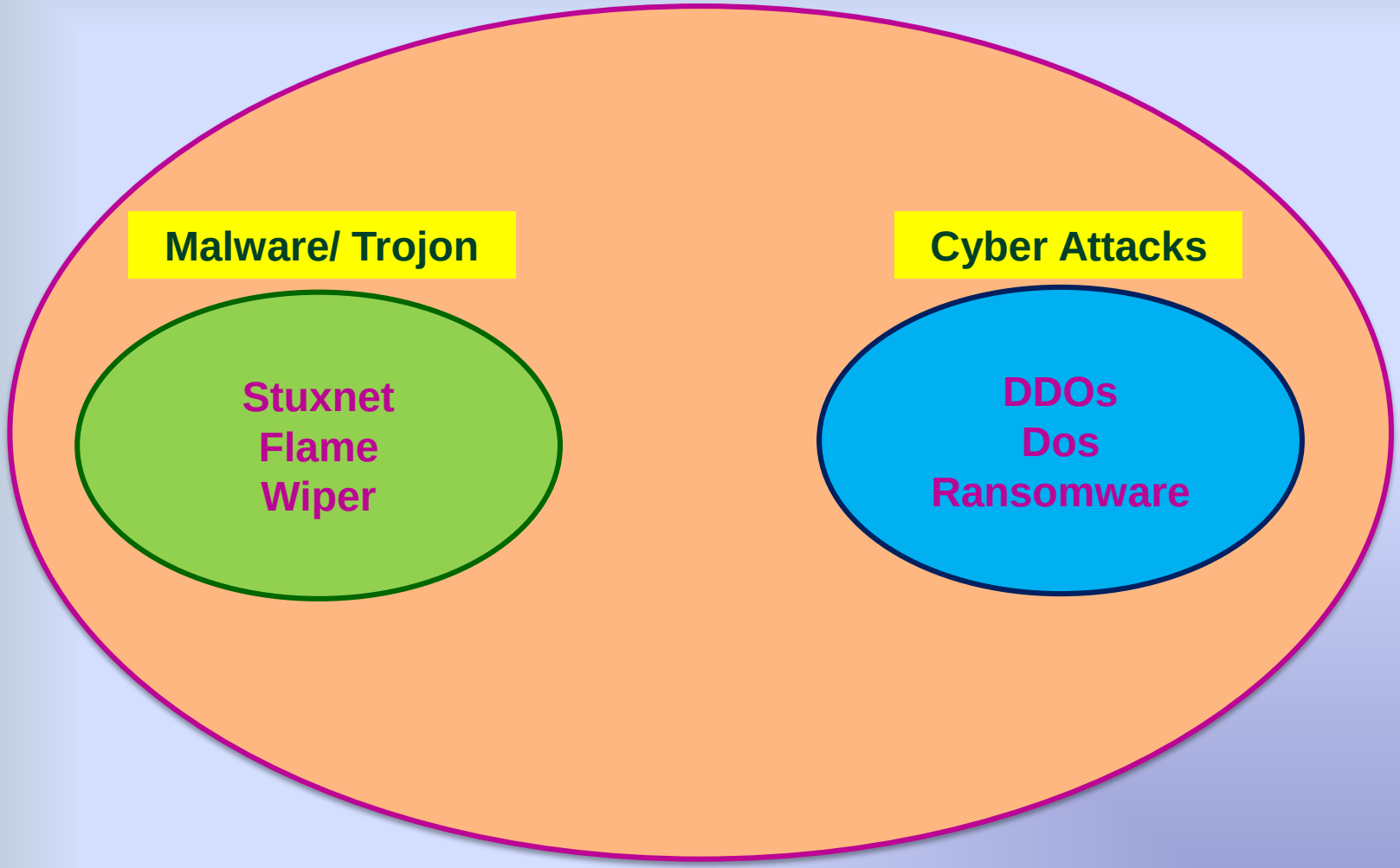
Bit Coin – Virtual Currency

- Not in control of any Country
- Anonymity on the Internet
- International movement without restrictions
- Acceptable for Hawala /Crime Transactions
- Replace the gold or cash as a payment for illegal transaction or tax evasion

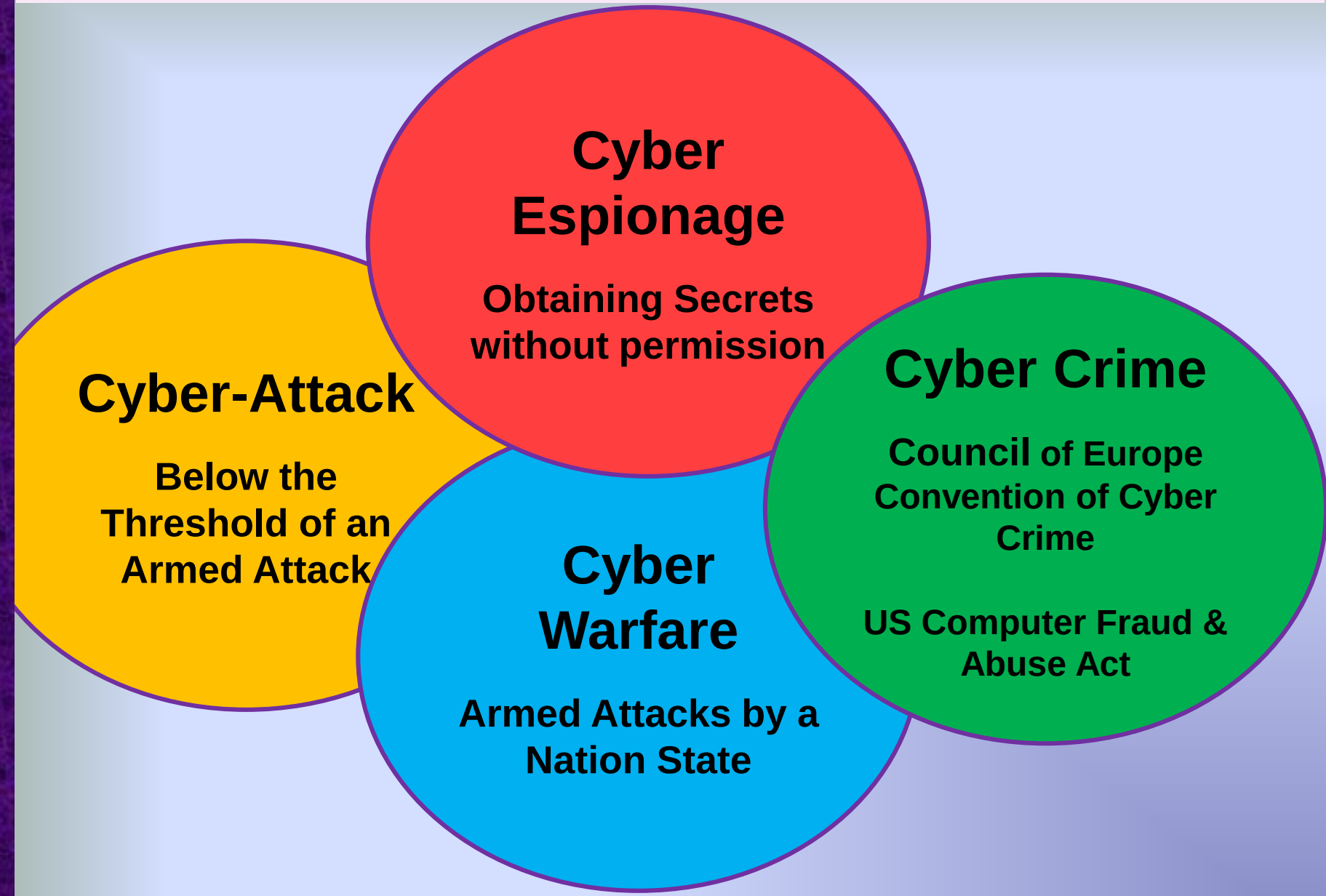
Cybercrime Economy

- **Ransomware**
  - organized at international & national level
  - Segmented & Coordinated
- **Darknet**
  - Sale of Vulnerabilities and exploits online
  - Crime ware tool kits
  - Stolen data Credit card numbers, PINs
  - Email ids, passwords
  - FTP credentials
  - Sale of Botnets
  - DDoS as a Service
  - Hacking as a Service

Cyber Warfare and Cyber terrorism



Distinguishing Among Cyber Events



Processing an Attack

- Is this an Act of War, A Crime or Espionage?
- Can I Attribute the attack ?
- What is the proper response?
- How can risk be reduced?

Section 66F- "Cyber Terrorism"

Whoever ,

(1) with the intent to threaten the unity,

integrity, security or sovereignty of India or to strike terror in any section of the people.

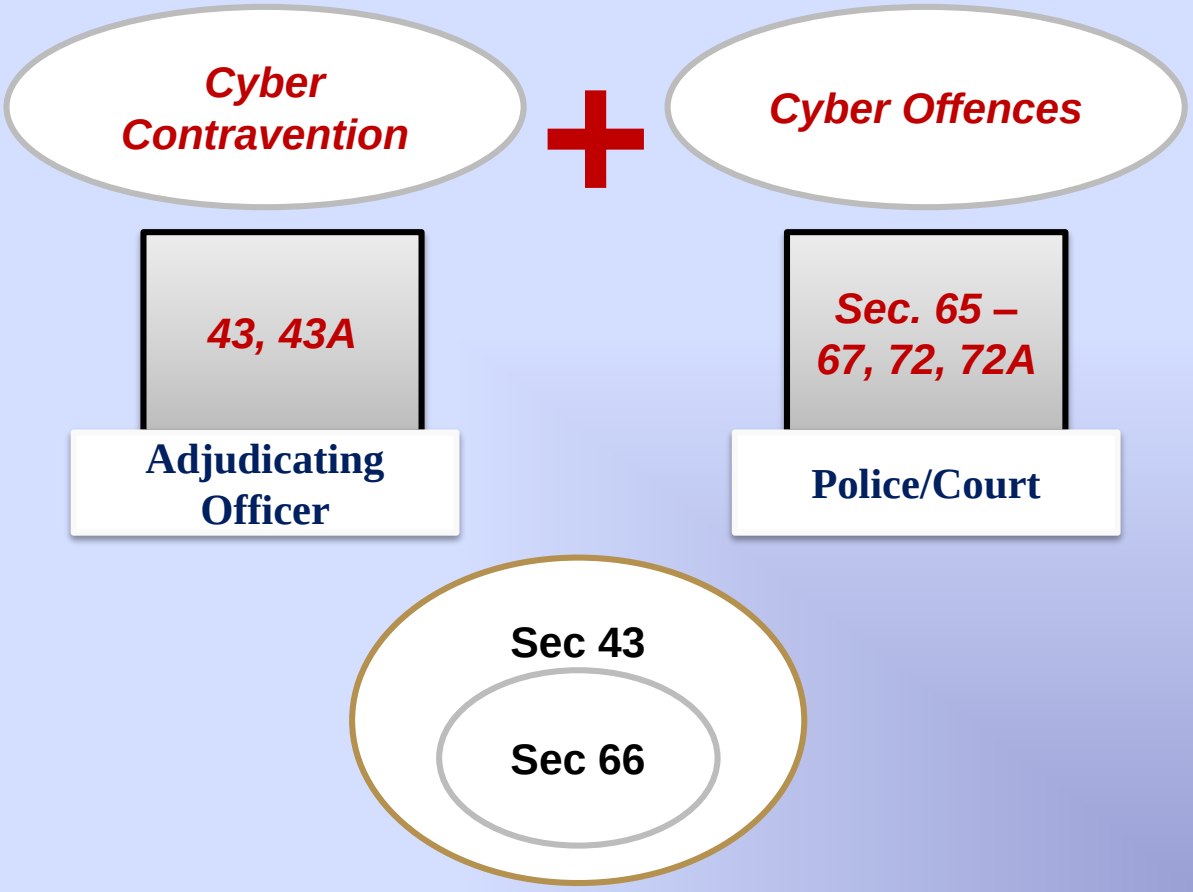
- one who causes denial of access to computer resources,
- or has unauthorized access to a computer resource,
- or introduces a virus, or containment
- Effect to cause death, injury to person or damage/destruction of property, disruption of essential supplies.

(2) unauthorized access to information, data restricted for security of State.

Regulatory Framework under IT Act, 2000

- Controller of Certifying Authorities
- Adjudicating Officer
- Cyber Appellate Tribunal
- Criminal Court
- High Court & Supreme Court

Offences & Contraventions



Cyber Contravention – Sec. 43

- **Unauthorized access –**
  - If any person without permission of the owner or any other person who is the in charge of a computer, computer systems or computer network commits any violation in Section 43 (a) – (j).

- **Penalty and compensation –**
  - Liable to pay damages by way of compensation to the tune of Rs. 5 Crores.

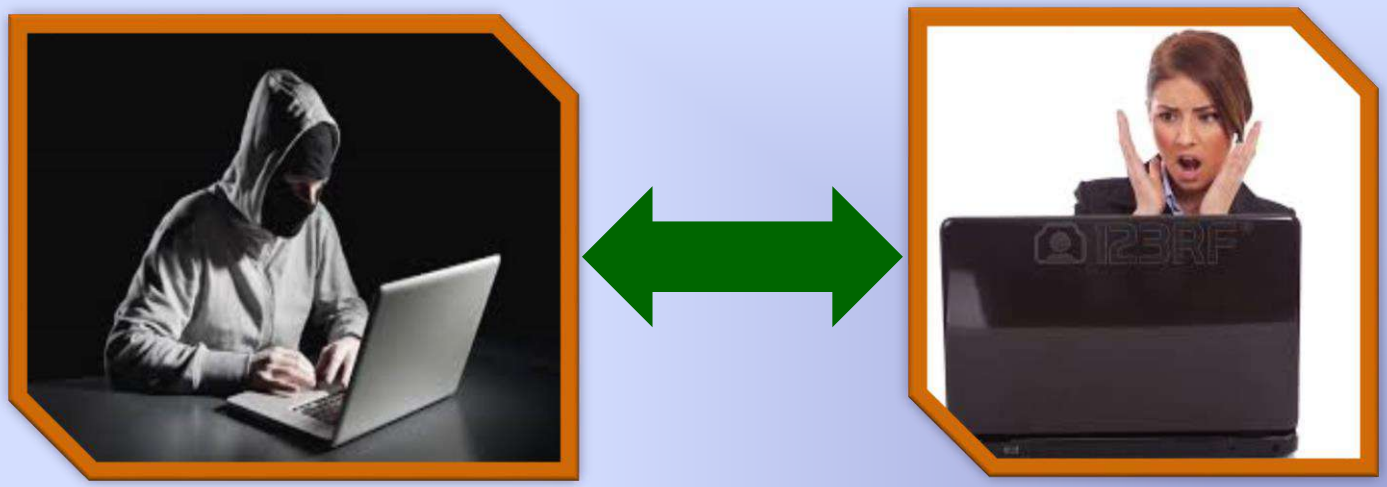
Section 66- Computer Related Offences

- "If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both."
  - Dishonestly or fraudulently as defined u/s 24/25 IPC
  - Cognizable & Bailable.

Cyber Crimes – Sec43(a) IT Act

- "If any person, dishonestly, or fraudulently, does any act referred

Unauthorized Access to the Computer

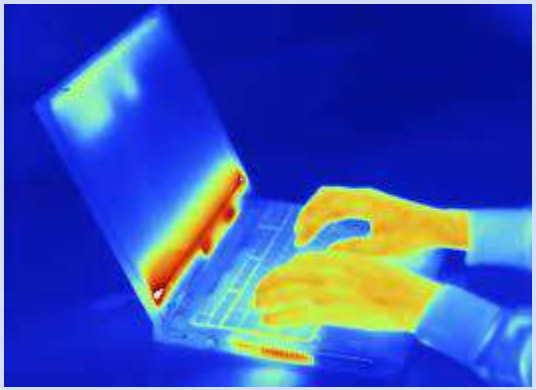


Cyber Crimes – Sec43(b) IT Act

Downloading, Copying or Extracting

any Data from

any Computer



Cyber Crimes – Sec43(c) IT Act

Introducing Computer

Virus/Containment/Spyware

Cyber Crimes – Sec43(d) IT Act

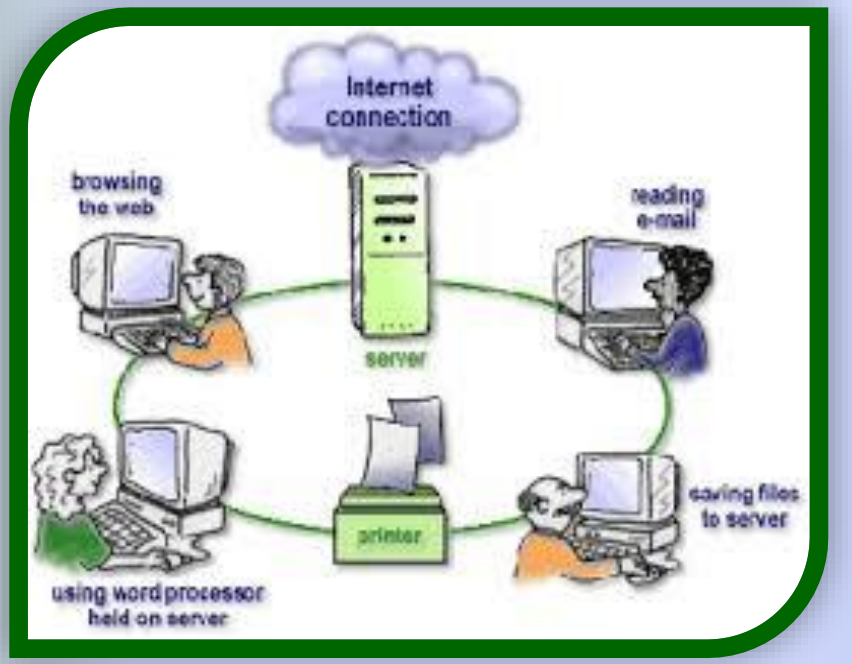
Damaging any Computer/Computer System/Database /Program

Cyber Crimes – Sec43(e) IT Act

Disrupt or Causing Disruption

to Computer or

Computer Network



Cyber Crimes - Sec43(f) IT Act

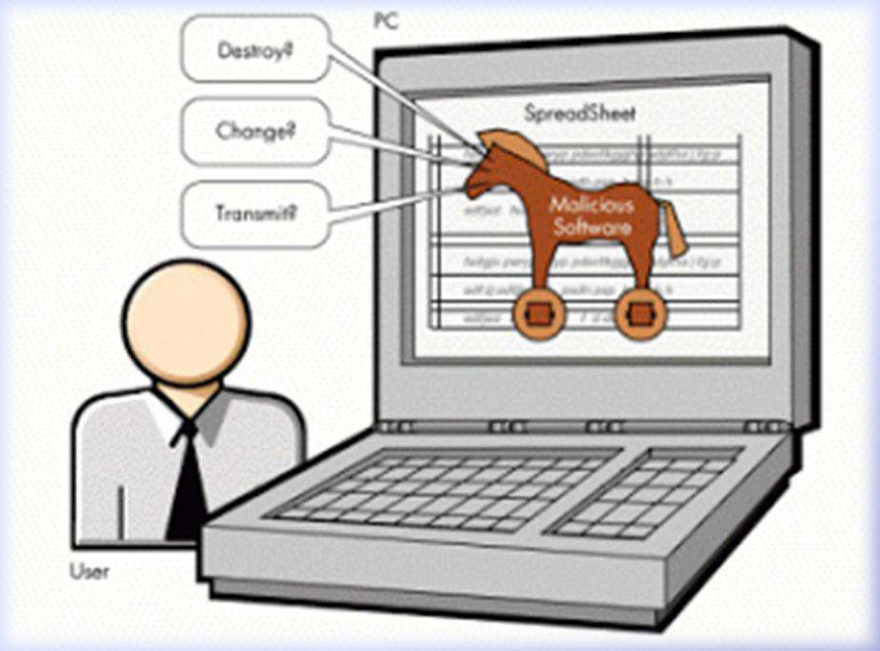
Denial-of-Access

to

Any Person

Cyber Crimes – Sec43(g) IT Act

Assistance to Facilitate Unauthorized Access to Computer



Cyber Crimes – Sec43(h) IT Act

Charges the Services to the Account of Another by Tempering with Computer

Using Stolen Credit Cards

or

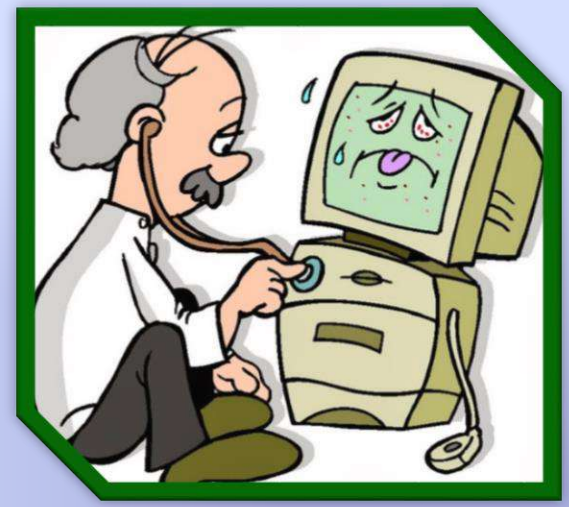
Others Bank Accounts

Cyber Crimes – Sec43(i) IT Act

Destroyed, Delete or Alter

An Information

Regarding in the Computer



Diminishes its value or effects it injuriously

Cyber Crimes – Sec43(j) & Sec65 IT Act

Steal, Conceal or Destroy Computer Source Code

If source code is required to be maintain by Law, such offence would be cognizable U/S 65

Section 66C- Punishment for Identity Theft

- **"Whoever,**
  - fraudulently or dishonestly make use of
  - the electronic signature, password or any other unique identification feature of any other person,
  - shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh"

Section 66D – Punishment for Cheating by Personation by Using Computer Resource

- **"Whoever,**
  - by means of any communication device or computer resource
  - cheats by personation,
  - shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees"

Punishment for "Video Voyeurism" -Section 66E

- **captures, publishes or transmits**
- **the image of a private area of any**
- **person without his or her consent,**
- **under circumstances violating the privacy**
- **"Private Areas"** means the naked or undergarment clad genitals, pubic area, buttocks or female breast"
- **"Under circumstances violating privacy"**
  - One could disrobe in privacy
  - One's private area would not be visible to the public

Section 67–Transmission of Obscenity in Electronic Form

Section 67-Transmission of Obscenity in Electronic Form

- **"Whoever publishes or transmits or causes to be published or transmitted in the electronic form"**
  - any material which is lascivious or appeals to the prurient interest or
  - if its effect is such as to tend to deprave and corrupt persons
  - who are likely, having regard to all relevant circumstances,
  - to read, see or hear the matter contained or embodied in it

- **Punishment for 3 yrs on first conviction and subsequent 5 yrs.**

Section 67- Transmission of Material Containing Sexually Explicit Act in Electronic Form

Section 67A–Transmission of Material Containing Sexually Explicit Act in Electronic Form

- **Whoever -**
  - publishes or transmits or causes to be published or transmitted in the electronic form any material.
  - which contains sexually explicit act or conduct.
  - shall be punished on first conviction with imprisonment upto 5 yrs & fine upto 10 lac and subsequent conviction upto 7 yrs & fine upto 10 lac."
  - this Section covers **"Sexually Explicit Content"** transmitted in electronic form

Section 67B –Child Pornography in Electronic Form

- **67B. Punishment for publishing or transmitting child Pornography in electronic form- Whoever—**
  - publishes or transmits material depicting children engaged in sexually explicit act
  - creates text or digital images, collects, seeks, browses, downloads, distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
  - cultivates, entices or induces children to online relationship on sexually explicit act
  - facilitates abusing children online, or records in any electronic form pertaining to sexually explicit act with children,

Section 67B – Child Pornography

Lt. Colonel arrested for surfing Child Pornography

- A serving Indian Army officer of the rank of Lt. Colonel has been nabbed by the Mumbai Police .
- He was allegedly uploading, possessing & disseminating obscene pictures of foreign children between the ages of 3 & 10 on the Internet.
- The German Federal Bureau spotted the photos on a child pornography site and traced the pictures to India.
- The German agency alerted the Interpol which in turn passed the information to CBI which in turned tipped the Mumbai Police.
- The Mumbai police has taken two hard drives from the Lt. Colonel's house as evidence against him.

Privacy of personal sensitive data

Citibank Mphasis Call Center Fraud

IT ACT

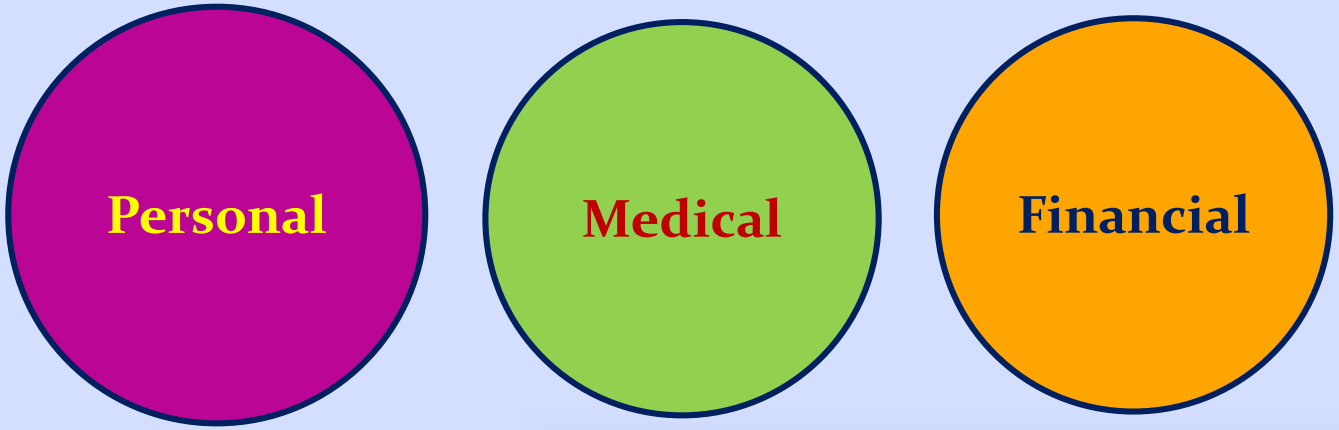
HIPPA
RBI
Regulation

Privacy of Data

- **Section 43A –**
  - Where a body corporate possessing, dealing and handling any sensitive personal data.
  - Which it owns, control or operates
  - Is negligent in implementing and maintaining reasonable security practices and procedures
  - Such a body corporate shall be liable to pay compensation.
  - The Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal Data or Information), Rules 2011.

  A body corporate means any company includes a firm, sole proprietorship or other association of individual engages in professional and commercial practices.

Privacy of personal sensitive data



Your Medical Record is Worth 10 Times More to Hackers Than Your Credit Card

OECD - Privacy Principles

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

Privacy Issues

WhatsApp

Facebook

Truecaller

WeChat

WhatsApp – Facebook Issue

Mobile & Web Applications

Privacy of Data

- **Section 72A**
  - This Section deals with Data base security & privacy.
  - A person including an intermediary is held liable if he discloses "personal information" which he accessed while providing services under a contract.
  - The liability arises if the disclosure was made with an intention to cause or knowing that he is likely to cause wrongful loss or wrongful gain to a person;

Section 70 – Protected System

1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

2) Unauthorised access or attempt to access is punishable.

3) National Nodal Agency responsible for research and development to protect the critical information structure.

Liability of internet service provider(ISP Liability)–section 79

- **The Section extends the immunity to the ISP from prosecutions under other laws including IT Act, as the provisions starts with the wordings, "Notwithstanding anything contained in any law…".**
- **The intermediary is not liable for third party information, data or communication link hosted by him if –**
  - The intermediary function is limited to providing access to communication system.
  - The intermediary has not initiated the transmission, selected the receiver of the transmission and interfered/modify the transmission.
  - The intermediary observes due diligence and guidelines of the central government.

Other Important Provisions

Contd...

Liability of Internet Service Provider

- **The intermediary is only liable for third party information, data or communication link hosted by him if –**
  - if the intermediary has conspired in the commission of the unlawful act or
  - if it has actual knowledge or the appropriate government has notified it that any information, data residing in it is being used to commit the unlawful act, and it fails to expeditiously remove on that resource without vitiating the evidence in any manner

NOTICE & TAKE DOWN APPROACH

Liability of Companies

Offences by Companies (Section 85)

- **In case of offence is committed by the company, every person:**
  - Incharge of
  - Was responsible to the
  - For the conduct of the business of the company as well as company shall be liable

- **A person would not be liable If he proves that :**
  - The offence is took place without his knowledge
  - He exercised all due diligence to prevent such contravention


Q&A

THANKYOU !

Neeraj Aarora
Cyber Lawyer & Forensic Examiner
E-mails: aarora.neeraj@gmail.com
M:+91-9871435035