IIBF & NISM Adda

Certificate Examination in
Prevention of Cyber Crimes and Fraud Management

(IIBF & Other Exams)

Compiled by

Srinivas Kante B.Tech, CAIIB

About Certificate Examination in Prevention of Cyber Crimes and Fraud Management

IIBF Certificate Examination

OBJECTIVE:

The objective of the course is to make the bankers familiar with different types of cyber crimes perpetrated across the globe and acquire necessary knowledge and skill to prevent the occurrence of such crimes in organizations.
DIPLOMA IN INFORMATION SYSTEM AUDIT (DISA)
Candidates who clear all the following three Certificate examinations under the revised syllabus will be given a "DIPLOMA IN INFORMATION SYSTEM AUDIT (DISA)" from May 2017 :
a) Certificate Examination in IT Security (Revised Syllabus)

b) Certificate Examination in Prevention of Cyber Crimes and Fraud Management

(Revised Syllabus)
c) Certificate Examination in Information System Banker (Revised Syllabus)

Candidates who clear all the above three Certificates under revised syllabus will however have to apply for DISA certificate by paying Rs.500/- plus taxes as applicable.
For candidates who have already cleared any or all the above three examinations under the old syllabus, i.e. prior to May 2017 need to apply and clear the examination under revised syllabus to become eligible for DISA Certificate.
ELIGIBILITY
i) Employees of a Bank or Financial Institutions.

ii) Any graduate of a recognised university or its equivalent.

SUBJECT OF EXAMINATION
Cyber Crimes and Fraud Management
PASSING CRITERIA:
Minimum marks for pass in the subject is 50 out of 100.

EXAMINATION FEES* : Particulars	For Members	For Non-Members
First attempt	Rs.1,000/- *	Rs.1,500/- *
Subsequent each attempt	Rs.1,000/- *	Rs.1,500/- *

Please Note : Candidates are required to Register for every attempt separately.
As a measure to streamline the traffic for registration, Institute will charge regular examination fee to candidates who registers for the examination during the regular open period of registration. For the extended days of registration, late fee of Rs.200 plus taxes, will be charged in addition to regular examination fee. This extended days of registration, also gives candidates addition opportunity to register for the examination, having missed the regular open period of registration.
The fee once paid will NOT be refunded or adjusted on any account.
MEDIUM OF EXAMINATION :
Examination will be conducted in English only.
PATTERN OF EXAMINATION:
(i) Question Paper will contain 120 objective type multiple choice questions for 100 marks.

(ii) The examination will be held in Online Mode only

(iii) There will NOT be negative marking for wrong answers.

DURATION OF EXAMINATION:
The duration of the examination will be of 2 hours.
PERIODICITY AND EXAMINATION CENTRES:
a) Examination will be conducted on pre-announced dates published on IIBF Web Site. Institute conducts examination on half yearly basis, however periodicity of the examination may be changed depending upon the requirement of banking industry.

b) List of Examination centers will be available on the website. (Institute will conduct examination in those centers where there are 20 or more candidates.)

PROCEDURE FOR APPLYING FOR EXAMINATION
Application for examination should be registered online from the Institute's website www.iibf.org.in. The schedule of examination and dates for registration will be published on IIBF website.
PROOF OF IDENTITY
Non-members applying for Institute's examinations / courses are required to attach / submit a copy of any one of the following documents containing Name, Photo and
Signature at the time of registration of Examination Application. Application without the same shall be liable to be rejected.
1) Photo I / Card issued by Employer or 2) PAN Card or 3) Driving Licencse or 4) Election Voter's I / Card or 5) Passport 6) Aadhaar Card
STUDY MATERIAL / COURSEWARE
The Institute has developed a courseware to cover the syllabus. The courseware (book) for the subject/s will be available at outlets of publisher/s. Please visit IIBF website www.iibf.org.in under the menu "Exam Related" for details of book/s and address of publisher/s outlets. Candidates are advised to make full use of the courseware. However, as banking and finance fields are dynamic, rules and regulations witness rapid changes. Therefore, the courseware should not be considered as the only source of information while preparing for the examinations. Candidates are advised to go through the updates put on the IIBF website from time to time and go through Master Circulars / Master Directions issued by RBI and publications of IIBF like IIBF Vision, Bank Quest, etc. All these sources are important from the examination point of view. Candidates are also to visit the websites of organizations like RBI, SEBI, BIS, IRDAI, FEDAI etc. besides going through other books & publications covering the subject / exam concerned etc. Questions based on current developments relating to the subject / exam may also be asked.
Cut-off Date of Guidelines / Important Developments for Examinations
The Institute has a practice of asking questions in each exam about the recent developments / guidelines issued by the regulator(s) in order to test if the candidates keep themselves abreast of the current developments. However, there could be changes in the developments / guidelines from the date the question papers are prepared and the dates of the actual examinations.
In order to address these issues effectively, it has been decided that:
(i) In respect of the examinations to be conducted by the Institute for the period February to July of a calendar year, instructions / guidelines issued by the regulator(s) and important developments in banking and finance up to 31st December will only be considered for the purpose of inclusion in the question papers".

(ii) In respect of the examinations to be conducted by the Institute for the period August to January of a calendar year, instructions / guidelines issued by the regulator(s) and important developments in banking and finance up to 30th June will only be considered for the purpose of inclusion in the question papers.

The table given below further clarifies the situation.

Cut-off Date of Guidelines / Important

Particulars	Developments for Examination/s
For the examinations to be conducted by the Institute for the period February 2018 to July 2018	31st December 2017
For the examinations to be conducted by the Institute for the period August 2018 to January 2019	30th June 2018

INDEX

2. Syllabus
Certificate Examination in Prevention of Cyber Crimes and Fraud Management

The details of the prescribed syllabus which is indicative are furnished below. The Institute however,also reserves to itself the right to vary the syllabus / rules / fee structure from time to time. Any alterations made will be notified.

Module - A :
Cyber Crime Overview :
1. Introduction to Cyber Crime : Concepts and Techniques

2. Channels of Cyber Crimes

3. Cyber Crime Methods

• Stalking & Cyber Squatting

• Cyber Extortion & Cyber Cheating

• Cyber warfare & Cyber Terrorism

• Phishing & Hacking

4. Computer Insecurity

• Internet Crime & Internet fraud

• User Failures & Causes

• Bank Failure

5. Computer Hackers

Module - B :
Fraud Management :
6. Computer Fraud Protection

• Prevention Controls

• Detection Controls

• Mitigation Controls

• Encryption / Decryption

7. Incident of Cyber crimes

• Cyber Crime Reporting

• Cyber Crime Investigation

• Cyber Crime Management

• Evidence Collection & Chain of Custody

• Cyber Crime Risk Management

• Cyber Forensics

Module - C :
Electronic Transactions :
8. Online Transactions - (Concepts, Emerging Trends and Legal Implications)

9. Global Payment Processing

10. Payment Cards & Data Security

11. Electronic Card Frauds
• ATM Cards
• Credit Cards
• Smart Cards
Module - D :
Cyber Laws & Regulatory Compliance :
12. Cyber Law in India

• Information Technology Act - 2000

13. Electronic Transactions and Taxation Issues

14. Human traits

• Associates

• Behavior

15. Regulatory Compliance

Short notes (Important Points for Prevention of cyber fraud & crime exam point of view)

- 3 aspects of crime fraud triangle are 1.Need 2. Opportunity 3. Rationalization(Criminal commits the crime himself)
- cyber-crime is not defined in IT act 2000 and amendment 2008 also
- Crimes comes under Indian penal code 1860
- Script kiddies means hacker who is having lacks of any serious technical expertise like child –like manner
- Spammers ..spam like keep sending advertisement and discount offer mails
- Vulnerabilities are the opportunities provided by system itself
- Threat vector to understand the modes of operandi
- In case of copy right infringement to the actual offender Vitim can apply for **John doe order**
- Which is legal remedy to obtained untraced offender

Import acts Information Technology (Amendment) Act, 2008 (hereinafter referred to as 'Amendment Act'), has been passed by the Lok Sabha on 22nd December 2008 and by Rajya Sabha on 23rd December 2008 and received the assent of the President on 5th February 2009. The Act came into force with effect from 27th October 2009. By the Amendment Act, various provisions of Information Technology Act, 2000 (hereinafter IT Act or 'the Act') have been amended and the major amendments are described hereunder.

- Tampering with computer source Documents Sec.65
- Hacking with computer systems , Data Alteration Sec.66
- Sending offensive messages through communication service, etc Sec.66A
- Dishonestly receiving stolen computer resource or communication device Sec.66B
- Identity theft Sec.66C
- Cheating by personation by using computer resource Sec.66D
- Violation of privacy Sec.66E
- Cyber terrorism Sec.66F
- Publishing or transmitting obscene material in electronic form Sec .67
- Hackers scans the computer pre attack to identify - Vulnerability in the systemPunishment for publishing or transmitting of material depicting children in sexually explicit act, etc.
- in electronic form Sec.67B
- Preservation and Retention of information by intermediaries Sec.67C
- Powers to issue directions for interception or monitoring or decryption of any information through
- any computer resource Sec.69
- Power to issue directions for blocking for public access of any information through any computer
- resource Sec.69A
- Power to authorize to monitor and collect traffic data or information through any computer resource
- for Cyber Security Sec.69B
- Un-authorized access to protected system Sec.70

- Penalty for misrepresentation Sec.71
- Breach of confidentiality and privacy Sec.72
- Publishing False digital signature certificates Sec.73
- Publication for fraudulent purpose Sec.74
- Fast flux is a networking technique changing IP address in very fast and frequent intervals
- Hackers scans the computer pre attack to identify due to Vulnerability in the system
- Cyber stalking simple personal harassment
- Cyber squatting means occupying the space in a Internet domain name or registing domain. Simply by trademark issues
- ICANN international organisation IPAddres space, NIXI for india
- Cyber extortion Threatening someone by force in digital world. Recently happen Ransomware attack
- In Cyber warfare supervisory control will take place..SCADA
- CIA Triad

"Confidentiality" means information is accessible only to those authorized to have access.

- "Integrity" means safeguarding the accuracy and completeness of information and processing methods

- "Availability" means ensuring that authorized users have access to information and associated assets as per commitment when required

- Non repudiation will tell creator ,sender,receiver& network providers has own responsibilty to send message to next stage properly.
- Authorisation will confirm the authorized user access
- Authentication will authenticated the type of transaction by the user
- 1 factor Authentification 1FA.. simply PIN access
- 2FA …. OTP & PIN
- 3FA….2FA+ Biometric access
- Electronic Signature As per Section 2(ta) of the IT Act, as inserted by the Amendment Act, 'Electronic Signature' means the authentication of any electronic record by a subscriber by means of the electronic techniques specified in the Second Schedule to the IT Act and includes digital signature.'Electronic Signature Certificate' has been defined as an Electronic Signature Certificate issued under Section 35 and includes Digital SignatureCertificate [Section 2(tb)]. (As per Section 35, any person can make an application to the Certifying Authority for the issue of a Electronic Signature Certificate, by paying the prescribed fee and giving such other details) A new Section has been inserted as Section 3A, wherein it is stated that notwithstanding anything in respect of the authentication of an electronic record by affixing digital signature (under Section 3), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule. For this purpose, an electronic signature or electronic authentication technique shall be considered reliable, if –

(i) the signature creation data or the authentication data are, withinthe context in which they are used, linked to the signatory or, as the case may be, the authenticator and no other person;

(ii) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(iii) any alteration to the electronic signature made after affixing such signature is detectable;

(iv) any alteration to the information made after its authentication by

electronic signature is delectable; and

(v) electronic signature should also fulfil such other conditions which may be prescribed under the rules.

- Trapdoors..Disabling access controls intentionally
- Trespassing.. gaining access to hardware resource
- Masquerading using fake ID getting access
    - CRYPTOGRAPHY

There are two basic types of Encryption algorithms:

(i) Symmetric encryption
(ii) Asymmetric Encryption
Symmetric Encryption: In this encryption technique the sender and receiver encrypts and decrypts the message with the same key. Examples are Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, 3DES, Skipjack etc.

Asymmetric encryption: In this encryption technique the sender encrypts the message with the receiver's public key and the receiver decrypts the information with recipient's private key. Hence this technique is called public key encryption. Examples are: Diffie-Hellman, RSA, ECC, ElGamal, DSA etc.

Among the various models of symmetric cipher analyzed the Rijndael is the best. Actually it is the role model of DES and AES. This model is adopted by different information security agencies like NSA, NIST and FIPS.

Among the various asymmetric ciphers, RSA is a moderate and most useful cipher for small data encryption like digital signature, ATM Pin etc.

But as discussed above, RSA (asymmetric technique) is much slower than Rijndael (symmetric technique) and other symmetric cipher techniques. But the scalability of asymmetric cryptosystem is far higher than the symmetric cryptosystem. Thus where the number of users is huge and required keys are very high, asymmetric cryptosystem proves to be superior.

- A few more kinds of attacks

- **Phishing:** Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Phishing has become rampant now a days and entities worldwide have lost their sensitive data and money.

- **Spoofing:** In the context of computer security, a spoofing attack is a situation in which one person or program successfully pretending as another by falsifying data, thereby gaining an illegitimate

advantage. Spoofing is of two types. (1) Email spoofing is the creation of email messages with a forged sender address. Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message. (2) Network spoofing-in computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system.

- **Sniffing:** Sniffing is the act of intercepting and inspecting data packets using sniffers (software or hardware devices) over the network. On the other hand, Spoofing is the act of identity

- impersonation. Packet sniffing allows individuals to capture data as it is transmitted over a network and is used by network professionals to diagnose network issues, and by malicious users to capture unencrypted data, like passwords and usernames.

- **Spamming**: Electronic spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media too. Spam can also be used to spread computer viruses, Trojan or other malicious software. The objective may be identity theft, or worse (e.g., advance fee fraud). Some spam attempts to capitalize on human greed, while some attempts to take advantage of the victims' inexperience with computer technology to trick them (e.g., phishing).

- **Ransomware**: Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the computer's Master File Table (MFT) or the entire hard drive. Thus, ransomware is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key.

Some examples of ransomware are Reveton, Cryptolocker, Cryptowall, Fusob and WannaCry. Wide-ranging attacks involving encryption-based ransomware began to increase through Trojans such as CryptoLocker, which had procured an estimated US$3 million before it was taken down by authorities, and CryptoWall, which was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over $18m as ransom money by the attackers by June 2015.

In May 2017, the WannaCry ransomware attack spread through the Internet, using an exploit vector that Microsoft had issued a "Critical" patch for (MS17-010) two months before on March 14, 2017. The ransomware attack infected lakhs of users in over 150 countries, using 20 different languages to demand money from users.

Measures against attacks

Against Phishing attacks, obviously there cannot be an antivirus tool for checking. Only appropriate user education and generating awareness can prevent or reduce phishing menace

Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message

To protect against sniffing, we need to encrypt all important data we send or receive, scan our networks for any issues or dangers and use only trusted Wi-Fi networks.

To prevent spamming, most of the email services, viz., Gmail, Yahoo, Hotmail etc. provide filtering facilities and also enable users to categorize certain messages as spam.

Best measures for protection against ransomware are taking regular backups of data, applying OS patches regularly and using latest anti-malware solution.

- **Types of Computer Frauds**

1. Sending hoax emails to scare people
2. Illegally using someone else's computer or "posing" as someone else on the internet
3. Using spyware to gather information about people
4. Emails requesting money in return for "small deposits"
5. Pyramid schemes or investment schemes via computer with the intent to take and use someone else's money
6. Emails attempting to gather personal information used to access and use credit cards or social security numbers
7. Using the computer to solicit minors into sexual alliances
8. Violating copyright laws by coping information with the intent to sell it
9. Hacking into computer systems to gather large amounts of information for illegal purposes
10. Hacking into or illegally using a computer to change information such as grades, work, reports, etc.
11. Sending computer viruses or worms with the internet to destroy or ruin someone else's computer

Precautions

Refrain from opening e-mail and e-mail attachments from individuals you do not know. Have ALL external storage devices scanned by virus-scanning software before inserted on your PC. Secure your Internet Web browsing.

- Compensation for Failure to Protect Data

A new Section 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gains to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. The explanation to Section 43A defines 'body corporate' as any company including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. Further, 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for thetime being in force and in the absence of such agreement or any law, suchreasonable security practices and procedures as may be prescribed by theCentral Government in consultation with such professional bodies rassociations as it may deem fit. 'Sensitive personal data or information'means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or association as it may deem fit

- **Computer related Offences**

Section 66 of the IT Act prior to its amendment, dealing with 'Hacking with Computer System' has been substituted with a new Section titled as 'Computer related Offences'. As per the new Section, if any person dishonestly or fraudulently does any act for damage to computer system, etc. as stated 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 Rs.5 lacs or with both. For the purpose of this Section, the words 'dishonestly' and 'fraudulently' shall have the meanings assigned to it in Section 24 and 25 of Indian Penal Code respectively.A host of new Sections have been added after Section 66 as Sections 66A to 66F prescribing punishment for offences such as, obscene electronic message transmissions, identity theft, cheating by impersonation using computer resources, violation of privacy and cyber terrorism. The details of such offences are given below. Section 66A deals with punishment for sending offensive messages through communication services, etc. As per this section, any person who sends by means of a computer resource or a communication device, -

(i) any information that is grossly offensive or has menacing character; or

(ii) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, persistently by making use of such computer resources or a communication device; or

(iii) any electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term, this may extend to three years and with fine.

For the purpose of above stated Section, terms 'electronic mail' and 'electronic mail message' means a message or information created or transmitted or received on a computer or a computer system, computer resources or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Section 66B deals with the punishment for dishonestly receiving stolen computer resource or communication device. As per this Section, whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe, the same to be stolen computer resource or communication device shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to one lac rupees or with both.

Section 66C deals with the punishment for identity, theft. As per this Section, whoever fraudulently or dishonestly makes 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 one lac rupees. Section 66D deals with the punishment for cheating by personation by using computer resource. As per this Section, whoever by means for any communication device or computer resource, cheats by personating, shall be punished with the 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 lac rupees.

Section 66E deals with the punishment for violation of privacy. As per this Section, whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding Rs.2 lacs or with both.

Section 66F deals with the punishment for cyber terrorism. As per this Section, whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend imprisonment for life. The offence of cyber terrorism has been defined as whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resources; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information, infrastructure specified under the Section 70 dealing with protected system.

- ***And more points exam point of view***

1. Who Coordinates with Interpol in India ? - CBI
2. Which department was designated as Nodal Agency for Cyber Crime prevention - CERT-IN
3. What is the difference between Virus and Worm - Virus need human intervention to activate or multiply whereas worm automatically get multiplied
4. Worms are mainly used by hackers to - Occupy more space in the system/heavy usage of bandwidth in the network
5. One of the employee carefully watching the password entered by the Manager. What type of threat it is - Shoulder Surfing
6. Leaving a Logged in Computer by an employee - is human negligence
7. Hackers scans the computer pre attack to identify - Vulnerability in the system
8. Hackers inject worms/virus into the network to reach the target system and it - exploits the Vulnerability
9. Non updation of antivirus is - one of the major vunerability
10. One customer recieved a call in his mobile phone and the person posing himself as a bank manager collected the card credentials from him.This type is called - Phising
11. Online Banking sites are borne to what risk - Phising/IP spoofing
12. Data transfer between systems vide Network can be secured by - PKI
13. Customers can make sure that they deal with the authenticated website - by checking the Lock icon near the address bar
14.In https, S denotes - Secured/Security
15.This kind of worms directly attacks the root directory - Rootkits
16. This worms are really hard to detuct and delete - Rootkits
17. The compromised systems in the network are commonly termes as - Zombies
18. Customer security credentials were compromised by way of fraudulent SMS is called - smishing
19. The employees who try to hack their own company's site/find the vulnerabilities are called - White hat hackers
20.DDos - Distributed Denial of Service
21.Ransomware which blocks the access to the website demanding ransom for the same is - Denial of Service attack
22. Using same method for both encryption and decryption is called - symmetric encryption
23. Providing Last Login detail in Internet banking site is to - to detect any unauthorised usage earlier
24.Limits for retrying the passwords is - to avoid the unauthorised access
25. To safeguard from the Key Loggers attack - Use Virtual Key board to enter passwords
26.UTM stands for - Unified Threat Management
27.Setting up smoke detectors in the branch is - Detective Method
28.Placing Security guard in system room to avoid - Physical damage/attack on systems
29. Following the authorised person to enter into system room and making entry into the room is - Tailgatting
30.Dumbster Driving is a method - Searching for vulnerability in deleted files and data
31.FIrewall is - Intrusion Detection System
32.Authentication of electronic data/document can be assertained by - Digital Signature
33. When two or more persons illegally tries to enter into a critical room with single id/same id - Masquerading
34.Detection is normally - Post incedent
35. Post incident study mainly for the purpose of - study the impact of the attack and lessons for future prevention
36. Indian Agency working on Digital Forensics and Cyber security - C-DAC

37. OLTP refers to - On line Transaction Processing
38. OLTP is also termed as - Payment Gateway
39. Payment Gateway the Acquiring Bank to - Issuing bank through the Card Scheme to complete the transaction
40.Security Concerns arise in Payment Gateways are - At the User Level, Bank level and Merchant POS
41. Credit Card data theft through POS is falls under - Merchant PoS Security
42.Data encrypted using Private key can be decrypted by the public key available with - the Receiver
43. Cross verifying the Signature on the Slip against the Signature in the back side of the ATM card is doen by - the Merchant
44.Data should be secured in the following stages - Saved, Transit and Retrival
45.Intruder software in a network which attacks the data while in trnasit and thus commits data theft - Man in the Middle Attack
46. Captures a widows sessio for the purpose of data theft before it reaches the recipient is - Session Hijacking
47. Limits set for retrying of password is to avoid - Brute Force attack
48. ISSP stands for - Information System Security Policy
49.ICANN stands for - International Corporation for Assigned Names and Numbers
50.TLD stands for - Top Level Domain
51.Globally recognized set of rules defined for electronic records is - e-UCP
52.Technique used to redirect traffic from the infected device is called - Sinkholding
53. The technique which can intercept unencrypted data transit of mobile apps is called - Wi FI Snifing
54. This is one type of malware which doesnot affect the system/network - Ad-ware
55. This usually comes as a Pop up/add on screen which carries link for dubious websites - Ad-ware
56.EMV cards follow standard of - ISO/IEC No 7816
57. EMV cards follow this standard for Contactless card - ISO/IEC 14443
58. NFC is the technique used in contactless cards - Near Field Communication
59.PCI - DSS stands for - Plastic Card Industries - Data Security Standards
60. NFC cards works under - RFID Technology
61. Providing Access controls to employess based on roles/need is - Risk based Authentication
62. Seeking PIN to complete a transaction in PoS is - 2FA
63.SSL - Secure Socket Layering
64.SSL ensures - Encrypted link between a web server and a browser
65. Sending annoying messages to a person causing irritation/nuisance - Cyber Stalking
66. Black mailing a person using Computer/or network is - Cyber Extortion
67. Ransomware is type of - Cyber Extortion
68. Disputes on Domain names and protest are redressed globally by - UDRP
69. Phising/Vishing is type of - Cyber Cheating
70. Group of people attacks a Computer/ group of computers for propagating a objective - Cyber Terrorists
71. Hackers with common interest attack rival government's department site and database are - Cyber terrorists
72. ____ refers to the quality of secrecy associated with the data and the state of keeping an information asset secret - Confidentiality
73.____ refers to the state of remaining in the same format and not allowing for any tampering/manipulation - Integrity
74. ____ refers to the state o confirmation that the user has the authority to issue the command to the system - Authorisation

75. Quality of non denial, the stake holders are not permitted to denythe particular act of doing the act is - Non-repudiation
76. CAPTCHA refers to - Completely Automated Public Turing test to Tell Computers and Humans Apart
77. Placing letters in different sizes and styles which is hard to read by systems/robots is called - CAPTCHA
78. _____ is an important component for study and analysis to under the modus operandi of a Cyber Attack - Threat Vector
79. In cyber Crime, Threat landscape is denoted as - Study of entire overview of the network which was attacked
80. Conventional Crimes are - Physical crimes that involve thet of systems and hardware devices
81.Cyber Crimes are - System Crimes that involves data theft or tampering
82.Insider Attack Threat is - attack on the system/network by own employee without any permission/authentication
83._____ is the most dangerous attack in cyber crimes - Insider Attack
84. An employee copied and sold the sensitive information to a competitor concern is an example of - Insider Attack
85. Hackers scan the port/system and develop worm or codes to attack the same based on this - Vulnerability
86. ____ doesnot wait for any executable file to run for getting activated in the target system - Worm
87.____ refers to small piece of programs injected into the target system to spy on the activities - Spyware
88. Drones are classified as - Spying Devices
89. UAV stands for - Unmanned Aerial Vehicle
90. Most of the UAV used by the polic/defence authorities for - Surveliance purposes
91.The persons who are hired by companies to hack their own website/to identify the Vulnerability are - Blue Hat Hackers
92. System of effectively taking care of URL filterig, web-filtering, anti-virus, as all in one solution is referred as - Unified Threat Management
93. Force Log out option in Internet banking after certain time of Idleness is to guard the system against - Session Hijacking
94. Installing anti virus into the system is - Preventive Method
95.A statement used to create, alter, drop objects in a database is called - Data Definition Language
96. Fault Detection, isolation nad recovery are closely associated wiht - Detection Control
97. Installing Bio Metric devices to check unauthorised entry is - Physical Control
98. Unless properly logged, straightaway accessing the database through a SQL is termed as - Back end Access
99.IT Act 2008 describes the activity of hacking as a criminal activity in section no 66
100. IT Act 2000 came in force on - 17 October 2000
101. IT Amendment Act came into force on - 27 October 2009
101. IT Act consists of - 13 Chapters and 90 Sections
102. The Section which deals with cyber crimes as civil offence - Section 43
103. The Section deals with cyber crimes as Criminal Offences - Section 66
104. IT Amendment Act included the following which is not in the IT Act 2000 - Electronic Signature
105. Electronic Signature has been dealt in - Section 15
106. Under Section 43A, if any body corporate handling any sensitive personal data is negligent in implementing and maintaining reasonable security the compensation may go upto - five crore rupees
107. Under Section 43, if one found guilty on Data theft/alters/destroys the same the

penalty/compensation may go upto - One Crore rupees
108. Tampering with Computer Source Documents - Section 65
109. Punishment under Section 65 may go upto - Three years imprisonment and extend upto Two Lakhs Fine
110. Computer Related offences which were dealt under section 43 can also be dealt as criminal offence under section - 66
111. Punishment under Section 66 may go upto - two three years and/or fine upto five lakhs rupees
112. Crime of Cyber Stalking (sending electronic messages for the purpose of causing annoyance/inconvenience/decieve/mislead the recipient) may lead to - two three years imprisonment
113. Identity Theft is dealt under Section - 66c
114. Punishment of Identity Theft - may extend to three years term and/or fine upto One lakhs rupees
115. Puishment for Cyber Cheating - may extend to three years term and/or fine upto One lakhs rupees
116. Cyber Cheating is dealt under - Section 66D
117. Punishment for Cyber Terrorism may extend upto - Life time Imprisonment
118. Cyber Terrorism is dealt under - Section 66F
119. Publishing obscene material in electronic form dealt under - Section 67
120. Punishment under Section 67 may extend upto - two three years term and/or five lakhs fine
121. Punishment for Sudsequent conviction of the same crime under section 67 is - 5 years term and/or ten lakhs rupees fine
122. Sexually explicit content in electronic form dealt under - Section 67A
123. Punishment under Section 67A is - Five years term with fine
124.Punishment for Sudsequent conviction of the same crime under section 67A is - 7 years term and/or ten lakhs rupees fine
125. CERT-IN has been designated as Nodal agency for Critical Information Infrastructure Protection under Section - 70B
126. Mispresentation/Suppression of material Fact dealt under - Section 71
127. Penalty under Section 71 - Two years term and/or fine upto One lakh rupees
128. Breach of confidentiality and Privacy dealt under Section - 72
129. Analysing the style of writing or the langauage style for the purpose of Crime Investigation is - Stylometry
130. RBI issues licenses for Payment Banks in India based on approval from - BPSS
131. NTRO stands for - National Technical Research Organisation
132. Netra, the light weight UAV was developed by - DRDO
133.NCIIPC stands for - National Critical Information Infrastructure Protection Centre
134. DSCI - Data Security Council of India
135. Digital Forensic tools used by our Police Department were developed by - C-DAC
136. C-DAC stands for - Centre for Development of ADvanced Computig
137. NTRO works under - Prime Minister's Office
138. Two acts which are mainly handled by ED - FEMA and PMLA
139. Money laundering using banking systems/Internet banking is - Conventional Crime
140. Obtaining an IP address similar to some other and demanding a ransom for forego the same is - Cyber Squatting
141. Data Protection while in transit using non repudiation techniques can be achieved through - Public Key Infrastructure
142. Card Skimming is a technique mostly used th steal the card details and it mostly placed on - ATM manchines
143. Card Skimming Data Theft can be avoided using - Contactless Cards/NFC Cards

144. To avoid the Card Credentials in Online sites these cards were introduced - Virtual Cards
145. Smart Cards which are loaded with Money prior to issue is called - Prepaid Cards
146. Virtual Cards normally comes with a validity of - 24 hours to 48 hours
147. Maximum loading permitted in a Prepaid as per RBI instruction is - 50000/-
148. Hackers try to capture the login credentials by analysing the keys pressed in the Key boards. the worms captures such data is called as - Key Loggers
149. By clicking unauthenticated link, customers may diverted to fake websites to capture the sensitive personal. This is type of - Website spoofing/IP Spoofing
150. Ad wares are used not to harm the computers but to - make a catch by making the user to click on the dubious link to fake websites

Now for Subjective knowledge

Cyber Crimes in India

The advancement of technology has made man dependent on Internet for all his needs. Internet has given man easy access to everything while sitting at one place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the medium of internet. Internet is used in almost every sphere. With the development of the internet and its related benefits also developed the concept of cyber crimes. Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day.

In a report published by the National Crime Records Bureau report (NCRB 2011), the incidence of cyber crimes under the IT Act has increased by 85.4% in the year 2011 as compared to 2010 in India, whereas the increase in incidence of the crime under IPC is by 18.5% as compared to the year 2010. Visakhapatnam records the maximum number of incidence of cases. Maharashtra has emerged as the center of cyber crime with maximum number of incidence of registered cases under cyber crimes. Hacking with computer systems and obscene publication were the main cases under IT Act for cyber crimes. Maximum offenders arrested for cyber crimes were in the age group 18-30 years. 563 people in the age group 18-30 years were arrested in the year 2010 which had increased to 883 in the year 2011.

1.1 Cyber Crime Types

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism,

creation and/or distribution of viruses, Spam and so on.

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

DIFFERENT TYPES OF CYBER CRIMES

Cyber Crimes can be categorized in two ways:

1. The crimes in which the computer is the target. Examples of such crimes are hacking, virus attacks, DOS attack etc.

2. The crime sin which the computer is used as a weapon. These types of crimes include cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc.

DIFFERENT KINDS OF CYBER CRIMES
The different kinds of cyber crimes are:

1. Unauthorized Access and Hacking:
Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

2. Web Hijacking:
Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

3. Cyber Stalking:
In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

How do Cyber Stalkers operate?
They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

a. The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.
b. People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

c. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

d. Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

e. In online stalking the stalker can make third party to harass the victim.

f. Follow their victim from board to board. They "hangout" on the same BB's as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will "flame" their victim (becoming argumentative, insulting) to get their attention.

g. Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

h. Contact victim via telephone. If the stalker is able to access the victim's telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.

i. Track the victim to his/her home.

4. Denial of service Attack:

This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

5. Virus attacks:

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available.

Trojan Horse is a program that acts like something useful but do the things that are quiet damping. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

6. Software Piracy:

Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them .

7. 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 the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

8. Phishing:

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an

attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

9.Sale of illegal articles:
This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

10. Online gambling :
There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.

11. Email spoofing :
Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

12. Cyber Defamation:
When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

13. Forgery:
Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

14. Theft of information contained in electronic form :
This includes theft of information stored in computer hard disks, removable storage media etc.

15. Email bombing :
Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

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

17. Internet time theft :
Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

18. Theft of computer system :
This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

19. Physically damaging a computer system :
This crime is committed by physically damaging a computer or its peripherals.

20. Breach of Privacy and Confidentiality :
Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information.
Confidentiality means non disclosure of information to unauthorized or unwanted persons. In addition to Personal

information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.
Generally for protecting secrecy of such information, parties while sharing information forms an agreement about he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality. Special techniques such as Social Engineering are commonly used to obtain confidential information.

21. Data diddling:
Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also include automatic changing the financial information for some time before processing and then restoring original information.

22. E-commerce/ Investment Frauds:
An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

23. Cyber Terrorism:
Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.
Cyber terrorism is an attractive option for modern terrorists for several reasons.
It is cheaper than traditional terrorist methods.
Cyber terrorism is more anonymous than traditional terrorist methods.
The variety and number of targets are enormous.
Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
Cyber terrorism has the potential to affect directly a larger number of people.
The list of offenses given above is not exhaustive and would also include any other types of offenses that would be committed through a computer or against a computer in the future

2. CYBER LAWS

Introductory background for Cyberlaws :

Since the beginning of civilization, man has always been motivated by the need to make progress and better the existing technologies. This has led to tremendous development and progress which has been a launching pad for further development. Of all the significant advances made by mankind from the beginning till date, probably the important of them is the development of Internet. To put in a common man's language, Internet is a global network of computers, all of them speaking the same language. In 1969, America's Department of Defense commissioned the construction of a Super network called ARPANET. The Advanced Research Projects Agency Network (ARPANET), basically intended as a military network of 40 computers connected by a web of links & lines. This network slowly grew and the Internet was born. By 1981, over 200 computers were connected from all around the world. Now the figure runs into millions.

The real power of today's Internet is that it is available to anyone with a computer and a telephone line. Internet places at an individual's hands the immense and invaluable power of information and communication.

Internet usage has significantly increased over the past few years. The number of data packets which flowed through the Internet have increased dramatically. According to International Data Corporation ("IDC"), approximately 163 million individuals or entities will use the Internet by the end of this year as opposed to 16.1 million in 1995. If left to its own measure, it is highly unlikely that such a trend can reverse itself. Given this present state of the Internet, the necessity of Cyberlaws becomes all the more important.

Need for Cyber law :

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws.

What is Cyber law :

Internet is believed to be full of anarchy and a system of law and regulation therein seems contradictory. However, cyberspace is being governed by a system of law and regulation called Cyberlaw. There is no one exhaustive definition of the term “Cyberlaw”. Simply speaking, Cyberlaw is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyberlaw. The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyberlaw.

Importance of Cyberlaw

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Cyber crimes are anew class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes.

The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

2.1. Cyber crimes under the IT Act :

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

2.2. Cyber Crimes under IPC and Special Laws :

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

2.3. Cyber Crimes under the Special Acts:

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Arms Act

Cyber crime act in India:

1. Tampering with computer source Documents Sec.65
2. Hacking with computer systems , Data Alteration Sec.66
3. Sending offensive messages through communication service, etc Sec.66A
4. Dishonestly receiving stolen computer resource or communication device Sec.66B
5. Identity theft Sec.66C
6. Cheating by personation by using computer resource Sec.66D
7. Violation of privacy Sec.66E
8. Cyber terrorism Sec.66F
9. Publishing or transmitting obscene material in electronic form Sec .67
10. Publishing or transmitting of material containing sexually explicit act, etc. in electronic form Sec.67A
11. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form Sec.67B
11. Preservation and Retention of information by intermediaries Sec.67C
12. Powers to issue directions for interception or monitoring or decryption of any information through

any computer resource Sec.69
13. Power to issue directions for blocking for public access of any information through any computer resource Sec.69A
14. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security Sec.69B
15. Un-authorized access to protected system Sec.70
16. Penalty for misrepresentation Sec.71
17. Breach of confidentiality and privacy Sec.72
18. Publishing False digital signature certificates Sec.73
19. Publication for fraudulent purpose Sec.74
29. Act to apply for offence or contraventions committed outside India Sec.75
21. Compensation, penalties or confiscation not to interfere with other punishment Sec.77
22. Compounding of Offences Sec.77A
23. Offences with three years imprisonment to be cognizable Sec.77B
24. Exemption from liability of intermediary in certain cases Sec.79
25. Punishment for abetment of offences Sec.84B
26. Punishment for attempt to commit offences Sec.84C
Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act
27. Offences by Companies Sec.85
28. Sending threatening messages by e-mail Sec .503 IPC
29. Word, gesture or act intended to insult the modesty of a woman Sec.509 IPC
30. Sending defamatory messages by e-mail Sec .499 IPC
31. Bogus websites , Cyber Frauds Sec .420 IPC
32. E-mail Spoofing Sec .463 IPC
33. Making a false document Sec.464 IPC
34. Forgery for purpose of cheating Sec.468 IPC
35. Forgery for purpose of harming reputation Sec.469 IPC
36. Web-Jacking Sec .383 IPC
37. E-mail Abuse Sec .500 IPC
38. Punishment for criminal intimidation Sec.506 IPC
39. Criminal intimidation by an anonymous communication Sec.507 IPC
40. When copyright infringed:- Copyright in a work shall be deemed to be infringed Sec.51
41. Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of Sec.63
42. Enhanced penalty on second and subsequent covictions Sec.63A
43. Knowing use of infringing copy of computer programme to be an offence Sec.63B
44. Obscenity Sec. 292 IPC
45. Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail Sec.292A IPC
46. Sale, etc., of obscene objects to young person Sec .293 IPC
47. Obscene acts and songs Sec.294 IPC
48. Theft of Computer Hardware Sec. 378
49. Punishment for theft Sec.379
50. Online Sale of Drugs NDPS Act
51. Online Sale of Arms Arms Act.

3.Cyber crime methods

3.1 Cyber stalking:

Cyberstalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium. Cyberstalking can also occur in conjunction with the more traditional form of stalking, where the offender harasses the victim offline. There is no unified legal approach to cyberstalking, but many governments have moved toward making these practices punishable by law.

Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking

3.2. DOMAIN NAMES:

IP address :

The Internet is a network of computers. Each computer on the said network has its own distinct entity and presence. That is the reason why every computer is given a distinct Electronic Address called the Internet Protocol address or in short IP address. This IP address is given by numerical values like 202.54.15.75. The IP address is just like any telephone number which identifies a particular computer on the Internet.

Domain Name :

Since it is not possible to remember each and every numerical value of an IP address, the system of domain names evolved. Internet domain names, in a common man's language, are used as an easy-to-remember alias which point to a specific IP address. The dominant purpose of the domain name is simply to provide an easy method for remembering another's electronic address. It's a unique name used to identify, among other things, a specific Web site. Thus a typical domain name would be http:// www.iibf.org

Components of a Domain Name :

Any domain name consist of two components, namely the top level domain name(TLD) and a second level domain name. Thus in the said example, http://www.iibf.org, ".org" would be the top level domain name while "iibf" would be second level domain name.

Categories of Top Level Domain Names (TLDs)

As on date, there are two categories of top level domain names. In the first category comes the domain names .com, .net, .org, .edu. When the system of registering domain names began, the norms were that the .com name is to be given to commercial organizations, while others such as .org, .net, .gov and .edu are to be assigned to non-commercial organizations, network providers, government agencies and educational institutions respectively. However, as time has passed, due to the enhanced volumes of domain name registrations, the said norms have been abandoned and today anyone can, without any restriction of any kind whatsoever, can register any domain name.

The second category of top level domain names is the country code TLDs denoted by a two letter country code. For instance, the top level domain name for India is .in. The responsibility for assigning the same is given in each country to a specified country domain name registrar. In India, the TLD.in is registered by NCST at Bombay.

The domain names were initially registered by Network Solutions only, who had the sole monopoly to register the said TLDs. This monopoly of Network Solutions continued for many years and only in 1999, the Internet Corporation Assigned Names and Numbers (ICANN) allowed other accredited registrars to register domain names. Today there are more than 100 registrars with whom one can register a TLD.

The unique feature of domain names is that the said domain names are given on "first come, first served"

basis. This feature of domain names gives rise to numerous legal issues and disputes. Thus the important thing in domain names registration is speed. To take an example, the domain name www.microsoft.org was available and was registered by Amit Mehrotra much before Microsoft Corporation could think of it. This led to numerous ticklish legal issues. Microsoft Corporation, despite having the trademark Microsoft, could not get the domain name www.microsoft.org because of the "first come, first served" criteria of domain name registration.

Domain Names different from Trade Marks :

To put it simply, Domain names are indeed different from trademarks. While it is possible that the same trademark may be registered by different persons in different categories and different lines of businesses, it may be possible to only register one domain name corresponding to such trademark. This aspect of domain names has led to numerous legal problems.

3.3 Cyber Squatting:

Another legal issue surrounding domain names is that of Cybersquatting. Cybersquatting is the practice by means of which a person or legal entity books up the trade mark, business name or service mark of another as his own domain name for the purpose of holding on to it and thereafter selling the same domain name to the other person for valuable premium and consideration. Cybersquatters book up domain names of important brands in the hope of earning quick millions .

3.1 Recent trends relating to tackling Cybersquatters

The Internet history has shown that while some corporate players have been willing to and have indeed coughed up money to get back their legitmate domain names, the recent trend is more towards taking the cybersquatters by the horns and fighting them out by legal processes. Courts throughout the world, including in India, have been proactive and have been granting injunctions to stop cybersquatters from operating their web sites.

3.2 Latest most effective remedy against Cybersquatting

The latest breath of fresh air in the fight against Cybersquatting has been the Uniform Domain Name Dispute Resolution Policy which has been duly approved by ICANN. Under the said Domain Names Dispute Resolution Policy, a summary procedure is adopted to adjudicate the complaint of any complainant relating to any domain name on payment of processing fees. This policy has been in operation since the end of last year.

Under the said policy, Indian companies are also beginning to get back their legitimate domain names. The domain name www.theeconomictimes.com and www.timesofindia.com have been won back under the said policy. Two recent success for Indian Companies under the said policy include winning back the domain names www.tata.org and www.philipsindia.com by TATA and Philips India respectively.

3.4 Cyber Extortion

Cyberextortion is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack.

Cyber-extortion can come in many different forms, but at its simplest, it is when someone online threatens some sort of harm unless you meet their demands.

For example, the cybercriminal may use "ransomware" to encrypt your data, which means you can't read your data without the encryption key – and the cybercriminal will withhold this key until payment is made.

Today, distributed denial-of-service (DDoS) attacks are the bread and butter of cyber extortionists. This is an attack where…

A hacker overwhelms a target's server with malicious traffic. Typically, the attacker will use a botnet (i.e., a network of infected computers) to generate a flood of traffic on the server.

The traffic sends more connection requests than a server can handle. Or, the botnet sends the target huge amounts of data to use up its bandwidth
.
The target's site is shut down. Believe it or not, some people pay extortionists to silence websites they don't like. Shutting down a small site or keeping a small organization offline for a week can cost as little as 10000/-

If a business doesn't meet the extortionist's demands, the hacker could keep the site offline long enough to run the business into the ground. Or, the hacker may be able to remotely access control panels and start deleting files necessary to keep the site or business running.

So what's at risk of being "held hostage" by cyber attackers?

Any of your…

Websites.

Computer systems.
Severs.

The attackers will only cease and desist when their demands have been met. Because most small businesses operate with the help of computers, cyber extortion is a growing problem.

3.5 Cyber warfare

Cyberwarfare is any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems. Waged via the Internet, these attacks disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and services.

Cyberwarfare is also known as cyber warfare or cyber war.

Cyberwarfare involves the following attack methods:

- Sabotage: Military and financial computer systems are at risk for the disruption of normal operations and equipment, such as communications, fuel, power and transportation infrastructures.
- Espionage and/or security breaches: These illegal exploitation methods are used to disable networks, software, computers or the Internet to steal or acquire classified information from rival institutions or individuals for military, political or financial gain.

3.6 Cyber Terrorism

A premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and subnational groups. The main aim behind cyber terrorism is to cause harm and destruction.

Cyber terrorism can be explained as internet terrorism. With the advent of the internet, individuals and groups are misusing the anonymity to threaten individuals, certain groups, religions, ethnicities or beliefs. Cyber terrorism can be broadly categorized under three major categories:

- Simple: This consists of basic attacks including the hacking of an individual system.
- Advanced: These are more sophisticated attacks and can involve hacking multiple systems and/or networks.
- Complex: These are coordinated attacks that can have a large-scale impact and make use of sophisticated tools

3.7 Phishing

Phishing is the fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification and account usernames and passwords. Using a complex set of social engineering techniques and computer programming expertise, phishing websites lure email recipients and Web users into believing that a spoofed website is legitimate and genuine. In actuality, the phishing victim later discovers his personal identity and other vital information have been stolen and exposed.

Similar to fishing in a lake or river, phishing is computer lingo for fishing over the Internet for personal information. The term was first used in 1996, when the first phishing act was recorded.

Phishing uses link manipulation, image filter evasion and website forgery to fool Web users into thinking that a spoofed website is genuine and legitimate. Once the user enters vital information, he immediately becomes a phishing victim.

Fortunately, phishing victimization is preventable. The following security precautions are recommended:

- Use updated computer security tools, such as anti-virus software, spyware and firewall.
- Never open unknown or suspicious email attachments.
- Never divulge personal information requested by email, such as your name or credit card number.

- Double check the website URL for legitimacy by typing the actual address in your Web browser.
- Verify the website's phone number before placing any calls to the phone number provided via ema

3.8 Vishing

Vishing is the illegal access of data via voice over Internet Protocol (VoIP).
Vishing is IP telephony's version of phishing and uses voice messages to steal identities and financial resources. The term is a combination of "voice" and "phishing."

Vishing attacks are designed to generate fear and immediate response and therefore occur within short time frames. They are difficult to trace.

For example, a vishing perpetrator (visher) may gain access to a group of private customer phone numbers. The visher may then call the group. When a potential victim answers the phone, he or she hears an automated recording informing him that his bank account has been compromised. He then calls the specified toll-free number to reset his security settings and hears another automated message requesting the user's bank account number and/or other personal details via the phone keypad.

3.9 Smishing

SMS phishing occurs when a cell phone receives a SMS (Instant Message or IM) from a fake person or entity. The unsuspecting cell phone user will respond to a fake SMS and visit a URL, inadvertently downloading malware and installing a Trojan without the user's knowledge. Phishing is all about extracting useful information, so in the case of SMS phishing, the Trojan harvests the data areas of the cellphone and transmits them to the person who created the Trojan at the earliest opportunity.

SMS phishing is also known as SMiShing.

SMS phishing attempts occur when cell phone user is the recipient of a message acknowledging receipt of an unknown purchase. To terminate bogus purchases and avoid monthly or daily charges, consumers are directed to phishing websites. Unknowingly, customers go directly to the website, allowing hackers to access personal cell phone information. SMS phishing has become increasingly prevalent on social website networks, such as Facebook.

SMS Phishing is a way of performing identity theft, as the inadvertently downloaded malware captures and transmits all of the stored cellphone data, including stored credit card details, names, addresses and other data, like password details for email accounts, which, when opened, increase the vulnerability of online banking and other accounts.

The malware can then cover its tracks by wiping the phone clean, including all call records, causing repeated rebooting or similar odd behavior rendering the phone unusable. Thus, the original phishing attack is easily unnoticed by the user.

Viruses and phishing scams are far reaching to all types of digital devices. Wise consumers should choose their products according to available product security software and data recovery technologies.

3.10 Pharming

Pharming refers to redirecting website traffic through hacking, whereby the hacker implements tools that redirect a search to a fake website. Pharming may cause users to find themselves on an illegitimate website without realizing they have been redirected to an impostor site, which may look exactly like the

real site.

Pharming occurs when hackers locate vulnerabilities in domain name server (DNS) software. Pharming can also occur by rearranging the host's file on the targeted computer. Online banking websites as well as e-commerce organizations have become popular pharming targets. Desktops are also vulnerable to pharming threats due to their lack of security administration. Pharming and phishing threats have been used simultaneously and these can cause the most potential for online identity theft. Unfortunately, anti virus and anti-spyware software are often incapable of protecting against this type of cybercrime

Routers have been surfacing as being just as vulnerable to pharming as hosts files. Unfortunately, router pharming is much more difficult to detect. Harmful DNS information can land on routers in two ways:

1. Existing administrator settings can be incorrectly configured
2. Entire rewrites of embedded software (also known as firmware) can occur

Routers give administrators the option to choose a trusted DNS as opposed to a suggested one. If the administrator isn't well-versed in computers, he or she should avoid a custom DNS, because hackers are more able to choose a DNS under the administrator's control compared to a legitimate one.

Pharming is certainly nothing new, but it is being used more often and is causing increasing harm in the computing world. Computer experts point the finger of blame at domain registrars for security loopholes and a general lack of standards for keeping domains exclusive. Suggestions for mitigating these problems include asking registrars for their written policies as well as insisting on immediate notification should a registrar receive a domain move request. Other suggestions include keeping domains locked and keeping authoritative contact information current, as well as using registrars with round-the-clock availability. If none of these suggestions works in preventing pharming, contacting **VeriSign**, which is the domain registry for .com and .net, may be useful

4.COMPUTER INSECURITY

Security and systems design

Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a trusted system. Some knowledgeable observers consider this to be a disastrous mistake, and point out that this distinction is the cause of much of the insecurity of current computer systems - once an attacker has subverted one part of a system without fine-grained security, he or she usually has access to most or all of the features of that system. [citation needed] Because computer systems can be very complex, and cannot be guaranteed to be free of defects, this security stance tends to produce insecure systems.

The 'trusted systems' approach has been predominant in the design of many Microsoft software products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use' over security. Since Microsoft products currently dominate the desktop and home computing markets, this has led to unfortunate effects. However, the problems described here derive from the security stance taken by software and hardware vendors generally, rather than the failing of a single vendor. Microsoft is not out of line in this respect, just far more prominent with respect to its consumer marketshare.

It should be noted that the Windows NT line of operating systems from Microsoft contained mechanisms to limit this, such as services that ran under dedicated user accounts, and Role-Based Access Control (RBAC) with user/group rights, but the Windows 95 line of products lacked most of these functions. Before the release of Windows 2003 Microsoft has changed their official stance, taking a more locked down approach. On 15 January 2002, Bill Gates sent out a memo on Trustworthy Computing, marking the official change in company stance. Regardless, Microsoft's operating system Windows XP is still plagued by complaints about lack of local security and inability to use the fine-grained user access controls together with certain software (esp. certain popular computer games).

Financial cost

Serious financial damage has been caused by computer security breaches, but reliably estimating costs is quite difficult. Figures in the billions of dollars have been quoted in relation to the damage caused by malware such as computer worms like the Code Red worm, but such estimates may be exaggerated. However, other losses, such as those caused by the compromise of credit card information, can be more easily determined, and they have been substantial, as measured by millions of individual victims of identity theft each year in each of several nations, and the severe hardship imposed on each victim, that can wipe out all of their finances, prevent them from getting a job, plus be treated as if they were the criminal. Volumes of victims of phishing and other scams may not be known.

Individuals who have been infected with spyware or malware likely go through a costly and time-consuming process of having their computer cleaned. Spyware and malware is considered to be a problem specific to the various Microsoft Windows operating systems, however this can be explained somewhat by the fact that Microsoft controls a major share of the PC market and thus represent the most prominent target.

Reasons

There are many similarities (yet many fundamental differences) between computer and physical security. Just like real-world security, the motivations for breaches of computer security vary between attackers,

sometimes called hackers or crackers. Some are teenage thrill-seekers or vandals (the kind often responsible for defacing web sites); similarly, some web site defacements are done to make political statements. However, some attackers are highly skilled and motivated with the goal of compromising computers for financial gain or espionage. An example of the latter is Markus Hess who spied for the KGB and was ultimately caught because of the efforts of Clifford Stoll, who wrote an amusing and accurate book, The Cuckoo's Egg, about his experiences. For those seeking to prevent security breaches, the first step is usually to attempt to identify what might motivate an attack on the system, how much the continued operation and information security of the system are worth, and who might be motivated to breach it. The precautions required for a home PC are very different for those of banks' Internet banking system, and different again for a classified military network. Other computer security writers suggest that, since an attacker using a network need know nothing about you or what you have on your computer, attacker motivation is inherently impossible to determine beyond guessing. If true, blocking all possible attacks is the only plausible action to take.

Vulnerabilities

To understand the techniques for securing a computer system, it is important to first understand the various types of "attacks" that can be made against it. These threats can typically be classified into one of these seven categories:

Exploits

Software flaws, especially buffer overflows, are often exploited to gain control of a computer, or to cause it to operate in an unexpected manner. Many development methodologies used by embedded software licensing professionals rely on testing to ensure the quality of any code released;; this process often fails to discover extremely unusual potential exploits. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in certain programs' processing of a specific file type, such as a non-executable media file.

Eavesdropping

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system (ie, with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware such as TEMPEST. The FBI's proposed Carnivore program was intended to act as a system of eavesdropping protocols built into the systems of internet service providers.

Social engineering and human error

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords. This deception is known as Social engineering.

Denial of service attacks

Denial of service (DoS) attacks differ slightly from those listed above, in that they are not primarily a means to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately guessing a wrong

password 3 consecutive times and thus causing the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behavior of whole networks needs to be analyzed, not only the behaviour of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers") are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion. Another technique to exhaust victim resources is through the use of an attack amplifier - where the attacker takes advantage of poorly designed protocols on 3rd party machines, such as FTP or DNS, in order to instruct these hosts to launch the flood. There are also commonly vulnerabilities in applications that cannot be used to take control over a computer, but merely make the target application malfunction or crash. This is known as a denial-of-service exploit.

Indirect attacks

Attacks in which one or more of the attack types above are launched from a third party computer which has been taken over remotely. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system.

Backdoors

Methods of bypassing normal authentication or giving remote access to a computer to somebody who knows about the backdoor, while intended to remain hidden to casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing "legitimate" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports. It may also fake information about disk and memory usage.

Direct access attacks

Common consumer devices that can be used to transfer data surreptitiously.
Common consumer devices that can be used to transfer data surreptitiously.

Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as keydrives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the harddrive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system.

Reducing vulnerabilities

Computer code is regarded by some as just a form of mathematics. It is theoretically possible to prove the correctness of computer programs though the likelihood of actually achieving this in large-scale practical systems is regarded as unlikely in the extreme by some with practical experience in the industry -- see Bruce Schneier et al.

It's also possible to protect messages in transit (ie, communications) by means of cryptography. One method of encryption —the one-time pad —has been proven to be unbreakable when correctly used. This method was used by the Soviet Union during the Cold War, though flaws in their implementation allowed some cryptanalysis (See Venona Project). The method uses a matching pair of key-codes,

securely distributed, which are used once-and-only-once to encode and decode a single message. For transmitted computer encryption this method is difficult to use properly (securely), and highly inconvenient as well. Other methods of encryption, while breakable in theory, are often virtually impossible to directly break by any means publicly known today. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

In practice, only a small fraction of computer program code is mathematically proven, or even goes through comprehensive information technology audits or inexpensive but extremely valuable computer security audits, so it's usually possible for a determined cracker to read, copy, alter or destroy data in well secured computers, albeit at the cost of great time and resources. Extremely few, if any, attackers would audit applications for vulnerabilities just to attack a single specific system. You can reduce a cracker's chances by keeping your systems up to date, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful backing up and insurance.

Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes:

1. Prevention,
2. Detection, and
3. Response.

* User account access controls and cryptography can protect systems files and data, respectively.
* Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.
* Intrusion Detection Systems (IDS's) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
* "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored.

Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and is normally implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide realtime filtering and blocking. Another implementation is a so called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet (though not universal, as demonstrated by the large numbers of machines "cracked" by worms like the Code Red worm which would have been protected by a properly-configured firewall). However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place.

Difficulty with response

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

* Identifying attackers is difficult, as they are often in a different jurisdiction to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymising procedures which make backtracing difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.

* The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (eg, cable modem) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks are made by automated vulnerability scanners and computer worms.

* Law enforcement officers are often unfamiliar with information technology, and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as DNA testing, and improved forensics mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increase

4.1 PILLERS OF INFORMATION SECURITY

Security is a constant worry when it comes to information technology. Data theft, hacking, malware and a host of other threats are enough to keep any IT professional up at night.

Information security follows three overarching principles:

- Confidentiality: This means that information is only being seen or used by people who are authorized to access it.
- Integrity: This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.
- Availability: This means that the information is accessible when authorized users need it.

Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. There are commonly five terms associated with the definition of information assurance:

- Integrity
- Availability

- Authentication
- Confidentiality
- Nonrepudiation

IA is a field in and of itself. It can be thought of as a specialty of Information Technology (IT), because an IA specialist must have a thorough understanding of IT and how information systems work and are interconnected. With all of the threats that are now common in the IT world, such as viruses, worms, phishing attacks, social engineering, identity theft and more, a focus on protection against these threats is required. IA is that focus.

1. Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

Confidentiality is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, integrity and nonrepudiation.

Sensitive information or data should be disclosed to authorized users only. In IA, confidentiality is enforced in a classification system. For example, a U.S. government or military worker must obtain a certain clearance level, depending on a position's data requirements, such as, classified, secret or top secret. Those with secret clearances cannot access top secret information.

Best practices used to ensure confidentiality are as follows:

An authentication process, which ensures that authorized users are assigned confidential user identification and passwords. Another type of authentication is biometrics.

Role-based security methods may be employed to ensure user or viewer authorization. For example, data access levels may be assigned to specified department staff.

Access controls ensure that user actions remain within their roles. For example, if a user is authorized to read but not write data, defined system controls may be integrated.

2. Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification. Integrity is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, confidentiality and nonrepudiation.

Data integrity maintenance is an information security requirement. Integrity is a major IA component because users must be able to trust information. Untrusted data is devoid of integrity. Stored data must remain unchanged within an information system (IS), as well as during data transport.

Events like storage erosion, error and intentional data or system damage can create data changes. For example, hackers may cause damage by infiltrating systems with malware, including Trojan horses, which overtake computer systems, as well as worms and viruses. An employee may create company damage through intentionally false data entry.

Data integrity verification measures include checksums and the use of data comparison

3.Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format. Availability is one of the five pillars of Information Assurance (IA). The other four are integrity, authentication, confidentiality and nonrepudiation.

When a system is regularly non-functioning, information availability is affected and significantly impacts users. In addition, when data is not secure and easily available, information security is affected, i.e., top secret security clearances. Another factor affecting availability is time. If a computer system cannot deliver information efficiently, then availability is compromised.

Data availability must be ensured by storage, which may be local or at an offsite facility. In the case of an offsite facility, an established business continuity plan should state the availability of this data when onsite data is not available. At all times, information must be available to those with clearance.

4 Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption. It is one of the five pillars of information assurance (IA). The other four are availability, integrity, confidentiality and authentication.

Nonrepudiation is often used for digital contracts, signatures and email messages.

By using a data hash, proof of authentic identifying data and data origination can be obtained. Along with digital signatures, public keys can be a problem when it comes to nonrepudiation if the message recipient has exposed, either knowingly or unknowingly, their encrypted or secret key..

5. In the context of computer systems, authentication is a process that ensures and confirms a user's identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and nonrepudiation.

Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.

A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems.

The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity. There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.

4.2 Two-Factor Authentication

Two-factor authentication is a security mechanism that requires two types of credentials for authentication and is designed to provide an additional layer of validation, minimizing security breaches.

Two-factor authentication is also known as strong authentication.

Two-factor authentication works with two separate security or validation mechanisms. Typically, one is a physical validation token, and one is a logical code or password. Both must be validated before accessing a secured service or product. Generally, an authenticating procedure requires a physical token or identity validation, followed by a logical password or personal identification number (PIN).

The security procedure for an ATM machine is a common example of two-factor authentication, which requires that a user possess a valid ATM card and PIN

4.3 Single Sign-On (SSO)

Single sign-on (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials. SSO is a common procedure in enterprises, where a client accesses multiple resources connected to a local area network (LAN).

SSO advantages include:

- Eliminates credential reauthentication and help desk requests; thus, improving productivity.
- Streamlines local and remote application and desktop workflow.
- Minimizes phishing.
- Improves compliance through a centralized database.

- Provides detailed user access reporting.

With SSO, a user logs in once and gains access to different applications, without the need to re-enter log-in credentials at each application. SSO authentication facilitates seamless network resource usage. SSO mechanisms vary, depending on application type.

SSO is not suited for systems requiring guaranteed access, as the loss of log-in credentials results into denial of access to all systems. Ideally, SSO is used with other authentication techniques, such as smart cards and one-time password tokens.

4.4 Software Security

Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication and availability.

Any compromise to integrity, authentication and availability makes a software unsecure. Software systems can be attacked to steal information, monitor content, introduce vulnerabilities and damage the behavior of software. Malware can cause DoS (denial of service) or crash the system itself.

Buffer overflow, stack overflow, command injection and SQL injections are the most common attacks on the software.

Buffer and stack overflow attacks overwrite the contents of the heap or stack respectively by writing extra bytes.

Command injection can be achieved on the software code when system commands are used predominantly. New system commands are appended to existing commands by the malicious attack. Sometimes system command may stop services and cause DoS.

SQL injections use malicious SQL code to retrieve or modify important information from database servers. SQL injections can be used to bypass login credentials. Sometimes SQL injections fetch important information from a database or delete all important data from a database.

The only way to avoid such attacks is to practice good programming techniques. System-level security can be provided using better firewalls. Using intrusion detection and prevention can also aid in stopping attackers from easy access to the system.

4.5 Hardware Security

A hardware security is a secure crypto processor focused on providing cryptographic keys and also provides accelerated cryptographic operations by means of these keys. The module acts as a trust anchor and provides protection for identities, applications and transactions by ensuring tight encryption, decryption and authentication for a variety of applications. The hardware security module includes protection features such as physical tamper resistance and strong authentication. Although the module is physically isolated like smart cards and back tapes, it provides a greater level of security as it does not have an operating system and is thus virtually invulnerable to attacks over a network.

Hardware security module systems come in different flavors and form factors, and are less susceptible to corruption and system failures. This is because they do not have an operating system and are externally attached to the device they are serving. Examples of hardware security module systems include physically shielded LAN appliances, smart cards and PCI plugin cards. Hardware security modules provide protection against internal and external intruders using two-factor authentication.

Hardware security modules provide many distinct benefits, including:

- Providing certifications that conform to security standards
- Dual control access protection
- Load distribution and reliability
- Support for all standard cryptographic algorithms
- Several transactions per second
- Greater availability of keys with just one hardware security module

The software and hardware present in the modules are specifically dedicated for security functions and thus provide faster and superior results.

4.6 Physical Security

Physical security describes measures designed to ensure the physical protection of IT assets like facilities, equipment, personnel, resources and other properties from damage and unauthorized physical access. Physical security measures are taken in order to protect these assets from physical threats including theft, vandalism, fire and natural disasters

Physical security is often the first concern in facilities with high asset concentration, especially that used in critical systems for business processes. Physical security is especially important for IT resources, as their proper operation demands that the hardware assets and infrastructure they are running on be kept away from anything that could hinder their function. This includes tampering by unauthorized personnel and unforeseen events like accidents and natural disasters.

There are two phases of physical security:

- Deterrence: Methods and measures that are meant to deter attackers and intruders or prevent natural events and accidents from affecting protected assets. The simple method for this is through the use of physical barriers and signs. The signs serve as a warning to any intruder that their actions will bring physical harm or prosecution. The physical barriers are meant to prevent access entirely or simply to provide protection from external factors like storms or vehicular accidents.
- Detection: Allows security personnel to detect and locate potential intruders using surveillance equipment like cameras, motion sensors, security lights and personnel like security guards and watch dog

4.7 Network Security

Network security is an over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.

This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing or altering secure information.

The first layer of network security is enforced through a username/password mechanism, which only allows access to authenticated users with customized privileges. When a user is authenticated and granted specific system access, the configured firewall enforces network policies, that is, accessible user services.

However, firewalls do not always detect and stop viruses or harmful malware, which may lead to data loss. An anti-virus software or an intrusion prevention system (IPS) is implemented to prevent the virus and/or harmful malware from entering the network.

Network security is sometimes confused with information security, which has a different scope and relates to data integrity of all forms, print or electronic.

Some of the cyber crimes related to securities

1. Masquerade Attack

A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Masquerade attacks may happen in a number of ways. In case of an insider attack, a masquerade attacker gains access to the account of a legitimate user either by stealing the victim's account ID and password, or by using a keylogger. Another common method is by exploiting a legitimate user's laziness and trust. For example, if a legitimate user leaves the terminal or session open and logged in, a co-worker may act as a masquerade attacker.

Vulnerable authentication is one of the other factors that can trigger a masquerade attack, as it helps the attacker to gain access much more easily. Once the attackers gain access, they can get into all of the organization's critical data and can delete or modify it, steal sensitive data, or alter routing information and network configuration.

For example, although a unique IP address is assigned to each individual computer, a hacker can convince another system that it is the authorized user through spoofing, essentially convincing the target computer that the hacker's computer has the same IP.

A standard strategy to resist this kind of attack is to create innovative algorithms that can efficiently detect the suspicious actions, which could result in the detection of imposters

2.Trap doors

A backdoor is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data. The backdoor access method is sometimes written by the programmer who develops a program.

A backdoor is also known as a trapdoor.

Backdoor threats increase when multiuser and networking operating systems are used by many organizations. In a login system, a backdoor used for system access may be in the form of a hard-coded username and password.

A network administrator (NA) may intentionally create or install a backdoor program for troubleshooting or other official use. Hackers use backdoors to install malicious software (malware) files or programs, modify code or detect files and gain system and/or data access. Even backdoors installed by network administrators pose security risks because they provide a mechanism by which the system can be exploited if discovered.

BYOT

BYOT, or "bring your own technology" - also simply known as BYO or "bring your own device" (BYOD) - is more than just an IT trend: It's a new a way of life. And while BYOT may have its roots with executives, who've long demanded the ability to use the latest mobile devices for work, it has spread among the ranks, along with the proliferation of smartphones and tablet computers. The catchphrase often heard in discussions of BYOT is "consumerization of IT." In other words, it's no longer just the geeks or the execs that want the best technology.

Not long ago, employees were thrilled simply to have a company phone. Now, employees become angry when stuck with anything other than the latest and greatest models. As people increase dependence on personal mobile devices in many life areas, it's no wonder they want to be able to access company emails and applications without giving up the convenience of their favorite devices.

INTERNET CRIMES

Virus

A virus is a type of malicious software (malware) comprised of small pieces of code attached to legitimate programs. When that program runs, the virus runs.

Viruses are malicious programs that spread throughout computer files without user knowledge. Most widespread virus infections spread through email message attachments that activate when opened. The vicious cycle of a virus perpetuates as infected emails are forwarded to multiple users. Viruses also spread through shared media, such as Universal Serial Bus (USB) drives.

Initially created as pranks, viruses are responsible for widespread and significant computer system and file destruction. Installing anti-virus software helps prevent, block or remove previously installed viruses

Worm

A worm is a type of malicious software (malware) that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path.

A worm locates a computer's vulnerability and spreads within its connected network like an infection, while continually seeking new vulnerabilities. Like viruses, worms often originate from e-mail attachments that appear to be from trusted senders. Worms then spread to a user's contacts via his e-mail account and address book.

Some worms spread and then do nothing while tthers cause harm. In such cases, the worm's code is known as payload.

Malicious Software (Malware)

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Malware is software designed to cause harm to a computer and user. Some forms of malware "spy" on user Internet traffic. Examples include spyware and adware. Spyware monitors a user's location and if enabled, it can capture sensitive information, e.g., credit card numbers, promoting identity theft. Adware also acquires user information, which is shared with advertisers and then integrated with unwanted, triggered pop-up ads.

Worms and viruses behave differently, as they can quickly proliferate and undermine an entire computer system. They also may perform unsavory activities from a user's computer without the user's knowledge. In the wake of a virus or worm, a computer system can experience significant damage.

Anti-malware should determine if there are threats by scanning a computer and removing them, if found. Prevention is better than corrective action after infection. Although anti-virus programs should be continually enabled and updated, certain types of threats, like spyware, often make their way into a computer system.

At all times, a firewall should be in place for additional security. Multiple, compatible protective sources are encouraged as additional insurance against malware.

Adware

Adware is free computer software that contains commercial advertisements. Adware programs include games, desktop toolbars or utilities. Commonly, adware is Web-based and collects Web browser data to target advertisements, especially pop-ups.

Adware is also known as freeware and pitchware.

Adware is categorized as follows:

- Legitimate: Free or trial product sponsored advertisements
- Spyware: Tracks user website preferences and compromises privacy

Adware may appear innocuous and provide users with legitimate business software but then unleash spyware that collects browser search data for targeted user-specific advertisements.

Uninstalling adware generally requires anti-adware software. A variety of free and paid versions are available, but licensed adware is the most reliable, aggressive and recommended. Anti-adware software is also included in virus scanning packages.

Trojan Horse

A Trojan horse is a seemingly benign program that when activated, causes harm to a computer system.

A Trojan horse is also known as a Trojan virus or Trojan.

The Trojan horse is named for ancient Greece's apparent gift of peace to the Trojans, when a giant wooden horse was secretly filled with Greek warriors. After the Trojans allowed the horse to enter their great city, the Greek warriors emerged from the horse gained control of the city of Troy.

The following are types of trojan horses:

- **Backdoor Trojan**: opens a back door for a user to access a victim's system at a later time
- **Downloader**: This Trojan downloads malicious software and causes harm to the victim's computer system.
- **Infostealer**: This Trojan attempts to steal information from the victim's computer.
- **Remote Access Trojan (RAT**): This can be hidden in games or other programs of a smaller variety and give the attacker control of the victim's computer.
- **Data Sending Trojan**: This gives the perpetrator sensitive information like passwords or other information programmed to be hijacked.
- **Destructive Trojan**: This destroys the victim's files.
- **Proxy Trojan**: As a proxy server, this allows the attacker to hijack a victim's computer and conduct illegal activities from the victim's computer.

Spyware

Spyware is infiltration software that secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user's computer. Spyware exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users.

Peer-to-peer (P2P) file sharing has increased the proliferation of spyware and its ramifications.

Anti-spyware applications locate and remove spyware and are recommended as a preventative line of defense against infiltration and damage.

Anti-virus software removes PC viruses, but anti-virus scans do not always detect spyware. Spyware and cookies are similar, but spyware conducts infiltration activity continuously until it is removed by specific anti-spyware tools.

Users should take the following precautions to prevent spyware attacks:

- Maintain anti-virus and anti-spyware updates and patches.
- Download from well-known and reputable sites only.
- Use a firewall for enhanced security

Internet Bot

An Internet bot, in its most generic sense, is software that performs an automated task over the Internet. More specifically, a bot is an automated application used to perform simple and repetitive tasks that would be time-consuming, mundane or impossible for a human to perform.

Bots can be used for productive tasks, but they are also frequently used for malicious purposes.

The term "bot" comes from robot. An Internet bot may also be known as a Web robot or WWW robot.

One of the best examples of a good bot is a search engine spider. Such bots troll the Web and index new pages for a search engine. Other examples include the original Internet relay chat bots and chatterbots.

Malicious bots are typically blended threats that come as part virus/worm, part bot and are used in a identity theft or to launch denial of service attacks. This is especially prevalent in a botnet, which is a grouping of computers that are all infected with a malicious bot. Other illegal, or at least questionable uses, involve bots that harvest email addresses for spam, scrape content or manipulate comments/votes on sites that allow user feedback.

Rootkit

A rootkit is software used by a hacker to gain constant administrator-level access to a computer or network. A rootkit is typicially installed through a stolen password or by exploiting a system vulnerabilities without the victim's consent or knowledge.

Rootkits primarily aim at user-mode applications, but they also focus on a computer's hypervisor, the kernel, or even firmware. Rootkits can completely deactivate or destroy the anti-malware software installed in an infected computer, thus making a rootkit attack difficult to track and eliminate. When done well, the intrusion can be carefully concealed so that even system administrators are unaware of it.

Rootkits may be also presented as a Trojan or even as a hidden file along with a seemingly harmless file. This can be a graphic or even a silly application distributed via email. When the victim clicks the program or graphic, the rootkits are installed on their system without their knowledge.

Some of the impacts of rootkits are often to:

- Provide the attacker with complete backdoor access, permitting them to falsify or steal documents.
- Hide other malware, especially keyloggers. The keyloggers may then be used to access and steal the victim's sensitive data.
- Enable the attacker to use the infected machine as a zombie computer to trigger attacks on others

Spoofing

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.

Email spoofing is one of the best known spoofs. Since core SMTP fails to offer authentication, it is simple to forge and impersonate emails. Spoofed emails may request personal information and may appear to be from a known sender. Such emails request the recipient to reply with an account number for verification. The email spoofer then uses this account number for identity theft purposes, such as accessing the victim's bank account, changing contact details and so on.

The attacker (or spoofer) knows that if the recipient receives a spoofed email that appears to be from a known source, it is likely to be opened and acted upon. So a spoofed email may also contain additional threats like Trojans or other viruses. These programs can cause significant computer damage by triggering unexpected activities, remote access, deletion of files and more.

5. COMPUTER HACKERS

Hacker

A hacker utilizes alternative system access methods to sabotage computer systems and networks.

Hacking actions are differentiated as illegal and unacceptable (black/grey hat hacking), or legal and acceptable (white hat hacking).

Hacker is a term that refers to many different computing topics. However, in the mainstream, a hacker is any individual or group that circumvents security to access unauthorized data.

Most hackers are highly skilled computer programmers that locate security gaps and access secure systems via unique analytical skills. A great hacker is known to be able to "think outside the box."

Hacker types are delineated according to intent, as follows:

- Black hat hackers break into computer systems illegally and cause harm by stealing or destroying data, i.e., a banking system to steal money for personal gain.
- White hat hackers use their skills to help enterprises create robust computer systems.
- Grey hat hackers perform illegal hacking activities to show off their skills, rather than to achieve personal gain.

5.2 Hacking Tool

A hacking tool is a program or utility designed to assist a hacker with hacking. It can also be proactively utilized to protect a network or computer from hackers.

Hacking is intentional modification of computer software or hardware that is outside the architectural perimeters and design. Hacking tools come in a wide variety of applications and are specifically created to assist in hacking. A hacking tool is commonly used to gain unauthorized access to a PC to insert worms, siffers, viruses and Trojan horses.

A hacking tool is a tool or program that is specially designed to help a hacker. The true meaning of hacking is derived from "hacking away", which is used to refer to someone who is extremely proficient in computer technology and hacks away at the bits and bytes. Today's definition of hacking refers to a self-taught prodigy or specialized programmer who is able to modify computer hardware or software outside a developer's architectural design.

5.3TYPES OF HACKING

White Hat Hacker

A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them. White hat hackers are usually seen as hackers who use their skills to benefit society. They may be reformed black hat hackers or they may simply be well-versed in the methods and techniques used by hackers. An organization can hire these consultants to do tests and implement best practices that make them less vulnerable to malicious hacking attempts in the future.

For the most part, the term is synonymous with "ethical hacker." The term comes from old Western movies where the cliché was for the "good guy" to wear a white cowboy hat. Of course, the "bad guys" always seemed to wear a black hat

.

Black Hat Hacker

A black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons. This differs from white hat hackers, which are security specialists employed to use hacking methods to find security flaws that black hat hackers may exploit.

Black hat hackers can inflict major damage on both individual computer users and large organizations by stealing personal financial information, compromising the security of major systems, or shutting down or altering the function of websites and networks.

Grey Hat Hacker

A gray hat hacker (also spelled grey hat hacker) is someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers. Gray hat hackers may engage in practices that seem less than completely above board, but are often operating for the common good. Gray hat hackers represent the middle ground between white hat hackers, who operate on behalf of those maintaining secure systems, and black hat hackers who act maliciously to exploit vulnerabilities in systems

Computer Fraud Protection

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

They can be classified by several criteria. For example, according to the time that they act, relative to a security incident:

- Before the event, **preventive controls** are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders;
- During the event, **detective controls** are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police;
- After the event, **corrective controls** are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

According to their nature, for example:

- **Physical controls** *e.g.* fences, doors, locks and fire extinguishers;
- **Procedural controls** *e.g.* incident response processes, management oversight, security awareness and training;
- **Technical controls** *e.g.* user authentication (login) and logical access controls, antivirus software, firewalls;
- **Legal and regulatory or compliance controls** *e.g.* privacy laws, policies and clauses.

A similar categorization distinguishes control involving people, technology and operations/processes.

In the field of information security, such controls protect
the **confidentiality**, **integrity** and/or **availability** of information - the so-called CIA Triad

Systems of controls can be referred to as frameworks or standards. Frameworks can enable an organization to manage security controls across different types of assets with consistency.

Controls Overview
Controls are the means by which risk can be mitigated. Individual controls may reduce the probability of a particular cybersecurity occurrence or the impact of such an occurrence. Typically, to reduce both probability and impact of the occurrence multiple controls will be applied.

Types of Controls
The word "controls" tends to conjure up images of electromechanical devices, but in the cyber security context controls can take on many forms. Some examples of
Example control types

Directive Controls: Directive controls may be administrative instruments such as policies, standards and procedures. An example of a directive control would be the creation of an Acceptable Use Policy for employee use of information resources

Preventive controls A preventative control attempts to make the occurrence of a breach less likely by making it more difficult for the threat source to cause one.
Examples are security guards, security fences, security training, firewalls and intrusion prevention systems

Detective Controls A detective control detects a security breach once it has occurred. Examples are intruder alarms, intrusion detection systems, system monitoring and log monitoring

Corrective Controls :A corrective control reduces the effect of a security breach. An example is an anti-virus system isolating an infected file

Recovery controls: A recovery control aims to restore business operations after a security breach.

Encryption

(i) Encryption Types:

Symmetric encryption is the use of the same key and algorithm by the creator and reader of a file or message. The creator uses the key and algorithm to encrypt, and the reader uses both to decrypt. Symmetric encryption relies on the secrecy of the key. If the key is captured by an attacker, either when it is exchanged between the communicating parties, or while one of the parties uses or stores the key, the attacker can use the key and the algorithm to decrypt messages or to masquerade as a message creator.

Asymmetric encryption lessens the risk of key exposure by using two mathematically related keys, the private key and the public key. When one key is used to encrypt, only the other key can decrypt. Therefore, only one key (the private key) must be kept secret. The key that is exchanged (the public key) poses no risk if it becomes known. For instance, if individual A has a private key and publishes the public key, individual B can obtain the public key, encrypt a message to individual A, and send it. As long as an individual keeps his private key secure from disclosure, only individual A will be able to decrypt the message.

(ii) Typical areas or situations requiring deployment of cryptographic techniques, given the risks involved, include transmission and storage of critical and/or sensitive data/information in an 'un-trusted' environment or where a higher degree of security is required, generation of customer PINs which are typically used for card transactions and online services, detection of any unauthorised alteration of data/information and verification of the authenticity of transactions or data/information.

(iii) Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management systems are based on an agreed set of standards, procedures, and secure methods that address

a. Generating keys for different cryptographic systems and different applications
b. Generating and obtaining public keys and distributing keys to intended users, including how keys should be activated when received
c. Storing keys, including how authorized users obtain access to keys and changing or updating keys, including rules on when keys should be changed and how this will be done
d. Dealing with compromised keys, revoking keys and specifying how keys should be withdrawn or deactivated
e. Recovering keys that are lost or corrupted as part of business continuity management
f. Archiving, destroying keys
g. Logging the auditing of key management-related activities
h. Instituting defined activation and deactivation dates, limiting the usage period of keys

(iv) Secure key management systems are characterized by the following precautions:

a. Additional physical protection of equipment used to generate, store and archive cryptographic keys
b. Use of cryptographic techniques to maintain cryptographic key confidentiality
c. Segregation of duties, with no single individual having knowledge of the entire cryptographic key (i.e. two-person controls) or having access to all the components making up these keys
d. Ensuring key management is fully automated (e.g., personnel do not have the opportunity to expose a key or influence the key creation)
e. Ensuring no key ever appears unencrypted
f. Ensuring keys are randomly chosen from the entire key space, preferably by hardware
g. Ensuring key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key. (A key encrypting key is used to encrypt other keys, securing them from disclosure.)
h. Make sure that keys with a long life are sparsely used. The more a key is used, the greater the opportunity for an attacker to discover the key
i. Ensuring keys are changed frequently.
j. Ensuring keys that are transmitted are sent securely to well-authenticated parties.
k. Ensuring key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.

Normally, a minimum of 128-bit SSL encryption is expected. Constant advances in computer hardware, cryptanalysis and distributed brute force techniques may induce use of larger key lengths periodically. It is expected that banks will properly evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international cryptographer community or approved by authoritative professional bodies, reputable security vendors or government agencies

CYBER FRAUD

Introduction:

With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. Fraudsters have also followed customers into this space. However, the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer. There is also a lack of clarity amongst banks on the reporting of these instances as frauds.

A need is therefore felt to have an industry wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. This note endeavours to bring out the challenges and suggests a framework which can be implemented across banks to effectively tackle the electronic fraud menace. It would be useful to recall the definition of fraud at this stagyuo]\j;'e.

'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.

This definition has been recommended as per para 9.1 of the Report of the Study Group on Large Value Bank Frauds set up by the Reserve Bank of India in 1997. It follows that like other bank frauds, various IT related frauds need to get captured through the fraud reporting system and banks should take adequate steps to mitigate such risks.

- Roles/Responsibilities and Organizational structure for fraud risk management:

Indian banks follow the RBI guideline of reporting all frauds above ₹ 1 crore to their respective Audit Committee of the Board. Apart from this, banks are also putting up a detailed annual review of frauds to their Audit Committee of the Board. The Board for Financial Supervision (BFS) of RBI has observed that in terms of higher governance standards, the fraud risk management and fraud investigation must be 'owned' by the bank's CEO, Audit Committee of the Board and the Special Committee of the Board.

Special Committee of the Board for monitoring large value frauds

Banks are required to constitute a special committee for monitoring and follow up of cases of frauds involving amounts of ₹ 1 crore and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of frauds in general.

Most retail cyber frauds and electronic banking frauds would be of values less than ₹ 1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is imperative that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud, modus operandi and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor and review the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values at least on a quarterly basis.

(c) Separate Department to manage frauds

The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent group in the bank. The group should be adequately staffed and headed by a senior official of the Bank, not below the rank of General Manager.

(d) Fraud review councils

Fraud review councils should be set up by the above fraud risk management group within various business groups in the bank. The council should comprise of head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet every quarter to review fraud trends and preventive steps taken by the business group, and report the same to the Special Committee.

- Components of fraud risk management:

(i) Fraud prevention practices

A strong internal control framework is the strongest deterrence for frauds. The fraud risk management department along with the business/operations/support groups, continuously reviews various systems and controls, to remove gaps if any, and to strengthen the internal control framework. The following are some of the fraud prevention practices that are recommended for banks.

(a) Fraud vulnerability assessments

Fraud vulnerability assessments should be undertaken across the bank by the fraud risk management group. Apart from the business and the operations groups, such assessment also cover channels of the bank such as branches, internet, ATM and phone banking, as well as international branches, if any. During the course of a vulnerability assessment, all the processes should be assessed based on their fraud risk. Controls need to be checked and improvements suggested for tightening the same. These should be reviewed in the fraud review councils.

'Mystery Shopping' is an important constituent of vulnerability assessment. Transactions are introduced in 'live' scenarios to test the efficacy of controls. The results of the mystery shopping exercises should be shared with the relevant groups in the fraud review councils and be used for further strengthening of controls.

(b) Review of new products and processes

No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analysed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.

(c) Fraud loss limits

All residual/open risks in products and processes need to be covered by setting 'fraud-loss' limits. 'Fraud-loss' limits need to be monitored regularly by the fraud risk management group and a review needs to be undertaken with the respective business group when fraud loss amount reaches 90% of the limit set. In case it is difficult to set a fraud- loss limit, a limit on the total number or total value of frauds may be defined. For the purpose of deciding how much a product or a process has used up the limit set, the cumulative value of frauds in that product or process during the financial year needs to be considered.

(d) Root cause analysis

All actual fraud cases above ₹ 10 lakhs and cases where a unique modus operandi is involved, should be reviewed immediately after such a fraud is detected. The findings should be used to redesign products and processes and remove the gaps so that they do not recur.

(e) Data/information/system security

Most banks have incorporated several security measures for their documents, information, systems and customer deliverables such as cheque books/debit cards. Security measures have also been incorporated during delivery of instruments such as cards/cheque books/internet passwords to

customers through couriers. Internet banking systems have security features such as separate transaction passwords, two factor authentication, multi-channel process for registering payees, upper limit on transaction value and SMS alerts to customers. It is also necessary that customer confidential information and other data/information available with banks is secured adequately to ensure that fraudsters do not access it to perpetrate fraudulent transactions. Appropriate steps need to be taken to ensure data/information/system security at the Bank, as indicated earlier in the report. Information security and appropriate access control procedures ensure that only employees who are required to know particular information have access to the same and can put through transactions. Further, a bank's systems need to be adequately secured to ensure that no un-authorised person carries out any system modifications/changes. Appropriate verification procedures should also be incorporated at all channels such as phone banking, ATMs, branches and internet to ensure that only genuine transactions are put through. All the above security measures should be under continuous review for further strengthening. Details in this regard were covered in chapter on information security.

(f) Know Your Customer (KYC) and know your employee/vendor procedures

A strong KYC process is the backbone of any fraud prevention activity. Such a process enables banks to prevent unscrupulous elements from gaining entry into the bank's environment, which gives them an opportunity to carry out their fraudulent intentions. Similarly, appropriate due diligence procedures before recruitment of employees and vendors is essential to prevent known fraudsters or people with fraudulent motives to have access to a bank's channels. Banks have to implement strong procedures to carry out due diligence of potential customers, employees and vendors before they are enrolled.

(g) Physical security

All banks have a dedicated team to take care of the security of the physical infrastructure. This team should conduct regular security audits of various offices to check for deviations/lapses. It is the responsibility of this team to ensure that physical assets and data copied on magnetic/optical media do not go out of the offices of the bank without authorisation.

(h) Creation of fraud awareness amongst staff and customers

Awareness on how to prevent and detect frauds is the basis of fraud management. Banks need to adopt various measures to create awareness amongst staff and customers.

(ii) Fraud detection

- A) Detection of fraud

Despite strong prevention controls aimed at fraud deterrence, fraudsters do manage to perpetrate frauds. In such cases, the earlier the fraud is detected, the better the chance of recovery of the losses and bringing the culprits to book. System triggers that throw up exceptional transactions, opening up channels that take note of customer/employee alerts/disputes, seeding/mystery shopping exercises and encouraging employees/customers/ well- wishers to report suspicious transactions/behaviours are some of the techniques that are used for detection of frauds. The exceptional/suspicious transactions/activities reported through these mechanisms should be investigated in detail.

b) Transaction monitoring

Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitisation for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

c) Alert generation and redressal mechanisms

Appropriate mechanisms need to be established in banks, to take note of the disputes/exceptions or suspicions highlighted by various stakeholders including transaction monitoring teams in banks and to investigate them thoroughly. Banks should have a well publicised whistle blowing mechanism.

d) Dedicated email ID and phone number for reporting suspected frauds

Banks can have dedicated email IDs and phone numbers for customers to report any fraudulent activity that they may notice. A dedicated team can be created to reply to customer queries and concerns through the above email IDs. Phone banking officers and branch staff should also be trained on response to customers' queries and concerns on frauds.

e) Mystery shopping and reviews

Continuous supervision and control by managers/supervisors on activities is important to detect any abnormal activity. However, considering a bank's size and scope, this needs to be supplemented by mystery shopping to detect system flaws and also to identify unscrupulous employees/vendors. Immediate action needs to be taken on the findings of such reviews.

f) Importance of early detection of frauds

A bank's fraud management function is effective if it is able to minimise frauds and when fraud occurs, is able to detect the fraud so that the loss is minimised.

(iii)Fraud investigation

The examination of a suspected fraud or an exceptional transaction or a customer dispute/alert in a bank shall be undertaken by:

- Fraud risk management group
- Specific committee/team of employees constituted to examine the 'suspected fraud'
- External agencies, if any, as appointed by the bank

) Fraud Investigation function

It is widely accepted that fraud investigation is a specialised function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies. The first step in an investigation process is gathering the entire transaction details, documents and complete details of the customer/employee or vendor. In order to investigate into suspected cases, the group would adopt various advanced techniques including computer forensics, forensic accounting and tools to analyse large volumes of data.

The investigation team may conduct oral interviews of customers or employees to understand the background and details of the case. In case an interview of the person accused of fraud is required to be undertaken, the investigation group should follow a prescribed procedure and record statements appropriately. The investigation activities need to be carried out discreetly and within a specified time line. The investigating team should take into account all the relationships of the involved parties with the bank while investigating and submitting an investigation report. The investigation report will help the respective business groups take a decision on all the relationships of the customer with the Bank. The investigation report should conclude whether a suspected case is a fraud and thereafter the report would form the basis for further actions such as regulatory reporting.

In case of employee involvement in the fraud, the investigation report may be the basis of staff accountability and HR actions. It may be noted that, during the course of the investigations, banks should adopt only means permitted by law, regulations and code of conduct of the bank and any inconvenience to customers or general public should be avoided. It is also important to note that certain investigations are best carried out by law enforcement authorities and the bank should refer cases to such authorities at the appropriate time, to enable them to carry out their responsibilities efficiently.

In case of need, the investigating team should seek the support of other specialised groups within the bank, such as the audit group to carry out investigations efficiently.

At times, investigation of a fraud wherein money has come into the country to an account in a bank through another bank in the same country needs to be done. The intermediary bank does not investigate or report the case stating that it is merely an intermediary while the recipient bank states that it has no knowledge of the transaction and is merely a recipient of the funds sent by the intermediary bank. In this case, it is clarified that the bank whose customer has received the money should investigate and report the case.

b) Recovery of fraud losses

The concerned group in a bank, in which the fraud has occurred, should make all out efforts to recover the amount lost. They may use specialised groups like legal or collections for this purpose. The investigation team may also be able to recover some amounts during the course of their investigation. The Police may also recover some amount during their investigation. This would be deposited in Court pending final adjudication. The bank should liaise with the Police and keep track of such amounts.

(iv)Reporting of frauds

As per the guidelines on reporting of frauds as indicated in the RBI circular, dated July 1, 2010, fraud reports should be submitted in all cases of fraud of ₹ 1 lakh and above perpetrated through misrepresentation, breach of trust, manipulation of books of account, fraudulent encashment of instruments like cheques, drafts and bills of exchange, unauthorised handling of securities charged to the bank, misfeasance, embezzlement,

misappropriation of funds, conversion of property, cheating, shortages, irregularities, etc. Banks should also report frauds in the electronic channels and the variants of plastic cards used by a bank and its customers for concluding financial transactions.

a) Frauds in merchant acquiring business

A special mention needs to be made here of frauds done by collusive merchants who use skimmed/stolen cards on the POS terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. It is imperative that the bank which has provided acquiring services to such merchant, reports the case to RBI.

b) Frauds in ATM acquiring business

Also, it has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money. The facts of the case would decide as to which bank will bear the loss.

c) Filing of police complaints

Banks should readily share data and documents requested by the police even in cases where the bank in question is not the victim of the fraud but has been a receiver of fraudulent monies into its accounts.

(v) Customer awareness on frauds

- Creation of customer awareness on frauds

Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Banks should thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in banks to create fraud risk awareness amongst their respective customers. The fraud risk management group should share its understanding of frauds with each group, identify areas where customer awareness is lacking and if required, guide the groups on programmes to be run for creation of awareness amongst customers. The groups should ensure that in each of their interaction with customers there is at least one message to make the customer aware of fraud risk.

The following are some of the recommended measures to create awareness amongst customers:

- Publications in leading newspapers
- Detailed 'do's and don'ts' on the web site of the bank
- Messages along with statement of accounts, either physical or online
- Messages printed on bank's stationery such as envelopes, card covers, etc.
- SMS alerts
- Message on phone banking when the customer calls
- As inserts or on the jackets of cheque books
- Posters in branches and ATM centres
- Interstitials on television and radio

It should be ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper precautions aimed at preventing frauds. Such communication should be reviewed periodically by the fraud risk management group to judge its effectiveness.

(vi) Employee awareness and training

(a) Creation of employee awareness

Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums. Banks may use the following methods to create employee awareness:

Class room training programmes at the time of induction or during risk related training sessions

Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank

E-learning module on fraud prevention

Online games based on fraud risks in specific products or processes

E-tests on prevention practices and controls

Detailed 'do's and don'ts' put up on the worksite of the employee

Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.
Emails sent by the respective business heads
Posters on various safety measures at the work place

Messages/discussions during daily work huddles

- Rewarding employees on fraud prevention

A positive way of creating employee awareness is to reward employees who have gone beyond their call of duty, and prevented frauds. Awards may be given to employees who have done exemplary work in preventing frauds. Details of employees receiving such awards may be published in the fraud newsletters.

Incident management

(i) Incident management is defined as the process of developing and maintaining the capability to manage incidents within a bank so that exposure is contained and recovery achieved within a specified time objective. Incidents can include the misuse of computing assets, information disclosure or events that threaten the continuance of business processes.

(ii) Major activities that need to be considered as part of the incident management framework include:

a. Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents
b. Establishing escalation and communication processes and lines of authority
c. Developing plans to respond to and document information security incidents
d. Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.
e. Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers)
f. Integrating information security incident response plans with the organization's disaster recovery and business continuity plan
g. Organizing, training and equipping teams to respond to information security incidents
h. Periodically testing and refining information security incident response plans
i. Conducting post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future

(iii) Common incident types include, but not limited to, outages/degradation of services due to hardware, software or capacity issues, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, denial of service attacks and data integrity issues.

(iv) A bank needs to have clear accountability and communication strategies to limit the impact of information security incidents through defined mechanisms for escalation and reporting to the Board and senior management and customer communication, where appropriate. Incident management strategies would also typically assist in compliance with regulatory requirements. Institutions would also need to pro-actively notify CERT-In/IDRBT/RBI regarding cyber security incidents.

(v) All security incidents or violations of security policies should be brought to the notice of the CISO.

Electronic cards:

Credit cards and Debit cards

As mentioned above India is one of the fastest growing countries in the plastic money segment. Already there are 130 million cards in circulation, which is likely to increase at a very fast pace due to rampant consumerism. India's card market has been recording a growth rate of 30% in the last 5 years. Card payments form an integral part of e-payments in India because customers make many payments on their card-paying their bills, transferring funds and shopping.

Ever since Debit cards entered India, in 1998 they have been growing in number and today they consist of nearly 3/4th of the total number of cards in circulation.

Credit cards have shown a relatively slower growth even though they entered the market one decade before debit cards. Only in the last 5 years has there been an impressive growth in the number of credit cards- by 74.3% between 2004 and 2008. It is expected to grow at a rate of about 60% considering levels of employment and disposable income. Majority of credit card purchases come from expenses on jewellery, dining and shopping.

Another recent innovation in the field of plastic money is co branded credit cards, which combine many services into one card-where banks and other retail stores, airlines, telecom companies enter into business partnerships. This increases the utility of these cards and hence they are used not only in ATM's but also at Point of sale (POS) terminals and while making payments on the net.

. **PREPAID PAYMENT INSTRUMENTS** :

Eligibility : Banks who comply with the eligibility criteria would be permitted to issue all categories of pre-paid payment instruments. Non-Banking Financial Companies (NBFCs) and other persons would be permitted to issue only semi-closed system payment instruments. Capital requirements : Banks and Non-Banking Financial Companies which comply with the Capital Adequacy requirements prescribed by Reserve Bank of India from time-to-time, shall be permitted to issue pre-paid payment instruments. All other persons shall have a minimum paid-up capital of Rs 100 lakh and positive net owned funds. Safeguards against money laundering (KYC/AML/CFT) provisions - The maximum value of any pre-paid payment instruments (where specific limits have not been prescribed including the amount transferred) shall not exceed Rs 100,000/-.

Deployment of Money collected: Non-bank persons issuing payment instruments are required to maintain their outstanding balance in an escrow account with any scheduled commercial bank subject to the following conditions:- The amount so maintained shall be used only for making payments to the participating merchant establishments. No interest is payable by the bank on such balances.

Validity: All pre-paid payment instruments issued in the country shall have a minimum validity period of six months from the date of activation/issuance to the holder. The outstanding balance against any payment instrument shall not be forfeited unless the holder is cautioned at least 15 days in advance as regards the expiry of the validity of the payment instrument

RuPay Debit Cards: It is a domestic card payment network established by National Payment Corporation of India (NPCI) having more than 100 Banks in India as members with its ATM network spread across the country. These cards can be used at all ATMs of NPCI network and POS terminals & e-com transactions (Internet) enabled for RuPay acquiring. The various types of RuPay Debit cards are as under:

Card Type Meant for

RuPay Kisan Farmers availing Agriculture production loans (Crop Loans)

RuPay Aadhaar Beneficiaries of Electronic Benefit Transfer (EBT) scheme

RuPay Debit Beneficiaries under Financial Inclusion schemes

It provides accidental insurance cover up to ?1 lakh without any charge to the customer. To avail this benefit, the card must be used minimum once in 90 days. The existing identification modes used in new delivery channels has a major drawback as it recognize the PIN but not the person. Sometimes, it leads to impersonation and may cause financial loss. To overcome the problem, biometric technologies such as Fingerprint Recognition, Face Recognition, Voice Authentication, Hand Geometry, Retinal Scanning,

Iris Scanning and Signature Verification have come in to force. Whenever the user access to delivery channel, it verifies with the server and deliver the service if found correct.
Recently, NPCI introduced two variants of cards viz., Rupay Platinum and Rupay Select with value added features at competitive interchange fee compared to VISA/Master

Data security

i. Banks need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.
ii. A data security theory seeks to establish uniform risk-based requirements for the protection of data elements. To ensure that the protection is uniform within and outside of the institution, tools such as data classifications and protection profiles can be used, as indicated earlier in the chapter.

iii. Data classification and protection profiles are complex to implement when the network or storage is viewed as a utility. Because of that complexity, some institutions treat all information at that level as if it were of the highest sensitivity and implement encryption as a protective measure. The complexity in implementing data classification in other layers or in other aspects of an institution's operation may result in other risk mitigation procedures being used. Adequacy is a function of the extent of risk mitigation, and not the procedure or tool used to mitigate risk.
iv. Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and otherwise mitigate risks to data. If protection profiles are not used, the policies should accomplish the same goal as protection profiles, which is to deliver the same degree of residual risk without regard to whether the information is in transit or storage, who is directly controlling the data, or where the storage may be.
v. There should be secure storage of media. Controls could include physical and environmental controls such as fire and flood protection, limiting access by means like physical locks, keypad, passwords, biometrics, etc., labelling, and logged access. Management should establish access controls to limit access to media, while ensuring that all employees have authorization to access the minimum data required to perform their responsibilities. More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimize the distribution of sensitive information, including printouts that contain the information. Periodically, the security staff, audit staff, and data owners should review authorization levels and distribution lists to ensure they remain appropriate and current.

vi. The storage of data in portable devices, such as laptops and PDAs, poses unique problems. Mitigation of those risks typically involves encryption of sensitive data, host-provided access controls, etc.
vii. Banks need appropriate disposal procedures for both electronic and paper based media. Contracts with third-party disposal firms should address acceptable disposal procedures. For computer media, data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive data like physical destruction, overwriting data, degaussing etc.

viii. Banks should maintain the security of media while in transit or when shared with third parties. Policies should include contractual requirements that incorporate necessary risk-based controls, restrictions on the carriers used and procedures to verify the identity of couriers.

ix. Banks should encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

x. A few other aspects that also needs to be considered include appropriate blocking, filtering and monitoring of electronic mechanisms like e-mail and printing and monitoring for unauthorised software and hardware like password cracking software, key loggers, wireless access points, etc.

xi. Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (DLP). It provides a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.

Most DLP solutions include a suite of technologies that facilitate three key objectives:

- Locate and catalogue sensitive information stored throughout the enterprise
- Monitor and control the movement of sensitive information across enterprise networks
- Monitor and control the movement of sensitive information on end-user systems Banks may consider such solutions, if required, after assessing their potential to improve data security.

The Information Technology (Amendment) Act, 2008

The main Indian act that addresses legal challenges specifically as they relate to the Internet is the Information Technology (Amendment) Act, 2008, or for short, the IT Act. We highlight the sections that have the greatest relevance for the Internet and democracy. This includes sections relating to government takedowns, monitoring and interception of communication and intermediary liability.

Section 69A and the Blocking Rules: Allowing the Government to block content under certain circumstances

Section 69A of the IT (Amendment) Act, 2008, allows the Central Government to block content where it believes that this content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. A set of procedures and safeguards to which the Government has to adhere when doing so have been laid down in what have become known as the Blocking Rules.

- **Section 79 and the IT Rules: Privatising censorship in India**

Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India.

- **Sections 67 and 67A: No nudity, please**

The large amounts of 'obscene' material that circulate on the Internet have long attracted comment in India. Not surprsingly, then, in the same way as obscenity is prohobited offline in the country, so it is online as well. The most important tools to curtail it are sections 67 and 67A of the IT Act, prohibiting obscene and sexually explicit material respectively.

- **Section 66A: Do not send offensive messages**

Section 66A of the Information Technology (Amendment) Act, 2008 prohibits the sending of offensive messages though a communication device (i.e. through an online medium). The types of information this covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of 'causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will.' If you're booked under Section 66A, you could face up to 3 years of imprisonment along with a fine.

- **Freedom of expression**

To balance freedom of expression with other human rights is, at times, a difficult and delicate task. From hate speech to intermediary liability, we tease out and shed greater light on the various challenges that make this task particularly complicated, proposing ways forward that can further strengthen and promote the right to freedom of expression, in India and beyond, as well.

- **Cyber security, surveillance and human rights**

With the advent of new technology, new security threats have emerged for people, businesses and states. Oftentimes, responses to such threats, including states' exercise of their unprecedented power to surveil their populations, have been criticised for their negative impact on human rights. Can security and human rights no longer be reconciled in the Internet age?

The Information Technology (Amendment) Act, 2008 an act to amend the IT Act 2000 received the assent of the President on 5th February 2009. Several legal & security experts are in the process of analyzing the contents and possible impacts of the amendments. The objective of this note is to try and study the possible implications and impacts on Indian companies. This note is not intended to be a comprehensive analysis of the amendments, but only certain key points which could impact Indian Companies

Data Protection

The IT Act 2000 did not have any specific reference to Data Protection, the closet being a provision to treat data vandalism as an offense. The Government introduced a separate bill called "Personal Data Protection Act 2006" which his pending in the Parliament and is likely to lapse. The ITA 2008 has introduced two sections which address Data Protection aspects to an extent, which gives rise to certain key considerations for the sector.

The sections under consideration are:

Section 43A: Compensation for failure to protect data

Section 72A: Punishment for disclosure of information in breach of lawful contract

Section 43A states

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

By way of explanation: "Body corporate means Indian companies"

"Reasonable security practices mean a mutual contract between the customer and service provider OR as per the specified law. In absence of both then as specified by the Central Government

Hence it would be important for Indian companies to seriously look at SLA's and agreements which have been signed with clients to understand the data protection implications. The same goes for understanding the applicable laws.

A major modification is that this clause doesn't mention the compensation limit of Rs. 1 Crore which was there as part of section 43 of the ITA 2000. This implies that there is no upper limit for damages that can be claimed. This essentially is "unlimited liability" for Indian companies, which could cause serious business implications.

Section 72A:

Under this section disclosure without consent exposes a person including an "intermediary" to three years imprisonment of fine upto Rs. Five lacs or both.
This section uses the term "personal information" and not "sensitive personal information" as in section

43A. Hence it could apply to any information which is obtained in order to deliver services. Hence in some ways broadens the definition of information.

2. Information Preservation

Across the amendments there are several references to “service providers” or “intermediaries”, which in some form would apply to all Indian companies.

e.g. Section 67C: Preservation and Retention of information by intermediaries.

Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe”. Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to 3 years and shall also be liable to fine.

The notifications on time for preservation etc. are not yet released. However since this is a “cognizable” offense any police inspector can start investigations against the CEO of a company.

Apart from the two aspects discussed in this note, there are other areas which could also be considerations for E.g.

Sec 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.etc.

In summary, IT Risk management and response needs to be looked at by all companies for various reasons including customer assurance, compliance, customer regulations, protection of information assets etc. The ITA 2008 amendments provide us with few additional factors for considerations which could have significant impact on business. Information technology regulations and laws would only get more stringent and defined; hence it’s imperative for organizations to be aware and prepared.

The Information Systems (IS) audit group assesses the University's critical systems, technology architecture and processes to assure information assets are protected, reliable, available and compliant with University policies and procedures, as well as applicable laws and regulations. We emphasize the importance of mitigating security risks during our audit coverage of the University’s application, operating and networking systems. Through our integrated and IT governance audits, we evaluate information technology’s impact on the University’s processes and its abilities to achieve its goals and objectives. Our evaluations are objective and professional, utilizing COBIT (Control Objectives for Information and related Technology) framework, an international standard for good IT control practices.

ISA provides the following audit services:

- IT **Governance** - IT governance audits include reviewsof the organization’s fiduciary responsibility in satisfying the quality of IT delivery services while aligning with the business objectives and establishing an adequate system of internal controls.
- Information Systems - Information systems audits focus on security controls of physical and logical security of the server including change control, administration of server accounts, system logging and monitoring, incident handling, system backup and disaster recovery.
- Integrated Audits - Integrated audits include reviews of the business operations and their dependency of automated systems to support the business process. We consider information technology and financial and operational processes as mutually dependent for establishing an effective and efficient control environment. From the technology perspective, the audit focuses on application controls,

administration of user access, application change control and backup and recovery to assure reliability, integrity and availability of the data.

- Control Self-assessments - Control Self-assessments are designed for department that manages and operates a technology environment. These self-assessment tools can be used to identify potential areas of control weakness in the management of the technology environment.
- Compliance - Compliance audits include University policies and procedures, Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA) and any other applicable laws and regulations.

Financial Regulatory Bodies in India

In India, the financial system is regulated with the help of independent regulators, associated with the field of insurance, banking, commodity market, and capital market and also the field of pension funds. On the other hand, the Indian Government is also known for playing a significant role in controlling the field of financial security and also influencing the roles of such mentioned regulators. You must be aware of the regulatory bodies and their functions, before a final say. The most prominent of all is RBI or Reserve Bank of India. Let us look in detail about various Financial Regulatory Bodies in India.

RBI – Reserve Banks of India :

Reserve Bank of India : Reserve Bank of India is the apex monetary Institution of India. It is also called as the central bank of the country.

The Reserve Bank of India was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. The Central Office of the Reserve Bank was initially established in Calcutta but was permanently moved to Mumbai in 1937. The Central Office is where the Governor sits and where policies are formulated. Though originally privately owned, since nationalization in 1949, the Reserve Bank is fully owned by the Government of India.

The Central Office is where the Governor sits and is where policies are formulated. Though originally privately owned, since nationalization in 1949, the Reserve Bank is fully owned by the Government of India.

SEBI – Securities and Exchange Board of India :

Apart from RBI, SEBI also forms a major part under the financial body of India. This is a regulator associated with the security markets in Indian Territory. Established in the year 1988, the SEBI Act came into power in the year 1992, 12th April. The board comprises of a Chairman, Whole time members, Joint secretary, member appointed, Deputy Governor of RBI, secretary of corporate affair ministry and also part time member. There are three groups, which fall under this category, and those are the investors, the security issuers and market intermediaries.

PFRDA – Pension Fund Regulatory and Development Authority :

Pension Fund regulatory is a pension related authority, which was established in the year 2003 by the Indian Government. It is authorized by the Finance Ministry, and it helps in promoting income security of old age by regulating and also developing pension funds. On the other hand, this group can also help in protecting the interest rate of the subscribers, associated with the schemes of pension money along with the related matters. PFRDA is also responsible for the appointment of different other intermediate agencies like Pension fund managers, CRA, NPS Trustee Bank and more.

FMC – Forward Markets Commission :

Other than the financial bodies mentioned above, FMC also plays a major role. It is the chief regulator of the commodity(MCX, NCDEX, NMCE, UCX etc) of the Indian futures market. As per the latest news feed, it has regulated the amount of Rs. 17 trillion, under the commodity trades. Headquarter is located in Mumbai, and the financial regulatory agency is working in collaboration with the Finance Ministry. The chairman of FMC works together with the Members of the same organization to meet the required ends. The main aim of this body is to advise the Central Government on matters of the Forwards Contracts Act, 1952.

IRDA – Insurance Regulatory and Development Authority :

Lastly, it is better to mention the name of IRDA or insurance regulatory and Development authority, as a major part of the financial body. This company is going to regulate the apex statutory body, which will regulate and at the same time, develop the insurance industry. It comprised of the Indian Parliamentary act and was passed duly by the Indian Government. Headquarter of this group is in Hyderabad, and it was shifted from Delhi to Hyderabad. These are some of the best-possible points, which you can try and focus at, while dealing with financial bodies of India.

The Reserve Bank of India issued new guidance in April 2011 for banks to mitigate the risks of use of information technology in banking operations. RBI guidelines are result of the Working Group's recommendations on information security, electronic banking, technology risk management and cyber fraud. The Working Group was formed under the chairmanship of G. Gopalakrishna, the executive director of RBI in April 2010.
The guidance is largely driven by the need for mitigating cyber threats emerging from increasing adoption of IT by commercial banks in India.

Recommendations are made in nine broad areas, including-

1. IT Governance: emphasizes the IT risk management accountability on a bank's board of directors and executive management. Focus includes creating an organizational structure and process to ensure that a bank's IT security sustains and extends business strategies and objectives.

2. Information Security: maintaining a framework to guide the development of a comprehensive information security program, which includes forming a separate information security function to focus exclusively on information security and risk management, distinct from the activities of an information technology department. These guidelines specify that the chief information security officer needs to report directly to the head of risk management and should not have a direct reporting relationship with the chief information officer.

3. IT Operations: specialized organizational capabilities that provide value to customers, including IT service management, infrastructure management, application lifecycle management and IT operations risk framework.

4. IT Services Outsourcing: places the ultimate responsibility for outsourcing operations and management of inherent risk in such relationships on the board and senior management. Focus includes effective selection of service provider, monitoring and control of outsourced activities and risk evaluation and management.

5. Information Security Audit: the need for banks to re-assess IS audit processes and ensure that they provide an independent and objective view of the extent to which the risks are managed. This topic focuses on defining the roles and responsibilities of the IS audit stakeholders and planning and execution of the audit.

6. Cyberfraud: defines the need for an industry wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. Focus includes creating an organizational structure for fraud risk management and a special committee for monitoring large value fraud.

7. Business Continuity Planning: focuses on policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. Also, this topic emphasizes implementing a framework to minimize the operational, financial, legal, reputational and other material consequences arising from such a disaster.

8. Customer Education: the need to implement consumer awareness framework and programs on a variety of fraud related issues.

9. Legal Issues: defines the need to put effective processes in place to ensure that legal risks arising from cyber laws are identified and addressed at banks. It also focuses on board's consultation with legal department on steps to mitigate business risks within the bank.

Background :

Technology has become a part of all walks of life and across all business sectors, and even more so in banking. There has been massive use of technology across many areas of banking business in India, both from the asset and the liability side of a bank's balance sheet. Delivery channels have immensely increased the choices offered to the customer to conduct transactions with ease and convenience. Various wholesale and retail payment and settlement systems have enabled faster means of moving the money to settle funds among banks and customers, facilitating improved turnover of commercial and financial transactions. Banks have been taking up new projects like data warehousing, customer relationship management and financial inclusion initiatives to further innovate and strategise for the future and to widen the reach of banking.

The dependence on technology is such that the banking business cannot be thought of in isolation without technology, such has been the spread of technology footprints across the Indian commercial banking landscape. Developments in IT have also brought along a whole set of challenges to deal with. The dependence on technology has led to various challenges and issues like frequent changes or obsolescence, multiplicity and complexity of systems, different types of controls for different types of technologies/systems, proper alignment with business objectives and legal/regulatory requirements, dependence on vendors due to outsourcing of IT services, vendor related concentration risk, segregation of duties, external threats leading to cyber frauds/crime, higher impact due to intentional or unintentional acts of internal employees, new social engineering techniques employed to acquire confidential

credentials, need for governance processes to adequately manage technology and information security, need for appreciation of cyber laws and their impact and to ensure continuity of business processes in the event of major exigencies.

Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information. Compliance risk is also an outcome in the event of non-adherence to any regulatory or legal requirements arising out of the use of IT. These issues ultimately have the potential to impact the safety and soundness of a bank and in extreme cases may lead to systemic crisis.

Keeping in view the changing threat milieu and the latest international standards, it was felt that there was a need to enhance RBI guidelines relating to the governance of IT, information security measures to tackle cyber fraud apart from enhancing independent assurance about the effectiveness of IT controls. To consider these and related issues, RBI announced the creation of a Working Group on Information Security, Electronic Banking, Technology Risk Management and Tackling Cyber Fraud in April, 2010. The Group was set up under the Chairmanship of the Executive Director Shri.G.Gopalakrishna.

The Group delved into various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas are IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal issues.

Major Recommendations of the Working Group

The Group felt that the recommendations are not “one-size-fits-all” and the implementation of these recommendations need to be based on the nature and scope of activities engaged by banks and the technology environment prevalent in the bank and the support rendered by technology to the business processes.

On IT Governance:

- Banks need to formulate a Board approved IT strategy/plan document. An IT policy needs to be framed for regular management of IT functions and ensure that detailed documentation in terms of procedures and guidelines exists and are implemented. The strategic plan and policy need to be reviewed annually.

- A need was felt to create an exclusive Board level IT Strategy Committee with a minimum of two directors as members, one of whom should be an independent director. All members of the IT Strategy Committee would need to be technically competent while at least one member would need to have substantial expertise in managing/guiding technology initiatives.

- A need was felt for the position of CIO in banks, to be the key business player and play a part in the executive decision-making function. The key role of the CIO would be to act as an owner of the IT function and enable the alignment of business and technology.

- IT Steering Committee needs to be created with representations from various IT functions, HR, Legal and business functions as appropriate. The role of the IT Steering Committee would be to assist the Executive Management in the implementation of the IT strategy approved by the Board.

- The IT Steering Committee should assess whether the IT Governance structure fosters accountability, is effective and transparent, has well defined objectives and actions and unambiguous responsibilities for each level in the organization.

- The organizational structure for IT should be commensurate with the size, scale and nature of business activities carried out by the bank and the underlying support provided by information systems for business functions.

- Key focus areas of IT Governance that need to be considered include strategic alignment, value delivery, risk management, resource management and performance management.
- Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately. A periodic assessment of the training requirements for human resources should be made to ensure that sufficient, competent and capable human resources are available.
- The Board needs to be adequately aware of IT resources and infrastructure available to meet required strategic business objectives and ensure that a process is in place to record the resources available/ potentially available to the bank.
- Performance of IT function should be monitored to ensure delivery on time and within budget, with appropriate functionality and with intended benefits.
- Banks need to establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT strategy. The model should facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, cost-effective, timely, secure and resilient to failure
- There is also a need to maintain an "enterprise data dictionary" that incorporates the organization's data syntax rules. This should enable the sharing of data among applications and systems, promote a common understanding of data among IT and business users and preventing incompatible data elements from being created
- Procedures to assess the integration and interoperability of complex IT processes such as problem, change and configuration management need to exist, depending upon the extent of technology leverage in a bank.
- An appropriate programme and project management framework needs to be implemented for the management of all IT projects, which ensures correct prioritization and co-ordination
- For managing project risks, a consistent and formally defined programme and project management approach should be applied to IT projects that enable appropriate stakeholder participation and monitoring of project risks and progress
- For major projects, formal project risk assessment needs to be carried out and managed on an ongoing basis
- The bank-wide risk management policy or operational risk policy needs to include IT related risks and the Risk Management Committee should periodically review and update the same (at least annually).
- IT function needs to support a robust and comprehensive Management Information System with respect to various business functions as per business needs and in coordination with business personnel so as to provide inputs for effective decision making by management
- Components of well-known IT control frameworks such as COBIT as applicable to each bank's technology environment may be considered for implementation in a phased manner providing a standardized set of terms and definitions that are commonly interpreted by all stakeholders.
- Effective IT control practices and their monitoring are required to avoid breakdowns in internal control and oversight, increase efficiency, use resources optimally and increase the effectiveness of IT processes.
- Information on major IT projects that have a significant impact on the bank's risk profile and strategy needs to be reported to appropriate levels of management and undergo appropriate strategic and cost/ reward analysis on a periodic basis.
- Project level steering committees needs to be created to take responsibility for execution of the project plan, achievement of outcomes and project completion.

- An IT balanced scorecard may be considered for implementation, with approval from key stakeholders, to measure IT performance along different dimensions such as financial aspects, customer satisfaction, process effectiveness, future capability, and for assessing IT management performance.
- Banks may also consider assessing their IT maturity level, based on well known international standards, design an action plan and implement the plan to reach the target maturity level.
- A forum in India, under the aegis of IDRBT, akin to the Financial Services Technology Consortium in the US, can work collaboratively to solve shared problems and challenges, as well as pioneer new technologies that benefits all banks.
- An exclusive forum for CIO and senior IT officials of banks, under the aegis of IDRBT, can be encouraged to enable sharing of experiences and discuss issues of contemporary relevance for the benefit of the industry as a whole.

On Information Security:

- The major role of the Board/ Top Management should involve approving information security policies, establishing necessary organizational processes/ functions for information security and providing necessary resources.
- Each bank needs to create a separate information security function to focus exclusively on information security management. The organization of the information security function should be commensurate with the nature and size of activities of a bank and extent of IT leverage and e-delivery channels. The function should be adequately resourced in terms of the number of staff, their range and level of skills, and tools or techniques.
- A sufficiently senior level official of the rank of GM/DGM/AGM needs to be designated as the Chief Information Security Officer (CISO) responsible for articulating and enforcing the policies that a bank uses to protect its information assets apart from coordinating the information security related issues / implementation within the organization as well as relevant external agencies. The CISO needs to report directly to the Head of the Risk Management function and should not have a direct reporting relationship with the CIO.
- A Board approved Information security policy needs to be in place and reviewed at least annually. The policy framework should take into consideration, inter-alia, aspects like :alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organizational structure; information security roles and responsibilities; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.
- Risk assessment is the core competence of information security management for a bank. The risk assessment must, for each asset within its scope, identify the threat/ vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance and/or contractual perspective.
- Job descriptions, including roles and responsibilities, employment agreements and policy awareness acknowledgements from staff increase accountability for security. Management can communicate general and specific security roles and responsibilities for all employees based on their job descriptions. Management should expect all employees, officers, and contractors to comply with information security and/or acceptable-use policies and protect the institution's assets, including information.
- Digital evidence needs to be considered as similar to any other form of legal proof. It needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by the concerned personnel. A policy needs to be in place in this regard.
- Maintaining detailed inventory of information assets and classification of information/data are among the key components of information security management.

- Banks need to grant authorisation for access to information assets only where a valid business need exists and only for a definite time period for which the access is required.
- Personnel with elevated system access privileges should be closely supervised.
- Information security needs to be considered at all stages of an information asset's (like hardware, software) life-cycle which typically includes: planning and design; acquisition and implementation; maintenance and support; and disposal so as to minimise exposure to vulnerabilities.
- Banks should have a process in place to verify job application information on all new employees. The sensitivity of a particular job or access level may warrant additional background and credit checks.
- Banks should implement suitable physical and environment controls taking into consideration threats, and based on the entity's unique geographical location, building configuration, neighboring entities, etc.
- There is a vital need for initial, and ongoing, training/awareness programmes on information security for employees and vendor personnel. There should also be a mechanism to track the effectiveness of the training programmes periodically through an assessment process designed for testing the understanding of relevant policies.
- A robust incident management process needs to be in place to maintain the capability to manage incidents within an enterprise, to enable containment of exposures and to achieve recovery within a specified time period. Incidents could include aspects relating to misuse of computing assets, information disclosure or events that threaten the continuance of business processes.
- A bank needs to have clear accountability mechanisms and communication plans (for escalation and reporting to the Board and senior management and customer communication where appropriate) to limit the impact of information security incidents. Institutions would also need to pro-actively notify CERT-In/IDRBT/RBI regarding major cyber security incidents.
- There should be documented standards/procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties needs to be enforced.
- Every application affecting critical/sensitive information, for eg. impacting financial, customer, control, risk management, regulatory and statutory aspects, must provide for detailed audit trails/ logging capability with details like transaction id, date, time, originator id , authorizer id, actions undertaken by a given user id, etc. Other details like logging IP address of client machine, terminal identity or location also need to be available. Alerts regarding use of the same machine for both maker and checker transactions need to be considered. The logs/alerts/exception reports with regard to systems should be analyzed and any issues need to be remedied at the earliest.
- The audit trails should satisfy a bank's business requirements apart from regulatory and legal requirements. It should also be facilitating the conduct of audit, serving as forensic evidence when required and assisting in dispute resolution including for non-repudiation purposes. Audit trails should be secured to ensure the integrity of the information captured and preservation of evidence.
- Banks may obtain application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).
- Data security measures need to be in place. Banks need to define and implement procedures to ensure the integrity and consistency of all critical data stored in electronic form, such as databases, data warehouses and data archives.
- Direct back-end updates to database should not be allowed except during exigencies, in the event of a genuine business need and after due authorization as per relevant policy

- Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process.

- For all critical applications, either source code must be received from the vendor or a software escrow agreement needs to be in place with a third party to ensure source code availability in case the vendor goes out of business. It needs to be ensured that product updates and programme fixes are also included in the escrow agreement.

- Data transfer from one process to another or from one application to another, particularly in respect of critical or financial applications, should not have any manual intervention in order to prevent any unauthorized modification. The process needs to be automated and properly integrated through "Straight Through Processing" methodology with an appropriate authentication mechanism and audit trails.

- In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign banks, there needs to be suitable controls like segregation of data and strict access controls based on 'need to know' and robust change controls. The bank should be in a position to adequately prove the same to the regulator. Regulator's access to such data/records and other relevant information should not be impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees or other persons.

- Robust system security testing needs to be carried out.

- Multi-tier application architecture needs to be implemented for critical e-banking systems like internet banking which differentiate session control, presentation logic, server side input validation, business logic and database access.

- A bank needs to have a documented migration policy specifying a systematic process for data migration and for ensuring data integrity, completeness and consistency. Explicit sign offs from users/application owners need to be obtained after each stage of migration and also after the migration process has been completed. Audit trails need to be available to document the conversion, including data mappings and transformations.

- Banks need to carry out due diligence with regard to new technologies/systems since they can potentially introduce additional risk exposures

- Any new business products introduced, along with the underlying information systems, need to be assessed as part of a formal product approval process which incorporates, inter-alia, security related aspects and fulfilment of relevant legal and regulatory prescriptions.

- Cryptographic techniques need to be used to control access to critical and sensitive data/information in transit and storage. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.

- Normally, a minimum of 128-bit SSL encryption is expected. Constant advances in computer hardware, cryptanalysis and distributed brute force techniques may induce use of larger key lengths periodically. It is expected that banks will properly evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required.

- Banks need to scan frequently for vulnerabilities and address discovered flaws proactively to avoid the likelihood of having their computer systems compromised. Automated vulnerability scanning tools need to be used against all systems in their networks on a periodic basis.

- Banks need to have monitoring processes in place to identify suspicious events and unusual behavioural patterns that could impact the security of IT assets. The strength of the monitoring controls should be based on the criticality of an IT asset. A bank would need to establish a clear allocation of

responsibility for regular monitoring mechanism, and the tools and processes in this regard need to be commensurate with the level of monitoring required.

- Critical functions , for example relating to financial, regulatory and legal, MIS and risk management, need to be done through proper application systems and not manually or in a semi-automated manner through spreadsheets which pose risks relating to data integrity and reliability. Use of spreadsheets in this regard should be restricted and should be replaced by appropriate IT applications in a phased manner within a definite timeframe.

- A robust process needs to be in place for "effective malware control". Typical controls to protect against malicious code use layered combinations of technology, policies and procedures and training. The controls are of the preventive and detective/corrective in nature.

- Establishing a robust network protection strategy and layered security based on the principle of defence-in-depth is an absolute necessity for banks.

- There should be arrangements for monitoring and reporting of the information security condition of the organization, which are documented, agreed with top management and performed regularly. Security related metrics can be used to measure security policy implementation.

- Given the multiplicity of devices and systems, banks should deploy suitable automated tools for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis.

- Security and Audit Processes of Critical service providers/vendors need to be assessed regularly since ineffective third-party controls can weaken the ability of a bank to achieve its control objectives.

- Commercial banks should implement ISO 27001 based Information Security Management System (ISMS) best practices for their critical functions. Additionally, other reputed security/IT control frameworks may also be considered by banks.

- Strong controls need to be initiated against any remote access facility. The management should establish policies restricting remote access and be aware of all remote-access devices attached to the bank's systems. These devices should be strictly controlled.

- Events that trigger the implementation of a business continuity plan may have security implications. Risk assessments should consider the changing risks that appear in business continuity scenarios and different security postures that may need to be established.

- Information security assurance needs to be obtained through periodic penetration testing exercises, audits and vulnerability assessments. The assurance work needs to be performed by appropriately trained and independent information security experts/auditors. The strengths and weaknesses of critical internet-based applications, other critical systems and networks needs to be carried out before each initial implementation, and at least annually thereafter. Any findings needs to be reported and monitored using a systematic audit remediation or compliance tracking methodology.

- Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking should be issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. A customer should not be forced to opt for services in this regard. Banks should provide clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.

- In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for critical activities like fund transfers and changing customer related details through internet banking facility.

- The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution's internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/commercial); customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to the bank and the volume of transactions involved.

- While not using the asymmetric cryptosystem and hash function is a source of legal risk, the banks, at the least, need to implement dynamic two-factor authentication through user id/password combination and second factor like (a) OTP/dynamic access code through various modes like SMS over mobile phones or hardware token or (b) a digital signature, through a card/token containing a digital certificate and associated private key (preferably for corporate customers).

- To enhance online processing security, confirmatory second channel procedures(like telephony, SMS, email etc.) should be applied with regard to transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.

- Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. It should, however, be noted that SSL does not provide end-to-end encryption security at the application layer but is only designed to encrypt data in transit at the network transport layer.

- A risk based transaction monitoring or surveillance process needs to be put in place. The banks may consider dynamic scoring models and related processes to trigger or alert transactions which are not normal to improve preventive/detective capability. Study of customer transaction behavioral patterns and stopping irregular transactions or obtaining prior confirmation from customers for outlier transactions may be incorporated as part of the process.

- Chip based cards house data on microchips instead of magnetic stripes, making data more difficult to steal and cards more difficult to reproduce. It is recommended that RBI may consider moving over to chip based cards along with requiring upgradation of necessary infrastructure like ATMs/POS terminals in this regard in a phased manner.

- For debit / credit card transactions at the POS terminals, PIN based authorization system needs to be put in place (without any looping) in place of the existing signature based system and the non-PIN based POS terminals need to be withdrawn in a phased manner.

- Given that control, security and legal issues on cloud computing are still evolving, a bank needs to be cautious and carry out due diligence to assess the risks comprehensively before considering cloud computing.

- There needs to be forum of CISOs who can periodically interact and share experiences regarding any information security threats. It is reported that a CISO forum is already functional under IDRBT. The forum may, among other functions, endeavour to share good practices, identify any specific information security issues and flag them to appropriate stakeholders like the regulator, IBA etc.

- There is a need for a system of information sharing akin to the functions performed by FS-ISAC (Financial Services Information Sharing Agency) in the US. IDRBT as a sub-CERT to the banking system can function as a nodal point for information sharing.

- Accreditation and empanelment of security audit qualifications/certifications and security audit vendors can be considered at a wider level by the Government of India/CERT-In or by IDRBT for the banking sector.

- In order to reduce the time, cost, and complexity of software assurance and to ensure its security, sustainability and resilience and increase the effectiveness of the methods used by the banking industry for software assurance, an initiative similar to FSTC Software Assurance Initiative (SAI) in the US can be considered in India, possibly under the aegis of IDRBT along with various stakeholders.

- There is a need for IBA, IDRBT and reputed institutions like DSCI to collaborate and develop security frameworks and detailed implementation methodologies and procedures for the benefit of the banking sector, based on the information security related aspects covered in this report.

- There is an increasing need for specific detailed research in security of banking technology and bringing out innovative and secure banking products in collaboration with reputed academic bodies like the IITs. IDRBT can expand its activities/initiatives in this regard.

- Given the nature of the problem of cyber security, there needs to be engagement at a wider level nationally and internationally, with the government, law enforcement agencies, various industrial associations and academic institutions.

- RBI can consider having a multi-disciplinary Standing Committee on Information Security with representation from various stakeholders to consider new security related developments and also legal developments, and based on the same, provide recommendations for suitable updation of guidelines on periodic basis.

- Collaborative efforts may also be made by reputed bodies like IDRBT, IIBF and DSCI coordinated by IBA to create customized indigenous certification courses to certify specific knowledge and skillsets in IT/information security areas for various categories of bank personnel at operational and managerial levels so as to create a large and diverse pool of requisite talent within the banking system.

On IT operations:

- The Board of Directors and Senior Management should oversee the implementation of a safe and sound IT operations environment. The policies and procedures defined as part of IT operations should support a bank's goals and objectives as well as follow statutory and regulatory requirements.

- IT operations include business services which are available to the internal or external customers of the organization using IT as a service delivery component. Instances include Mobile Banking and Internet Banking. IT Operations also include IT components which are used to support IT Operations, which can be service desk application, ticketing tools, event management tools etc. Banks may consider including test environment, quality assurance environment and any other such environment besides production environment within the scope of IT Operations.

- Banks should analyze their IT operation environment, including technology, human resources and implemented processes to identify threats and vulnerabilities and conduct a periodic risk assessment. As part of risk identification and assessment, banks should identify events or activities that could disrupt operations or negatively affect reputation or earnings and assess compliance to regulatory requirements. Banks should define various attributes for each risk component like probability of occurrence, financial impact etc. These attributes along with the business process involved should be used to prioritize risk mitigation actions and control framework.

- IT Strategy as framework should provide feedback to IT operations on the services to be supported, their underlying business processes, prioritization of these services etc. A well-defined IT strategy framework will assist IT operations in supporting IT services as required by the business and defined in SLAs.

- Service Valuation is the mechanism that can be considered by banks to quantify the services which are available to its customers (internal / external) and supported by IT operations in financial terms. Service Valuation will assist the IT Operation Function to showcase the involvement of the function in supporting the core business of the banks.

- Demand Management process provides guidelines which may be used by banks to understand the business processes IT operations support to identify, analyze and codify Patterns of Business Activities (PBA) to provide sufficient basis for capacity requirement.

- The components which should be considered when designing a new IT service or making a change to the existing IT service include business processes, service level agreements, IT infrastructure, IT environment etc.

- Over the years, the IT infrastructure in banks has grown and developed, and there may not be a clear picture of all the IT services currently being provided, and the consumers for each service. In order to establish an accurate IT landscape it is recommended that an IT Service Catalogue is defined,

produced and maintained. The Service Catalogue can be considered a repository that provides information on all the IT services supported by the IT Operations framework.

- Banks need to institute a Service Level Management process for planning, coordinating, and drafting, agreeing, monitoring and reporting of service attributes used to measure the quality of service. The framework needs to include guidelines for ongoing reviews of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved. The Service Level Management framework defined by the banks should also have guidelines defined for logging and management including escalation of complaints and compliments.

- A Capacity Management process is required to ensure that cost-justifiable IT capacity for IT services exists and matches the current and future business requirements as identified in the Service Level Agreement. Banks adopting the capacity management process should ensure that the framework encompasses all areas pertaining to technology i.e. hardware, software, human resources, facilities etc.

- The availability and reliability of IT services can directly influence customer satisfaction and the reputation of banks. Availability Management is essential in ensuring IT delivers the right level of service required by the business to satisfy its business objectives. When defining Availability targets for a business service, banks should consider identifying Vital Business Function (VBF).

- Attributes that can be used by banks to report availability of IT services include availability (in percentage), Mean Time between service incidents, Mean Time between Failures and Mean Time to Repair.

- Implementation of Service Asset and Configuration Management framework has cost and resource implications and therefore there need to be strategic discussions about the priorities to be addressed.

- Banks need to implement a 'change management' process for handling any changes in technology and processes to ensure that the changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner and environment.

- Operations phase as part of the Service Management lifecycle is responsible for executing and performing processes that optimize the cost of the quality of services. As part of the organization, it is responsible for enabling the business to meets its objectives. As part of technology, it is responsible for the effective functioning of components that support business services. The various aspects that banks need to consider include event management, incident management, problem management and access management.

<u>On IT outsourcing:</u>

- The Board and senior management are ultimately responsible for outsourced operations and for managing risks inherent in such outsourcing relationships. Responsibilities for due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the bank, Board and senior management.

- Banks need to assess the degree of 'materiality' inherent in the outsourced functions. Whether an outsourcing arrangement is 'material' to the business context or not is a qualitative judgment and may be determined on the basis of criticality of service, process or technology to the overall business objectives. Where a Bank relies on third party employees to perform key banking functions such as applications processing, etc. on a continuous basis, such outsourcing may also be construed as 'material', whether or not the personnel are located within the premises of the Bank.

- Outsourcing of non-financial processes, such as technology operations, is 'material' and if disrupted, has the potential to significantly impact business operations, reputation and stability of a Bank.

- Risk evaluation should be performed prior to entering into an outsourcing agreement and reviewed periodically in light of known and expected changes, as part of the strategic planning or review process.

- Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet a bank's own standards and any external requirements.

- While negotiating/ renewing an outsourcing arrangement, appropriate diligence should be performed to assess the capability of the technology service provider to comply with obligations in the outsourcing agreement. Due diligence should involve an evaluation of all information about the service provider including qualitative, quantitative, financial, operational and reputational factors.

- Banks must be required to report to the regulator where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology / process outsourcing

- The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by the bank's legal counsel on their legal effect and enforceability.

- Banks should ensure that the contract brings out the nature of the legal relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages. Contracts should clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses. Any 'limitation of liability' consideration incorporated by the service provider should be assessed in consultation with the legal department.

- In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end to end solution for the financial institution, the bank remains responsible for understanding and monitoring the control environment of all service providers that have access to the bank's systems, records or resources.

- Banks should establish a structure for management and control of outsourcing, based on the nature, scope, complexity and inherent risk of the outsourced activity.

- Management should include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize performance criteria to measure the quality and quantity of service levels. For outsourced technology operations, specific metrics may be defined around service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization.

- Banks should evaluate the adequacy of the internal controls environment offered by the service provider. Due consideration should be given to implementation by the service provider of various aspects like information security policies and employee awareness of the same, logical access controls, physical and environmental security and controls, controls for handling data etc.

- Outsourcing should not impede or interfere with the ability of the bank or the regulator in performing its supervisory functions and objectives. As a practice, institutions should conduct pre- and post- outsourcing implementation reviews. An institution should also review its outsourcing arrangements periodically (atleast annually) to ensure that its outsourcing risk management policies and procedures, and these guidelines, are effectively complied with.

- An institution should, at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations.

- Banks should also periodically commission independent audit and expert assessments on the security and control environment of the service provider.

- Banks should ensure that their business continuity preparedness is not compromised on account of outsourcing.

- Banks need to take effective steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated.

- In the event of outsourcing of technology operations, the banks should subject the same to enhanced and rigorous change management and monitoring controls since ultimate responsibility and accountability rests with the bank.

- Banks, while framing the viable contingency plan, need to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in-house in an emergency (for example, where number of vendors for a particular service is extremely limited) and the costs, time and resources that would be involved and be prepared to take quick action, if warranted.

- The engagement of service providers across multiple geographies exposes the organization to country risk – economic, social and political reasons in the country that may adversely affect the bank's business and operations. Banks should proactively evaluate such risk as part of the due diligence process and develop appropriate mitigating controls and as required, an effective exit strategy.

- Emerging technologies such as data center hosting, applications as a service and cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and in case of significant changes performed by the service provider.

- Banks should ensure that quality and availability of banking services to customers are not adversely affected due to the outsourcing arrangements entered into by the bank. Banks need to institute a robust grievance redressal mechanism, which should not be compromised in any way due to outsourcing.

- IBA may facilitate requisite data sharing between banks to maintain scoring information for existing / new service providers which may include any fraud or major operational lapses committed by the service providers.

- Detailed service provider assessment and monitoring frameworks and best practices from a banking context can be explored by IBA in collaboration with institutions like DSCI and IDRBT.

<u>On IS Audit:</u>

- To meet the responsibility to provide an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should provide an internal audit function which is capable of evaluating IT controls adequately.

- Banks should enable an adequately skilled composition of the Audit Committee to manage the complexity of the IS Audit oversight. A designated member of the Audit Committee needs to possess the relevant knowledge of Information Systems, IS Controls and audit issues. The designated member should also have relevant competencies to understand the ultimate impact of deficiencies identified in IT Internal Control framework by the IS Audit function. The Board or its Audit Committee members should seek training to fill any gaps in the knowledge related to IT risks and controls.

- The Audit Committee should devote appropriate and sufficient time to IS audit findings identified during IS Audits and members of the Audit Committee would need to review critical issues highlighted and provide appropriate guidance to the bank's management.

- Banks should have a separate IS Audit function within the Internal Audit department led by an IS Audit Head, assuming responsibility and accountability of the IS audit function, reporting to the Chief Audit Executive (CAE) or Head of Internal Audit. Where the bank uses external resources for conducting IS audit in areas where skills are lacking within the bank, the responsibility and accountability for such external IS audits still remain with the IS Audit Head and CAE.

- IS Auditors should act independently of the bank's management. In all matters related to the audit, the IS Audit should be independent of the auditee in both attitude and appearance. IS Auditors should be professionally competent, having the skills, knowledge, training and relevant experience to conduct an audit. IS Auditors should exercise due professional care, which includes following professional auditing standards in conducting the audit.

- Banks may decide to outsource the execution of segments of the audit plan to external professional service providers, as per the overall audit strategy decided in co-ordination with the CAE and the Audit Committee. The work outsourced shall be restricted to execution of audits identified in the audit plan. Banks need to ensure that the overall ownership and responsibility of the IS Audit including the audit planning process, risk assessment and follow up of compliance remains within the Bank. External assistance may be obtained initially to put in place necessary processes in this regard, if required.

- An Audit Charter / Audit Policy is a document which guides and directs the activities of the Internal Audit function. IS Audit, being an integral part of the Internal Audit function, should also be governed by the same Audit Charter / Audit Policy. The audit policy should be documented to contain a clear description of its mandate, purpose, authority and accountability (of relevant members/officials in respect of the IS Audit i.e. IS Auditors, audit management and the audit committee) and the relevant operating principles. The document should be approved by the Board of Directors.

- IS Audit policy/charter should be subjected to an annual review to ensure its continued relevance and effectiveness.

- The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys etc.) to understand the auditee's needs and expectations relevant to the IS audit function. These needs should be evaluated against the policy with a view to improving the service or changing the service delivery or audit charter, as necessary.

- Banks need to carry out IS Audit planning using the Risk Based Audit Approach. The approach involves aspects like IT risk assessment methodology, defining the IS Audit Universe, scoping and planning the audit, execution and follow up activities.

- The IS Audit Universe can be built around the four types of IT resources and various IT processes like application systems, information or data, infrastructure(technology and facilities like hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them that enable the processing of the applications) and people (internal or outsourced personnel required to plan, organize, acquire, implement, support, monitor and evaluate the information systems and services).

- The IS Auditor must define, adopt and follow a suitable risk assessment methodology. A successful risk-based IS audit program can be based on an effective scoring system arrived at by considering all relevant risk factors. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the Audit Committee or the Board of directors. Risk assessment related guidelines will vary for individual banks depending on their size, complexity, scope of activities, geographic diversity, and various technologies/systems used.

- The IS Audit Plan (either separately or as part of the overall internal audit plan) should be a formal document, duly approved by the Audit Committee initially and during any subsequent major changes. The Audit plan should be prepared so that it is in compliance with appropriate external regulatory/legal requirements, in addition to well-known IS Auditing Standards.

- The IS Audit Head is responsible for the annual IS Audit Plan which is prepared based on the scoping document and risk assessment. The Audit plan typically covers the overall audit strategy, scoped audit areas, details of control objectives identified in the scoping stage, sample sizes, frequency of audit based on risk assessment, nature and extent of audit and IT audit resources identification. A report on the status of planned versus actual IS audits, and any changes to the annual IS audit plan, needs to be presented periodically to the Audit Committee and Senior management.

- IT governance, information security governance related aspects, critical IT general controls like data centre controls and processes and critical business applications/systems having financial/compliance implications including MIS and regulatory reporting systems and customer access points (like delivery channels) need to be subjected to IS Audit(or integrated audit) atleast once a year (or more frequently, if warranted by risk assessment).

- IS Audits should also cover branches, with focus on large and medium branches, in critical areas like password controls, control of user ids, operating system security, anti-malware controls, maker-checker controls, segregation of duties, rotation of personnel, physical security, review of exception reports/audit trails, BCP policy and testing etc.

- Detailed pre-implementation application control audits and data migration audits with regard to critical systems need to be subjected to an independent external audit.

- Banks also need to conduct a post-implementation detailed application control audit. Furthermore, banks should also include application control audits in a risk based manner as part of the regular Internal Audit/IS Audit plans with focus on data integrity (among other factors). General internal auditors with requisite functional knowledge need to be involved along with the IS Auditors in the exercise to provide the requisite domain expertise.

- IS Auditors should periodically review the results of internal control processes and analyze financial or operational data for any impact on risk assessment or scoring. Accordingly, various auditee units should be required to keep auditors up to date on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, application conversions, significant changes in organization or staff , new regulatory and legal requirements, security incidents etc.

- IS Auditors should be reasonably conversant with various fraud risk factors and should assess the risk of occurrence of irregularities connected with the area under audit. The IS Auditor should also consider Fraud Vulnerability assessments undertaken by the Fraud Risk Management group, while identifying fraud risk factors as part of IT risk assessment and audit process.

- Banks should consider using testing accelerators — tools and techniques that help support the procedures IS Auditors will be performing — to increase the efficiency and effectiveness of the audit.

- Auditors need to enhance utilization of CAATs, which may be used effectively in areas such as detection of revenue leakage, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume and value of transactions are reported. Suitable “read-only” access rights should be provided to auditors for enabling use of CAATs.

- Banks may consider, wherever possible, a continuous auditing approach for critical systems, which involves performing control and risk assessments on a more frequent basis by using technology suitably.

- The Board (or the Audit Committee) should be informed of Senior Management’s decision on all significant observations and recommendations. When IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for it, they should discuss the matter with Internal Audit function and Senior Management. If the IS Auditors are not in agreement with the decision regarding residual risk accepted by the bank, IS Auditors and Senior Management should report the matter to the Board (or the Audit Committee) for resolution.

- Services provided by a third party are relevant to the scope of IS Audit of a bank when those services, and the controls within them, form part of the bank’s information systems. These need to be adequately assessed as part of the IS Audit process.

- In order to provide assurance to management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the Banks Internal Audit including IS Audit function to validate the approach and practices adopted by them in the discharge of their responsibilities as laid out in the Audit Policy.

- Accreditation and empanelment of IS audit qualifications/certifications and IS audit vendors/firms can be considered by the Government of India.

<u>On Cyber Fraud:</u>

- Most retail cyber frauds and electronic banking frauds would be of values less than Rs.1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the

Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values.

- The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent fraud risk management group in the bank. The group should be adequately staffed and headed by a senior official of the bank, not below the rank of General Manager/DGM.

- Fraud review councils should be set up by the fraud risk management group with various business groups in the bank. The council should consist of the head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet at least every quarter to review fraud trends and preventive steps taken that are specific to that business function/group.

- Various fraud prevention practices need to be followed by banks. These include fraud vulnerability assessments(for business functions and also delivery channels), review of new products and processes, putting in place fraud loss limits, root cause analysis for actual fraud cases above Rs.10 lakhs, reviewing cases where a unique modus operandi is involved, ensuring adequate data/information security measures, following KYC and Know your employee/vendor procedures, ensuring adequate physical security, sharing of best practices of fraud prevention and creation of fraud awareness among staff and customers.

- No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analyzed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.

- Banks have started sharing negative/fraudulent list of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.

- Quick fraud detection capability would enable a bank to reduce losses and also serve as a deterrent to fraudsters. Various important requirements recommended in this regard include setting up a transaction monitoring group within the fraud risk management group, alert generation and redressal mechanisms, dedicated e-mail id and phone number for reporting suspected frauds, mystery shopping and reviews.

- Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitization for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

- It is widely accepted that fraud investigation is a specialized function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies.

- Apart from the categories of fraud that need to be reported as per RBI Master Circular on Frauds dated July 2, 2010, it is recommended that this should also include frauds in the electronic channels and the variants of plastic cards used by banks and their customers to conclude financial transactions.

- It has been noted that there is lack of uniformity regarding the amount of fraud to be reported to RBI. Some banks report the net loss as the fraud amount (i.e. fraud amount minus recovery), while others report the gross amount. Some do not report a fraud if the entire amount is recovered. In the case

of credit card frauds, some banks follow the practice of reporting the frauds net of chargeback credit received while others report the amount of the original transactions. To overcome such inconsistency, a uniform rule of reporting amounts involved in frauds is being recommended.

- A special mention needs to be made of frauds done by collusive merchants who use skimmed/stolen cards at the point of sale (POS) terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. Many banks do not report such cases stating that the banks which have issued the cards are the ones impacted. However, in these cases, the merchants cause undue loss to the bank by siphoning off the credit provided. Hence such cases should be reported as frauds.

- It has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud to RBI. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money.

- Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums.

- A positive way to create employee awareness is to reward employees who have gone beyond the call of duty and prevented frauds. Details of employees receiving such awards may be published in the fraud newsletters.

- In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed and customers/banks have to shuttle between different police units on the point of jurisdiction. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department, authorized to register complaints from banks and get the investigations done on the same, needs to be taken up with respective police departments.

- To enhance investigation skills of the staff in the fraud risk management group, a training institute for financial forensic investigation may be set up by banks under the aegis of IBA.

- The experience of controlling/preventing frauds in banks should be shared between banks on a regular basis. The standing forum provided by the Indian Banks' Association (IBA) can be used to share best practices and further strengthen internal controls in respective banks.

- At each state, a Financial Crime Review Committee needs to be set up on frauds along the lines of the Security Committee that has been set up by the RBI to review security issues in banks with law enforcement authorities. The Committee can oversee the creation of awareness by banks among law enforcement agencies on new fraud types, especially technology based frauds.

- There needs to multi-lateral arrangements amongst banks to deal with on-line banking frauds. The lack of such an arrangement amongst banks may force a customer to interact with different banks/ organizations when more than one bank is involved. IBA could assist in facilitating such a mechanism.

<u>On Business Continuity Planning (BCP):</u>

- A bank's Board has ultimate responsibility and oversight over the business continuity planning of a bank and needs to approve the Business Continuity policy of the bank. A bank's Senior Management is responsible for overseeing the business continuity planning process which inter-alia includes determining how the institution will manage and control identified risks, prioritizing critical business functions, allocating knowledgeable personnel and sufficient financial resources to implement the BCP.

- A senior official needs to be designated as the Head of BCP function.

- Since electronic banking has functions which are spread across more than one department, it is necessary that each department understands its role in the plan and the support required to maintain the plan. In case of disaster, each department has to be prepared for the recovery process aimed at protection of the critical functions. To this end, a set up like the BCP Committee is charged with the implementation of the BCP in an eventuality and all departments are expected to fulfill their respective

roles in a co-ordinated manner. Hence, a BCP/Crisis Management Committee consisting of senior officials from various departments like HR, IT, Legal, Business functions and Information Security needs to be instituted.

- There need to be adequate number of teams for handling various aspects of the BCP at the Central Office level as well as individual Zonal/ Controlling Office and branch levels.
- Banks should consider various BCP methodologies and standards, like BS 25999,as inputs for their BCP framework.
- The failure of critical systems or the interruption of vital business processes could prevent timely recovery of operations. Banks must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the business impact analysis, which analyzes the correlation between system components and the services they provide.
- People aspect should be an integral part of a BCP. Too often, plans are focused on technical issues, therefore it is suggested that a separate section relating to people should be incorporated, including details on staff welfare, counseling, relocation considerations, etc.
- Pandemic planning needs to be incorporated as part of the BCP framework of banks.
- Banks must regularly test BCP to ensure that they are up to date and effective. Testing of BCP should include all aspects and constituents of the bank i.e. People, Processes and Resources (including Technology).
- Banks should involve their Internal Auditors (including IS Auditors) to audit the effectiveness of BCP and its periodic testing as part of their Internal Audit work and their findings/ recommendations in this regard should be incorporated in their report to the Board of Directors and Senior Management.
- Banks should consider having a BCP drill planned along with the critical third parties in order to derive reasonable level of assurance in ensuring continuity in respect of pre-identified minimal required processes during exigencies.
- Banks should perform the DR/BCP test without movement of bank personnel to the DR site. This will help in testing the readiness of alternative staff at the DR site.
- Business continuity plans should be maintained by atleast annual reviews and updates to ensure their continued effectiveness.
- Banks should also consider having an unplanned BCP drill, wherein only a restricted set of people and certain identified personnel may be aware of the drill and not the floor/business personnel.
- Various detailed requirements relating to procedural, infrastructural and HR related aspects of BCP have been provided so that banks can improve BCP processes and generate best outcomes.
- There are many applications and services in the banking system that are highly mission critical in nature and therefore require high availability and fault tolerance to be considered while designing and implementing the solution. This aspect is to be taken into account especially while designing and implementing the data centre solution and corporate network solution.
- The solution architectures of DC and DR are not identical for all applications and services. Generally, it is observed that critical applications and services, namely the retail, corporate, trade finance and government business solutions as well as the delivery channels have the same DR configurations whereas surround or interfacing applications do not have DR support. Banks will have to conduct periodic reviews with reference to the above aspect and upgrade the DR solutions from time to time and ensure that all critical applications and support services have perfect replicas in terms of performance and availability.
- The configurations of servers, network devices and other products at the DC and DR have to be identical at all times. This includes the patches that are applied at the DC periodically and the changes

made to the software from time to time by customization and parameterization to account for regulatory requirements, system changes etc.

- Periodic checks to ensure data and transaction integrity between DC and DR are mandatory. Suitable automated tools may be leveraged in this connection.

- DR drills currently conducted periodically come under the category of planned shutdown. Banks have to evolve a suitable methodology to conduct drills which are closer to a real disaster scenario so that the confidence levels of the technical team taking up this exercise are built up to address requirements in the event of a real disaster.

- Consideration of telecom related redundancy and alternative data and voice communication channels in the event of exigencies should be incorporated as part of the business continuity planning.

- It is to be ensured that the support infrastructure at the DC and DR, namely the electrical systems, air-conditioning environment and other support systems do not have a single point of failure and have a building management and monitoring system to continuously monitor the resources. Monitoring of uptime has to be made as per the requirements and agreements with respective vendors. The same requirements have to be taken care of in case the DC/DR set up is in an outsourced location or a common shared set up.

- Given the need for drastically minimizing data loss during exigencies and enabling quick recovery and continuity of critical business operations, banks need to consider near site DR architecture. Major banks with significant customer delivery channel usage and significant participation in financial markets/payment and settlement systems may need to consider a plan of action for creating a near site DR architecture over the medium term (say, three years).

- An industry-wide alarm and crisis forum/organization (in which the key market participants and the most important providers of financial infrastructure services are represented) may be established. The heads of BCP from the participating institutions can make up the top level of this crisis organization, with the lower levels forming a network between those responsible for the areas of liquidity, large-value payments, retail payment transactions and IT. Any of the institutions can invoke the alarm organization by activating the level affected.

- A website for industry-wide BCP related information for the benefit of the industry can be considered.

- There are programmes in the US like the Telecommunications Service Priority System (TSPS), Government Emergency Telecommunications service (GETS) and Wireless Priority Service Program (WPS) for provision of priority telecom availability and recovery services during exigencies for critical infrastructures and institutions. Similarly, the Government of India may declare the banking sector, including financial markets, as critical infrastructure and consider instituting such special measures for priority infrastructural services to enable conduct of critical banking services and financial market transactions during exigencies.

<u>On Customer Education:</u>

- The Board of Directors/Senior Management need to be committed to the process of consumer education initiatives by providing adequate resources, evaluating the effectiveness of the process and fine-tuning and improving customer education measures on an ongoing basis.

- To get desired support for the programme, it is important to identify and involve key stakeholders in decision-making, planning, implementation and evaluation. A working group or committee can be created to establish a clear goal for the endpoint in consultation with key stakeholders, clearly define roles, responsibilities and accountabilities, communicate in an open, clear and timely manner, allowing for flexibility in approaches to suit different stakeholder needs, support training and development to ensure a change in behaviour and culture, learn from previous and ongoing experiences and celebrate achievements.

- Banks need to follow a systematic process to develop an awareness programme through the stages of planning and design, execution and management, and evaluation and course correction.

- Since awareness programmes should be customized for the specific audience, it is important to identify and segment the target users for the programmes - like bank customers, employees, law enforcement personnel, fraud risk professionals, media partners, etc.

- Building consensus among decision makers and stakeholders for financial and administrative support is an important step in the programme. In this respect, both fixed and variable costs need to be identified.

- Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully.

- A research group should be formed to continually update the communications team with the latest trends and evolving modus operandi. The team would maintain a repository of material such as case studies, sample mails, samples of fraudulent documents, international practice/developments etc.

- Evaluation of the effects of various campaigns for specific target groups can be measured through qualitative (e.g. focus groups, interviews) and/ or quantitative (e.g. questionnaires, omnibus surveys) research. Evaluation against metrics, performance objectives, etc. should also be conducted to check the campaign's effectiveness, and to establish lessons learned to improve future initiatives.

- At the industry level, each bank should have a documented policy, training mechanisms and research units. Material can be pooled from these units to be used on a larger platform towards a common goal.

On Legal Issues:

- The Risk Management Committee at the Board level needs to put in place processes to ensure that legal risks arising from cyber laws are identified and adequately addressed. It also needs to ensure that the concerned functions are adequately staffed and the personnel handling it are trained to carry out the function efficiently. The Operational Risk Group needs to incorporate legal risks as part of the operational risk framework and take steps to mitigate the risks assessed. The legal function within the bank needs to advise business groups on legal issues arising out of the use of Information Technology.

- There should be a robust system in banks to keep track of the transactions of the nature referred to in statutory guidelines on AML (like PMLA and PMLR) and report the same within the prescribed period. Apart from the risk of penalty, this involves reputational risk for such entities.

- Under the NI Act, a cheque in the electronic form has been defined as "a mirror image" of a paper cheque. The expression 'mirror image' does not appear to be appropriate. The expression, "mirror image of" may be substituted by the expression, "electronic graphic which looks like" or any other expression that captures the intention adequately.

- The definition of a cheque in electronic form contemplates a digital signature with or without biometric signature and an asymmetric crypto system. Since the definition was inserted in the year 2002, it is understandable that it has captured only the digital signature and asymmetric crypto system dealt with under Section 3 of the IT Act, 2000. Since the IT Act,2000 has been amended in the year 2008 to make provision for an electronic signature also,a suitable amendment in this regard may be required in the NI Act so that the electronic signature may also be used on cheques in electronic form.

- There is uncertainty with respect to the meaning of a crucial expression like 'intermediary" as per the IT Act 2000 and as amended by the IT Amendment Act, 2008. As such, it is necessary that clarity is brought about by a statutory amendment with regard to the meaning of the expression 'intermediary' in so far as banks and financial institutions are concerned.

- A combined reading of Section 2(p) and sub-sections (1) and (2) of Section 3 of the IT Act makes it clear that in terms of the Act an electronic record may be authenticated by affixing a 'digital signature' and if a party wants to authenticate the electronic record by affixing a digital signature, the electronic method or procedure for affixing the digital signature shall be an asymmetric crypto system and hash

function. While authentication of an electronic record by affixing a digital signature is optional, the procedure for affixing the digital signature, namely, use of an asymmetric crypto system and hash function, is mandatory.

- The question that arises for consideration is whether a party may be bound by the transactions entered into through electronic means (whether through ATMs, Internet or otherwise) though the electronic records in question are not authenticated by using digital/electronic signatures. On reading Section 65B (1) of the Indian Evidence Act, it is clear that electronic records may be proved in court even though they are not authenticated by using digital or electronic signatures if the conditions mentioned therein are satisfied. The difficulty in proving the various conditions set forth in sub-sections (2) and (3) of section 65B of the Indian Evidence Act is ameliorated to a great extent by sub-section (4) thereof under which the certificate of a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate.

- The Government should specify sufficient number of agencies under section 79A of the Indian Evidence Act to assist courts to arrive at a decision on the evidentiary value of electronic records irrespective of whether a digital or electronic signature is affixed.

- Financial transactions such as operation of bank accounts and credit card operations are being carried on by banks in a big way by using cards, pin numbers and passwords, etc. Banks are using many security features to prevent frauds to the extent possible. The proposed 'two factor authentication method' (2F method) is also a step in the same direction. It may not be ideal to mandate a particular technology (digital signatures with asymmetric crypto system and hash function) for authenticating all electronic transactions by banks.

- As a short term measure, it is recommended that Rules may be framed by the Central Government under Section 5 of the IT Act, to the effect that, with respect to internet or e- banking transactions, the 2F method or any other technique of authentication provided by banks and used by the customers shall be valid and binding with respect to such transactions, even if a 'digital signature' or 'electronic signature' is not affixed.

- The ISP license restricts the level of encryption for individuals, groups or organizations to a key length of only 40 bits in symmetric key algorithms or equivalents. RBI has stipulated SSL/ 128 bit encryption as a minimum level of security. SEBI has stipulated 64/128 bit encryption for Internet Based Trading and Services. Information Technology (Certifying Authorities) Rules, 2000 require' internationally proven encryption techniques' to be used for storing passwords. An Encryption Committee constituted by the Central Government under Section 84A of the IT Act, 2000 is in the process of formulating rules with respect to encryption. Allowance for higher encryption strength may be allowed for banks.

- Section 43A of the IT Act deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term 'sensitive personal data,' nor has it prescribed a "standard and reasonable security practice". Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law.

- The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation upto ` 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond ` 5 crore in a court of competent jurisdiction. The top management of banks could also suffer exposure to criminal liability given the provisions of Chapter XI of the amended Information Technology Act and the exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life imprisonment, as also a fine. Further, various computer related offences are enumerated under various provisions of the Act.

- Of late there have been many instances of 'phishing' in the banking industry, posing a major threat to customers availing internet banking facilities. Though Section 66D of the amended IT Act could broadly be said to cover the offence of phishing, the attempt to commit the act of phishing is not made

punishable. It is suggested that there is a need to specifically provide for punishment for an attempt to phish as well, in order to deter persons from attempting it.

- The issue of whether Section 43A read with Section 72 and 72A of the IT Act, 2000 address the issue of data protection adequately or whether they need to be supplemented by long-term provisions(which can help facilitate effective and efficient protection and preservation of data), would depend on the prescriptions of the Central Government. Various suggestions have been offered in this report in this regard.
- It is necessary to balance the interests of customers and those of banks and provide protection to banks against any fraudulent or negligent acts by the customer. It is not appropriate to leave such an important issue to be dealt with in documentation. Appropriate statutory provisions need to be enacted in this regard.
- Though there is no specific legislation in India which deals only with 'electronic fund transfer' and which is consumer protection driven, certain concerns have been dealt with in the Payment and Settlement Systems Act, Rules, Regulations, directions, etc. issued thereunder as well as the provisions of general law. However, it may be apposite to have some provisions similar to those in the EFT Act which exempts the bank from liability in the event of fraud by the customer or a technical failure, etc. (for eg., provisions dealing with 'unauthorized electronic fund transfers' and the consumer's liability for unauthorized transfers).

CERT-In (the Indian Computer Emergency Response Team)

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology (IT) security organization. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

CERT-In was created by the Indian Department of Information Technology in 2004 and operates under the auspices of that department. According to the provisions of the Information Technology Amendment Act 2008, CERT-In is responsible for overseeing administration of the Act.

CERT organizations throughout the world are independent entities, although there may be coordinated activites among groups. The first CERT group was formed in the United States at Carnegie Mellon University.

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERTIn is the national nodal agency for responding to computer security incidents as and when they occur.
In the recent Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

Collection,analysis and dissemination of information on cyber incidents.
Forecast and alerts of cyber security incidents
Emergency measures for handling cyber security incidents
Coordination of cyber incident response activities.
Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.
Such other functions relating to cyber security as may be prescribed

MCQS

1. To be considered a computer crime, what needs to be involved in the crime?
A) Technology
B) Computers
C) Data
D) Networks

2. What category of software is designed to cause detriment to your computer?
A) Bugs
B) Malware
C) Systems software
D) Network snakes

3. What worm emailed people with the words "I LOVE YOU" in the year 2000?
A) The Love Bug
B) The Love Letter
C) The Valentine Connection
D) The Darling Link

4. What type of virus describes the awful consequences of not acting immediately?
A) Android
B) Spoofing
C) Misleading e-mail
D) Phishing

5. Which computer virus records every movement you make on your computer?
A) Malware Android
B) Key logger
C) DoS
D) Trapper

6. What is it called when someone changes the FROM section of an email so that the message you receive appears to come from a person other than the one who sent it?
A) Spoofing
B) DoS
C) Spam
D) Trapper

7. What program would you use to gain administrative rights to someone's computer?
A) Bot
B) Executive Android
C) Rootkit
D) Trojan horse

8. What is your computer called when it is infected with a malware bot?
A) Zombie
B) Android
C) E-Ogre
D) Dirty bot

9. What type of hacker was the 16 year-old individual who hacked into NASA networks and downloaded temperature and humidity control software worth $1.7 billion?
A) Thrill-seeker hacker
B) Black-hat hacker

C) Script kiddie
D) White-hat hacker

10. What is a person called when they try to hurt a group of people with the use of a computer?
A) White-hat intruder
B) Cracker
C) Social engineer
D) Cyber terrorist

ANSWERS:

1	2	3	4	5	6	7	8	9	10
B	B	A	C	B	A	C	A	D	D

MCQs 2

Q1. Computer crime or Cyber crime is crime that involves:
a) Computer
b) Network
c) Both of Above*
d) None of These

Q2. Net crime is criminal exploitation of the ___:
a) Browsers
b) Servers
c) Internet*
d) None of These

Q3. Crime through Internet includes:
a) Telemarketing
b) Internet fraud
c) Identity Theft
d) Credit Card account thefts
e) All of the Above*
f) None of These

Q4. Which among the following is correct about "Hacking":
a) Hacking is an illegal intrusion into a computer system and/or network.
b) Cracking term is equivalent to Hacking (In Indian Laws perspective there is no difference between the term hacking and cracking).
c) Every act committed towards breaking into a computer and/or network is hacking.

d) Hacker can hack or personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.
e) All of the Above*
f) None of These

Q5. Which among the following is correct about "Child Pornography":
a) Pedophiles lure the children by distributing pornographic material.
b) Pedophiles falsely represent their selves as of same age and win the confidence of children by chatting and by sending images.
c) Pedophiles after wining the confidence of children then offers then monetary as well as physical awards.
d) Pedophiles may sexually exploit the children by using them as sexual objects or by taking their pornographic pictures, in order to sell those over the internet.
e) All of the Above*
f) None of These

Q6. Which among the following characteristics are correct about 'Cyberstalking':
a) Cyberstalking is the use of the internet or electronics to stalk or harass an individual or any group.
b) It includes making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects
c) It may be offline as well as online
d) All of the Above*
e) None of These

Q7. Denial - of - service attack includes:
a) a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic
b) DoS attacks are included in it.
c) Both of Above*
d) None of These

Q8. Which among the following is wrong characteristic of "Phishing":
a) Fakers, by offering special rewards or money prize etc asked for personal information such as passwords, credit card information, social security and bank account numbers or other material information.
b) Main purpose is theft or misuse the acquired material
c) Both of Above
d) None of These*

Q9. Credit Card Fraud includes:
a) Credit cards are illegally get and used to get movable or immovable property
b) Unauthorized and illegal use of credit cards
c) Both of Above*
d) None of These

Q10. Punishment for Hacking in Inida is:
a) Imprisonment up to 3 years only
b) Fine (Depend on case to case) only
c) Both of Above*
d) None of These

Q11. Which among the following is best suitable for term "Software Piracy":
a) Counterfeiting original products

b) Illegal copying of genuine program
c) Both of Above*
d) None of These

Q12. Which among the following are Malicious Softwares:
a) Virus and Worms
b) Trojan Horse and Time Bomb
c) Logic Bomb and Rabbit and Bacterium
d) None of These
e) All of the Above*

Q13. IRC stands for:
a) Internet Relay Chat*
b) Internal Rely Chat
c) Information Relay Chat
d) None of These
Q14 MOD refers to:
a) Monitor of Deception
b) Master of Deception
c) Management of Deception *
d) None of These
Q15. INTER POL stands for:
a) International Police*
b) Internal Polythims
c) Internet Protocol
d) None of These

MCQs 3

1. The first computer virus is --------

A. I Love YouB. BlasterC. SasserD. Creeper*

2. MCAfee is an example of

A. Photo Editing SoftwareB. Quick HealC. VirusD. Antivirus*

3. Which of the following is known as Malicious software?

A. illegalwareB. badwareC. malware *D. maliciousware

4. To protect a computer from virus, you should install -------- in your computer.

A. backup wizardB. disk cleanupC. antivirusD. disk defragmenter

Answer c

5. VIRUS stands for

A. Very Intelligent Result Until SourceB. Very Interchanged Resource Under SearchC. Vital Information Resource Under SlegeD. Viral Important Record User Searched

Answer c

6. Which of the following is not an antivirus software?

A. AVGB. AvastC. Code RedD. MCAfee

Answer c

7. What is short for malicious software (is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems)?

A. MalwareB. MoleculewarC. MalisoftD. Malairasoft

Answer A

8. Which of the following is/are threats for electronic payment systems?

A. Computer wormsB. Computer virusC. Trojan horseD. All of the above

Answe ALL

9. Which of the following virus overtake computer system, when it boots and destroy information?

A. System infectorsB. TrojanC. Boot infectorsD. Stealth virus

Answer c

10. Key logger is a

A. FirmwareB. AntivirusC. SpywareD. All of the above

Answer c

11. To protect yourself from computer hacker, you should turn on a

A. ScriptB. FirewallC. VLCD. Antivirus

Answer c

12. Firewalls are used to protect against --------

A. data driven attacksB. fire attacksC. virus attacksD. unauthorised access

Answer d

13. Which of the following would most likely not be a symptom of a virus?

A. The web browser opens to an unusual home pageB. Odd message or images are displayed on the screenC. Existing program files and icons disappearD. The CD–ROM stops functioning

Answer d

14. Code red is a(n) ----------

A. Word Processing SoftwareB. AntivirusC. VirusD. Photo Editing Software

Answer b

15. -------- software are programs that are installed onto your computer and can scan and remove known viruses which you may have contracted.

A. FirmmwareB. AdwareC. KeyloggerD. Antivirus

Answer d

16. Which of the following describes programs that can run independently travel from system to system and disrupt computer communication?

A. VirusesB. TrojansC. DroppersD. Worm

Answer d

17. A -------- is a computer program that can replicate itself and spread from one computer to another.

A. AntivursB. PenDriveC. MouseD. Computer Virus

Answer d

18. Authentication is

A. modificationB. insertionC. hard to assure identity of user on a remote systemD. none of the above

Answer c

19. -------- are attempts by individuals to obtain confidential information from you to falsifying their identity.

A. Computer virusesB. Phishing scamsC. Phishing tripsD. Spyware scams

Answer b

20. A virus that migrates freely within a large population of unauthorized email user is called a -------

A. flame warB. wormC. macroD. plagiarism

Answer c

21. -------- are often delivered to a PC through an email attachment and are often designed to do harm.

A. SpamB. EmailC. PortalsD. Virus

Answer d

22. The altering of data so that it is not usable unless the changes are undone is

A. ergonomicsB. compressionC. biometricsD. encryption

Answer d

23. When a logic bomb is activated by a time related event, it is known as -------

A. virusB. trojan horseC. time related bomb sequenceD. time bomb

Answer d

24. A ------- is a computer program that can invade computer and perform a variety of functions ranging from annoying(e.g. popping up messages as a joke) to dangerous (e.g. deleting files

or destroying your hard disk).

A. Ms WordB. Ms AccessC. AntivirusD. Computer Virus

Answer D

Recollected questions:

Cyber crimes are handled by which organization in india
Type 1 crime
Preventive control
Detective control
Detterant control
Logical control
Sections and their fine with imprisonment in years
Committees of it security ,it governance, it controls
Netra by which organisation
Fast flux
Stux net
Phising
Shoulder surfing
Digital signature
Oldest agency in india
Few questions on cert in
Passive attack
Active attack
Direct attack
In direct attack
Logic bomb
Zeus
India own operating system boss in under whom
Confidentiality
Availability
Integrity
Conventional crime
Cyber crime
Same features of conv and cyber crime
Tailgating

imp topics are 1differences between viruses and worm
2 it act
3 different types of cyber crimes
4 various types of cards

5 gate way payment
6 prevention and detection control
7 pss act
8 2 tier authentication
9 passive and active attacks
mostly questions from 2 and 3 and 4...units

Cyber terrorism

Prevention of cyber crime and fruad management today's recollected questions

Cyber crime Recollected Questions date-08/07/18

Q1.what is honey pot.

Q2. What are steps involved in a Ecommerce transactions.

Q3. Difference between durability and consistency.

Q4. What is firewell.

Q5 .what is wankworm and NASA.

Q6. Eucp published in which year.

Q7.OLA is not a popular app store.

Q8.what is circumstantial evidences.

Q9.BOSS (Bharat operating system solution was developed by which organizations -CDAC

Q10.what is malicious code writer's.

Q11.What is multylayered security

Q12. What is data.

Q13.blackmailing is an example of cyber extortion.

Q14 what is SCADA.

Q15.what is cryptolocker

Q16.smart card in metrorailway stations are examples

Q17.packet filter firewall.

Q18.micro ATM.

Q19.cross site Scripting.

Q20. What is A hectivist...

Q21 . Rupay card is issued in which year.

Q22 what is Trojan hourse.

Q23. What is malware.

Q.24.data backup is an example of which type of control.

Q25.what is Lebance loop modulas oprendi in atm card frauds.

Q26.CCTV is an example of which control.

Q27.what is Cyber Smearing.

Q28.what is operating system vulnerability

Q29.what is full form of CISA cyber security information sharing Act.

Q30 what is zeus viruses.

Q31.what is hashh value and integrity.

Q32.w difference between Authirization and Authentication.

Q33. What is INFO stealer.

Q34.e.what is A beck End Access.

Q35.what is meaning of phrase of "Ab initio Unlawfully or Unlegally.

Q36.what is security Administration and Quality Assurance.

Q37.what is CAPTCHA.

Q38.Intentionally misrepresentation of Data is called A Fraud.

Q39. What is definition of Control. Q40.What is A John Deo Order. ...

Q41.what is payment walked and digital wallet

Q42 what is Anonymous.

Q43. What is trapdoor access. A

Q44..Total branch automation TMA.

Q45. .com and .org are TLD.

Q46. TCS fraud in Andhra Pradesh is an example of reasonable security practises and procedures.

Q47. The PVCL case in India refers to which Act of IT act Act_69 power to moniter,intercept or Block URL.

Q48.one question on CBS and TBA total branch Automations.

Q49. Sysadmin sysuser or teller all are examples of Spoofing.

Q50.what is A network Analysis.

Q51.what is vulnerability

Q52.what is DNS sinkholding.

Q53.e.Contactless smart card are example of which.

Q54 .Lebance Loop card fraud rubber band type material inside Atm Fraud.

Q55.what is Contigency pkanning.

Q56.what is Nigrean 419 Fraud.

Q57.Dumpster Diving.

Q58.what is diffrence between Steersman and script kiddle

Q59.Staganography.

Q60. What is SSL injections and Cross Site Scripting.....

Recollected questions from prevention of cyber crimes and fraud management...

Script kiddie

Prevention control, deterrent control,

Interpol (which indian agency co-ordinate with it)

Zeus

From which year UCP is effective

UTM

Asymmetric and symmetric encryption(2 questions)

Cert

I4C

IT act and IT amendment act(3 questions approx)

Blue hat hacker

Eavesdropping

Mitm

Didi

Digital signature

How to make email secure---SSL, SHA like tech

Integrity

Authentication

Basic questions Just for Knowledge

1. Explain risk, vulnerability and threat?

Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat e.g. Default username and password for a server – An attacker can easily crack into this server and compromise it.

2. What is the difference between Asymmetric and Symmetric encryption and which one is better?

Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption.

Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel.

Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using symmetric process.

3. What is an IPS and how does it differs from IDS?

IDS is an intrusion detection system whereas an IPS is an intrusion prevention system. IDS will just detect the intrusion and will leave the rest to the administrator for further action whereas an IPS will detect the intrusion and will take further action to prevent the intrusion. Another difference is the positioning of the devices in the network. Although they work on the same basic concept but the placement is different.

4. What is XSS, how will you mitigate it?

Cross site scripting is a JavaScript vulnerability in the web applications. The easiest way to explain this is a case when a user enters a script in the client side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client side.

Countermeasures of XSS are input validation, implementing a CSP (Content security policy) etc.

TIP: Know the different types of XSS and how the countermeasures work.

5. What is the difference between encryption and hashing?
TIP: Keep the answer short and straight.

Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.

Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity.

6. Are you a coder/developer or know any coding languages?
TIP: You are not expected to be a PRO; understanding of the language will do the job.

Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to automate tasks, exploit development etc. A little knowledge of the three can be of great advantage - both in the interview and on the floor.

7. What is CSRF?

Cross Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples and countermeasures.

8. What is a Security Misconfiguration?

Security misconfiguration is a vulnerability when a device/application/network is configured in a way which can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

9. What is a Black hat, white hat and Grey hat hacker?

Black hat hackers are those who hack without authority. White hat hackers are authorised to perform a hacking attempt under signed NDA. Grey hat hackers are white hat hackers which sometimes perform unauthorised activities.

10. What is a firewall?

A firewall is a device that allows/blocks traffic as per defined set of rules. These are placed on the boundary of trusted and untrusted networks.

11. How do you keep yourself updated with the information security news?

Be sure to check and follow a few security forums so that you get regular updates on what is happening in the market and about the latest trends and incidents.

12. The world has recently been hit by ……. Attack/virus etc. What have you done to protect your organisation as a security professional?

Different organisations work in different ways, the ways to handle incident is different for all. Some take this seriously and some not. The answer to this should be the process to handle an incident. Align this with one you had and go on… just don't exaggerate.

13. CIA triangle?

- Confidentiality: Keeping the information secret.
- Integrity: Keeping the information unaltered.
- Availability: Information is available to the authorised parties at all times.

14. HIDS vs NIDS and which one is better and why?

HIDS is host intrusion detection system and NIDS is network intrusion detection system. Both the systems work on the similar lines. It's just that the placement in different. HIDS is placed on each host whereas NIDS is placed in the network. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes processing power of the host as well.

15. What is port scanning?

Port scanning is process of sending messages in order to gather information about network, system etc. by analysing the response received.

16. What is the difference between VA and PT?

Vulnerability Assessment is an approach used to find flaws in an application/network whereas Penetration testing is the practice of finding exploitable vulnerabilities like a real attacker will do. VA is like travelling on the surface whereas PT is digging it for gold.

17. What are the objects that should be included in a good penetration testing report?

A VAPT report should have an executive summary explaining the observations on a high level along with the scope, period of testing etc. This can be followed by no of observations, category wise split into high,

medium and low. Also include detailed observation along with replication steps, screenshots of proof of concept along with the remediation.

18. What is compliance?

Abiding by a set of standards set by a government/Independent party/organisation. E.g. An industry which stores, processes or transmits Payment related information needs to be complied with PCI DSS (Payment card Industry Data Security Standard). Other compliance examples can be an organisation complying with its own policies.

19. Tell us about your Personal achievements or certifications?

Keep this simple and relevant, getting a security certification can be one personal achievement. Explain how it started and what kept you motivated. How you feel now and what are your next steps.

20. Various response codes from a web application?

1xx - Informational responses
2xx - Success
3xx - Redirection
4xx - Client side error
5xx - Server side error

21. When do you use tracert/traceroute?

In case you can't ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is firewall, ISP, router etc.

22. DDoS and its mitigation?

DDoS stands for distributed denial of service. When a network/server/application is flooded with large number of requests which it is not designed to handle making the server unavailable to the legitimate requests. The requests can come from different not related sources hence it is a distributed denial of service attack. It can be mitigated by analysing and filtering the traffic in the scrubbing centres. The scrubbing centres are centralized data cleansing station wherein the traffic to a website is analysed and the malicious traffic is removed.

23. What is a WAF and what are its types?

WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud based.

24. Explain the objects of Basic web architecture?
TIP: Different organisations follow different models and networks. BE GENERIC.

A basic web architecture should contain a front ending server, a web application server, a database server.

25. How often should Patch management be performed?

Patch should be managed as soon as it gets released. For windows – patches released every second Tuesday of the month by Microsoft. It should be applied to all machines not later than 1 month. Same is for network devices, patch as soon as it gets released. Follow a proper patch management process.

26. How do you govern various security objects?

Various security objects are governed with the help of KPI (Key Performance Indicators). Let us take the example of windows patch, agreed KPI can be 99%. It means that 99% of the PCs will have the latest or last month's patch. On similar lines various security objects can be managed.

27. How does a Process Audit go?

The first thing to do is to identify the scope of the audit followed by a document of the process. Study the document carefully and then identify the areas which you consider are weak. The company might have compensatory controls in place. Verify they are enough.

28. What is the difference between policies, processes and guidelines?

As security policy defines the security objectives and the security framework of an organisation. A process is a detailed step by step how to document that specifies the exact action which will be necessary to implement important security mechanism. Guidelines are recommendations which can be customised and used in the creation of procedures.

29. How do you handle AntiVirus alerts?

Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

30. What is a false positive and false negative in case of IDS?

When the device generated an alert for an intrusion which has actually not happened: this is false positive and if the device has not generated any alert and the intrusion has actually happened, this is the case of a false negative.

31. What is data leakage? How will you detect and prevent it?

Data leak is when data gets out of the organisation in an unauthorised way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorised upload of data to public portals, removable drives, photographs etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to internal network, restriction on printing confidential data etc.

32. What are the different levels of data classification and why are they required?

Data needs to be segregated into various categories so that its severity can be defined, without this segregation a piece of information can be critical for one but not so critical for others. There can be various levels of data classification depending on organisation to organisation, in broader terms data can be classified into:

- Top secret – Its leakage can cause drastic effect to the organisation, e.g. trade secrets etc.
- Confidential – Internal to the company e.g. policy and processes.
- Public – Publically available, like newsletters etc.

33. In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted?

Users are usually not provided with admin access to reduce the risk, but in certain cases the users can be granted admin access. Just ensure that the users understand their responsibility. In case any incident happens, the access should be provided for only limited time post senior management approval and a valid business justification.

34. What are your views on usage of social media in office?

Social media is acceptable, just ensure content filtering is enabled and uploading features are restricted. Read only mode is acceptable till the time it does not interfere with work.

CYBER CRIME TERMINOLOGY

Adware – Adware is software designed to force pre-chosen ads to display on your system. Some adware is designed to be malicious and will pop up ads with such speed and frequency that they seem to be taking over everything, slowing down your system and tying up all of your system resources. When adware is coupled with spyware, it can be a frustrating ride, to say the least.

Back Door – A back door is a point of entry that circumvents normal security and can be used by a cracker to access a network or computer system. Usually back doors are created by system developers as shortcuts to speed access through security during the development stage and then are overlooked and never properly removed during final implementation. Sometimes crackers will create their own back door to a system by using a virus or a Trojan to set it up, thereby allowing them future access at their leisure.

Black Hat – Just like in the old westerns, these are the bad guys. A black hat is a cracker. To add insult to injury, black hats may also share information about the "break in" with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures.

Bot – A bot is a software "robot" that performs an extensive set of automated tasks on its own. Search engines like Google use bots, also known as spiders, to crawl through websites in order to scan through all of your pages. In

these cases bots are not meant to interfere with a user, but are employed in an effort to index sites for the purpose of ranking them accordingly for appropriate returns on search queries. But when black hats use a bot, they can perform an extensive set of destructive tasks, as well as introduce many forms of malware to your system or network. They can also be used by black hats to coordinate attacks by controlling botnets.

Botnet – A botnet is a network of zombie drones under the control of a black hat. When black hats are launching a Distributed Denial of Service attack for instance, they will use a botnet under their control to accomplish it. Most often, the users of the systems will not even know they are involved or that their system resources are being used to carry out DDOS attacks or for spamming. It not only helps cover the black hat's tracks, but increases the ferocity of the attack by using the resources of many computer systems in a coordinated effort.

Cookies – A cookie is a small packet of information from a visited webserver stored on your system by your computer's browser. It is designed to store personalized information in order to customize your next visit. For instance, if you visit a site with forms to fill out on each visit, that information can be stored on your system as a cookie so you don't have to go through the process of filling out the forms each time you visit.

Cracker – When you hear the word hacker today, in reality it is normally referring to a cracker, but the two have become synonymous. With its origin derived from "safe-cracker" as a way to differentiate from the various uses of "hacker" in the cyber world, a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage. A cracker may destroy files, steal personal information like credit card numbers or client data, infect the system with a virus, or undertake many others things that cause harm. This glossary will give you an idea of what they can do and some of the means they use to achieve their malicious objectives. These are the black hats.

Denial of Service Attack (DOS) – A Denial of Service attack is an attack designed to overwhelm a targeted website to the point of crashing it or making it inaccessible. Along with sheer numbers and frequency, sometimes the data packets that are sent are malformed to further stress the system trying to process the server requests. A successful Denial of Service attack can cripple any entity that relies on its online presence by rendering their website virtually useless.

Distributed Denial of Service Attack (DDOS) – A Distributed Denial of Service attack is done with the help of zombie drones (also known as a botnet) under the control of black hats using a master program to command them to send information and data packets to the targeted webserver from the multiple systems under their control. This obviously makes the Distributed Denial of Service attack even more devastating than a Denial of Service attack launched from a single system, flooding the target server with a speed and volume that is exponentially magnified. As is normally the case with zombie drones and botnets, this is often done without the user of the controlled system even knowing they were involved.

Dumpster Diving – The act of rummaging through the trash of an individual or business to gather information that could be useful for a cyber-criminal to gain access to a system or attain personal information to aid them in identity theft or system intrusion. One person's garbage can indeed be a cyber-criminal's treasure.

Easter Egg – A non-malicious surprise contained in a program or on a circuit board installed by the developer. It could be as simple as a text greeting, a signature, or an image embedded on a circuit board, or comprise a more complex routine, like a video or a small program. The criteria that must be met to be considered an Easter Egg are that it be undocumented, non-malicious, reproducible to anyone with the same device or software, not be obvious, and above all – it should be entertaining!

Firewall – A firewall is a security barrier designed to keep unwanted intruders "outside" a computer system or network while allowing safe communication between systems and users on the "inside" of the firewall. Firewalls can be physical devices or software-based, or a combination of the two. A well designed and implemented firewall

is a must to ensure safe communications and network access and should be regularly checked and updated to ensure continued function. Black hats learn new tricks and exploit new techniques all the time, and what worked to keep them out yesterday may need to be adjusted or replaced over time.

Grey Hat – A grey hat, as you would imagine, is a bit of a white hat/black hat hybrid. Thankfully, like white hats, their mission is not to do damage to a system or network, but to expose flaws in system security. The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data: they want to expose the security weaknesses of a particular system and then notify the "victim" of their success. Often this is done with the intent of then selling their services to help correct the security failure so black hats cannot gain entry and/or access for more devious and harmful purposes.

Hacker – This is the trickiest definition of the group and controversy has followed its use for decades. Originally, the term hacker had a positive connotation and it actually had nothing to do with computer systems. In 1946, the Tech Model Railroad Club of MIT coined the term to mean someone who applies ingenuity to achieve a clever result. Then, when computers came along, "hacker" took on the meaning of someone who would "hack" away on a program through the night to make it better. But in the 80s everything changed, and Hollywood was the catalyst. When the personal computers onslaught started invading our daily lives, it didn't take long for clever screen-writers to bring the black hat villains of the cyber world to the forefront of our collective consciousness, and they haven't looked back since. They associated our deepest fears with the word hacker, making them the ones that unravelled our privacy, put our safety in jeopardy, and had the power to take everything from us, from our material possessions to our very identities. And they could do it all anonymously, by hacking away in a dark room by the dim light of a computer monitor's glow. Needless to say, right or wrong, it stuck! Even many professionals in the computing field today have finally, albeit grudgingly, given in to the mainstream meaning of the word. "Hacker" has thus become the catch-all term used when in fact it should be "cracker."

Keylogger – A keylogger is a non-destructive program that is designed to log every keystroke made on a computer. The information that is collected can then be saved as a file and/or sent to another machine on the network or over the Internet, making it possible for someone else to see every keystroke that was made on a particular system. By breaking down this information, it can be easy for a black hat cracker to recreate your user names and passwords, putting all kinds of information at risk and susceptible to misuse. Just imagine your online banking login information falling into the wrong hands! Finding out you have a keylogger installed, however, does not necessarily mean you were the victim of a black hat, as some companies install them on employee computers to track usage and ensure that systems are not being used for unintended purposes. Keyloggers are, for obvious reasons, often considered to be spyware.

Logic Bomb – A logic bomb is a malicious program designed to execute when a certain criterion is met. A time bomb could be considered a logic bomb because when the target time or date is reached, it executes. But logic bombs can be much more complex. They can be designed to execute when a certain file is accessed, or when a certain key combination is pressed, or through the passing of any other event or task that is possible to be tracked on a computer. Until the trigger event the logic bomb was designed for passes, it will simply remain dormant.

Malware – Simply put, malware is a malicious program that causes damage. It includes viruses, Trojans, worms, time bombs, logic bombs, or anything else intended to cause damage upon the execution of the payload.

Master Program – A master program is the program a black hat cracker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

Payload – The payload is the part of the malware program that actually executes its designed task.

Phishing – Phishing is a form of social engineering carried out by black hats in electronic form, usually by email, with the purpose of gathering sensitive information. Often these communications will look legitimate and sometimes they will even look like they come from a legitimate source like a social networking site, a well-known entity like Paypal or Ebay, or even your bank. They will have a link directing you to a site that looks very convincing and ask you to verify your account information. When you log in to verify your information on the bogus site, you have just given the black hat exactly what they need to make you the next victim of cyber-crime. Phishing is done in many forms – sometimes it's easy to spot, sometimes not.

Phreaker – Considered the original computer hackers, phreakers, or phone phreakers, hit the scene in the 60s and made their mark by circumventing telecommunications security systems to place calls, including long distance, for free. By using electronic recording devices, or even simply creating tones with a whistle, phreakers tricked the systems into thinking it was a valid call. One of the first to find prominence was "Captain Crunch," a phreaker who realized the toy whistle that came as a prize in a box of Captain Crunch cereal could be used to mimic the tone frequencies used by telecommunications companies to validate and route calls.

Polymorphic Virus – A polymorphic virus is a virus that will change its digital footprint every time it replicates. Antivirus software relies on a constantly updated and evolving database of virus signatures to detect any virus that may have infected a system. By changing its signature upon replication, a polymorphic virus may elude antivirus software, making it very hard to eradicate.

Rootkit – Without a doubt, the biggest fear in IT security is an undetected intrusion. A rootkit is a tool that can give a black hat the means for just such a perfect heist. A rootkit is a malware program that is installed on a system through various means, including the same methods that allow viruses to be injected into a system, like email, websites designed to introduce malware, or downloading and/or copying to the system with an unsafe program. Once a rootkit is introduced, this will create a back door for a black hat that will allow remote, unauthorized entry whenever he or she chooses. What makes a rootkit particularly lethal: it is installed and functions at such low system levels that it can be designed to erase its own tracks and activity from the now vulnerable system, allowing the black hat to navigate through entire networks without being exposed. Often, black hats will use social engineering to gain physical access to particularly well protected system so the rootkit can be directly installed from CD or a tiny USB drive (it only takes a minute) in order either to circumvent a particularly troublesome firewall or gain access to a system that is not normally accessible from the outside. Once the rootkit is introduced, the black hat has free reign and even skilled IT security departments will have a lot of trouble even seeing the activity as its happening. Rootkits are a definite 10 on the scary scale of cyber intrusions.

Script Kiddie – An individual who does not possess, or just doesn't use, their own skills and know-how to hack or crack a computer system or network, but uses a pre-written program or piece of code, a script. While they may not possess the computing talent, they can be just as dangerous!

Social Engineering – In the realm of the black hats, social engineering means to deceive someone for the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords. For instance, when fictitious Mr. Smith calls from IT services to inform you of new user name and password guidelines being implemented by the company and asks you to reveal yours so he can make sure they meet the new guidelines, you have been a target of social engineering. They can be very clever and resourceful, and very, very convincing. The only way to make sure you are not a victim of social engineering is never to give your personal and sensitive information to anyone you are not absolutely sure about. There are very few occasions that anyone legitimate would ever ask you for a password, and you should always be the one contacting them, not the other way around.

Spam – Spam is simply unsolicited email, also known as junk email. Spammers gather lists of email addresses, which they use to bombard users with this unsolicited mail. Often, the emails sent are simply advertising for a product or a service, but sometimes they can be used for phishing and/or directing you to websites or products that will introduce malware to your system. When you receive spam, the best practice is to delete it immediately.

Sometimes you will see a note in a spam email that gives you instructions on how to be removed from the list – never do it! This will only confirm to the spammer that they have a valid email address and the spam will just keep coming. They could also then sell your email address to another spammer as a confirmed email address and more spam will show up in your inbox. Most mail services have spam filters and these should be employed whenever possible.

Spoofing – Spoofing is the art of misdirection. Black hat crackers will often cover their tracks by spoofing (faking) an IP address or masking/changing the sender information on an email so as to deceive the recipient as to its origin. For example, they could send you an email containing a link to a page that will infect your system with malware and make it look like it came from a safe source, such as a trusted friend or well-known organization. Most of the true sources have security measures in place to avoid tampering with sender information on their own mail servers, but as many black hat spammers will launch attacks from their own SMTP (Simple Mail Transfer Protocol), they will be able to tamper with that information. When in doubt, check with the source yourself.

Spyware – Spyware is software designed to gather information about a user's computer use without their knowledge. Sometimes spyware is simply used to track a user's Internet surfing habits for advertising purposes in an effort to match your interests with relevant ads. On the other side of the coin, spyware can also scan computer files and keystrokes, create pop-up ads, change your homepage and/or direct you to pre-chosen websites. One common use is to generate a pop-up ad informing you that your system has been infected with a virus or some other form of malware and then force you to a pre-selected page that has the solution to fix the problem. Most often, spyware is bundled with free software like screen savers, emoticons and social networking programs.

Time Bomb – A time bomb is a malicious program designed to execute at a predetermined time and/or date. Time bombs are often set to trigger on special days like holidays, or sometimes they mark things like Hitler's birthday or 9/11 to make some sort of political statement. What a time bomb does on execution could be something benign like showing a certain picture, or it could be much more damaging, like stealing, deleting, or corrupting system information. Until the trigger time is achieved, a time bomb will simply remain dormant.

Trojan – A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there. Once introduced, a Trojan can destroy files, alter information, steal passwords or other information, or fulfil any other sinister purpose it was designed to accomplish. Or it may stay dormant, waiting for a cracker to access it remotely and take control of the system. A Trojan is a lot like a virus, but without the ability to replicate.

Virus – A virus is a malicious program or code that attaches itself to another program file and can replicate itself and thereby infect other systems. Just like the flu virus, it can spread from one system to another when the infected program is used by another system. The more interconnected the host is, the better its chances to spread. The spread of a virus can easily occur on networked systems, or it could even be passed along on other media like a CD or memory stick when a user unwittingly copies an infected file and introduces it to a new system. A virus could even be emailed with an attachment. "Virus" is often incorrectly used as a catch-all phrase for other malicious programs that don't have the ability to self-replicate, like spyware and adware.

Wardriving – Wardriving is the act of driving around in a vehicle with the purpose of finding an open, unsecured Wi-Fi wireless network. Many times, the range of a wireless network will exceed the perimeter of a building and create zones in public places that can be exploited to gain entry to the network. Black hats, and even grey hats, will often use a GPS system to make maps of exploitable zones so they can be used at a later time or passed on to others. Wardriving is not the only way this task is performed – there are Warbikers and Warwalkers too. As you can see, it

is imperative that your WiFi network is secure because there are entities out there looking for any opening to ply their trade.

White Hat – While black hats use their skill for malicious purposes, white hats are ethical hackers. They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks. If a black hat decides to target you, it's a great thing to have a white hat around. But if you don't, you can always call on one of ours at Global Digital Forensics.

Worm – A worm is very similar to a virus in that it is a destructive self-contained program that can replicate itself. But unlike a virus, a worm does not need to be a part of another program or document. A worm can copy and transfer itself to other systems on a network, even without user intervention. A worm can become devastating if not isolated and removed. Even if it does not cause outright damage, a worm replicating out of control can exponentially consume system resources like memory and bandwidth until a system becomes unstable and unusable.

Zero Day Threat/Exploit – Every threat to your computer security has to start somewhere. Unfortunately, the way most of us protect ourselves from cyber threats and intrusions, is to use detection programs that are based on analysing, comparing and matching the digital footprint of a possible threat to an internal database of threats that have been previously detected, reported and documented. That's why we all have to go through those seemingly never-ending updates to our antivirus programs, that's how the database is updated and the newest threats are added to the list of what the scanners look for. That inherent flaw in our scanners is what makes a Zero Day threat so dangerous. A Zero Day threat is pristine and undocumented. From the very first day a particular threat is ever deployed (zero day) until that threat is noticed, reported, documented and added to the index, it is an unknown. As far as standard protection goes, unknown means invisible – and when it comes to cyber threats, invisible can definitely mean trouble.

Zombie / Zombie Drone – A zombie is a malware program that can be used by a black hat cracker to remotely take control of a system so it can be used as a zombie drone for further attacks, like spam emails or Denial of Service attacks, without a user's knowledge. This helps cover the black hat's tracks and increases the magnitude of their activities by using your resources for their own devious purposes. Rarely will the user infected with a zombie even know it's there, as zombies are normally benign and non-destructive in and of themselves. Zombies can be introduced to a system by simply opening an infected email attachment, but most often they are received through non-mainstream sites like file sharing sites, chat groups, adult websites and online casinos that force you to download their media player to have access to the content on their site, using the installed player itself as the delivery mechanism.

Additional Information:

Information Technology (Amendment) Act, 2008

BRIEF HISTORY

The Indian Information Technology Act 2000 ("**Act**") was a based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law[1]; the suggestion was that all States intending to enact a law for the impugned purpose, give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. Thus the Act was enacted to provide legal recognition for transactions carried out by means of electronic data

interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involved the use of alternatives to traditional or paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies. Also it was considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. The Act received the assent of the President on the 9th of June, 2000.

The Act was subsequently and substantially amended in 2006 and again in 2008 citing the following objectives:

- With proliferation of information technology enabled services such as e-governance, ecommerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary **to declare such infrastructure as a protected system so as to restrict its access**.
- A rapid increase in the use of computer and internet has given **rise to new forms of crimes** like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.
- The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of the United Nations by its resolution No. 56/80, dated 12th December, 2001, recommended that **all States accord favorable consideration to the said Model Law on Electronic Signatures**. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonization with the said Model Law.
- The **service providers may be authorized** by the Central Government or the State Government to set up, maintain and upgrade the computerized facilities and also **collect, retain appropriate service charges** for providing such services at such scale as may be specified by the Central Government or the State Government.

EXTENT APPLICABILITY OF THE ACT

The Act extends to the whole of India, save as otherwise provided in this Act. It can also apply to any offence or contravention provided for in the Act, whether committed in India & outside India by any person, if the act or conduct constituting the offence involves a computer, computer system or computer network located in India .

The main provisions of the Act come in to force on the 9th of June 2000. Certain provisions were given effect on later dates by issuing specific notifications in this regards.

The Act shall not apply to documents or transactions specified in the First Schedule. Every notification issued to amend the first schedule shall be laid before each House of Parliament. Presently, the First schedule contains the following entries:

1. A negotiable instrument (other than cheque) as defined in negotiable instrument Act, 1881.
2. Power of Attorney as defined in P-O-A Act, 1882.
3. A trust as defined in Indian Trusts Act, 1882.
4. A will as defined in Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Any contract for sale or conveyance of immovable property or any interest in such property.

For this purpose every notification issued by the Central Government to add, amend or delete any item mentioned in the schedule as a pre-requisite place before both houses of the Parliament for their scrutiny and approval.

The provisions of the Act have an overriding effect, notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

DEFINITIONS

In this Act, unless the context otherwise requires, —

a. "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
b. "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
c. "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;
d. "affixing electronic signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature;
e. "appropriate Government" means as respects any matter,—

i. Enumerated in List II of the Seventh Schedule to the Constitution;

ii. relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

f. "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a electronic signature and a public key to verify the electronic signature;
g. "Certifying Authority" means a person who has been granted a licence to issue a Electronic Signature Certificate under section 24;

h. "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

i. "computer" means 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 communication facilities which are connected or related to the computer in a computer system or computer network;

j. "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through- —

i. the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

ii. terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

k. "computer resource" means computer, computer system, computer network, data, computer data base or software;

l. "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

m. "Controller" means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;

n. "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48;

(na). “cyber café” means any facility from where access to the internet is offered by any person in the ordinary course of his business to the members of the public;

(nb). "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

o. "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

p. "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

q. "digital Signature Certificate" means a Digital Signature Certificate issued under subsection (4) of section 35;
r. "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
s. "Electronic Gazette" means the Official Gazette published in the electronic form;
t. "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(ta). "electronic signature" means authentication of any electronic record by a subscriber by means of an electronic technique specified in the Second schedule and includes a digital signature;

(tb). "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes a Digital Signature Certificate.

u. "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
v. "information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:
w. "intermediary" with respect to any particular electronic record, means any person who on behalf of another person receives, stores or transmits that record or provides any service in respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes;
x. "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a electronic signature created by the private key;
y. "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case can be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, byelaws and orders issued or made thereunder;
z. "licence" means a licence granted to a Certifying Authority under section 24;

(za). "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb). "prescribed" means prescribed by rules made under this Act;

(zc). "private key" means the key of a key pair used to create a electronic signature;

(zd). "public key" means the key of a key pair used to verify a electronic signature and listed in the Electronic Signature Certificate;

(ze). "secure system" means computer hardware, software, and procedure that—

a. are reasonably secure from unauthorised access and misuse;

b. provide a reasonable level of reliability and correct operation;

c. are reasonably suited to performing the intended functions; and

d. adhere to generally accepted security procedures;

(zf). "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg). "subscriber" means a person in whose name the Electronic Signature Certificate is issued;

(zh). "verify" in relation to a electronic signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

a. the initial electronic record was affixed with the electronic signature by the use of private key corresponding to the public key of the subscriber;

b. the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the electronic signature.

Any reference in the Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, is to be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

SECTION 3 - AUTHENTICATION OF ELECTRONIC RECORDS BY USE OF DIGITAL SIGNATURE

AUTHENTICATION OF ELECTRONIC RECORDS

The Act provides that the authentication of the electronic record can be effected by the use of asymmetric crypto system and **hash** function which envelop and transform the *initial electronic* record into *another electronic record*.

A "*hash function*" is an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

a. to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
b. that two different electronic records can produce the same hash result using the algorithm.

The record can be accessed by the use of public key of the subscriber. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

SECTION 3A - AUTHENTICATION OF ELECTRONIC RECORDS BY USE OF ELECTRONIC SIGNATURE.

A subscriber can authenticate any electronic record by such an electronic signature or an electronic authentication technique which is considered reliable and may be specified in the schedules. In order for the electronic signature to be reliable

a. The signature creation data or authentication data are, within the context they are used, linked to the signatory, or as the case may be, the authenticator and to no other person;
b. The signature creation data or authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and to no other person;
c. Any alteration to the electronic signature made after affixing such signature is detectable.
d. Any alteration to the information made after its authentication by electronic signature is detectable.
e. It fulfills other prescribed conditions.

The Central Government can prescribe the procedure for the purpose of ascertaining who has affixed the signature. The Central Government can also, by notification in the Official Gazette, add or omit any reliable electronic signature or electronic authentication technique or the procedure for affixing the same. The notification of such method or procedure is required to be placed before both houses of the Parliament.

ELECTRONIC GOVERNANCE & LEGAL RECOGNITION OF ELECTRONIC RECORDS & ELECTRONIC SIGNATURES

SECTION 4 - ELECTRONIC RECORDS

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

a. rendered or made available in an electronic form; and
b. accessible so as to be usable for a subsequent reference.

SECTION 5 - LEGAL RECOGNITION OF ELECTRONIC SIGNATURES

Where any law requires that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement will be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as prescribed by the Central Government.

SECTION - 6 FOUNDATION OF ELECTRONIC GOVERNANCE

Where any law provides for the filing of any form, application or any other document with any authority, agency, owned or controlled by the appropriate Government in a particular manner, Or it provides for the issue or grant of any licence, permit, sanction or approval or the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force,

such requirement is deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as prescribed by the appropriate Government. The appropriate Government is empowered to prescribe rules regarding the manner and the format, in which such electronic records shall be filed, created or issued and the manner or method of payment of any fee for creating, filing or issuing such record.

SECTION 9 - NO RIGHT TO INSIST DOC. TO BE IN ELECTRONIC FORM.

NO Person is conferred the right to insist the Government or any body funded or controlled by it upon accepting, issuing, creating, retaining and preserving any document in the form of electronic records or effecting any monetary transaction in the electronic form.

SECTION 7 - RETENTION OF RECORDS:

Where any law provides that documents, records or information be retained for a specific period, then the requirement will be said to have been met if the documents are retained in electronic format and if the information contained therein remains accessible so as to be usable for subsequent reference in the format it was originally created, generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received, including the details of the identification of the origin, destination, dispatch or receipt of such electronic record are available in the electronic record. These conditions however do not apply to electronic documents which are generated automatically, solely for the purpose of enabling an electronic record to be retention of documents, records or information in the form of electronic records.

SECTION 7A - AUDIT OF DOCUMENTS IN ELECTRONIC FORM:

Where the audit of documents, records or information is required to be conducted under any law, the same shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

SECTION 8 - PUBLICATION OF RULE, REGULATION, ETC., IN ELECTRONIC GAZETTE:

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter will be published in the Official Gazette, then, such requirement is deemed to have been satisfied if such rule, regulation, etc is published in the Official Gazette or *Electronic Gazette* and the date of publication in such an Electronic Gazette is deemed to be the date of the Gazette which was first published in any form.

SECTION 10 - POWER TO MAKE RULES BY CENTRAL GOVERNMENT IN RESPECT OF ELECTRONIC SIGNATURE:

The Central Government is empowered to prescribe the type of electronic signature, the manner and format in which the electronic signature will be affixed so as to facilitate the identification of the person affixing the electronic signature. The Government will also prescribe the control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and any other matter which is necessary to give legal effect to electronic signatures.

In case of a contract, where the contract formation, the communication of proposals, the acceptance or revocation of the proposals, as the case may be, are expressed in electronic form or by means of an electronic record, the enforceability of the record will not be denied solely on the grounds that such electronic form or means were used to contract.

SECTION 11 - ATTRIBUTION OF ELECTRONIC RECORDS.

An electronic record can be attributed to the originator, if it can be demonstrated that it was sent by the originator himself or by a person authorised by the originator in respect of that electronic record; or by an information system programmed to operate automatically in this regards.

SECTION 12 - ACKNOWLEDGMENT OF RECEIPT

Where the originator (sender) & addressee (recipient) have not settled the manner and form in which the addressee is to acknowledge the of receipt of the electronic record, then in such a case the addressee will acknowledge the receipt of the electronic record either by communicating such receipt, through automated or other means; or by way of conduct of the addressee to indicate to the originator that the electronic record has been received.

Where the originator has stipulated that the electronic record will be binding only on receipt of an acknowledgment of such electronic record by him, then in such a case, unless the addressee sends such an acknowledgment and the originator receives the same, it will be assumed that the electronic record was never sent.

Where the originator has not stipulated that the electronic record will be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within a reasonable time or a agreed period, then the originator can give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if an acknowledgment is not received within the aforesaid time limit he can after giving notice to the addressee, treat the electronic record as though it has never been sent.

SECTION 13 - TIME AND PLACE OF DESPATCH AND RECEIPT OF ELECTRONIC RECORD

The Originator and the addressee can agree to the time and place of receipt of the electronic record. Generally, unless otherwise agreed to the contrary by the originator and the addressee, when an electronic record enters a computer resource outside the control of the originator or when it enters the computer resource of the addressee, it is deemed to have been dispatched.

If the addressee has designated a specific computer resource and the electronic record is sent to such a designated computer resource, then when the electronic record enters the designated computer resource is deemed to be the time of receipt. If instead of sending to the designated computer resource of the addressee, the originator sends to another computer resource then receipt occurs at the time when the electronic record is retrieved by the addressee from such a computer resource. These would apply even if the place where the computer resource is located in a different place.

An electronic record is deemed to "be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business inspite of the computer resources are located at any other place.

It is possible that the originator or the addressee may have more than one place of business, in such a case the principal place of business, will be the place of business for the purpose of receipt and despatch. If the originator or the addressee does not have a place of business, his usual place of residence will be deemed to be the place of business, in the case the addressee or the originator is a body corporate, then such usual place will be the place where such a body corporate is registered.

SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

SECTION 14 - SECURE ELECTRONIC RECORD

Where any security procedure is applied to an electronic record, at a specific point of time, then from such point onwards up to the time of verification, the record is deemed to be a secure electronic record.

SECTION 15 - SECURE ELECTRONIC SIGNATURE

An electronic signature is unique to the subscriber. Once the signature is affixed to an electronic record it can be used to identify the subscriber. It is presumed to be under the exclusive control of the subscriber. The signature signifies the time when it is affixed to an electronic record and the manner in which the signature was created. If any one tries to alter such a signed electronic record, then the signature gets invalidated. An electronic signature will be deemed to be secure if it can be proved that, it was under the exclusive control of the signatory at the time of affixing and the signature data (private key) was stored and affixed in the specified manner.

SECTION 16 - SECURITY PROCEDURE

The Central Government is empowered to prescribe the security procedure and practices considering the commercial circumstances, nature of transactions and such other related factors.

REGULATION OF CERTIFYING AUTHORITIES

SECTION 17 - APPOINTMENT OF CONTROLLER AND OTHER OFFICERS

The Central Government is empowered to appoint **a** Controller of Certifying Authorities ("**CCA**") and such number of Deputy Controllers and Assistant Controllers, other officers and employees. Such an appointment of the Controller, Deputy & Assistant Controllers is to be notified in the Official Gazette The Controller discharges his functions under this Act subject to the general control and directions of the Central Government. The Deputy Controllers ("**Dy CA**") and Assistant Controllers ("**ACA**"), other officers and employees in turn, perform the functions assigned to them by the Controller under the general superintendence and control of the Controller. Such assigned/ delegated functions are assigned by the CCA to the Dy CA & ACA in writing.

The Central Government can prescribe the requirements pertaining to the qualifications, experience and terms and conditions of service of CCA, the Dy CA and the ACA, other officers and employees. Further it can also require that the Head Office and Branch Office of the Controller will be at / established at all such places as specified by the Central Government. The Act provides that there will be a seal of the Office of the Controller.

SECTION 18 - FUNCTIONS OF CONTROLLER

The primary function of the CCA is to regulate the Certifying Authorities("**CA**"). For the purpose of regulating the CA the CCA may perform all or any of the following functions, namely:—

- certifying public keys of the Certifying Authorities;
- laying down the standards to be maintained by the Certifying Authorities;
- specifying the qualifications and experience which employees of the Certifying Authorities should possess;

- specifying the conditions subject to which the Certifying Authorities shall conduct their business;
- specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
- specifying the form and content of a Digital Signature Certificate and the key,
- specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
- specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- resolving any conflict of interests between the Certifying Authorities and the subscribers;
- laying down the duties of the Certifying Authorities;
- maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

SECTION 19 - RECOGNITION OF FOREIGN CERTIFYING AUTHORITIES

The CCA, with the prior approval of the Central Government and subject to the conditions and restrictions specified in this regards by regulations, by notification in the Official Gazette, can recognize any foreign CA as a CA for the purposes of this Act. Once a foreign CA is granted recognition by the CCA, an Electronic Signature Certificate ("**ESC**") issued by such Certifying Authority will be valid for the purposes of this Act.

If any foreign CA who has been granted recognition by the CCA and if the CCA is satisfied that such a CA has contravened any of the conditions or restrictions subject to which the CA was granted recognition under by the CCA, then the CCA after recording the reasons in writing, revoke such recognition by notification in the Official Gazette.

SECTION 21 - LICENCE TO ISSUE ELECTRONIC SIGNATURE CERTIFICATES

Any person can obtain a license to issue an ESC by making an application to the CCA. After receiving the application the CCA verifies whether or not such an applicant has satisfied the eligibility criteria, as specified by the Central Government in respect of qualification, expertise, manpower, financial resources and other infrastructure facilities. Once the eligibility of the applicant is ascertained, the CCA issues a license to the applicant. The licensee is thereafter subject such terms and conditions as are provided for in the regulations issued in this regards. Any license granted under this section is valid for such period as can be provided for by the Central Government. It may be noted that such a license is not transferable or inheritable.

SECTION 22 - APPLICATION FOR LICENSE:

Every application is required to be in the prescribed form. Along with the application the applicant is also required to file:

- a certification practice statement;
- a statement including the procedures with respect to identification of the applicant;
- payment of such fees, not exceeding twenty-five thousand rupees (as prescribed by the Central Government);
- such other documents, as can be prescribed from time to time by the Central Government

An application for renewal of a license is also required to be in the prescribed form accompanied by such fees, which cannot exceed five thousand rupees and has to be made at least forty-five days before the date of expiry of the period of validity of the existing license.

The CCA can, on receipt of an application, after considering the documents accompanying the application and such other factors, as the CCA deems fit, grant the license or reject the application. The applicant is granted a reasonable opportunity of presenting his case to the CCA before his application is rejected.

SECTION 25 - SUSPENSION OF LICENCE

If the CCA, after making an inquiry is satisfied that a CA has

- made an incorrect or false statement in his application for the issue or renewal of licence;
- failed to comply with the terms and conditions subject to which the licence was granted;
- has not maintained the standards required to be followed under this Act;
- contravened any provisions of this Act, rule, regulation or order made there under

then after giving a reasonable opportunity to show cause against the proposed revocation, revoke the license. In the alternative, pending such an inquiry, if the CCA is of the opinion that there exist circumstances for the revocation of the license of the CA, then the CCA can suspend the license till the completion of the inquiry. The period of suspension cannot however exceed a period of 10 days unless the CA has been given a reasonable opportunity of showing cause against the proposed suspension. The CA is barred from issuing any ESCs during his suspension period.

After making an inquiry into an allegation of default and after giving the defaulting CA a reasonable opportunity of being heard, if the CCA is satisfied that the license of the CA need to be suspended or revoked, he can proceed against the CA and suspend or revoke his license. The notice of such an action of suspension or revocation, as the case may be, by the CCA is required to be published in the database and all the repositories maintained by the CCA. The CCA is required also make available such a notice of suspension or revocation of license, through a website which is accessible round the clock. If considered appropriate by the CCA he may publicise the contents of database in appropriate electronic or other media. The CCA can delegate or authorize the Dy. CA or the ACA to exercise any of its power in respect of the regulation of Certified Authorities.

ACCESS TO COMPUTERS AND DATA

Without prejudice to the provisions of sub-section (1) of section 69, the CCA or any person authorized by him will, if he has reasonable cause to suspect that the provisions related to regulation of CAs, rules or regulations made there under, are being contravened, then they can search or access any computer system, any apparatus, data or any other material connected with such system to obtain any information or data contained in or available to such computer system. In doing so they can direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material,

to provide such reasonable technical and other assistance as the investigating authority may consider necessary.

POWER TO INVESTIGATE CONTRAVENTIONS.

The CCA or any officer authorised by him for this purpose can investigate into any contravention of the provisions of this Act, rules or regulations made thereunder. For the purpose of investigating the contraventions under this Act, the CCA or any authorized officer has the powers similar to the powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and the CCA can exercise such powers, subject to such limitations laid down under the Income-tax Act, 1961.

SECTION 30 - OBLIGATIONS OF THE CA

Every CA will, —

a. Make use of secure hardware, software and procedures to prevent intrusion and misuse;
b. Ensure a reasonable level of reliability in the services provided by it;
c. Adhere to security procedures to ensure that the secrecy and privacy of the electronic signatures are assured;
d. be the repository of all Electronic Signature Certificates issued under this Act;
e. publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and
f. Observe such other standards as may be specified by regulations;
g. Ensure that every person employed or otherwise engaged by it complies with the provisions of this Act, rules, regulations and orders made thereunder;
h. Display its licence at a conspicuous place of the premises in which it carries on its business;
i. surrender his licence, forthwith, to the CCA when the licence is suspended or revoked. Failure to do so, will be deemed be an offence, punishable with imprisonment which can extend up to six months or a fine which can extend up to ten thousand rupees or with both
j. disclose in the manner specified by regulations—

i. its ESC;

ii. any certification practice statement;

iii. notice of the revocation or suspension of its CA certificate, if any; and

iv. any other fact that materially and adversely affects either the reliability of a ESC, which that CA has issued, or the CA's ability to perform its services.

k. Where the CA is of the opinion that the situation so merits which can materially and adversely affect the integrity of its computer system or the conditions subject to which a ESC was granted, then, the CA will—

a. Reasonably notify any person who is likely to be affected by that occurrence; or

b. act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

The CCA can, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette make regulations consistent with this Act and the rules made there under to carry out the purposes of this Act. In particular, and without prejudice to the generality of the foregoing power, such regulations can provide for all or any of the following matters, namely:

a. the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority;
b. the conditions and restrictions subject to which the Controller can recognise any foreign Certifying Authority;
c. the terms and conditions subject to which a licence to issue a ESC can be granted;
d. other standards to be observed by a Certifying Authority;
e. the manner in which the Certifying Authority will disclose the information pertaining to ESC, the certification there to, the details of the suspension or revocation of any ESC etc;
f. the particulars of statement which will accompany an Certification of practice of a CA applying for licence to issue ESC;
g. the manner in which the subscriber will communicate the compromise of private key to
h. the certifying Authority.

ELECTRONIC SIGNATURE CERTIFICATES

SECTION 35 - CERTIFYING AUTHORITY TO ISSUE ELECTRONIC SIGNATURE CERTIFICATE.

Any person can make an application to the CA for the issue of a ESC. The application will be in the form prescribed by the Central Government. The application shall be accompanied with the prescribed fee not exceeding twenty five thousand rupees, to be paid to the Certifying Authority. The fee could be different fees for different classes of applicants'. In addition to the fees the application is also required to be accompanied with a certification practice statement or where there is no such statement, a statement containing such particulars, as may be required by regulations.

The CA can consider such an application accompanied with the certification practice statement, and after making the necessary inquiry, as the CA deems fit, either grant the ESC or for reasons to be recorded in writing, reject the application. The application can be rejected only after giving the applicant a reasonable opportunity of being heard.

REPRESENTATIONS UPON ISSUANCE OF ELECTRONIC SIGNATURE CERTIFICATE

A CA while issuing a ESC will certify that it is—

a. Has complied with the provisions, rules and regulations of this Act
b. Has published or made available the ESC to any person relying on it or to a subscriber who has accepted it.
c. The subscriber holds the private key corresponding to the public key, listed in the ESC;
d. the subscriber holds a private key which is capable of creating a digital signature;
e. the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;
f. The subscriber's public key and private key constitute a functioning key pair,
g. The information contained in the ESC is accurate; and
h. it has no knowledge of any material fact, which if it had been included in the Electronic Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d*).*

SUSPENSION OF ELECTRONIC SIGNATURE CERTIFICATE

Any ESC which is issued by a CA can be suspended by the CA on the occurrence of one of the following events:

a. on receipt of **a specific request** to that effect *from the subscriber of a ESC or a person duly authorized by such a subscriber*
b. if the CA is of the opinion that it is in the interest of the public to do so

The suspension of the ESC by the CA is required to be communicated to the subscriber. The CA cannot suspend the ESC for a period more than 15 days, without providing the subscriber, a reasonable opportunity of being heard.

REVOCATION OF ELECTRONIC SIGNATURE CERTIFICATE

A CA canrevoke a ESC issued by it on a specific request being made to it, by the subscriber or a person duly authorized by him in this regards. The CA can also revoke the ESC upon the death of the subscriber, where the subscriber is an individual, or on dissolution, where the subscriber is a firm or on the winding up, where the subscriber is a corporate entity.

An ESC can be revoked by the CA with immediate effect, after giving the subscriber a reasonable opportunity of being heard if, the CA is of the opinion that a material misrepresentation or concealment of the facts in the ESC or for non fulfillment of any requirement which were pre-requisites for the issue of the ESC or where the CAs private key or security system has been compromised in a manner materially affecting the ESCs reliability or where the subscriber has been adjudged insolvent or on account of death, dissolution or winding-up or any other circumstances as a result of which the subscriber to the ESC ceases to exist. The revocation of a ESC by the CA has to be communicated to the subscriber.

Any suspension or revocation of ESCs is required to be published in the public repositories (one or more as the case may be) maintained by the CA.

DUTIES OF SUBSCRIBERS

Where any Electronic Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Electronic Signature Certificate has been accepted by a subscriber,

then, the subscriber will generate the key pair by applying the security procedure. Further the subscriber shall perform such duties as may be prescribed.

ACCEPTANCE OF ELECTRONIC SIGNATURE CERTIFICATE

A subscriber is deemed to have accepted a ESC if he publishes or authorizes the publication of a ESC to one or more persons in a repository, or otherwise demonstrates his approval of the ESC in any manner.

By accepting a ESC the subscriber certifies to all who reasonably rely on the information contained in the ESC that the subscriber holds the private key corresponding to the public key listed in the ESC and is entitled to hold the same. Furthermore all representations made by the subscriber to the CA and all material relevant to the information contained in the ESC are true to the best of his belief.

CONTROL OF PRIVATE KEY

Every subscriber is required to exercise reasonable care to retain control of his private key, which corresponds to the public key listed in his ESC and take all steps to prevent its disclosure to a person not authorized to affix the electronic signature of the subscriber.

If the private key is compromised, then, the subscriber will communicate the same forthwith to the CA in specified manner. The subscriber is liable for all events occurring as a result of the compromising of the private key from the time compromise upto the time he has informed the CA of the private key being compromised.

PENALTIES, COMPENSATION AND ADJUDICATION

The Information Technology Amendment Act 2008 have introduced a host of offencies and prescribed penalties for these offences.

SECTION 43 - PENALTY FOR DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC

If any person without permission (or the knowledge) of the owner or any other person who is in-charge of a computer, computer system or computer network, —

a. accesses or secures access to such computer, computer system or computer network;
b. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
e. disrupts or causes disruption of any computer, computer system or computer network;
f. denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

g. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
h. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
i. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
j. Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

He can be made liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.— For this purposes,—

i. "computer contaminant" means any set of computer instructions that are designed—
   a. to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
   b. by any means to usurp the normal operation of the computer, computer system, or computer network;
ii. "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
iii. "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
iv. "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
v. "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form

SECTION 43A - COMPENSATION FOR FAILURE TO PROTECT DATA

When a body corporate is in possession, handling or dealing in sensitive personal data or information in a computer resource that it owns, controls or operates, is found negligent in implementing & maintaining reasonable security practices and procedures and thereby causes wrongful loss or gain to any person, then in such a case the body corporate will be held liable to damages as compensation to a sum not exceeding Rs 5 Crores to the person so effected.

For this purpose, "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

“Reasonable security practices and procedures” would include such practices and procedures which are designed to protect information from unauthorized access, damage, misuse, modification, disclosure etc, as may be agreed to between the parties or as determined by law in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

"Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Note: Refer Notification G.S.R. 313(E).— dated 11th April 2011 for Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Notified by the Central Government.

PENALTY FOR FAILURE TO FURNISH INFORMATION RETURN, ETC

If any person who under this Act or any rules or regulations made there under to—

a. Is required by the CCA or CA to furnish any document, return or report fails to do so, will be liable to a penalty not exceeding Rs 1,50,000/-for each such failure;
b. Is required to file any return or furnish any information, books or other documents within the time specified by the regulations, fails to do so, within the time specified, will be liable to a penalty not exceeding Rs 5000/- per day of such continuing default;
c. Fails to maintain books of accounts or records as required, will be liable to a penalty not exceeding
   Rs 10,000/- per day of such continuing default.

PUNISHMENT FOR DISCLOSURE OF INFORMATION IN BREACH OF LAWFUL CONTRACT

Unless otherwise provided under this act or under any other act, any person, including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to **three** years, or with a fine which may extend to five lakh rupees, or with both.

COMPENSATION, PENALTIES OR CONFISCATION NOT TO INTERFERE WITH OTHER PUNISHMENT

A penalty imposed or compensation awarded or confiscation under the Act, will not result in avoidance of an award of compensation or imposition of any penalty or punishment under any other law.

RESIDUARY PENALTY

Whoever contravenes any rules or regulations made under this Act, and no penalty has been separately provided for such contravention, will be liable to pay a compensation not exceeding Rs 25,000/- to the person affected by such contravention or a penalty of equal amount.

A penalty imposed under this Act, if it is not paid, can be recovered as an arrear of land revenue and the license or the ESC, as the case may be, can be suspended till the penalty is paid.

COMPOUNDING OF OFFENCES

Notwithstanding anything contained in Code of Criminal Procedure, an offence pertaining to

- Hacking with a computer system
- Transmission of obscene material / content
- Breach of confidentiality and privacy
- Misutilization of personal information

can be compounded under section 77A of the Act. However the benefit of compounding will not be available to a person who has been previously convicted for the same or similar offence or who is liable to enhanced punishment.

No court can take cognizance of any of the above-mentioned offences unless the person aggrieved by the offence lodges a complaint. Only an officer of rank of a Deputy Superintendent of Police can investigate cognizable offences under this act. When an officer in charge of a police station is given information pertaining to a non cognizable offence, he is required to record such information in such records as are prescribed by the State Government. The Officer who receives such information can exercise the same power of investigation (except the power to arrest without warrant), as an Officer in charge of police station would have under section 156 of code of criminal procedure.

SECTION 46 - POWER TO ADJUDICATE

Sec 46 confers the power to adjudicate contravention under the Act to an officer not below the rank of Director to Government of India or equivalent officer of state.

Such appointment shall be made by CG. Person so appointed shall have adequate exp. in field of Info. Technology and such legal and judicial experience as may be prescribed by CG.

The adjucating officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crores.

In respect of claim for injury or damage exceeding rupees five crores, jurisdiction shall vest with the competent court.

For the purpose of holding an inquiry and for the purposes of adjudication the Officer will have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under sub-section (2) of section 58. All the proceedings held before the Adjudicating Officer will be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code and for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 be deemed to be a civil court.

The Officer for the purpose of holding an inquiry, as prescribed by the Central Government, is required to give the person being accused of the contravention a reasonable opportunity for making representation in the matter. If after giving such an opportunity the officer is of the opinion that such person has as alleged contravened the provisions of the Act, or any Rules, regulations and direction there under, can impose such penalty or award such compensation as he thinks fit in accordance with the provisions.

Sec 47 provides that for the purpose of imposing penalty or for awarding compensation the Officer will take into consideration the following:

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

THE CYBER APPELLATE TRIBUNAL

ESTABLISHMENT & COMPOSITION OF CYBER APPELLATE TRIBUNAL

The Central Government, by notification, can establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal (**"tribunal")**. Such notification will also specify the matters and places in relation to which the Cyber Appellate Tribunal can exercise jurisdiction.

CONSITUTION & THE JURISDICTION OF A BENCH

The Central Government in consultation with the Chief Justice of India selects the Chairperson and other members. The Cyber Appellate Tribunal is made up of a Chairperson and such number of Members, as the Central Government deems fit. The Chairperson and one or two Members shal constitute a Bench of the Tribunal. The Tribunal exercises its jurisdiction and all the powers, authority through such a Bench. The Central Government has mandated that the Bench of the Tribunal will sit in New Delhi and at such places which the Central Government in consultation with the Chairperson may resolve. Once having resolved where the Bench will be situated, the Central Government demarcates the areas where the Bench will exercise its jurisdiction notifies such resolution in the Official Gazette. The Chairperson of the Tribunal can transfer the Member (s) from one Bench to another.

Where the circumstances so merit, at any time before or in the course of a case or a matter, if the Chairperson or the Member of the Tribunal are of the view that the nature of the case or matter is such that it ought to be heard by a Bench consisting of more Members, the case can be transferred by the Chairperson to such a Bench as the Chairperson deems fit.

QUALIFICATION OF THE CHAIRPERSON & THE MEMBERS OF THE TRIBUNAL

The Information Technology Amendment Act 2006 and the Information Technology Amendment Act 2008 have introduced a slew of changes in the manner of appointment of the Chairperson and the Members (Judicial as well as non Judicial) of the Cyber Appellate Tribunal. The changes include the basic eligibility criteria, the manner in which the salary and other emoluments will be given/ announced, the requirement of independence and retirement from earlier service.

Only a person who is, or has been, or is qualified to be, a Judge of a High Court. The Members of the Tribunal, barring the Judicial Member will be appointed by the Central Government. Such a Member shall from amongst persons who posses special knowledge and professional experience in the field of Information Technology, Telecommunication, Industry, Management and Consumer Affairs. The Government can only select the Members from the cadre of Central or State Government employees, holding the position of Additional Secretary for a period not less than 2 years or a Joint Secretary to the Government of India or an equivalent position with either the Central or the State Government for a period not less than 7 years.

Only a person who is a member of the Indian Legal Service and has held the position of an Additional Secretary for a period of one year or a Grade I post of the Legal Service for a period not less than 5 years, is qualified to be selected as the Judicial Members of the Tribunal.

Before the appointment of the Chairperson and the Members of the Tribunal, the Central Government satisfies itself that the candidate is an independent person and a person of integrity who will not be interested either financially or in any other way, that may prejudicially influence his discharging of the functions of a Chairperson or as a Member of the Cyber Appellate Tribunal. On his selection, either as a Member of Chairperson of the Tribunal, the candidate (officer of the Central / State Government) is required to retire from his service before he is allowed to join as the Member/ Chairperson of the Cyber Appellate Tribunal

TENURE OF THE CHAIRPERSON & THE MEMBERS OF THE TRIBUNAL

The Chairperson and the Members hold office for a term of five years from the date of entering his office or until they attain the age of sixty five years, which ever occurs earlier During the tenure the Chairperson and the Members will be entitled to such a salary, allowance and other benefits like gratuity, pension, etc as may be prescribed.

FUNCTIONING OF THE BENCH

The Chairperson has the power of general supervision and administration of the conduct of affairs of the Bench. In addition to presiding over the meetings of the Tribunal the Chairperson exercises and discharges such functions and powers as are prescribed in this regards.

The Chairperson distributes the business to a Bench of the Tribunal and directs the manner in which each matter will be dealt with. The Chairperson can also, on receipt of an application in this regards from any of the parties and after giving a notice to such parties and giving them a hearing as he deems proper or suo moto without such a notice, can transfer the matter from one Bench to another for its disposal.

If the Members of a Bench (consisting of 2 Members) differ in opinion on any point, they are required to state the point(s) that they differ on and refer the matter to the Chairperson. The Chairperson will then proceed to hear the point (s) /matter and then decide on the same on the basis of the majority view of the Members who have heard the case including those Members who have heard the case first.

FILLING UP OF VACANCIES, RESIGNATION OR REMOVAL OF A CHAIRPERSON

Once the Chairperson has been appointed neither the salary and allowances nor the other terms and conditions of his service can be varied to his disadvantage. If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson of a Cyber Appellate Tribunal, then the Central Government is to appoint another person in accordance with the provisions of this Act to fill the said vacancy and the proceedings can be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

The Chairperson of a Cyber Appellate Tribunal can, address to the Central Government his notice in writing, under his hand to resign his office. Unless a shorter period of relinquishment is permitted by the Central Government, the Chairperson can continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

The Central Government can remove the Chairperson from his office only by way of an order in writing on the grounds of proved misbehavior or incapacity after an inquiry. Such an inquiry can be made only by a Judge of the Supreme Court in which the Chairperson concerned has been informed of the charges against. The Chairperson has to be given a reasonable opportunity of being heard in respect of these charges. The Central Government can, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid Chairperson.

The order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal and no act or proceeding before a Cyber Appellate Tribunal shall not be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

STAFF OF THE CYBER APPELLATE TRIBUNAL

The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as required. The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer. The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be Public Servants within the meaning of section 21 of the Indian Penal Code.

APPEAL TO CYBER APPELLATE TRIBUNAL

Any person aggrieved by an order made by Controller or an adjudicating officer under this Act can prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. However no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. The appeal can be filed by the aggrieved person within a period of 45 days from the date of receipt of order in the prescribed form and accompanied by prescribed fee. The Cyber Appellate Tribunal can entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was sufficient cause for not filing it within the prescribed period. The provisions of the Limitation Act, 1963, will, as far as can be, apply to an appeal made to the Cyber Appellate Tribunal.

The appeal filed before the Cyber Appellate Tribunal is to be dealt with by it as expeditiously as possible and an endeavor will be made by the Cyber Appellate Tribunal to dispose of the appeal finally within six months from the date of receipt of the appeal. The appellant can either appear in person or through an authorized representative (one or more legal practitioners) or any of its officers, to present his or its case before the Cyber Appellate Tribunal.

The Cyber Appellate Tribunal can, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against. The Cyber Appellate Tribunal will send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating office

SECTION 58 - PROCEDURE AND POWERS OF THE CYBER APPELLATE TRIBUNAL

The Cyber Appellate Tribunal is not be bound by the procedure laid down by the Code of civil Procedure, 1908 but is be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal has the powers to regulate its own procedure including the place at which it shall have its sittings. For the purposes of discharging its functions under this Act, the Cyber Appellate Tribunal has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:—

a. summoning and enforcing the attendance of any person and examining him on oath;
b. requiring the discovery and production of documents or other electronic records;
c. receiving evidence on affidavits;

d. issuing commissions for the examination of witnesses or documents;
e. reviewing its decisions;
f. dismissing an application for default or deciding it *ex pane;*
g. any other matter which may be prescribed.

Every proceeding before the Cyber Appellate Tribunal is deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal is deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973. No Civil Court has the jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered, by or under this Act, to determine and no injunction will be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

SECTION 62 - APPEAL TO HIGH COURT

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal can file an appeal to the High Court within sixty days from the date of receipt of order of the Cyber Appellate Tribunal, on any question of fact or law arising out of such order. Any delay in filing the appeal to the High Court can be condoned by the High Court, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

SECTION 63 - COMPOUNDING OF CONTRAVENTIONS

At any time, before or after the institution of adjudication proceedings, the CCA or an Officer specially authorized in this regards or the Adjudicating Office can compound contraventions under the Act. The compounded amount however cannot, in any case, exceed the maximum penalty imposable for the contravention under this Act. Where any contravention has been compounded, no proceeding or further proceeding, as the case may be, can be taken for the compounded offence. Once a contravention has been compounded, the same person cannot seek relief of compounding for the same or similar contraventions committed within a period of 3 years from the date of compounding.

OFFENCES

The Act has specified that Tampering with computer source documents, Hacking computer system, Publishing of information which is obscene in electronic form or failure of a CA or its employees to follow the directions/ Orders of the CCA, failure to comply with Directions of Controller to a subscriber to extend facilities to decrypt information, accessing a protected system without proper authorization, material mis-representation, Penalty for publishing Electronic Signature Certificate false particulars, Publication for fraudulent purpose, sending of grossly offensive information, false information, etc will be offences.

The various offences and corresponding punishments are summarized and tabulated below with detailed explanation in the following paragraphs.

Section	Contents	Imprisonment Up to	Fine Up to
65	Tampering with computer source code documents	3 years or/and	200,000
66	Hacking with computer system dishonestly or fraudulently	3 years or/and	500,000

66B	receiving Stolen computer resource	3 years or/and	100,000
66C	Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	3 years and	100,000
66D	cheating by Personation by using computer resource	3 years and	100,000
66E	Violation of Privacy	3 years or/and	200,000
66F	Whoever,- A. with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by – 1. Denial of Access 2. Attempting to Penetrate computer resource 3. Computer containment B. knowingly or intentionally penetrates and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations, or likely to cause injury to the interests of the sovereignty and integrity of India	Imprisonment for Life	
67	Publish or transmit Obscene material - 1st time Subsequent Obscene in elec. Form	3 years and 5 years and	500,000 10,00,000
67A	Publishing or transmitting material containing Sexually Explicit Act - 1sttime Subsequent	5 years and 7 years and	10,00,000 10,00,000
67B	Publishing or transmitting material containing Children in Sexually Explicit Act - 1st time Subsequent	5 years and 7 years and	10,00,000 10,00,000
67C	Contravention of Retention or preservation of information by intermediaries	3 years and	Not Defined
68	Controller's directions to certifying Authorities or any employees failure to comply knowingly or intentionally	2 years or/and	100,000
69	Failure to comply with directions for Intercepting, monitoring or decryption of any info transmitted through any computer system/network	7 Years and	Not Defined
69A	Failure to comply with directions for Blocking for Public Access of any information through any computer resource	7 Years and	Not Defined
69B	Failure to comply with directions to Monitor and Collect Traffic Data	3 Years and	Not Defined

70	Protected system. Any unauthorised access to such system	10 years and	Not Defined
70B (7)	Failure to provide information called for by the *I.C.E.R.T or comply with directions	I year or	1,00,000
71	Penalty for Misrepresentation or suppressing any material fact	2 years or/and	100,000
72	Penalty for breach of confidentiality and privacy of el. records, books, info., etc without consent of person to whom they belong.	2 years or/and	100,000
72A	Punishment for Disclosure of information in breach of lawful contract	3 years or/and	500,000
73	Penalty for publishing False Digital Signature Certificate	2 years or/and	100,000
74	Fraudulent Publication	2 years or/and	100,000
75	Act also to apply for offences or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system or computer network located in India		
76	Confiscation of any computer, computer system, floppies, CDs, tape drives or other accessories related thereto in contravention of any provisions of the Act, Rules, Regulations or Orders made.		
77	Penalty and Confiscation shall not interfere with other punishments provided under any law.		
78	Power to investigate offences by police officer not below rank of Dy. Superintendent of Police.		

*I.C.E.R.T - Indian Computer Emergency Response Team to serve as national agency for incident response – Functions in the area of Cyber Security,-

a. collection, analysis and dissemination of information on cyber incidents
b. forecast and alerts of cyber security incidents
c. emergency measures for handling cyber security incidents
d. coordination of cyber incidents response activities
e. issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
f. such other functions relating to cyber security as may be prescribed.

TAMPERING WITH COMPUTER SOURCE DOCUMENTS,

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, can be punished with imprisonment up to three years, or with fine which can extend up to two lakh rupees, or with both. "Computer source code" means

the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

UNAUTHORIZED ACCESS TO A COMPUTER SYSTEM

If any person, dishonestly or fraudulently does any act which results in damage to a computer or a computer system or secures unauthorized access to a secure computer system or down loads or copies data etc (acts described under section43 of the Act), the he can be punished with a prison term which can extend upto two years or with a fine which can extend up to ₹Five Lakhs or both. Here the Act refers to the India Penal Code for interpreting the meaning of the words “dishonestly” and “fraudulently”

PUNISHMENT FOR SENDING OFFENSIVE MESSAGES THROUGH COMMUNICATION SERVICE

Any person who sends, by means of a computer resource or a communication device any information that is grossly offensive or has menacing character; or which he knows to be false, or sends any electronic mail or message so as to mislead the addressee about the origin of such message but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device, shall be punishable with imprisonment for a term which may extend to three years and with fine. Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

PUNISHMENT FOR DISHONESTLY RECEIVING STOLEN COMPUTER RESOURCE OR COMMUNICATION DEVICE

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

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 for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

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 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 VIOLATION OF PRIVACY.

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

"Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

"Capture", with respect to an image, means to videotape, photograph, film or record by any means;

"Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

"Publishes" means reproduction in the printed or electronic form and making it available for public;

"Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that he or she could disrobe in privacy, without being concerned that an image of his private area was being captured or any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

PUNISHMENT FOR CYBER TERRORISM

Any person with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by denying or cause the denial of access to any person authorized to access computer resource or attempting to penetrate or access a computer resource without authorisation or exceeding authorized access or introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

The person committing or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM

Any person who publishes or transmits or causes to be published 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, shall be punished on first conviction with imprisonment of either description for a term which may extend to **two three** years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to **five**years and also with fine which may extend to ten lakh rupees.

PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT,ETC. 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 of either description for a term which may extend to **five** years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to **seven years** and also with fine which may extend to ten lakh rupees.

PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT, ETC. IN ELECTRONIC FORM.

Whoever, publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or 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 with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or facilitates abusing children online or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

The above three provisions shall not be applicable to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form if the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern or which is kept or used for bonafide heritage or religious purposes

"Children" means a person who has not completed the age of 18 years.

PRESERVATION AND RETENTION OF INFORMATION BY INTERMEDIARIES

An intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe an any intermediary who intentionally or knowingly abstains from doing the same shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

POWER OF CONTROLLER TO GIVE DIRECTIONS

The CCA can direct a CA or the employees of such a CA to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person intentionally or knowingly failing to comply with such an order will have committed an offence and will be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

POWERS TO ISSUE DIRECTIONS FOR INTERCEPTION OR MONITORING OR DECRYPTION OF OR BLOCKING OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE

Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do

- in the interest of the sovereignty or integrity of India,

- defense of India,
- security of the State,
- friendly relations with foreign States
- public order
- for preventing incitement to the commission of any cognizable offence relating to above
- for investigation of any offence,

after recording the reasons there of in writing, can warrant or direct or order any agency of the Government to intercept or monitor or decrypt or block any information transmitted through a computer resource. The Government is required to specify safeguards, subject to which the interception or monitoring or decryption is to be done. Any person, be it a subscriber or an intermediary or any other person who is in charge of the computer resource, is bound to extend all possible cooperation, technical assistance and facility as may be required by the authorities to access or to secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information or intercept or monitor or decrypt or block the information, **as the case may be** or provide information stored in computer resource. Failure to do so is punishable with an imprisonment for a term which can extend to seven years and also liable to fine.

POWER TO AUTHORIZE TO MONITOR AND COLLECT TRAFFIC DATA OR INFORMATION THROUGH ANY COMPUTER RESOURCE FOR CYBER SECURITY

The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. The Intermediary or any person in-charge of the Computer resource shall when called upon by such agency provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information. The government shll prescribe procedure and safeguards for monitoring and collecting traffic data or information.

Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

"Computer Contaminant" shall have the meaning assigned to it in section 43

"Traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

PROTECTED SYSTEM

The Government has notified certain computer resources as Critical Information Infrastructure to be a protected system. Critical Information Infrastructure refers to computer systems or resources the destruction or incapacitation of which would result in a debilitating impact on the national security, economy, public health or safety. The appropriate Government can, by notification in the Official Gazette, declare that any computer, computer system or computer network which directly or indirectly affects the facility of a Critical Information Infrastructure, to be a protected system and authorize the persons who are authorized to access protected systems. In this regards the Government can prescribe specific

information security practices and procedures. Any person who secures unauthorized access or attempts to secure unauthorized access to a protected system, can be punished with imprisonment of either description for a term which can extend to ten years and can also be liable to fine.

CREATION OF NATIONAL NODAL AGENCY

The Central Government has the powers through notification to designate any organization of the Government as the national nodal agency for the protection of Critical Information Infrastructure Protection. Such agency shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

INDIAN COMPUTER EMERGENCY RESPONSE TEAM TO SERVE AS NATIONAL AGENCY FOR INCIDENT RESPONSE

The Central Government has the powers through notification to appoint an agency of the government to be called the Indian Computer Emergency Response Team. The Central Government shall provide such agency with a Director General and such other officers and employees as may be prescribed. The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

a. collection, analysis and dissemination of information on cyber incidents
b. forecast and alerts of cyber security incidents
c. emergency measures for handling cyber security incidents
d. Co-ordination of cyber incidents response activities
e. issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
f. such other functions relating to cyber security as may be prescribed

For carrying out the above functions, the agency may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person. Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with such direction shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

PENALTY FOR MISREPRESENTATION

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or ESC, as the case may be, can be punished with imprisonment for a term which can extend to two years, or with fine which can extend to one lakh rupees, or with both.

PENALTY FOR BREACH OF CONFIDENTIALITY AND PRIVACY

No person can publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that the CA listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, unless such publication is in the course of verifying a electronic signature created prior to such suspension or revocation. Such a contravention can be punished with imprisonment for a term which can extend to two years, or with fine which can extend to one lakh rupees, or with both.

PENALTY FOR PUBLISHING ELECTRONIC SIGNATURE CERTIFICATE FALSE IN CERTAIN PARTICULARS

Whoever knowingly creates, publishes or otherwise makes available a ESC for any fraudulent or unlawful purpose can be punished with imprisonment for a term which can extend to two years, or with fine which can extend to one lakh rupees, or with both.

ACT TO APPLY FOR OFFENCE OR CONTRAVENTION COMMITED OUTSIDE INDIA

The Act gives extra territorial jurisdiction in cases where the offence or contraventions are committed from outside India, by any person irrespective of his nationality. The provisions of this Act will apply also to any offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. No penalty imposed or confiscation made under this Act can prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

CONFISCATION

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act. rules, orders or regulations made there under has been or is being contravened, will be liable to confiscation. Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court can, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

INTERMEDIARIES NOT LIABLE IN CERTAIN CASES

Unless otherwise specifically provided to the contrary, an intermediary will be not liable for, any third party information, data or communication link made by him. This exemption is available only if:

- The intermediary's role is limited to providing access to a communication system over which third parties transmit information or temporarily store the same.
- The intermediary does not

1. Initiate the transmission
2. Select the receiver of transmission or,
3. Modify the information contained in the transmission.

The exemption would however stand withdrawn if intermediary conspires or abets the commission of an unlawful act or after having received the information from the government that any information, data or communication link residing in or connected with computer resources controlled by the intermediary, are being used to commit unlawful acts and such intermediary fails to act expeditiously in removing or disabling access to such link or resource.

EXAMINER OF ELECTRONIC EVIDENCE

For the purpose of providing an expert opinion on electronic form evidence, before any Court or other statutory body, can specify by notification in official gazette any department or body or agency of central government as an examiner of electronic evidence. Here, *electronic form evidence* means any information of probative value which is stored and transmitted in electronic form. It includes computer evidence, digital audio and digital video, cell phones, fax machines etc.

PROTECTION OF ACTION TAKEN IN GOOD FAITH

No suit, prosecution or other legal proceeding will lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

ENCRYPTION METHODS:

The Central Government can prescribe the modes and methods for encryption for the purposes of secure use of electronic medium and for promotion of e-governance and e-commerce.

PUNISHMENT FOR ABETMENT OF OFFENCES

When a person abets any offence and the act being abetted is committed in consequence of the abetment, such a person can be made liable for the same offence and penal consequences awarded as a result, even though abetment, by itself, can not be an offence. An act or offence is said to be committed in consequence of abetment, when it is committed as a consequence of the instigation or a conspiracy. Any person committing an offence punishable by this Act or causes such an offence to be committed, any act during the course of such an attempt is also an offence, punishable as if it were an offence and imprisonment would extend to one- half of the longest term of imprisonment imposable or a fine or both.

PUNISHMENT FOR ATTEMPT TO COMMIT OFFENCES

Any person who attempts to commit an offence punishable by this Act be punished with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

OFFENCES BY COMPANIES

Where a contravention of any of the provisions of this Act or of any rule, direction or order made under this Act is committed by a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, will be guilty of the contravention and will be liable to be proceeded against and punished accordingly. Any person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, will be absolved of the allegation of the contravention or committing the offence.

Where it is proved that the contravention, of any of the provisions of this Act or of any rule, direction or order has taken place /been committed by a company with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer will also be deemed to be guilty of the contravention and will be liable to be proceeded against and punished accordingly. Here "company" means any body corporate and includes a firm or other association of individuals; and "director", in relation to a firm, means a partner in the firm.

REMOVAL OF DIFFICULTIES

If any difficulty arises in giving effect to the provisions of this Act, the Central Government can, by order published in the Official Gazette, such order/ direction as it deems necessary or expedient, to remove such difficulties in the provisions of this Act. However, no order for removal of difficulties can be made after the expiry of a period of two years from the commencement of this Act. Every order made, for the removal of difficulties, will be laid as soon as may be after it is made, before each House of Parliament.

POWER OF CENTRAL GOVERNMENT TO MAKE RULES.

The Central Government can, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act. In particular, and without prejudice to the generality of the foregoing power, the rules can provide for all or any of the following matters, namely:—

a. the conditions for considering the reliability of electronic signature or authentication technique;
b. the procedure for ascertaining electronic signature or authentication;
c. the manner in which any information or matter can be authenticated by the means of an electronic signature;
d. the electronic form in which filing, issue, grant or payment will be effected;
e. the manner and format in which electronic records will be filed, or issued and the method of .payment;
f. the manner in which the appropriate service provider can collect, retain and appropriate service charges;
g. the matters relating to the type of electronic signature, manner and format in which it can be affixed;
h. the manner of storing and affixing electronic signature;
i. the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers;
j. the security procedures and practices to be followed;
k. the form in which an application for license for issue of ESC, the eligibility criteria of the applicant and the period of validity of such a license, the amount of fees payable and the the other documents which will accompany an application for licence, the form and the fee for renewal of a licence and the fee payable there of;
l. the form in which application for issue of a ESC can be made and the fee to be paid for the purpose;
m. the manner in which the adjudicating officer will hold inquiry;
n. the qualification and experience which the adjudicating officer will possess;
o. the salary, allowances and the other terms and conditions of service of the Chairperson and Members;
p. the procedure for investigation of misbehaviour or incapacity of the Chairperson and Members;
q. the salary and allowances and other conditions of service of other officers and employees;
r. the form in which appeal, to the Cyber Appellate Tribunal, can be filed the and the fee thereof;

s. any other power of a civil court required to be prescribed for the purposes of the Cyber Appellate Tribunal;
t. Duties of any subscriber and the reasonable security practices and procedures to be adopted while dealing with sensitive personal information
u. the powers and the functions of the Chairperson and the Members of the Cyber Appellate Tribunal
v. safeguards for the interception or monitoring or decryption of information
w. the information security procedures and practices to be followed in respect of protected systems
x. guidelines to be observed by intermediaries
y. modes and methods of encryption for promoting e-governance and e-commerce.

Every rule made by the Central Government notifying such class of documents or transactions as can be notified by the Central Government in the Official Gazette which are outside the purview of this Act and every rule made by it shall be laid, as soon as can be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which can be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

POWER OF CONTROLLER TO MAKE REGULATIONS

The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules in relation to the following matters:

- maintenance of data-base containing the disclosure record of every Certifying Authority
- the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority
- the terms and conditions subject to which a license may be granted to a CA
- other standards to be observed by a Certifying. Authority
- the manner in which the Certifying Authority shall disclose the matters specified in relation to DSC
- the particulars of certification practice statement which shall accompany an application
- the manner by which a subscriber communicates the compromise of private key to the Certifying Authority

Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive- sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall there after have effect only in such modified form or be of no effect, as the ease may be;

so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

POWER OF STATE GOVERNMENT TO MAKE RULES

The State Government can, by notification in the Official Gazette, make rules to carry out

the provisions of this Act. In particular, and without prejudice to the generality of the foregoing power, such rules can provide for all or any of the following matters, namely: —

a. the electronic form in which filing, issue, grant receipt or payment for e licences;
b. for e returns & e payments
c. any other matter which is required to be provided by rules by the State Government.

Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

AMENDMENT TO OTHER ACTS

The Indian Penal Code, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, shall be amended in the manner specified in the Schedules to this Act.

Glossary of Cybercrime Terms

back door -- a vulnerability intentionally left in the security of a computer system or its software by its designers

biometrics -- the use of a computer user's unique physical characteristics -- such as fingerprints, voice, and retina -- to identify that user

black hat -- a term used to describe a hacker who has the intention of causing damage or stealing information

bypass -- a flaw in a security device

ciphertext -- data that has been encrypted

Computer Emergency Response Team (CERT) -- an organization that collects and distributes information about security breaches

countermeasure -- any action or device that reduces a computer system's vulnerability

cracker -- a term sometimes used to refer to a hacker who breaks into a system with the intent of causing damage or stealing data

cracking -- the process of trying to overcome a security measure

cryptography -- protecting information or hiding its meaning by converting it into a secret code before sending it out over a public network

crypto keys -- the algorithms used to encrypt and decrypt messages

cybercrime -- crime related to technology, computers, and the Internet

decrypt -- the process of converting encrypted information back into normal, understandable text

denial of service (DoS) -- an attack that causes the targeted system to be unable to fulfill its intended function

digital signature -- an electronic equivalent of a signature

domain name -- the textual name assigned to a host on the Internet

dumpster diving -- looking through trash for access codes or other sensitive information

email -- an application that allows the sending of messages between computer users via a network

encryption -- the process of protecting information or hiding its meaning by converting it into a code

firewall -- a device designed to enforce the boundary between two or more networks, limiting access

hacker -- a term sometimes used to describe a person who pursues knowledge of computer and security systems for its own sake; sometimes used to describe a person who breaks into computer systems for the purpose of stealing or destroying data

hacking -- original term referred to learning programming languages and computer systems; now associated with the process of bypassing the security systems on a computer system or network

high risk application -- a computer application that, when opened, can cause the user to become vulnerable to a security breach

hijacking -- the process of taking over a live connection between two users so that the attacker can masquerade as one of the users

host -- a computer system that resides on a network and can independently communicate with other systems on the network

Hypertext Markup Language (HTML) -- the language in which most webpages are written

information security -- a system of procedures and policies designed to protect and control information

Internet -- a computer network that uses the Internet protocol family

Internet Relay Chat (IRC) -- a large, multiple-user, live chat facility

Internet service provider (ISP) -- any company that provides users with access to the Internet

intranet -- a private network used within a company or organization that is not connected to the Internet

intrusion detection -- techniques designed to detect breaches into a computer system or network

IP spoofing -- an attack where the attacker disguises himself or herself as another user by means of a false IP network address

keystroke monitoring -- the process of recording every character typed by a computer user on a keyboard

leapfrog attack -- using a password or user ID obtained in one attack to commit another attack

letterbomb -- an email containing live data intended to cause damage to the recipient's computer

malicious code -- any code that is intentionally included in software or hardware for an unauthorized purpose

one-time password -- a password that can be used only once, usually randomly generated by special software

packet -- a discrete block of data sent over a network

packet sniffer -- a device or program that monitors the data traveling over a network by inspecting discrete packets

password -- a data string used to verify the identity of a user

password sniffing -- the process of examining data traffic for the purpose of finding passwords to use later in masquerading attacks

pen register -- a device that records the telephone numbers of calls received by a particular telephone

phracker -- a person who combines phone phreaking with computer hacking

phreaker -- a person who hacks telephone systems, usually for the purpose of making free phone calls

piggyback -- gaining unauthorized access to a computer system via another user's legitimate connection

piracy -- the act of illegally copying software, music, or movies that are copyright-protected

Pretty Good Privacy (PGP) -- a freeware program designed to encrypt email

probe -- an effort to gather information about a computer or its users for the purpose of gaining unauthorized access later

risk assessment -- the process of studying the vulnerabilities, threats to, and likelihood of attacks on a computer system or network

smart card -- an access card that contains encoded information used to identify the user

sniffer -- a program designed to capture information across a computer network

social engineering -- term often used to describe the techniques virus writers and hackers utilize to trick computer users into revealing information or activating viruses

spam -- unsolicited commercial email

spoofing -- the process of disguising one computer user as another

trap and trace device -- a device used to record the telephone numbers dialed by a specific telephone

Trojan horse -- an apparently innocuous program that contains code designed to surreptitiously access information or computer systems without the user's knowledge

virus -- a computer program designed to make copies of itself and spread itself from one machine to another without the help of the user

war dialer -- software designed to detect dial-in access to computer systems

warez -- slang for pirated software

white hat -- a hacker whose intentions are not criminal or malicious

wiretapping -- the interception of electronic communications in order to access information

worm -- a computer program that copies itself across a network

ATM: Automated Teller Machine '
SWIFT: Society for worldwide Interbank Financial Telecommunication
SFMS: Structured Financial Messaging System
OLTAS: Online Tax Accounting System
CBS: Centralized/ core Banking Solution
PIN: Personal Identification Number
LAN: Local Area Network (used in the same building)
MAN: Metropolitan Area Network (used in the same city)
WAN: Wide Area Network (used in different locations)
1DRBT: Institute for development & Research in Banking Technology
Banknet: Payment System Network established by RBI
NICNFT: National Informatics Centre Network (currency chest operation)
WWW: World Wide Web

HTTP: Hyper Text Transfer Protocol
URL: Uniform Resource Locator
VSAT: Very Small Aperture terminal
Firewall: Software programme that restricts unauthorized access to data and acts as a security to private network
Booting: Starting of a computer
Hard Disk: A device for storage of data fitted in the processor itself
Modem: Modulator & Demodulator: A device used for converting digital signals to analog signals & vice-versa
Encryption: Changing the data into coded form
Decryption: Process of decoding the data
Virus: Vital Information Resources Under Seize: Software programme that slows down the working of a computer or damages the data. Main source of virus is internet (other sources are floppy or CD)
Vaccine: Anti Virus Software programme used for preventing entry of virus or repairing the same
Digital Sign: Authentication of. electronic records by a subscriber by means of electronic method or procedure
Key used: For digital signatures, there is a pair of keys, private key & public key
RTGS: Real time Gross Settlement
ECS: Credit: One account debited, number of accounts credited
ECS: Debit: One account credited, number of accounts debited
Hacking: Knowingly concealing, destroying, altering any computer code used for computer network
Address: The location of a file. You can use addresses to find files on the Internet and your computer. Internet addresses are also known as URLs

****BEST OF LUCK ****

Disclaimer
While every effort has been made by me to avoid errors or omissions in this publication, any error or discrepancy noted may be brought to my notice throughr e-mail to Srinivaskante4u@gmail.com which shall be taken care of in the subsequent editions. It is also suggested that to clarify any doubt colleagues should cross-check the facts, laws and contents of this publication with original Govt. / RBI / Manuals/Circulars/Notifications/Memo/Spl Comm. of our bank.

Blog for updates: https://iibfadda.blogspot.com/