Security and E Evidence Issues in E Commerce

Naavi

Dimensions of Security

- Security of the transaction
- Security of the E Commerce entity from legal obligations
- Security of the Customer from the Privacy and Data Protection perspectives

Security in E Commerce

Knowing the identity of the person/s at each end of the transaction

Keeping the Confidentiality of the data through access control

- Physical, logical controls including encryption

Preserving the integrity of data and guarding unauthorized modification

- Maintaining version control, Avoiding malware

Ensuring the availability of the data

- IDS and guarding against DDOS attacks

Ensuring compliance of PDPB 2019-Privacy Related controls to be taken into account along with the CIA controls

Transaction Security

- Verify the identity of each of the customer
  - At the time of registration
    - KYC obligations
  - At the time of a transaction
    - Two factor authentication
- Limited background check of the customer (Customer Due Diligence)
  - Refer Master guidelines from RBI
    - https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607

Need for a KYC policy

- There shall be a Know Your Customer (KYC) policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.
- The KYC policy shall include following four key elements:
  a. Customer Acceptance Policy;
  b. Risk Management;
  c. Customer Identification Procedures (CIP); and
  d. Monitoring of Transactions
- Include Money laundering and Terrorist financing risk assessment by the regulated entity
  – to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

Identity verification

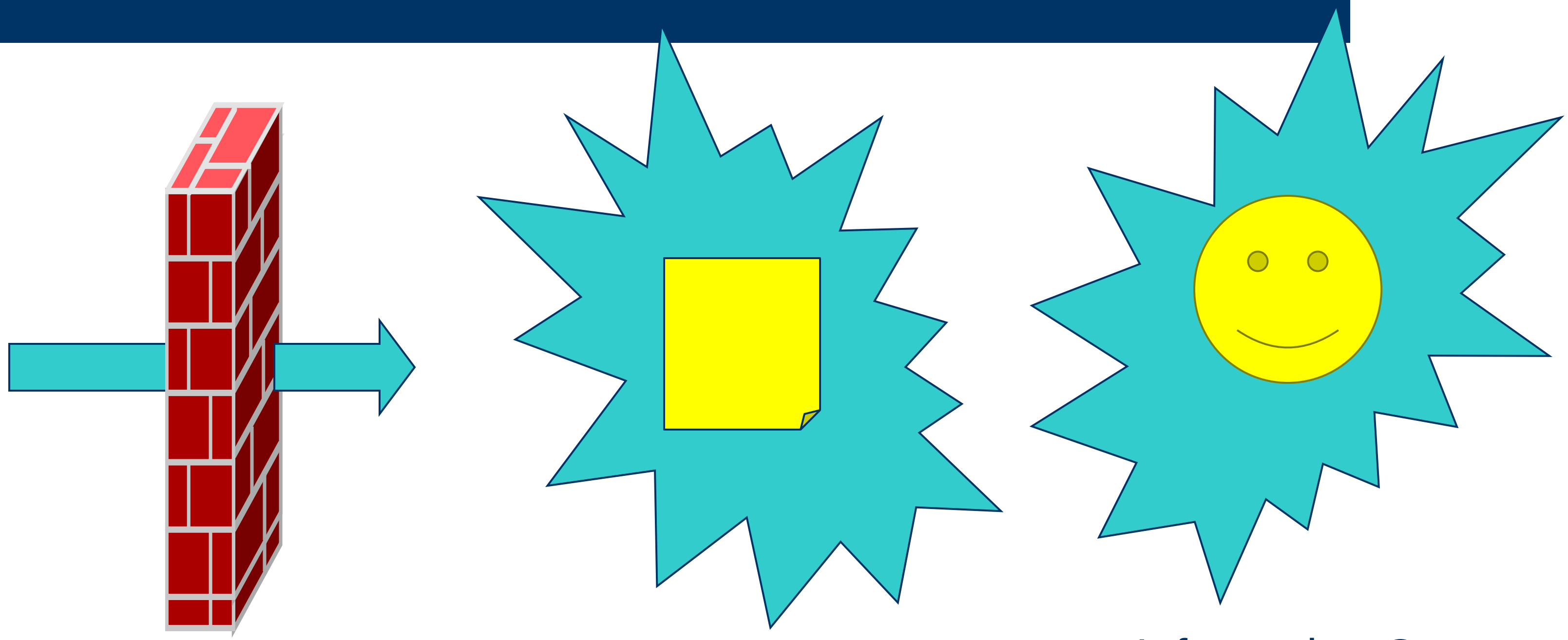
- Use of Aadhaar for KYC without storing the Aadhaar number
  - Aadhaar based eKYC
  - Offline KYC where customer collects an XML document with relevant information from the UIDAI and submits it to the entity
- Video KYC
  - Under digital KYC, authorised officer of the reporting entity (RE) will capture live photos and official valid document or the proof of possession of Aadhaar by the customer. Latitude and longitude of the location where the live photo was taken must also be documented. Only officials from regulated entities would be able to do the remote on-boarding.
- PDPA envisages consent managers who can act as KYC aggregators

Law has its own Prescriptions on Security

- ITA 2000/8
  - Section 43A and Section 79 address due diligence and Reasonable Security Practice
  - Section 67C indicates data retention requirements
  - Section 65 indicates preservation of data for evidentiary purposes

What is Information Security

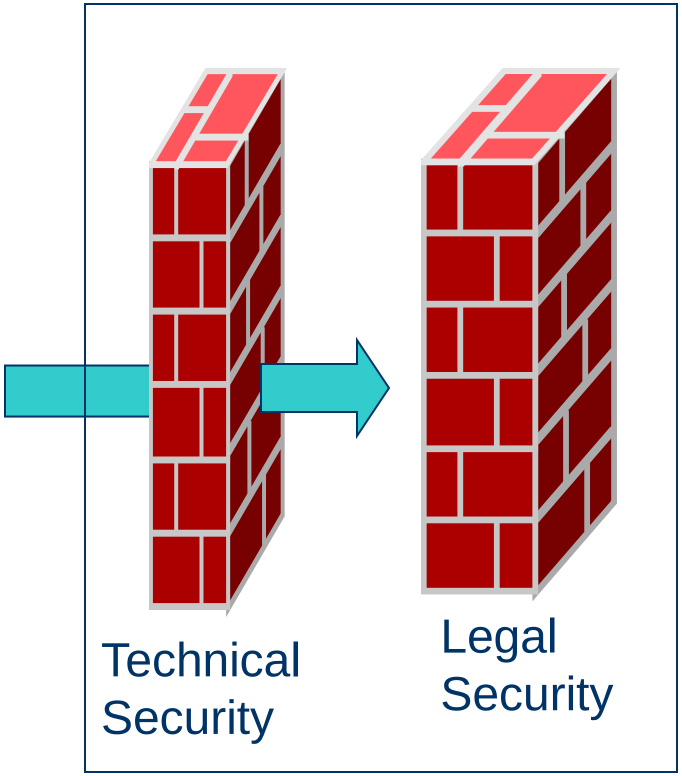
When Security is Breached…



Information damaged

Information Owner suffers a loss

Second Dimension of Information Security



Techno Legal Security

Three Dimensions of Information Security…

Technology	Legal	Behavioral
Use technical devices to manage Access Control, Malware, Integrity Management, Prevent DOS attacks etc…Encryption, Digital Signature..etc	Use and implement Policies and Procedures to be compliant with legal requirements. Fine tune technical security to meet legal requirements	Use trainings, background verification, incentives and and sanctions to build a security culture in the organization to supplement the technical and legal controls

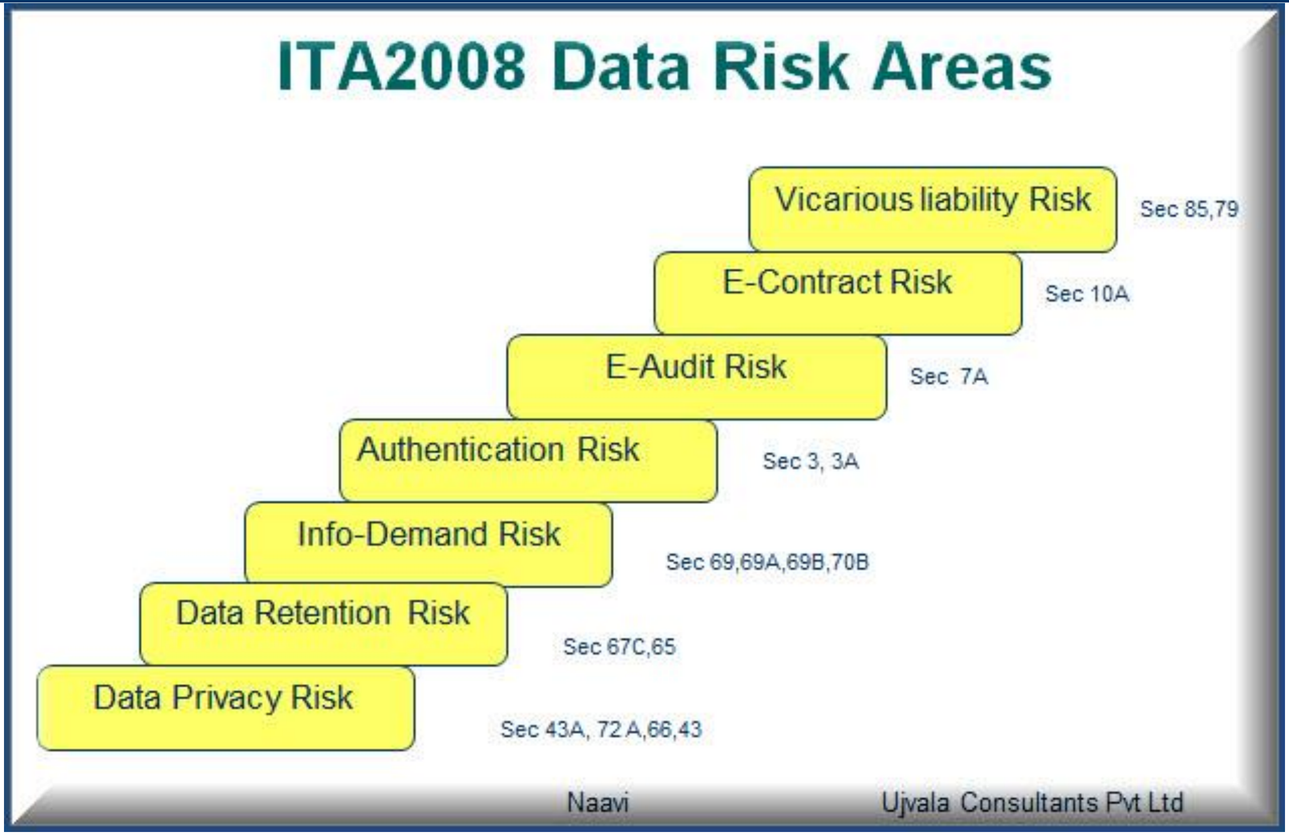
Law on Cyber Security

ITA 2000/8

ITA 2008 addressed

- Vicarious Liabilities on
  - Intermediaries
  - Company Executives
- Security Obligations
  - Due Diligence
  - Reasonable Security Practices
  - E Document Audit

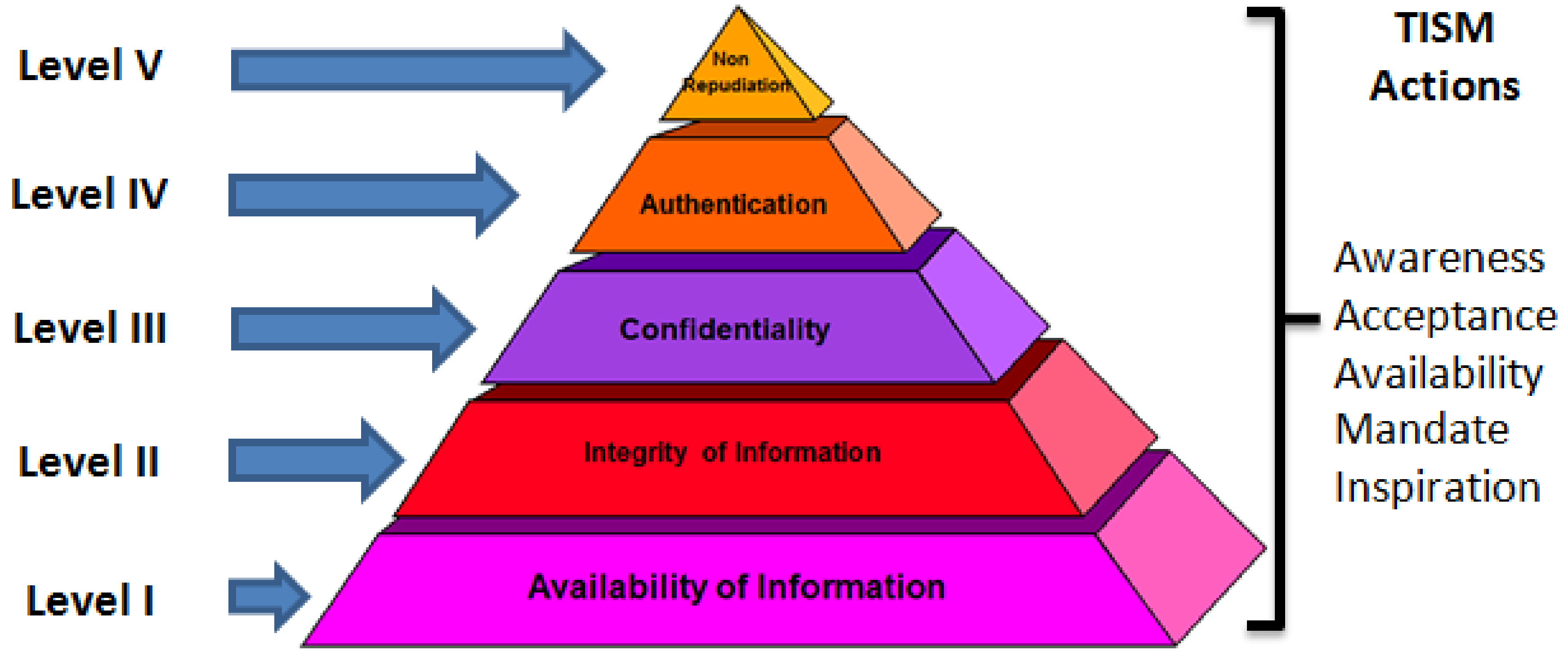
Risk Management under ITA 2008



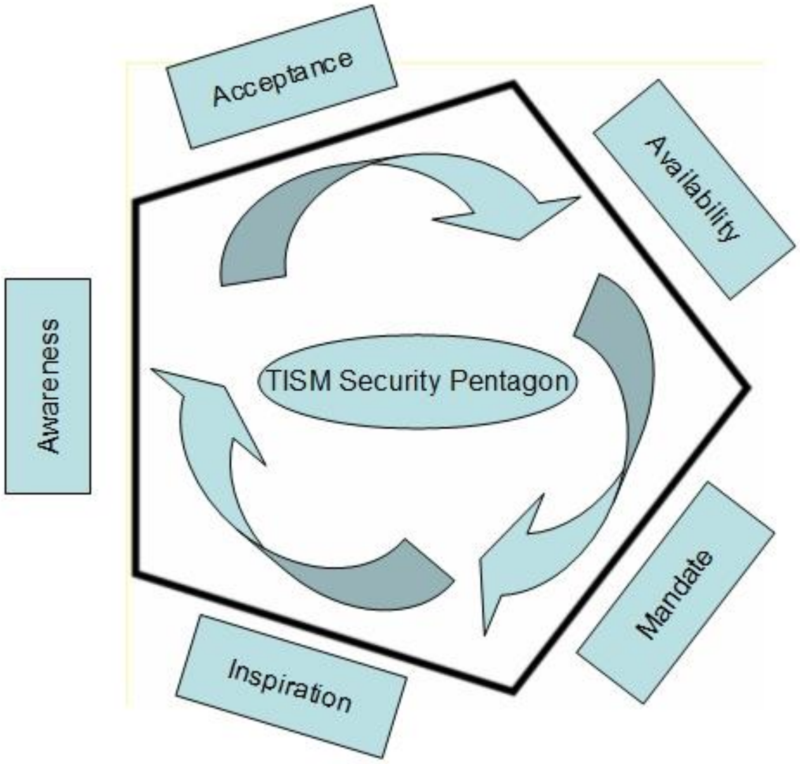
Total Information Assurance Approach

Confidentiality	**No Access Unless Authorized**
Integrity	**No Modification Unless Authorized**
Availability	**No Denial of access**
Authentication	**Ownership of activity and Data**
Non Repudiation	**Accountability at all levels**

Modular Implementation

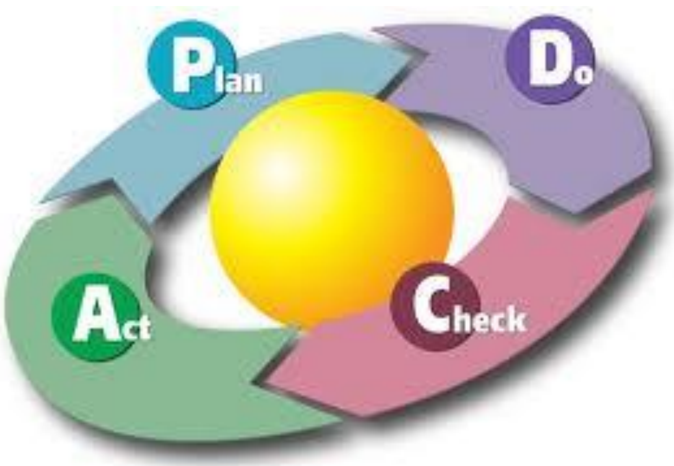


Implementation approach



Advantages of a Structured Approach

- Brings focus to the task of information security
- Sets a benchmark to the task
- Enables effective review
  - Assists in the PDCA Principle
    - Plan
    - Do
    - Check
    - Act



Indian Information Security Framework -IISF 309 (Naavi)

Top Management (6)	Middle Management(9)	HR (6)	Business(2)	IT(7)
Assigned Responsibility	Privacy and Security Practice Statement	Awareness and Declaration	Client Consent	Information Classification
ISMS Organization	IS Policy	Security Leadership	BA Agreement	Physical Access
External Reporting	IS internal Audit Policy	Internet Usage		Logical Access
External Audit	Web Presence	Media/Laptop/BYOD		Information Storage
Grievance Redressal	Hardware	Sanction		Information Transmission
Human Risk Management	Software	Background Verification		Incident Management
	E-Document Audit			Contingency
	IPR			
	Contract management			

PDPSI Framework

- Specially created for Data Security
- 12 Standards, 50 Implementation Specifications
  - Managerial-15
  - DPO-9
  - Legal-2
  - HR-4
  - Technology-20

Agenda for Typical Information Defense

- Know your assets
  - Hardware, Software, Applications
    - Inventory, Default configurations, source reliability
  - Understand the usage context
    - Who? How?
- Understand Threats in the environment
- Understand the Vulnerabilities in the systems
- Assess the Risks
  - Take steps for mitigation

Goals

- Risk Mitigation
  - Reduce Risk with a Risk-Reward trade-off
  - Assess Threats, Vulnerabilities,
  - Assess and Prioritize Risks
  - Estimate the cost of risk reduction and take appropriate decisions
- Risk Avoidance
  - Understand the Risk Appetite and undertake business process re-engineering to avoid risk
- Risk Transfer
  - Insurance
- Risk Retention
  - Accept and Absorb the risks as a conscious decision and budget for the loss

Continued…

..

Digital Evidence

Section 65B

65B. Admissibility of electronic records.-

Two Output Modes-
Print out,
Soft copy

- (1) Notwithstanding anything contained in this Act,
  - any information contained in an electronic record
  - which is **printed on a paper**,
  - **stored, recorded or copied** in optical or magnetic media produced by a computer
  - **(hereinafter referred to as the computer output)**
    - shall be deemed to be **also a document**, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and
      - shall be admissible in any proceedings, **without further proof or production of the original,**
      - as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Note

Computer output is also a "document"..and missible without…

65B. Admissibility of electronic records.-conditions

Said Period?
Person with lawful control?

Note

(2) The conditions referred to in sub-section (1) **in respect of a computer output** shall be the following, namely:—

- (a) the computer output containing the information **was produced** by the computer **during the period** over which the computer was used regularly to store or process information for the purposes of **any activities** regularly carried on over that **period** by the **person having lawful control over the use of the computer;**
- (b) during the said period, information **of the kind** contained in the electronic record or of the kind **from which the information so contained is derived** was regularly fed into the computer **in the ordinary course of the said activities**;
- (c) throughout the material part of the **said period**, the computer was **operating properly** or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
- (d) the information contained in the electronic record **reproduces** or is derived from such information fed into the computer in the ordinary course of the said activities.

65B. Admissibility of electronic records.-Multiple Computers

Note

- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of **sub-section (2**) was regularly performed by computers, whether—
  - (a) by a combination of computers operating over that period; or
  - (b) by different computers operating in succession over that period; or
  - (c) by different combinations of computers operating in succession over that period; or
  - (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,
- all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

65B. Admissibility of electronic records.-certification

- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—
  - (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
  - (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
  - (c) dealing with any of the matters to which the conditions mentioned in **sub-section (2)** relate,

Note

- and purporting to be signed by 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; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

65B. Admissibility of electronic records.-certification

- (5) For the purposes of this section,—
  - (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
  - (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
  - (c) a **computer output** shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
- Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

Note

65B. Admissibility of electronic records.-certification

- (5) For the purposes of this section,—
  - (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
  - (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
  - (c) a **computer output** shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
- Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

Note

Section 65B is all about the Computer Output

…and how the Computer output is admissible without the production of the original

Case Laws

- Suhas Katti
- Basheer
- Shafi Mohammed

Case Laws

- Suhas Katti
- Basheer
- Shafi Mohammed

2004: First Case in India when a Section 65B evidence was admitted and the accused convicted.

-Document was on the web..”yahoo groups” and was the evidence of crime..neither the server copy was seized nor produced as “Original”

-This was the first of the over 137 Section 65B Certificates provided so far by Naavi

Case Laws

- Suhas Katti
- Basheer →
- Shafi Mohammed

2014: Over turned the Afsan Guru (**2005**) verdict where electronic evidence had been accepted on the basis of Oral confirmation of witnesses without Section 65B Certificate
-Established the mandatory nature
-Established the difference between Admissibility and Challenge of Genuinity
-This was a verdict of the three member bench of the Supreme Court

Case Laws

- Suhas Katti
- Basheer
- Shafi Mohammed

2018: Two judge bench of Supreme Court hearing a SLP "clarified" ..

> -*"The applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by person who is in a position to produce such certificate being in control of the said device and not of the opposite party."*
> *..now under reference to a larger bench*

Cases on Section 65B

First use of Sec 65B

- State of Tamil Nadu Vs Suhas Katti- AMM Court Chennai (2004): 26th October 2004
  - Object of crime was a defamatory message in yahoo group
    - ..considered obscene..contained an impersonated name at the end of the message
    - Conviction was under Section 67 of ITA 2000 along with Section 469 (forgery for harming reputation) and 509 (insulting the modesty of woman)

First use of Sec 65B

- A print out of the copy of the message as seen on the yahoo server was produced by Naavi with Section 65B declarations (Certificate dt 18/2/2004)
  - Original not produced
  - Naavi was not a Government servant
  - Naavi was not the victim.. Was a third party
- Naavi was examined as an “Expert”
  - Court accepted the evidence and convicted the accused for a sentence of 2+2+1 years.
  - Session Courts on appeal upheld the conviction but reduced the sentence

Trisha Defamation Complaint in AMM-2004

- Police had produced CDs seized from a news paper office
- Court could play the CDs and accept it as evidence
  - Chose to call a third party private expert (Naavi) to view the CDs in the chamber, take print outs and certify under Section 65B so that it could be taken for further evidence

Afsan Guru Verdict

- Afzan Guru case, (Navjot Sandhu @Afzan Guru judgement dated 4/8/2005)
- Supreme Court accepted CDs of call records without Section 65B certificate because the persons who could have provided he certificate were also providing oral evidence

Basheer Judgement

- of Anvar P.V. Vs P.K.Basheer and others (Supreme Court of India Appeal No 4228 of 2012) …September 18,2014
- Over turned the Afsan Guru judgement and held
  - Section 65B certificate is mandatory for admissibility of any electronic evidence
  - Oral evidence in respect of an electronic document is not acceptable.
  - Admissibility is different from accepting genuinity
  - Section 65B is relevant at the stage of admissibility. Defence can question its genuinity during the trial

Basheer Judgement

- Construction by plaintiff, destruction by defendant.
  - Construction by pleadings, proof by evidence;
  - proof only by relevant and admissible evidence
- What is the nature and manner of admission of electronic records, is one of the principal issues arising for consideration in this appeal
- Genuineness, veracity or reliability of the evidence is seen by the court only after the stage of relevancy and admissibility.
  - These are some of the first principles of evidence.

Basheer Judgement

- First Respondent elected to Kerala Assembly in election held on 13/4/2011
  - Appeal was to set aside the election on the grounds of commission of corrupt practice
  - Evidence consisted of Electronic Records which was the major thrust in the arguments

Basheer Judgement

- Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B.
- Section 65B deals with the admissibility of the electronic record.
  - The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer.

Basheer Judgement

- Section 45 A only after admission
  - Only if the electronic record is duly produced in terms of Section 65B of the Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort can be made to Section 45A – opinion of examiner of electronic evidence.
    - P.S: Indicates that Section 45A has no relevance to Section 65B. Sec 65B is for admission and Section 45A is checking the genuineness

Retrospective Effect of Basheer Judgement

- Sonu vs Amar
  - A convict made an appeal that the conviction had to be set aside since the electronic evidence used was not Section 65B certified
    - Supreme Court held that though the Basheer judgement would be applicable retrospectively,   the appeal has to be rejected the appeal that it is not practical to re-open previous convicted cases and

Shafhi Mohammad Judgement

- The order dated 30th January 2018 by a two member judge was examining the procedure to be adopted by the Police in videographing the crime scenes.
  - A question was raised that it would be inconvenient to provide Section 65B certificate since the device was in the possession of a third party and not with the police.
  - The order sought to over rule the three member judgement of Basheer Case

Shafhi Mohammad Judgement

- The order stated in “Clarification” of the Basheer judgement that
  - *“The applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when*
  - *such electronic evidence is produced by person who is in a position to produce such certificate being in control of the said device and not of the opposite party.”*

Shafhi Mohammad Judgement

- The order also stated in complete contradiction of the Basheer judgement that
  - "In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded.
  - In such case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving,"

Shafhi Mohammad Judgement

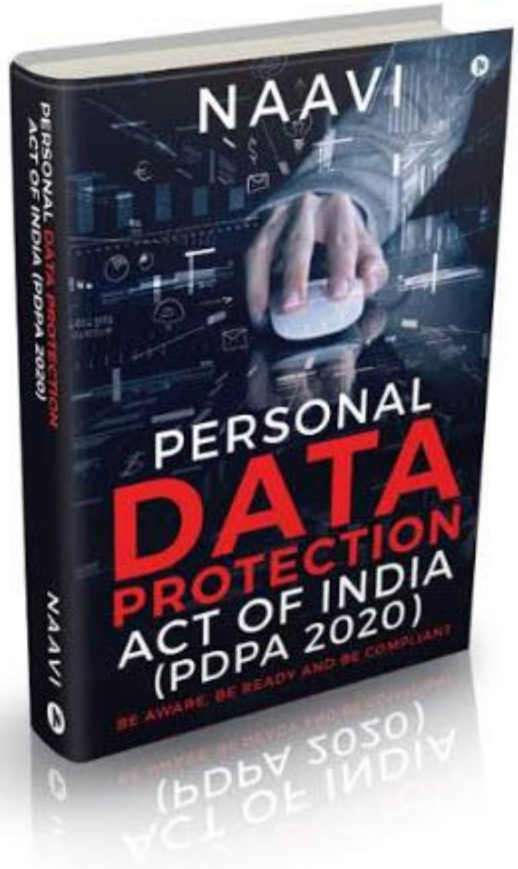
- The order is erroneous and misleading and contradicts a superior court verdict as well as the IEA.
  - In my personal opinion it cannot be considered as a precedent over Basheer judgement
    - Since it is a two member order against a three member speaking judgement
    - It is not in conformity with the IEA sections 22A, 65A

Shafhi Mohammad Judgement

- If applied,
  - Section 65B certificate would not be required for any Facebook, Twitter or Gmail or web document.
  - It would be required only in cases where the person is in possession of the device and if so, the provision is redundant since the original device itself can be brought before the Court
  - It will enable fraudulent documents to be produced at trial stage causing unimaginable problems to honest citizens since onus of proving the document produced as not genuine shifts to the defendant.

CYBER LAW GURU

Thank You



naavi@naavi.org

www.naavi.org

+919343554943