Cyber Crimes and Risk Management

V. Rajendran
Advocate and Cyber Law Consultant
Email: rajcyberlaw@gmail.com
URL: venkrajen.in
+91-44-22473849; +91-9444073849

Day 1 - Contents

- Cyber world and cyber space
- Data and Information
- cyber threat: Vulnerabilities and Risks
- cyber crime – What makes a crime a cyber crime
- White collar crimes and economic offences
- cyber stalking and cyber extortion
- Insider threat
- Hacker and cracker - script kiddies
- criminal profiling and deviant behaviour
- Motive and Targets in cyber crimes
- Cyber terrorism, cyber espionage, cyber warfare

Cyber….?

Interesting origin of the word “cyber”

Used in the formation of words relating to computers, computer networks, or virtual reality.

cybernetics, which was ushered into English in the 1940s by the scientist Norbert Wiener - the study of mechanical and electronic systems designed to replace human systems.

From the Greek term *kybernḗtēs* meaning “helmsman” or “steersman.” The first instance on record of *cyber* as a combining form is from 1961 in the *Wall Street Journal*: “A major difference between the Cybertron and conventional computers…is the ability of the Cybertron to make use of raw data and signals.” In 1966 fans of the popular sci-fi show *Doctor Who*heard other *cyber* combining form: *cybermen*.

(Source: Internet)

Cyber world and Cyber Space

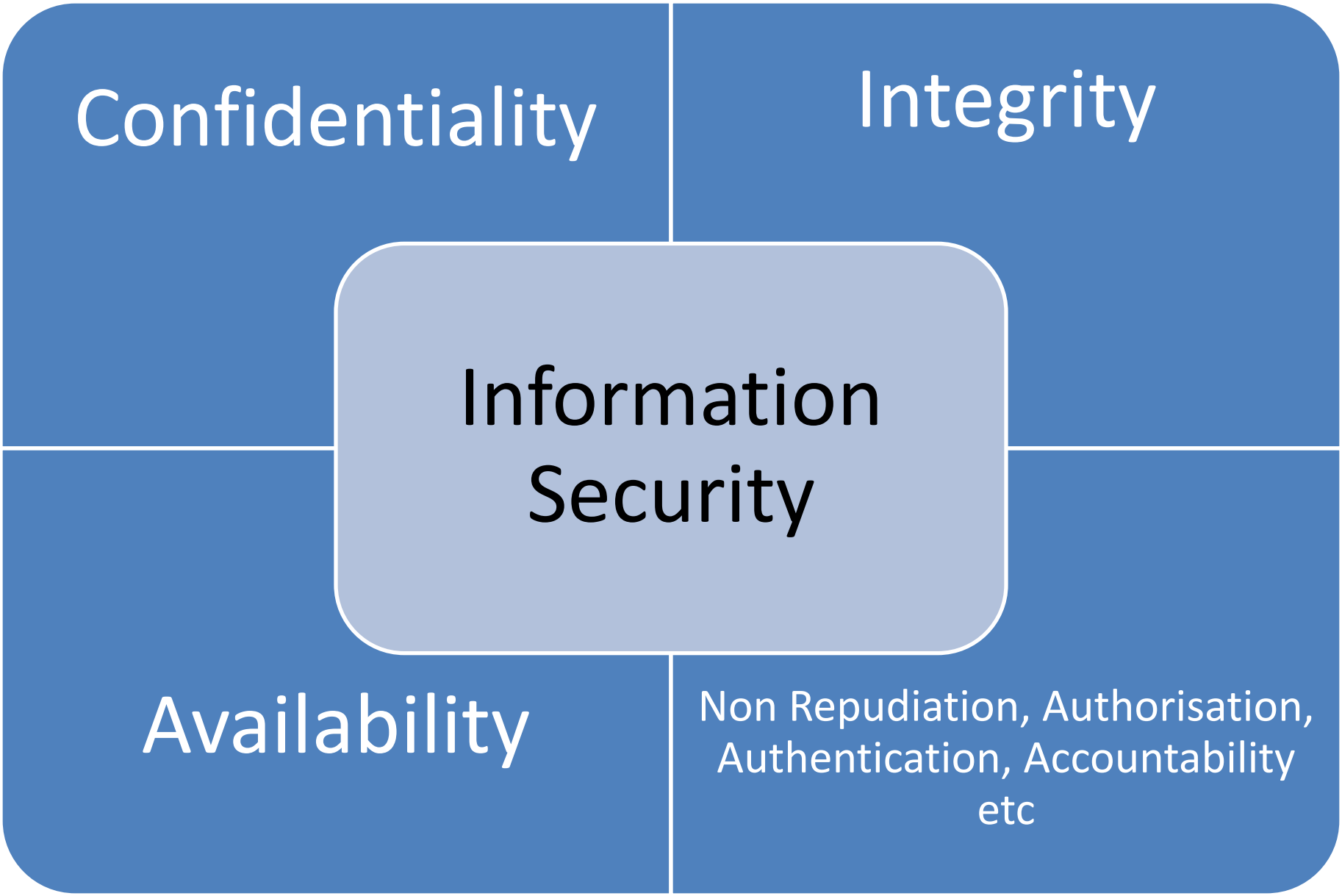
- Virtual world – cyber world – cyber space
- Physical world scenario – physical data
- Cyber data – electronic records and data
- Accessing physical world and cyber world
- Cyber Space and virtual space
- Access Control and Access Privileges
- Data and Information

Information Assets

- Physical Assets and Information Assets
- Asset Classification – Criticality of Data Asset
- Tangible and intangible and other classification
- Information Asset in transit
- Protection of Information Asset:
  - In transit, in storage, external storage devices etc
- Parties to an information asset
  – Owner, Custodian and User

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


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

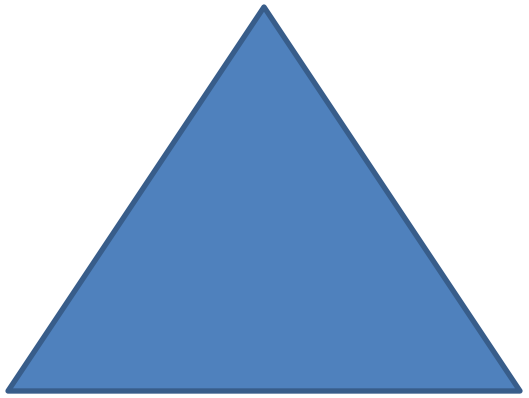
Cyber Crimes – Computer offences

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)

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 / circumventing the bio-metric data

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

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

Threat and Vulnerability

Threat: A circumstance or event with potential to cause harm to a system (either physical or a computer system);

Includes destruction, unauthorised disclosure or modification of data and/or denial of service;

An external factor or an event which may or may not occur;

A potentiality to harm or destroy the system resources.

Vulnerability: A weakness that could be exploited to cause damage to the system or the assets it contains;

A situation inside the system which may be (should be?) improved;

A weakness inside the system which may be plugged or attended to;

Requires top management's attention to plug the loophole;

May be inherent and has to be put up with but with knowledge.

Threats

Identify various threats like

- host threats
- application threats
- Human behaviour: internal or external
- Systemic failure: inherent or sudden
- External event: forecast or feared already
- force majeure

Threat types and perceptions

- Threats catalogues are:
- Force majeure
- Organizational shortcoming
- Human error
- Technical failure
- Deliberate acts

Threat evaluation

THEMIS: Threat Evaluation Metamodel for Information Systems is a description logic-based framework.

It can be used by law enforcement agencies and prosecutors to build legally credible arguments, and by network designers to keep their defensive and retaliatory measures within lawful limits.

THEMIS automates known quantitative measures of characterizing attacks, weighs their potential impact, and places them in appropriate legal compartments.

From the perspective of computer networks, it is a way to reason about the non-network related consequences of complex attacks from their atomic counterparts.

From the perspective of law, it relates to the development of rules that represent concepts and restrictions of heterogeneous legal domains.

Threat modelling

- Risk of an attack can be mitigated
- Cannot eliminate the actual threat
- Threats still exist regardless of the security actions and countermeasures
- Acknowledge presence of threats
- Manage risks thro' process of threat modeling
- Threat modeling can help you manage and communicate security risks across your team

Threat modelling process

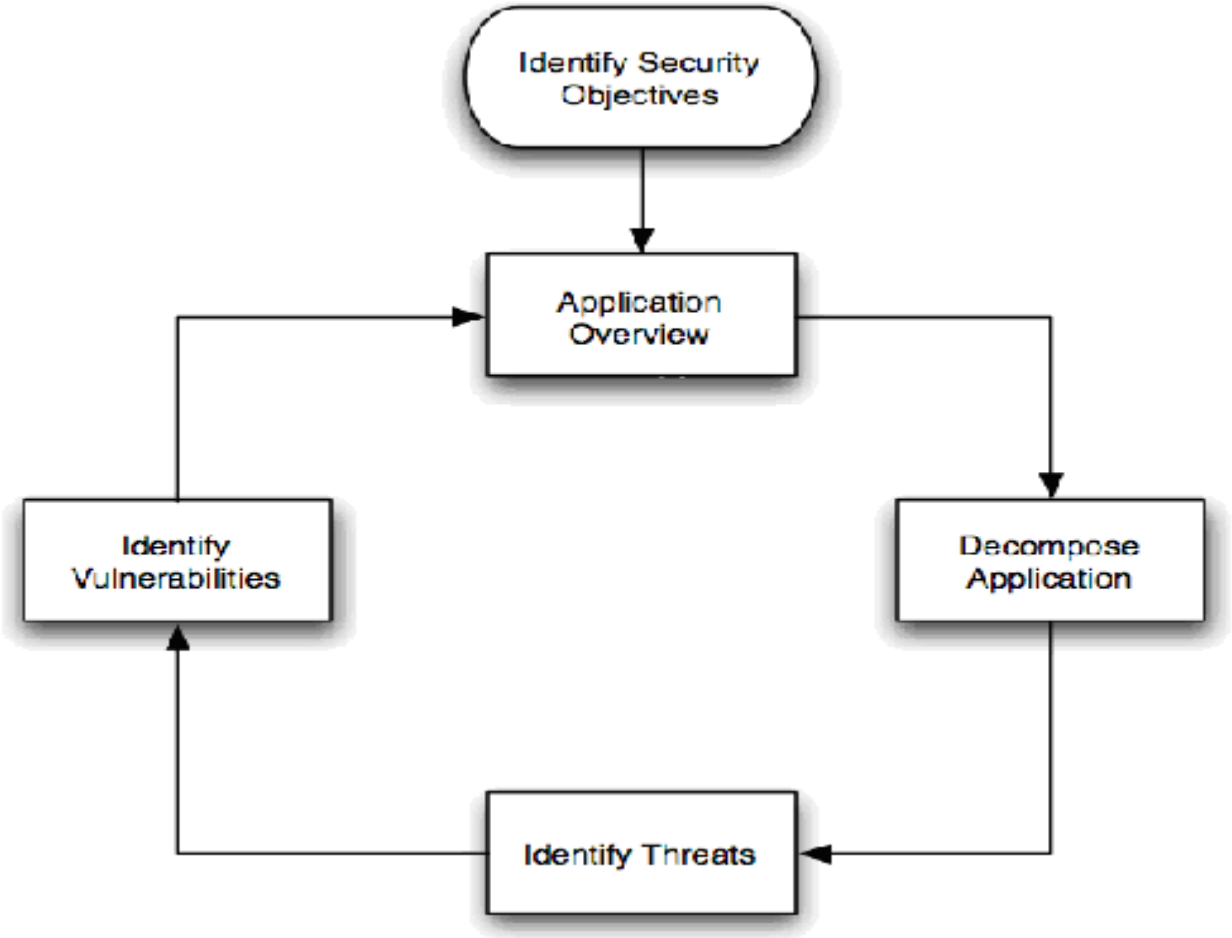
- **Identify assets**. that your systems must protect.
- **Create an architecture overview**. Document the architecture of your application, including subsystems, trust boundaries, and data flow.
- **Decompose the application**
- Create a security profile for the application
- Uncover vulnerabilities in the design, implementation, or deployment configuration of your application.
- **Identify the threats**. Keeping the goals of an attacker and potential vulnerabilities of your application
- **Document the threats** using a common template defining set of attributes
- **Rate the threats** to prioritize and address the most significant threats first
- Rating process weighs the probability of the threat against damage that could result should an attack occur
- Certain threats may not warrant any action at all

DREAD

- **D**amage potential: How great is the damage if the vulnerability is exploited?
- **R**eproducibility: How easy is it to reproduce the attack?
- **E**xploitability: How easy is it to launch an attack?
- **A**ffected users: As a rough percentage, how many users are affected?
- **D**iscoverability: How easy is it to find the vulnerability?

Considered to be a part of a system for risk-assessing computer security originally used at Microsoft.

Threat risk modeling is an essential process for secure web application development to determine the correct controls and to produce effective countermeasures.



STRIDE

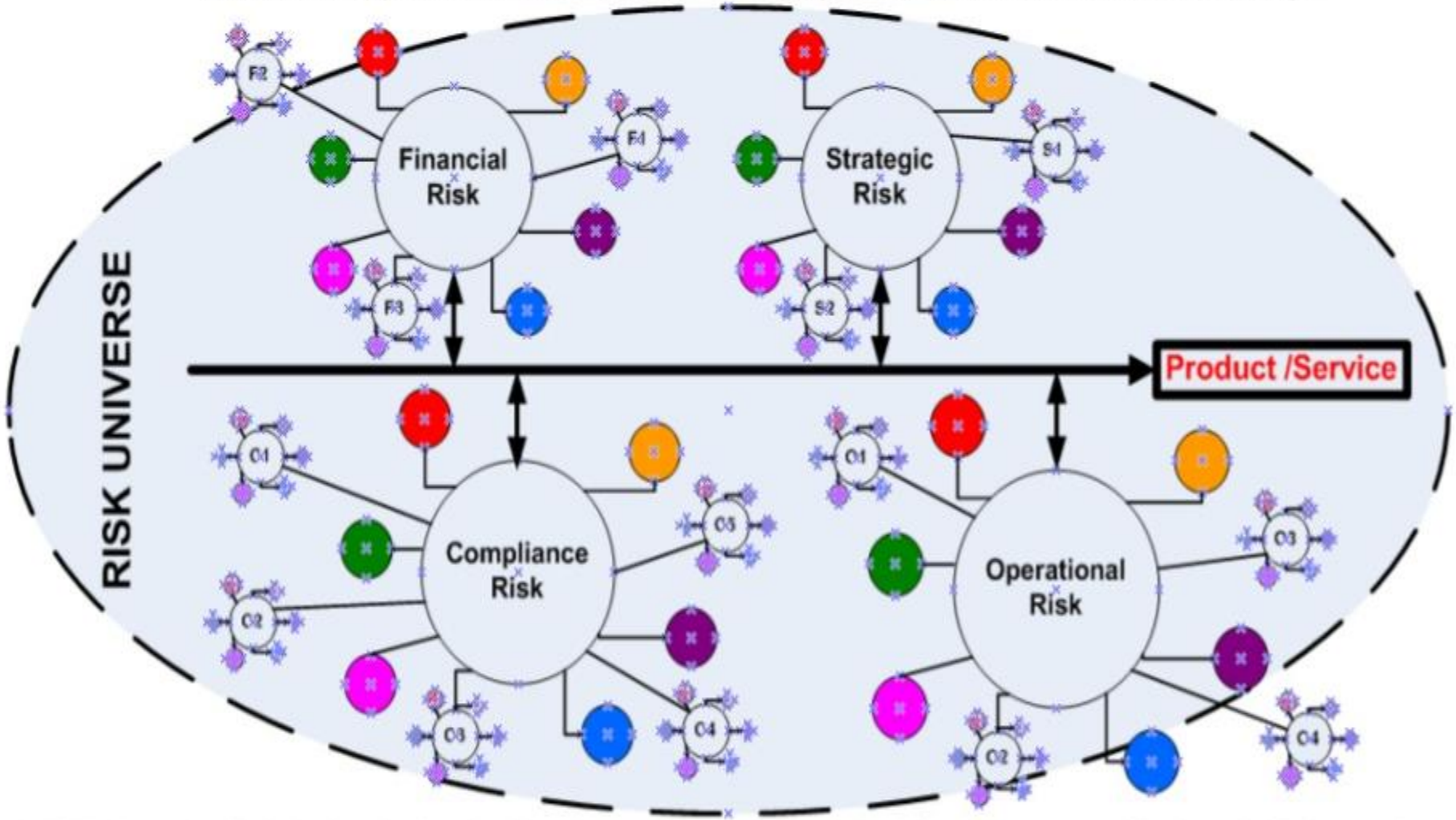
- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- DDoS
- Escalation of privilege rights

Cyber Attacks – Cost Benefit Analysis

- Attackers attack only when they believe that their cost of attack is lower than the expected benefits. Any change to a more popular platform, or one that uses common components, decreases these costs. Attackers are more likely to be familiar with the technology, so they don't need to spend time on training or research. Availability of resources is also important. A public cloud scenario, for example, that co-locates many different applications with various types of data is likely to increase the perceived benefit.

RISKS ASSOCIATED WITH SERVICE DELIVERY, PRODUCT, and REVENUE STREAMS

Generally the delivery of a product or service requires the collaboration of many departments within the Enterprise represented by a cluster. Each cluster managing risks associated with their speciality.



RISKS: **Strategic** - high-level goals, aligned with and supporting the organization's mission **Operational** - effective and efficient use of resource **Financial** - reliability of operational and financial reporting **Compliance** - compliance with applicable laws and regulations

Vulnerability

- Sometimes inherent in the system itself
- Weakness: May or may not be eliminated
- Study the level of exposure and the threat impact
- Impact Analysis to be done to ensure how serious the vulnerability is
- Sometimes dynamic and may increase over time
- When does a vulnerability become critical?
- Vulnerability Analysis and elimination
- Gap Analysis and best practices: Conformance

Impact Analysis

Done as a part of and as a supplementary to threat analysis to study the effect a threat has

A management level analysis to identify the effect of losing the organisation's resources.

BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data to enable the management in decision making on risk mitigation and continuity planning

A formal analysis of the effect on the business if a specific set of Information System services are not available

Identifies the minimum set of services that an organisation will require to continue operating

Definition of risk

Risk = Probability x Damage Potential

On a scale of 1-10 with probability and damage potential, rating can be done..

For example,

if **Probability**=10 and **Damage Potential**=1,

then Risk = 10 x 1 = 10. If **Probability**=1

and **Damage Potential**=10, then Risk = 1 x 10 = 10.

"Potential of damage to a system or associated assets that exist as a result of the combination of security threat and vulnerability"

Risk = Threat + Vulnerability → Impact

What is risk?

- Risk is probability of unfavorable condition; in financial sector it is the probability of actual return being less than expected return
- a source of danger; a possibility of incurring loss or misfortune
- Risks (defined in ISO 31000 as *the effect of uncertainty on objectives*, whether positive or negative)

Objectives of Risk Management

- Survival of the organisation
- Efficiency of operation
- Uninterrupted operation (BCP-DR)
- Identifying risk and acceptance levels
- Earning stability
- Continued and Sustained growth
- Corporate planning (organisational, HR etc)

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

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”

What makes a crime a cyber crime?

- Definition of cyber crime
- Cyber Crimes, cyber laws etc
- cyber police, cyber courts too?
- Electronic offences
- White collar crimes
- Jurisdictions issues
- Evidence and forensics – procedures
- Investigation and Trial

Types of cyber crimes

- Against persons:
  - defamation,
  - cyber stalking, harassment,
  - Phishing (against property too?
  - id theft
  - Social Engineering – Information Harvest
  - email spoofing
  - IP Spoofing
  - online gambling
  - card frauds
  - 419 Nigerian frauds
  - Virus
  - DoS and DDoS etc

Types of cyber crimes

- Against property:
  - Larceny and theft – data theft
  - Information Asset
  - Data and information in transit
  - software piracy
  - trade marks, copyrights, IPR etc
- Against government:
  - cyber terrorism
  - cyber war

Other types of cyber crimes

- Cyber Crimes in Banking and Financial Sector
- Electronic Delivery Channels in Banks
  - ATMs, Internet Banking, Cards,
  - Mobile Banking
  - Funds remittances like RTGS etc

- Cyber Crimes in Social networking Sites
  - Culprits and criminals – Innocent victims
- Planned and organised, for money
- Cyber Crime as a Service ? Professionals!

E-Delivery channels in Banks

- Electronic offences and financial frauds
- Meaning of electronic delivery channels
- Advantages of such alternate delivery channels
- ATMs, Internet Banking, Cards and Mobile Banking
- The common threats and risks in these
- Specific to some of these channels