E-banking – legal issues

An Overview

Naavi

What is E Banking?

Concept of E Banking

- We understand that Internet Banking and Mobile Banking is part of E Banking.
  - May be Core Banking and ATM Banking also are easily recognizable as parts of E Banking
  - But
    - What is the legal definition?
      - Is there a legal definition?
      - Should there be a legal definition?

What distinguishes E Banking?

- Traditional Banking used “Paper” as the means of
  - Recording of transactions
  - Exchange of material instructions between the Banker and Customer
  - Account opening was a contract under Indian Contract Act using paper based offer and acceptance documents
- Interaction with the customer was face to face
  - With the ledger clerk initiating a transaction
  - branch manager who authenticates a transaction
  - the cashier who dispenses cash
    - E Banking uses an electronic document or an electronic device for either record keeping or for interaction

What distinguishes E Banking

- It encompasses
  - Records in electronic form
    - Account opening is still a paper based contract
      - Internet Banking details are often only in electronic form
  - Hardware both at the Bank and the Customer end
  - Hardware in an intermediary place such as the ATM
  - Network that connects the customer with the back end system
  - All applications that run at the Bank , Customer end and at the Intermediary level in ATMs

Legal Definition?

- There is no separate definition.
- The derived definition
  - E Banking means
    - “Banking” with the use of electronic documents. Or
  - *“accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawable by cheque, draft, order or otherwise using electronic documents in the process”*
    - Use of electronic documents implies use of electronic devices

Is “Electronic Document” defined?

- Sec 2(t) of ITA 2008
  - "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;
    - "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;
    - "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;

What is “Electronic” Data?

- The essential feature of “Data” in electronic form is that
  - Data is stored and read in “Binary” language.

Legal Definition of E Banking

- E Banking means
  - *“accepting,*
    - *for the purpose of lending or investment,*
  - *of deposits of money*
    - *from the public,*
  - *repayable*
    - *on demand or otherwise, and*
  - *withdrawable*
    - *by cheque, draft, order or otherwise*
  - *using ~~electronic documents~~ binary expressions in the process of recording transactions and exchanging material instructions between the Banker and the Customer”*

Naavi

Advent of Internet banking

- Originated in 1997-ICICI bank
  - Now extended as a service by most banks
  - Viewing of Account transactions
  - Funds transfer within the bank (NEFT)
  - Fund transfer outside the banks (RTGS)
  - Bill payments
    - Virtual Banking scenario
    - Anywhere, Anytime Banking

E Banking and Virtual Banking

- Physical Existence
  - Virtual Banking Involves a Bank which may not have a physical existence
  - E Banking is a mode of transaction with a physical Bank
- Currency
  - Virtual Bank may use Virtual Currency and not use physical currency at all (eg: Linden Dollars, Game points, E bid coupons)
  - E Banking Is a mirror of physical banking and hence represents physical currency whose records are kept in electronic form
    - In India only Physical Society Banks can offer Internet Banking
    - All other bank like transactions need to be classified as E Commerce and not E Banking.

Card Banking

- Storage of Information
  - Magnetic Stripe or Chip
  - Elementary identity particulars or more
    - It is a data storage device or “Media” as per ITA 2008
    - The card swiping device reads the data and transmits the data.
      - It is a “Computer” as per ITA 2008
  - RFID tagged/Near field communication contact less cards
  - EMV standard with Microprocessor Chip

Social Media/E Mail Banking

- Facebook/Twitter
  - Send a message to the facebook page
  - Send a message to a Twitter account
  - Send payment to an e-mail address
    - Receiving Bank issues a payment authorization with a Pin acceptable at an ATM
- Customer ID is linked to the social media account/E Mail account
- Transmission of instruction is through the Internet

App based banking

- Bank specific App
  - Linked to a Bank
- Multi bank App (Wallet)
  - Is a Bank in itself.
- Apps that enable peripheral interaction with the core banking system
- Apps that are capable of carrying out full fledged transactions of money transfers in and out.

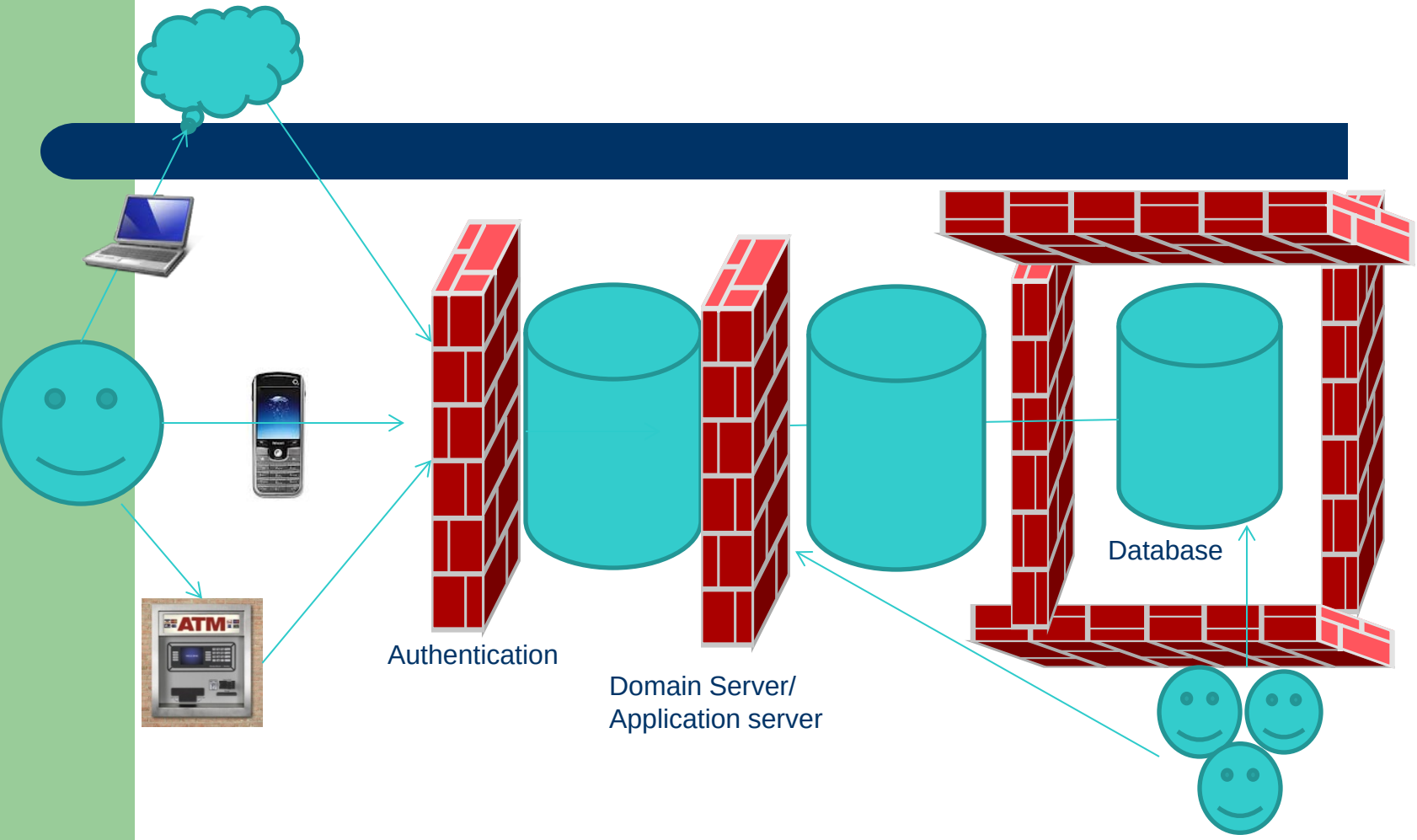
New Forms of Banking

- USSD Based Banking
- UPI
- IVR Banking
- Aadhar Based Banking
- Blockchain based Banking?

Technological Overview

- Electronic Documents held in a data base server
- Transaction applications are hosted in an application server
- Access is through an authentication gateway or Firewall

E Banking architecture



Naavi

Agenda

- Understanding Cyber Security
- Cyber Security Framework
  - Gopalakrishna Working group recommendations
  - Internet Banking Guidelines
  - Limited Liability Guidelines
- ITA 2000 and Digital Banking Challenges
  - Cyber Crimes in Digital Banking scenario
- Data Privacy Laws and the forthcoming legal issues
  - GDPR and PDPA 2018

Emerging Risks

Some Cases

- PNB Case
- Bank of Bangladesh Case
- ICICI Bank Case
- Bank of Muscat Case
- SBI Credit Card Fraud
- ATM Frauds
- BOM UPI Fraud
  - Stuxnet, OTP, Wannacry, Eurograbber, etc

PNB Case

- Suspected loss Rs 11,500/- crores
  - Similar to Harshad Mehta Case or Satyam Computers Case
    - Create a false asset and trade on them
    - If everything goes fine, fraud never surfaces
    - When things go wrong, there is a cascading effect accelerated by the media pressure

PNB Case

- Letters of Undertaking issued on behalf of PNB using the SWIFT messaging system
  - Based on which other banks gave loans
    - Lenders need to recover them from the borrowers failing which they have to initiate action against PNB.

PNB Case

- Is it a digital banking fraud?
  - Or is it the age old “Kite-flying fraud” in which digital communication played a part
  - What kind of digital and non digital controls could have prevented it?
  - Why no body could recognize the fraud earlier?
    - Was it a failure of the system design?
  - What controls should be there for issue of non funded liability creating letters?
    - At the time of issue
    - Before confirmation to the beneficiary?

PNB Case

- What is the root cause?
  - Every signature of an authorized official of the Bank has the legal effect of creating liability for the Bank.
  - Such signatures need to be Controlled, Managed and accounted for.
    - Whether they are in physical form or in digital form.
      - Have you heard of Section 7A of ITA 2008?
      - Have you heard of Section 3/3A/5 of ITA 2008?
        - Has there been a compliance of these in PNB?
        - Has Finacle been built of comply with law?

Bank of Bangladesh Case: $81 m

- Another Case involving Swift transactions
  - Executed with precision with the knowledge of holidays in Bangladesh and USA.
  - Passwords of officials were compromised
  - Attack carried out on Friday when Bangladesh was closed and USA was closed on the following two days
  - Instrument was a simple message from Bank of Bangladesh to New York Federal Reserve to transfer US$ 1 billion from the Nostro account of the Bank of Bangladesh
  - **Is Bank of Bangladesh responsible? Or SWIFT / or Federal Reserve of New York?**
    - Where did the fraud occur?
      - Bangaldesh? Or New York?

Warning signs missed

- First, all 35 messages used in the fraud lacked the names of “correspondent banks” – the necessary next step in the payment chain –That fault meant the orders could not immediately be fulfilled.
- Second, most of the payments were to individuals rather than institutions,
- And third, the slew of payments that morning was out of sync with the usual pattern of orders from Bangladesh Bank.
- Over the eight months to January 2016, Bangladesh Bank had issued 285 payment instructions to the Fed, averaging fewer than two per working day, None of those payments had been to an individual,
  - The U.S. central bank allows payments to individuals, but it’s not common and is generally discouraged,

Warning signals…

- When the first 35 messages from Bangladesh Bank were rejected for incorrect formatting, the hackers simply fixed the formatting and sent another 35 requests for payment to the same beneficiaries as before.
  - This time the New York Fed cleared five of them, despite the oddities.
  - They were properly formatted, SWIFT authenticated and went through automatically.
- The Fed monitors for unusual transactions, but its system had a weakness:
  - While credit card companies can spot unusual patterns in real time, the New York Fed typically looks back through payments, usually the day after they are requested, according to two of the former employees.

Phishing Attacks

- Umashankar Vs ICICI Bank Case
  - Customer responded to the phishing mail
    - Challenged for non use of digital signature in banking
    - Bank was held liable
    - Root cause was traced to non use of digital signatures as mandated by law and RBI
  - Use of Trojans does not need responding to the e-mail
- In Mobile Banking
  - SMS based text with hyperlinks can install malware to steal passwords or take over OTP responses

Disguised Attacks

- Coat tailing Trojan
  - When the customer is on an authorized session, the trojan sneaks in and conducts its own transactions
- Man in the Browser
  - Trojan alters the information entered by the customer in a web form before it leaves the computer making the receiving server believe that the altered information has actually come from the customer.

Bank of Muscat Card Fraud

- Hackers had targeted a credit card processor in India that handled transactions for prepaid MasterCard debit cards issued to customers of the National Bank of Ras Al-Khaimah PSC, or RAKBANK, in the United Arab Emirates.
- Card parameters altered from “Limited Prepaid Status” to “Unlimited Value”
  - At the systems of the back-end processors in India

Bank of Muscat Card Fraud

- US$45 million (Rs 250 crores) was withdrawn in cash through ATM in New York and 23 other countries on two days once in December 22 2012 and again in February 9, 2013
- The gang first struck December 22, 2012 and $5 million in cash in more than 4,500 ATM withdrawals in five accounts in 20 countries
- The gang struck again on February 19, beginning around 3pm and continuing until 1:30 the next morning.
- They withdrawals were made out of 12 prepaid card accounts in 24 countries who, within 10 hours, made off with about $40 million in a coordinated operation involving 36,000 ATM withdrawals.

The SBI Card Data Breach

- SBI recalled 6 lakhs debit cards suspecting a as a potential data breach
- A total of 32 lakh cards are estimated to have been compromised in the incident
  - Belong to multiple Banks

Source of the Data Breach

- HITACHI ATM machines/POS devices were compromised in one of the Yes Bank's Network and a malware gained entry.
- Malware wormed itself to the ATM Switch operated by NPCI and is suspected to have sniffed at all card transactions passing through for over 3 months until the breach was disclosed.
- More than 1000 fraudulent withdrawals have been reported.
- Hopefully the cards have been replaced and malware removed

WannaCry and Petya

- Wannacry-May 2017, Petya June 2017
- WannaCry was a ransomware which asked a ransom of 2 bitcoins
- Petya disguised itself as ransomware but was a Wiper malware designed to destroy data.
- Exploitation of Vulnerabilities of an old OS-WindowsXP
  - Even after the patch was provided by Microsoft
    - Enabled spreading in the network

ATM Frauds

- Fixing of Card skimmers and CCTV cameras goes undetected because there is no supervision on ATMs by Banks
  - ATMs must have an owner who is responsible..it does not always happen
- System deficiencies
  - Manipulation of the keys by matchstick insertion
  - Cash not removed fully
- Urgent Need
  - System modifications required to be addressed
  - Physical security has to be improved

BOM-UPI Fraud

- Rs 25 crores withdrawn from accounts in which there was no sufficient balances
  - UPI transaction successful
  - Not reflected in the back end CBS system
  - Even when CBS declined the transaction, Bank end UPI system used to send a successful response to NPCI
- Three Banks had used the same software but only Bank of Maharashtra suffered.
  - There was no back end check on whether the CBS system and UPI system were correctly synched

Lessons from these cases

- Security Risks can arise from multiple avenues
  - Our system, Customer's system, Websites, Apps hardware, software, etc
- We need to identify the threats and vulnerabilities and compute the risks so that effective mitigation steps can be initiated.
- Every Cyber Crime reported anywhere in the world is a lesson for us to learn
- Our IS management team should therefore collate such experiences and create knowledge which can be shared across the institution.

Concern for Security in Digital Banking

- Has been in existence since the introduction of technology in Banking in the 90's
- More recently, it has surfaced in the form of
  - Internet banking Guidelines June 2001
  - Banking Ombudsman 1995
    - Revised from time to time and extended to Digital payments
  - GGWG Guidelines April 2011
  - Cyber Security Framework June 2016
  - Limited Liability Circular July 2017 and its extension to PPI

Follow RBI Guidelines..

- Internet Banking Guidelines 2001
  - Declared Internet Banking as an extension of Banking…
    - Banker Customer relationship and inter-se liabilities as we understand over the years prevails
  - Consumer Rights prevail as per current laws and continue to be protected under Internet Banking.
  - Assume legal risk if digital signatures are not used
  - Banks to adopt Cyber Insurance to cover their risks

E banking Security Guidelines

- **GGWG Guidelines**
  - On April 29, 2011, RBI released the most comprehensive circular on E Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds
    - As a follow up of the G Gopalakrishna Working Group (GGWG)
      - This was a continuation of Internet Banking Guidelines of 16th June 2001 after SR Mittal Group

Legal Aspects of E Banking

Naavi

What is the Applicable Law?

- All laws and regulations applicable to Banking
  - RBI Act, Banker's Book Evidence Act, Banking Regulation Act, Negotiable Instrument Act, Consumer Protection Act, Indian Contract Act
  - Superimposed with the law applicable for use of electronic documents..ITA 2008
  - Payment and Settlement Act 2007
    - Under review now
- Regulations of RBI from time to time

What are the legal responsibilities

- Conduct Banking as per Banking law and regulations
  - If not, be responsible for the liabilities that may arise.
- Conduct Banking which is “Secure” from the view point of the customer
  - Besides protecting its own interests

Responsibilities under ITA 2000/8

- Enter into a valid Banker Customer Contract
  - Application form on paper? Terms on website?
- Enforceability of Click Wrap and Standard form contracts
- Enforceability of undigitally signed contracts and transaction instructions
- Responsibility for following insecure methods of storage, processing, transmission of sensitive personal data, critical banking transaction data, evidence handling
- Responsibility for omissions and commissions of outsource agents

When Fraud Occurs…

- Root cause could be
  - Criminal activity of an outsider
  - Negligence of the customer
  - Technology failure
  - Negligence of the Bank
  - Criminal activity of an employee

Principle of Proximate cause..

- When multiple factors cause a problem,
  - And between multiple innocent persons
  - he who had an opportunity to prevent last and failed to do so is more responsible than the others
    - The important point to note is that the proximate cause is the nearest cause and not a remote cause.

Vicarious Liability Principle

- Section 85 and Section 79 of ITA 2000/8 as well as IPC recognizes that
  - Liabilities can be borane by persons who have not been beneficiaries or perpetrators of a fraud
    - solely because they had a responsibility for security and were negligent.

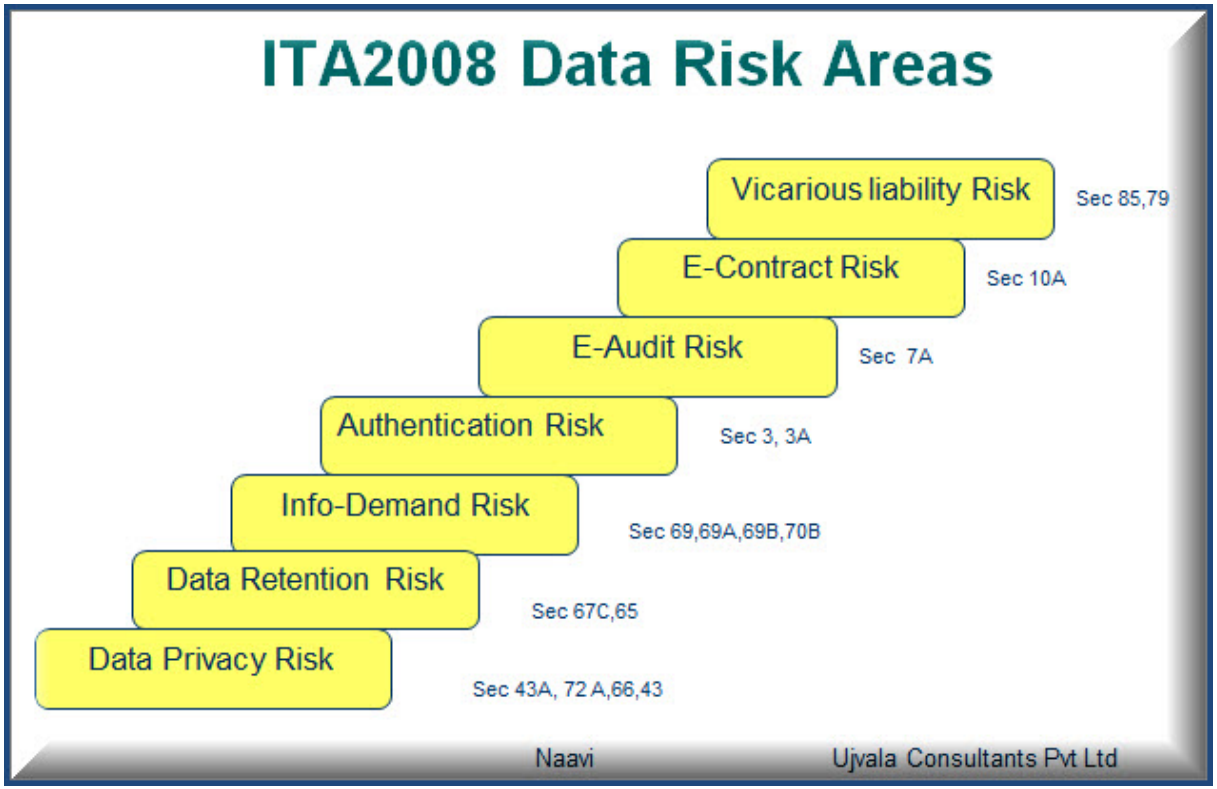
Direct Liability..

- Assistance and Abetment are considered equal to commission of a contravention under Section 43 and Section 84B
  - Passive Assistance can be implied through negligence

Bank’s Role….Cyber Security

- Reasonable Security Practice under Section 43A
- Due Diligence under Section 79
- Ability to provide assistance to designated authorities under Sections 69.69A,69B, 70B etc
- Ability to preserve evidence under Section 65 and other laws such as IPC

Where Liabilities can arise..



Bank's Role….Cyber Security

- ISO 27001 or PCI DSS etc are only means to an end and not the end in itself
- Banks Role is to maintain an infrastructure which takes into account all reasonable security measures to prevent losses occurring to its customers and to itself.
  - "Reasonable" is subject to interpretation and can be stretched
    - Principal guideline is the law of the land and includes what RBI mandates

Follow RBI Guidelines

- Cyber Security Framework of June 2, 2016
  - Continuation of GGWG guidelines of 2011
    - Continuation of the Internet Banking guidelines of 2001

Follow RBI Guidelines..

- Internet Banking Guidelines 2001
  - Wanted Banks to adopt Cyber Insurance
  - Assume legal risk if digital signatures are not used
- GGWG guidelines of 2011
  - Wanted Banks to mandatorily conduct ITA 2008 compliance exercise
  - Gave a comprehensive structure for information security management including
    - Organizational structure, Outsource agents management, Customer education etc besides technical requirements
      - How much of these guidelines we have complied with?

Follow RBI Guidelines

- Cyber Security Framework of June 2, 2016
  - Required a Gap analysis to be completed by July 31, 2016
  - Required compliance by September 30, 2016

Cyber Security Framework

- 24 baseline controls indicated
- Cyber SOC mandated
  - To include monitoring of zero day vulnerabilities
- Cyber Incidents to be Reported

Salient Features of the CSF-2016

- Board's responsibility increased
  - Board to be approved of the Gap report to be submitted to RBI (by July 31, 2016)
  - Board to approve Cyber Security Policy (by Sept 30, 2016)
- Continuous Surveillance indicated
  - Not "Audit" approach…good for the day and time the auditor signs off.
  - Requires setting up of an SOC either on its own or in consortium

Salient Features of the CSF-2016

- Banks to assume responsibilities for data with its sub contractors
  - suitable systems and processes across the data/information lifecycle need to be put in place by banks.

Salient Features of the CSF-2016

- Cyber Crisis Management Plan to be developed
  - Wider than the DRP/BCP
  - Should incorporate CERT IN and IDRBT suggestions
- CCMP Should address the following four aspects:
  - (i) Detection
  - (ii) Response
  - (iii) Recovery and
  - (iv) Containment

Salient Features of the CSF-2016

- Zero day vulnerabilities/attacks to be taken note of
  - Mere patching of vulnerabilities insufficient
  - Requires maintenance of Honeypots either on own or on consortium basis
- Ransomware/Cryptoware defense to be built
- Threats such as
  - business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.
    - to be guarded against

Salient Features of the CSF-2016

- Cyber Security Preparedness indicators to be developed and
- audits to be conducted against such measurable parameters
- Summary level information to be reported to RBI
- CISO Forum to be used for sharing information

Key Measures

- Phishing
  - Identify and Bring down Phishing websites ASAP
  - Use legally acceptable means of access and not commercially convenient methods
    - Digital Signatures instead of passwords or biometrics
  - Don’t Rely on 2F authentication
    - Neither legally sound nor technically secure

Website malware

- Watch every page of the Bank’s website in real time for injection of malware either through modified content or advertisements

ATM Watch

- ATMs are extended Bank premises
  - Includes ATMs managed by other Banks or agents
  - A Customer may consider his Bank as responsible for any loss arising out of his visit to the ATM.
  - Malfunctioning CCTVs, guards or installation of “card skimmers”, “lebanese loop”, “key blocking matchsticks”, etc are the responsibilities of the Bank

Five Commandments…R Gandhi, ED-RBI

- Thou shall know your customer
- Thou shall know your employee
- Thou shall keep your IT Systems up-to-date and free of all risky components
- Thou shall provide for maximum IT Governance
- Thou shall ensure continued Cyber Security Awareness

Essence of GGWG

Guidelines covered under 9 chapters

1. Information Technology Governance
2. **Information Security**
3. IT Operations
4. **IT Services Outsourcing**
5. IS Audit
6. **Cyber Frauds**
7. Business Continuity Planning
8. Customer Education
9. Legal Issues

Impact on Outsource Partners

- Under Chapter 2: (IS)
  - Digital evidence must be carefully tracked and documented and suitably authenticated
- Under Chapter 4 (Outsourcing)
  - Appropriate Governance mechanism should be instituted by the Board incorporating risk based policies and procedures to effectively identify, measure, monitor and control risks associated with Outsourcing

Impact on Outsource Partners.

- Under Chapter 4 (Outsourcing)
  - Define approval authority for outsourcing who should be the owner of the outsourcing arrangement
  - Evaluate Risks and communicate to Board
  - Perform due diligence evaluation
  - If there are multiple service providers for a single service, there should be a “Lead Service Provider”

Impact on Outsource Partners.

- Under Chapter 4 (Outsourcing)
  - Mandate Controls to ensure data security
    - Data confidentiality
    - Service provider's liability
    - Preservation of documents by service provider in accordance with legal provisions
  - Review on half yearly basis
  - Report adverse developments to RBI

Limited Liability for E Banking Frauds

July 6 2017

Essential Features of Limited Liability

- When a loss occurs on account of an E Banking Fraud, the fraud would be classified as
  - **A: Zero Liability Incident**
  - **B: Limited Liability Incident**

Zero Liability Incident

- The **“Zero Liability Incident”** is one in which the Customer shall not be liable and the Banks should reverse the amount lost within 10 days.
  - This is applicable when the security architecture and systems of the bank for electronic banking transactions are not able to protect the customer in case of
  - **a) Fraud or Negligence on the part of the Bank**
    - irrespective of whether the loss was reported by the customer or not
  - **b) Third party breach**
    - where the fault lies neither with the Bank nor with the customer and
    - the **customer notifies the Bank within three working days** of receiving communication from the bank regarding the unauthorized transaction
  - **C) after the customer reports** the unauthorized transaction to the Bank

Limited Liability Incident

- The **“Limited Liability Incident”** is one where the customer has to bear the loss to a limited extent and would cover the following cases.
  - a) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the Bank nor the Customer and
    - the customer notifies the Bank of the unauthorized nature of the transaction between 4 to 7 days
    - -the liability of the customer is limited to the lower of the transaction value or
      - Rs 5000/- (BSBD accounts)
      - Rs 10000 for accounts with average balance of upto Rs 25 lakhs and Credit card wuth limit upto Rs 5 lakhs, or
      - Rs 25000 for others

Limited Liability Incident

- **Involving Negligence of the customer**
  - such as sharing of payment credentials?
  - Not able to protect against malware?
    - Will the customer bear the loss?
  - Though the limited liability circular may hold that no protection may be available to the customer,
    - Judiciary may adjudicate differently
    - In a recent incident Ombudsman held that the liability has to be shared 50:50
    - Umashankar Case is a landmark case
    - Recent Kerala High Court case also supports that Bank should be liable

Policy for settlement

- Where the customer notifies the Bank after 7 days, the liability will be determined as per the Bank's approved policy.
- **Banks shall provide the details** of their policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts.
- Banks shall also display their approved policy in public domain for wider dissemination. The **existing customers must also be individually informed** about the bank's policy.
  - It is reasonable to expect that the liability will be still limited and cannot be 100% of the transaction value

Credit within 10 days

- Bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account **within 10 working days** from the date of such notification by the customer (without waiting for settlement of insurance claim, if any).
- **Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence.**
- The credit shall be value dated to be as of the date of the unauthorised transaction.
- Further the complaint shall be resolved by the Bank within 90 days failing which the Band should reimburse the amount to the customer ensuring that there is no interest loss to the customer.

Burden of Proof

- The burden of proving customer liability in case of unauthorised electronic banking transactions will lie on the bank.

Security Procedures to be adopted

- The circular mandates that the systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions.
- To achieve this, banks must put in place:
  - appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
  - robust and dynamic fraud detection and prevention mechanism;
  - mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events;
  - appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and
  - a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud

Mobile alert

- It is the Bank’s responsibility to ensure that a mobile alert is provided for “All Debits”.
- When an alert comes in, the customer needs to check and if the transaction is not authorized, he should immediately report to the Bank for which Bank should publish contact information and provide for a “Reply” to the message.
- If the customer is missing any alert, he should record it by informing the Bank and keeping record of such reports.
- If the customer is going abroad where he may miss the alert, he should ensure that the account is suitably locked or alternate arrangements are made by limiting the transaction limits.

Mobile alert

- Whenever the Bank receives any instruction from the customer, the banks should match the location of the transaction with the known location of the customer (eg: he is abroad or he is in the village when the transaction is reported from elsewhere etc).
- Even the OTP is answered from a mobile whose location is easily available to the Bank and if they are not having systems to monitor these, it should be considered as “Inadequate security” and challenged.

Mobile Alert

- We suggest that Banks introduce a system by which the transactions should have a mandatory gap of at least 5 minutes between two successive transactions to avoid such frauds besides an option to the customer to switch off the transactions any time he wants.
- Customers should be able to switch on the transactions at will and switch it off immediately after the transaction.
- For this purpose the alert should have an automatic option to switch off for a stated period like we put our WhatsApp on “mute” from time to time

Defining Case Laws

Umashankar Case was the eye opener

- The order of the Adjudicator of Tamil Nadu was released on 12th April 2010
  - Holding ICICI Bank liable for the loss suffered by the customer which was attributed to his answering a phishing e-mail
  - Upheld by TDSAT on 18th January 2019
    - Not following security guidelines is
      - "assistance" in commission of contravention
      - Section 85 is applicable for negligence

Umashankar Case-TDSAT

- For the purpose of Section 43(g), all assistance are to be considered as
  - misfeasance which is rendered by the charged person without permission of the owner or in-charge of the computer, so as to facilitate access to such gadgets “in contravention of the provisions of this Act, rules or regulations made thereunder”.
    - P.S: The customer was represented by Naavi at the Adjudication, CyAT and TDSAT under a power of attorney.
      - Presently a review on costs is pending

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- Customer is an NRI working in Brazil and holds an NRE account
  - Works in an of shore rig and stays in India 28 days for every 28 days of work
  - While in India, money was withdrawn in Brazil through ATMs in different locations
  - informed the Bank and ATM Card was blocked on the same day (26/3/2012)

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- SBI contended that the withdrawals are not possible from the account without his knowledge and hence SBI is not liable
- Loss is not caused due to any action or inaction of SBI
  - Trial court dismissed the suit. Appeal court reversed the decision. SBI went on further appeal.

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- It was also contended by the learned senior counsel that in a case of this nature, the plaintiff should have set the criminal law in motion in the foreign country for redressal of his grievance
- SMS alerts were given by the defendant to the plaintiff in respect of the disputed withdrawals, the plaintiff should have requested for blocking of the account immediately and in so far as the plaintiff has not responded to the SMS alerts given to him by the defendant, the defendant is not liable for the loss caused to him.

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- The relationship between a bank and its customer, in so far as it relates to the money deposited in the account of a customer, is that of debtor and creditor.
- Duties of care is an accepted implied term in the contractual relationship that exists between a bank and its customer
- It is impossible to define exhaustively the duties of care owed by a bank to its customer. …It depends on the nature of services extended by the bank to its customers.
- But one thing is certain that where a bank is providing service to its customer, it owes a duty to exercise reasonable care to protect the interests of the customer….Needless to say that a bank owes a duty to its customers to take necessary steps to prevent unauthorised withdrawals from their accounts.
- As a corollary, there is no difficulty in holding that if a customer suffers loss on account of the transactions not authorised by him, the bank is liable to the customer for the said loss.

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- Coming to electronic banking regime,
  - it is the obligation of the banks providing such services, to create a safe electronic banking environment to combat all forms of malicious conducts resulting in loss to their customers.
  - The basis of the said obligation is the implied term in the contracts entered into by the banks with their customers to exercise care to protect their money from transactions not authorised by them.

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- In short, there is also no difficulty in holding that
  - if a customer suffers loss in connection with the transactions made without his junction by fraudsters,
  - it has to be presumed that it is on account of the failure on the part of the bank to put in place a system which prevents such withdrawals, and
  - the banks are, therefore, liable for the loss caused to their customers.

Kerala High Court: SBI Vs P.V.George (9th January 2019)

- The defendant has no case that there is a contract between them and the plaintiff to the effect that if the plaintiff does not respond to the SMS alerts given by them regarding the withdrawals from his accounts, they would not be liable for the loss, if any, caused to the plaintiff.
  - Bank cannot be exonerated from the liability merely on the ground that the customer has not responded to the SMS

Advent of PDPA 2018

What is PDPA

- Personal Data Protection Act is a new legislation in the pipeline
  - Meant to protect the information privacy of individuals who share their personal information
  - The collectors of such information who are presently required to follow “Reasonable Security Practice” under Section 43A of ITA 2000/8 are now required to follow prescriptions under PDPA

Essence of PDPA 2018/19

- Redefines the Relationship between the Data subject and the Data Controller as a Fiduciary relationship
- Establishes DPA, Adjudicators, an Appellate Tribunal
- Establishes Codes and Practices, new Audit requirements
- Mandatory DPO, Mandatory annual Data Audit
- Recognizes Data Fiduciaries of different kinds
  - Significant Data Fiduciaries, Guardian Data Fiduciaries
- Emphasizes on Data Localization
- Applicability to Indian entities and Activities in India
- Has Criminal penalties
- Right to Forget is subject to Adjudication

Grievance Redressal Mechanism

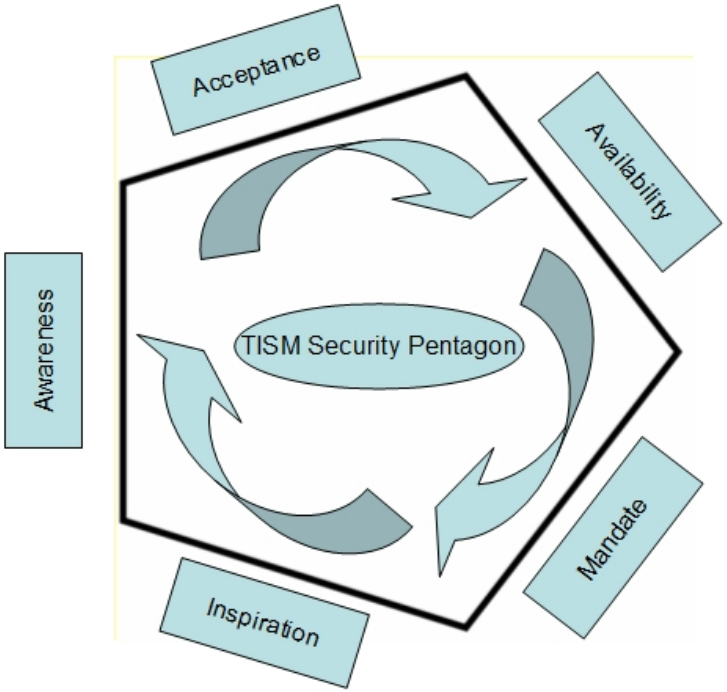
- Grievances may arise from Data Principals and relate to the execution of the Data Subject's Rights
  - Is my data being processed? If so what is being processed, why and how?
  - Is the data correct? Complete? Updated?
  - Data Portability?.. Data Provided, generated during the provision of services, part of the profile
  - Right to Forget?.. Is the purpose over?
    - Reference to Adjudication?
      - The Grievance Redressal officer may be different from DPO?

Compliance Challenges

- Compliance has three dimensions
  - Technical, Legal and Behavioural
  - Technology is not perfect and can be over ridden by determined hackers
  - Law is ruthless and imposes civil and criminal liabilities
  - Success of policies, procedures and use of preventive technology depends on the people and their attitude.

Compliance Challenges

- The biggest challenge is how to motivate our people for security.
- Motivation for security is a combination of Awareness, Acceptance, Availability, Mandate and Inspiration
  - Theory of Information Security Motivation



Structured Approach to Information Security (IISF309)

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			

Thank You

- Naavi
- www.naavi.org
- www.fdppi.in
- naavi@naavi.org
- 9343554943