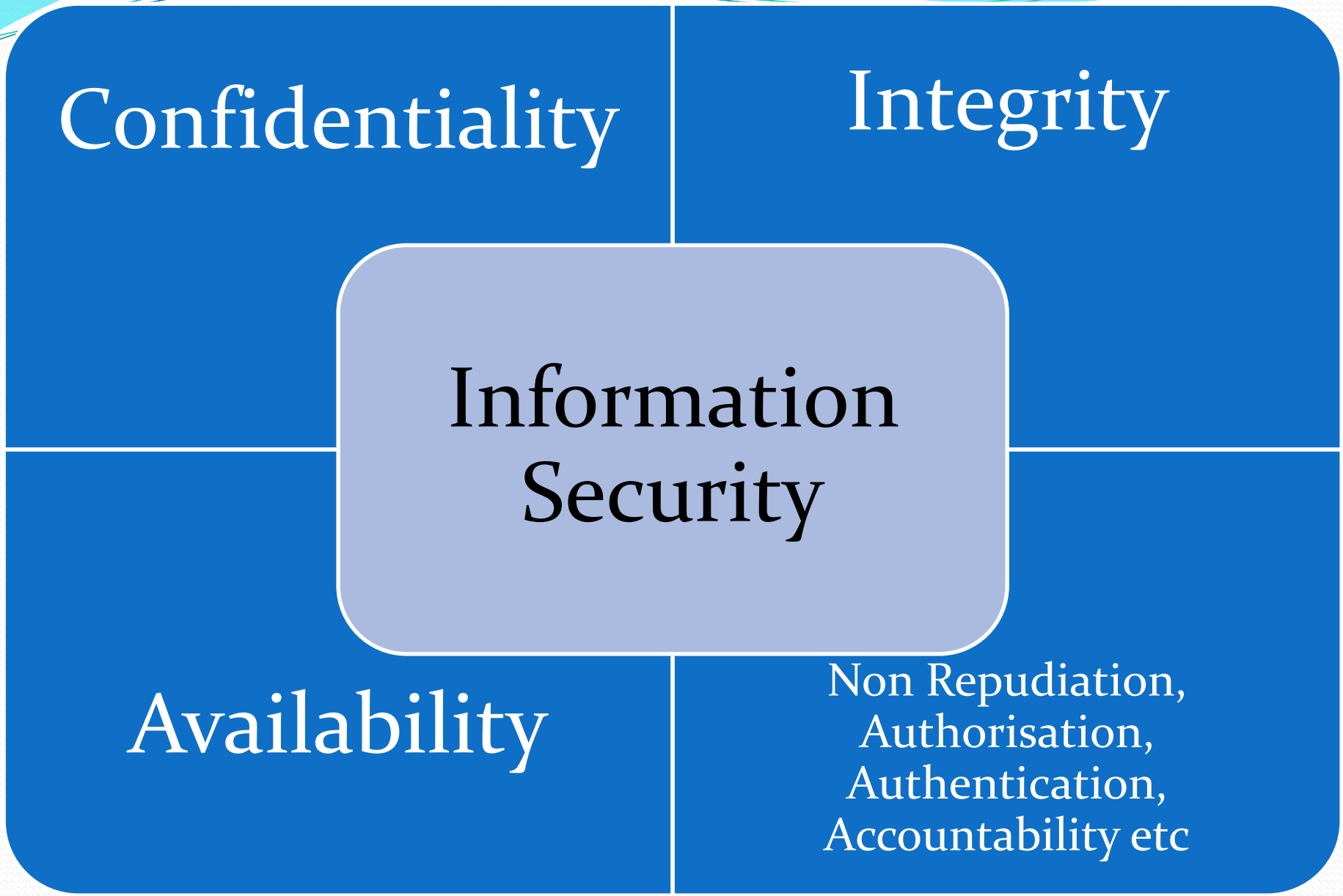
Cyber Crimes: Information Security, Digital Evidence and Cyber Laws

V Rajendran
venkrajen@yahoo.com
http://venkrajen.in
044-22473849; 9444073849

Security: Definition, Need and types

- Security: Being free from danger, defence against failure, Freedom from anxiety, safeguarding assets
- Safety, freedom, protection: *of* (Assets) *from* (individuals and threats) *against (*loss, injury etc)
- Information Assets and other assets
- Asset Classification: Criticality, Volatility, Confidentiality
- Parties to an Info Asset: Owner, Custodian, User
- Protection of information assets from threats
- Risks: Vulnerabilities and threats, Impact


Confidentiality
Integrity
Information Security
Availability
Non Repudiation, Authorisation, Authentication, Accountability etc

Cyber Security - Definition

Cyber Security: "Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction" - I.T.A.A. 2008 Sec 2 D (nb)

What constitutes cyber security?

key-words in the definition :

Data, Information, access, stored, communication device

Security: Physical and electronics/cyber

- Security refers to

  what, *from what*, why, how, when, whom

  Physical security: its features
- Electronic Security: features and specialities
- Some common features:

  Access Control

  Intrusion Prevention

  Intrusion Detection

  Incident Reporting Mechanism

  Post incident review

  Corrective and Preventive action

Distinct features of electronic security

- The three factor authentication in security
- Requirements in electronics security

  What you have (Physical possession)

  What you are (Bio-metric features)

  What you know (Password, PIN, Passphrase)

- Possibilities of breach and break of these factors

  Stealing of physical items

  Manipulating and circumventing the bio-metric data

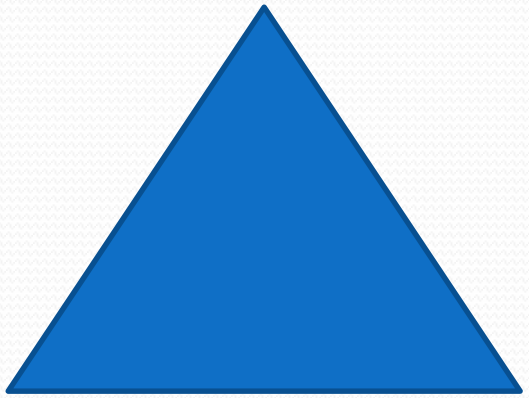
  Password crackers, ID theft, tail-gating, key-loggers

Cyber Crime – Definition and genesis

- Definition of crime, offence, fraud
- Definition of cyber crime, cyber offence ??
- Any crime or offence wherein a 'computer' is used as an object or a target of offence/crime.
- Definition of 'computer' as per I.T.A 2000: "any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or opticl impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to….."

Cyber Crimes – Computer offences

- Cyber Crime not defined in ITA
- Electronic Crime or Cyber Crimes are electronic variants of normal crimes
- Fraud triangle:



1. Intention/Necessity,
2. Opportunity
3. Rationalisation to commit the crime

- Genesis and Basis is the same
- 'Mens rea' – Criminal Intent and motive unique in the earlier cyber crimes like hacking, virus etc (like just for the heck of it or to show one's technological superiority)

Cyber Crimes

Definition of Cyber Crime, computer crimes, cyber frauds, computer frauds etc.

Legal definition: I.T. Act – No

Accepted definitions and usages

"Illegal behaviour that targets the security of computer systems and/or the data accessed and processed by computer networks"

"An act where computer is an object or a subject of crime"

"Any crime where an I.T. gadget is used in the act"

Cyber Crimes are technological variants of normal crimes.

The Act of committing, investigation, trial, evidence .. ALL VARY

Theft, forgery, fraud, blackmail, harassment, law of torts....

Cyber Crimes and Normal crimes

- Modus Operandi is different
- Investigation mechanism and process
- Process of trial
- E-evidence: Volatility, production of an e-evidence
- Acceptability, retrieval issues, technological issues
- Jurisprudence and related issues
- Irrefutability and reliability of records and process
- “Justice should not only be done but should also appear to have been done”

Cyber Crimes in banking

- Economic offences
- White collar frauds
- Cyber Crimes in Banking
- Cyber crime in e-commerce
- E-Banking frauds
- Electronic Delivery Channels:
  - ATMs
  - Internet Banking
  - Cards: Debit, Credit, Smart card etc
  - Mobile Banking

Offences in social networking

- Information theft: Access, copying, data misuse
- *'Information harvest'* - id theft: for abuse, illegal use
- Personating for cyber cheating, e-forgery
- Harassment via email Cyber stalking
- Morphing and spoofing: IP and email
- Steganography – technology or a crime?
- Cyber Squatting – creating a website – crime?
- Defamation and character assassination
- DoS and DDoS – criminal intention "mens rea"
- Spamming, Junk Mails – technology or a crime?
- Writing blogs – crime?

virtual community for people to share daily activities, interest in a particular topic, or to increase their circle of acquaintances. Online service platform, or site for building social networks or relations among people.

Why share personal information???


myspace.com
a place for friends
facebook
reddit
hi5
orkut
YouTube
YAHOO! 360°
friendster
Meetup
bebo
LinkedIn
newsvine.com
digg
flickr
twitter
delicious
social bookmarking
ryze
Business Networking

Types of cyber crimes

- Against persons: defamation, cyber stalking, phishing, id theft, email spoofing, online gambling, card frauds, virus, DoS, phishing etc
- Against property: larceny, data, information, software piracy, trade marks, copyrights, IPR etc
- Against government: cyber terrorism
- Combination of one or more of the 3

Data related computer crimes

- Data diddling (False data entry)
- Data manipulation
- Data spying
- Scavenging
- Dumpster Diving
- Data Leakage
- Piggy backing and tailgating
- Masquerading

Software related crimes

- Virus related crimes
- Trojan Horses
- Salami Techniques
- Trapdoors
- Logic Bombs and Time Bombs
- Software Piracy
- Program and source code manipulation
- Hacking, phishing,
- Email Spoofing, IP spoofing etc

Cyber Crime: Scene and Evidence

Where does a cyber offence take place?

Hard-disk? Network? Software logs? Operating System Logs? Other peripherals and related devices?

What is the scene of crime in a cyber offence?

Bank premises, Customer's residence, cyber café?

A remote location? A foreign land? ISP's premises?

To mark the scene of cyber crime and preserve

what to mark, where and how?


CRIME SCENE
CRIME SCENE


CRIME SCENE-D
FreeFoto.com


CAUTION

Investigation of cyber crimes

- Investigation on reported cases: civil and criminal
- Investigation on bank related crimes
- Bank's Management side investigation
  - Internal Inspection
  - Verification of specific instances
  - Periodic inspection
  - Vigilance and Disciplinary Action Cell
  - Fraud Containment Cell – Routine actions
- Bank's role in police investigation
- Bank's co-operation with the police:

  Bank as Victim or co-accused?

Investigation process

- Modus Operandi in cyber crimes:
  - Id theft, Password misuse, data theft, social engineering, personation, insider threats, collusion, staff involvement
  - Staff as victims or sometimes as co-accused
- Logs and Trails in the computers:
  - Application – user specific logs
  - Operating Systems logs
  - RDBMS or front-end driven logs
  - Print-outs and other outputs
  - Network driven and network stored logs
  - Data in the network and in transit and with ISP/NSP etc

Investigation tools

- Trace IP
- Trace email
- Trace through the tower – Mobile communication
- CDR Call Detail Record or Call Data Record
- Other utility websites like cellphonetracker.co.in
- Analysis of CDR and other logs from NSP/ISPs
- O/s and other logs and trails

Cyber Forensics

- Use of digital evidence in disputes
- Civil disputes between two individuals
- Common mechanism to store e-records
- Commonly accepted digital library
- Private forensics initiatives
- Private digital evidence and experts' views
- Private forensics warehouses

Physical Forensics

Manual creation
Known where it lies
Manual preservation
Needs storage (bags, containers)
Produced easily
Physically carried
Easy to understand
Experts from different fields
Shown as exhibits in courts
Irrefutability can be proved

Cyber Forensics

Manual creation
Systemic preservation
Needs software and hardware to store
Cannot be produced easily
Understandable with some expertise
Difficult to assess the location
Complex system of preservation
Preservation needs hardware and software
Production needs hw and sw
Irrefutability proved with difficulty

Evidence and the legal position

I.T. Act 2000 defines ‘data’, ‘information’, ‘digital signature’, ‘computer’, ‘computer network’, ‘computer resource’ etc

Defines ‘electronic record’ as 2(1) (t) :

data, record or data generated, image or sound stored, received or sent in an electronic form, or micro film, or computer generated micro fiche etc.

IT Act - Background

- U.N. Gen Assembly resolution 30-1-1997
- Model Law on e-com UN Comn International Law
- I.T Act in India preamble: equally aims at legalising e-commerce and to curb any offences arising therefrom.
- Act not comprehensive enough
- Does not attempt to define cybercrime
- Cybercrime and Cyberspace are new areas
- Act relies (and the investigators rely) on IPC

Definitions

- Definition of crime, offence, fraud
- Definition of cyber crime, cyber offence ??
- Not defined in ITA or any other law
- Any crime or offence wherein a 'computer' is used as an object or a target of offence/crime.
- Definition of 'computer' as per I.T.A 2000: "any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or commnication facilities which are connected or related to....."

IT Act - Records

- Recognition to electronic records is a big step
- Reliance on electronic records
- Acceptability of electronic signatures as an authentication mechanism
- Procedures for trying a cyber crime described
- Search and seizure powers and extra territorial powers etc
- Role of CERT-In (or ICERT) recognised

Especially in a bank – role of e-records and an exhaustive e-record Maintenance Policy

Adjudication in I.T. Act

- Meaning and definition of adjudication
- Role of an adjudicator
- Functions and duties of adjudicator
- A significant step – Grossly underutilised
- Very useful for civil disputes and losses in e-transactions
- Powers of a court vested with the IT Adjudicator (IT Secy)
- Has it served the purpose so far??

What needs to be done to make the process successful?

Section 43

- Unauthorised access, download, or copy data
- Destroys, deletes or alters any info or damages or causes to damage…..
- Disrupts or causes to disrupt etc (DoS attack)
- Computer contaminant definition of virus etc
- ‘diminishes its value or utility or affects…
- computer source code: listing of programmes, computer commands, design, layout and programme analysis…

Section 43-A

- A significant addition in ITAA 2008
- Compensation for failure to protect data
- Body corporate dealing or handling any personal data ….negligent in maintining reasonable security practices…cause wrongful losses or wrongful gain…liable to pay damages by way of compensation…
- 'Body corporate', 'sensitive personal data' and 'reasonable security practices' are defined in the section as a major step in compliance for ITO's and CSO's
- Cyber Law Compliance to be taken seriously
- Responsibility and liability of CTO's/CEO's as non-compliance of these provisions..

Section 65 and 66 List of offences

65 Tampering with source code etc

66A Offensive messages thro communication service

66B Dishonestly receiving stolen computer resource

66C Electronic signature or other identity theft

66D Cheating by personation - computer resource

66E Privacy violation – Publishing or transmitting

66F Cyber terrorism – sovereignty of the nation

Life imprisonment

Sec 67 A now widened

- Publishing or transmitting obscene material Lascivious or appealing to prurient interest Deprave or corrupt persons …
- 67A Publishing sexually explicit act in e-form
- 67B e-publishing child pornography
- 67C Preservation and retention by intermediaries
- 69 Power to monitor, intercept, decrypt any information trough any computer resource: Criticised to be draconian – Privacy of information?

National Nodal Agency

- 69-A Power to issue directions for blocking for public access of any information through any computer resource - Procedures and safeguards to be prescribed
- 69-B Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security – Intermediary to provide data
- 70 Protected system and critical infrastructure (at times read with Copyrights Act and protection available there)
- 70-A and B: Cert-In will be the national nodal agency and will have all powers as per the Act

Role of CERT In being now debated…Powers of CERT In, especially power to intercept, block websites etc

Other provisions…

- 72 Penalty for breach of confidentiality and privacy
- 75 offence/contravention committed outside India
- 76 Confiscation powers
- 77 compounding of offences
- 78 – Power to investigate: Inspector
- 79 NSPs not liable in certain cases like when he information is not initiated and observe due diligence and guidelines are followed

What is due diligence? Much debated often…

Cyber Crime Scenes

Amendments to other Acts

ITA 2000 has amended the relevant sections of:

- Indian Penal Code
- Indian Evidence Act
- Bankers Book Evidence Act
- Reserve Bank of India Act

Subsequently Negotiable Instruments Act
was amended giving recognition to Cheque Truncation.

Best wishes

V. Rajendran

Advocate and Cyber Law Consultant

President, Cyber Society of India

+91-22473849; +91-9444073849