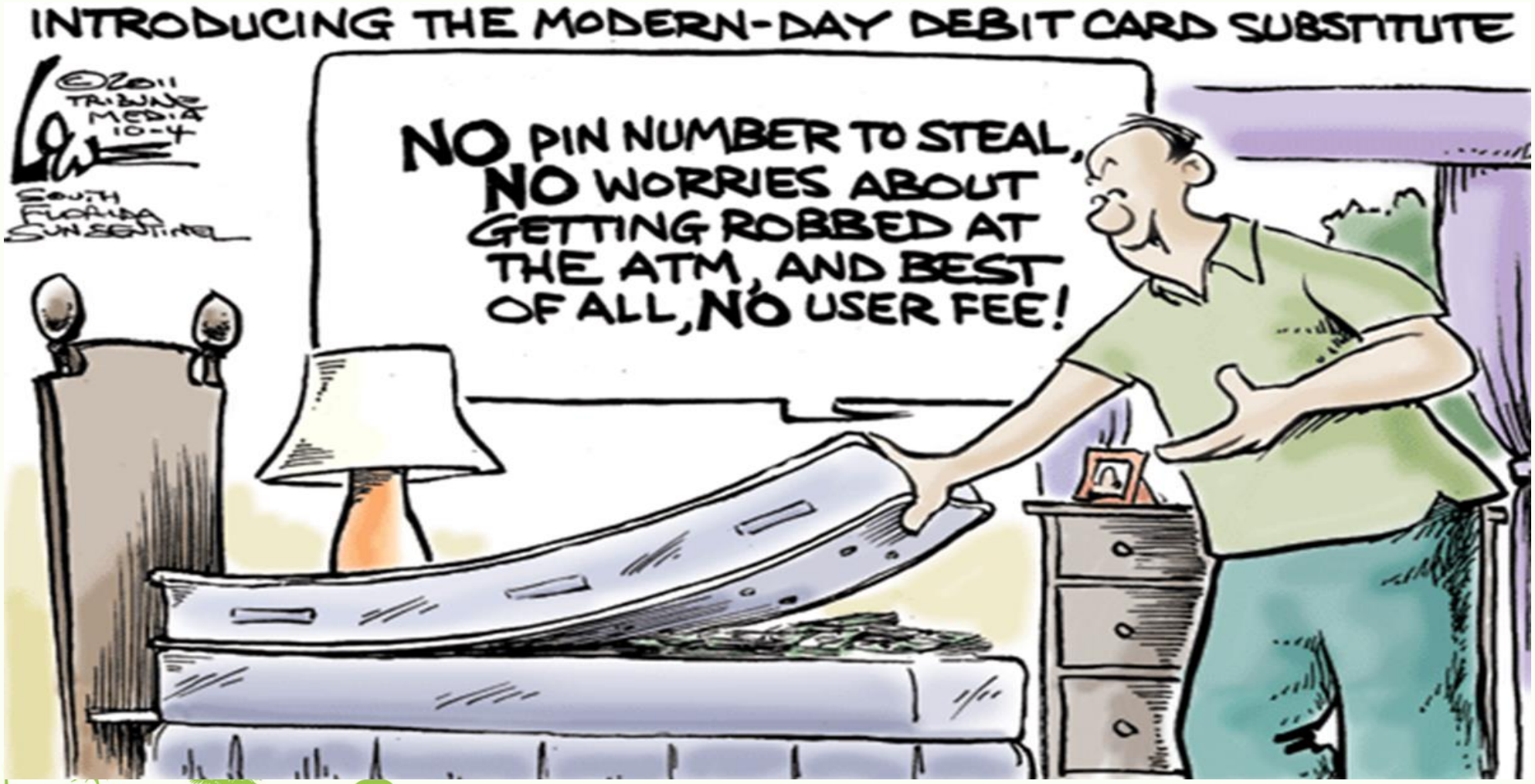
NABARD

Cyber Security/Crime

BANKERS INSTITUTE OF RURAL DEVELOPMENT, KOLKATA

Importance of Cyber Security



Banking Options

Cyber Crimes

Coverage
Definition
Conventional vs Cyber Crime
What are cyber crime threats
Motives and Reasons for cyber crime
Types of cyber criminals
How Cyber Criminals Work
Classification of Cyber Crimes
Management of risk

Cyber crime

What is Cyber Crime?

- Criminal Activity
- Using Computers & Internet
- Break laws & cause harm

“Criminal activity perpetrated using computers and the internet”

Cyber crime

What are the features of Cyber Crime?

- Unlawful act
- Computer is used

- as a tool or
- a target or
- both

- Tool – Computer is used
- Target – Attacked to steal information/ other assets

Conventional Crime vs Cyber crime

- No great differences
- Only difference is the medium through which crime is committed
- Knives and weapons vs port scanners, viruses, and worm to gain access
- Against groups or individuals
- Intention is embezzlement of money or something of value
- Physical presence of criminal at the site of crime is not must

What are Cyber Crime Threats

- Damage to reputation and morale
- Theft of identifiable information
- IP theft including theft of data
- Service disruption
- Financial loss
- Regulatory risks
- Cost of investigation and damage control

Motives and Reasons for Cyber Crime

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mind set

Aspects of Technology that make Cyber Crime an Easier Option

- Storage of Large Amount of Data in Comparatively Small Spaces
- Easy accessibility to data
- Lapses in operating system
- Negligence of human beings
- Lack of physical evidence

Types of Cyber Criminals

- Traditional criminals
- Fraudsters and thieves
- Hackers and computer tress passers, password hackers
- Malicious code writers and distributors
- Music, movie and software pirates
- Harassers and extortionists
- Stalkers, pedophiles and other cyber sex offenders
- Academic cheats
- Organised criminals including ethnic based gangs
- Corporate, government and free lance spies
- Cyber terrorists

How Cyber Criminals Work

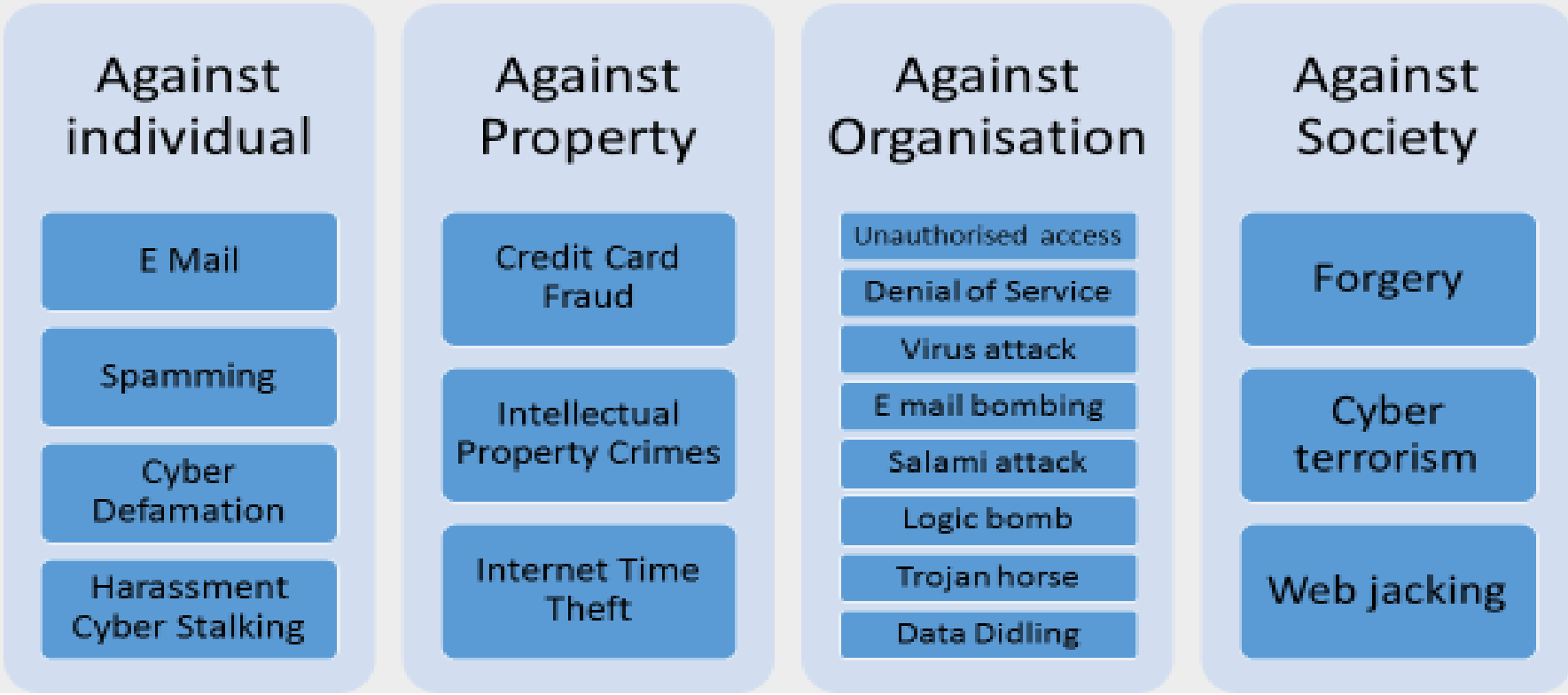
- Very professional and organized
- Not spontaneous – ground work necessary

- Coders
- Kids
- Drops
- Mobs

Classification of Cyber Crimes

1. Cyber crimes against individuals
2. Cyber crimes against property
3. Cyber crimes against government
4. Cyber crimes against society

Classification of Cyber Crimes



Crime against Individual

- E-mail Spoofing

A spoofing mail is the formation of email messages by impersonating correspondent identity.
It shows its origin to be different from which actually it originates.

- E-mail Spamming

Spam is a message also called as junk mail; send with a web link or business proposal.
Clicking on this link or replying to commercial offer send to a phishing website or set up a malware in your workstation.

Crime against Individual

- **Cyber Defamation**

Act of imputing any individual with intention to lower the person in the estimation of the right-thinking members of society generally or to cause him to be ignored or sidestepped or to rendering him to hate, disrespect or ridicule.

- **Cyber Stalking**

stalking is "pursuing stealthily"

following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms visited by the victim, continually attacking the victim with emails, etc.

Crime against Property

- Credit Card Frauds

Online fraud and cheating are most money-spinning trades that are rising nowadays in the cyber space.

- Intellectual Property Crimes

Any illegal act due to which, the owner is deprived entirely or partly of his human rights is a crime.
Very common form of IPR abuse - software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.

Crime against Property

- Internet Time Theft

Internet time theft comes under hacking.

It is the use by an unofficial individual, of the Internet hours paid for by another individual.

Crime against Organisation

- **Unauthorized Access**

This is generally denoted to as ‘Hacking’.

- **Denial of Service Attack**

Denial-of-Service referred the act by which a user of any website or service denied to use the service or website.

Offenders aim the web server of the websites and flow a large number of requests to that server

Maximum bandwidth of the website gets used, and it goes slow down or not available for some times.

Crime against Organisation

- **Virus Attack**
  A computer virus is a type of malware that, when executed, replicates by implanting the replicas of itself (probably altered) into other computer programs, data files or the boot sector of the hard drive
- **Email Bombing**
  In email bombing, a user sending vast numbers of email to target address and due to this that email address or mail server crashed.
- **Salami Attack**
  when minor attacks make up a major attack which becomes untraceable because of its nature. It is also called as Salami Slicing.

Crime against Organisation

- **Logic Bomb**

  A piece of code intentionally inserted into a software system that will initiate mischievous features under definite conditions
- **Trojan Horse**

  Non-self-duplicating kind of malware program comprising malicious code that, when implemented, carries out actions determined by the nature of the Trojan, usually causing damage or stealing of data, and likely system damage.
- **Data Diddling**

  Data Diddling is illegal modifying of data. When an individual enters some data to his system and output is different from input then he may victim of data diddling. It is done by a virus program that changes the entered data.

Crime against Society

- Forgery

  When a perpetrator alters documents saved in electronic form, the crime committed may be forgery.

- Cyber Terrorism

  To distinguish between cyber terrorism and cybercrime. Both are criminal acts.

  (1) Putting the public or any section of the public in fear; or

  (2) Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

  (3) Coercing or overawing the government established by law; or

  (4) Endangering the sovereignty and integrity of the nation

Crime against Society

- **Web Jacking**

  The word ‘Web Jacking’ comes from Hijacking. In this type of cyber-crime, the cybercriminals hacks the control of a website. They may able to change the content of that website. They use that website as owner and the real owner of website has no more control on the website. Sometime attackers ask for ransom to the owner of the website.

Types of Cyber Crimes

- Financial Crime
- Fraud and cheating
- Information theft
- Cyber extortion
- Drug trafficking
- Weapons and illegal goods/activities
- Harassment
- Cyber stalking
- Dissemination of obscene or offensive content
- Defamation

Types of Cyber Crimes

- Cyber terrorism
- Cyber warfare
- Denial of service
- Intellectual property theft
- Computer vandalism

Techniques of Cyber Crimes

- Dumpster diving – Treasure in trash
- Wire tapping – penetrate telecom networks
- Eavesdropping on emanations – pick up data from signals
- Denial of service – load a computer with numerous requests
- Phishing / Masquerading – use a mail message to look like a real site
- Data attacks -
- Unauthorised copying of data
- Trap doors
- Traffic analysis
- Harassment
- Software piracy
- Session hijacking

Risk Management

- Process of identifying critical information assets, assessing the risks, threats and vulnerabilities that these assets face, estimating the impact of these risks and launching countermeasures
- Countermeasures:-
  - Accepting the risk
  - Transferring the risk
  - Avoiding the risk
  - Applying control

Security Controls

- Specify, design, implement, operate and maintain security controls
- Security Managemnent Framework – ISO/IEC 27002

What the control “does”

- Preventive controls
- Detective controls
- Corrective controls

What the control “is”

- Physical controls
- Technical controls
- Administrative controls

Preventive Controls

- Physical Controls - Backup files, security guards, fences, badge systems, double door systems, locks and keys, fire extinguishers
- Technical controls - Access control software, antivirus software, passwords, smart cards
- Administrative controls - security awareness and technical training, Separation of duties, supervision of duties

Detective Controls

- Physical Controls – CCTVs
- Technical controls- Intrusion detection systems
- Administrative controls – Review of security trails of a system administrator

Corrective Controls

- Physical Controls – CCTVs
- Technical controls- all systems loaded with anti virus software systems
- Administrative controls – action on security audit findings

Other Controls

- Deterrent control – security guard with gun, barbed wire fencing, policy containing punishments
- Recovery controls – Disaster recovery plan, Backups for systems
- Compensating controls – when normal controls fail - Review of log report, review of activities of administrator
- Directive controls – mandatory

- Cryptography
- Encryption

Thanks