

IMPACT OF ITA 2008 ON BANKERS

Naavi
Oct 25, 2010
ITC Windsor, Bangalore

LEGAL ENVIRONMENT UNDER TRANSITION

- ✖ Banking has been traditionally under the legal environment bound by legislations such as
 - + Contract Act
 - + Sale of Goods Act
 - + Transfer of Property Act
 - + Negotiable Instruments Act
 - + Banking Regulation Act

2

Naavi

TECHNOLOGY INTRODUCTION IN BANKS

- ✖ Banking which was once characterized by ledger books underwent changes in the 80s and 90s with the introduction of Computers at various stages
 - + From interbank reconciliation
 - ✖ To Automatic Ledger Posting Machines
 - ✖ To local area networks in branches
- ✖ By 2000 first steps had already been taken into
 - ✖ Core Banking and
 - ✖ Internet Banking

3

Naavi

ADVENT OF DIGITAL SOCIETY DAY

- ✖ 17th October 2000 changed the Legal environment in India
 - + Electronic Documents and Digital Signature gained Judicial recognition
 - ✖ Digital Contracts became a legal reality

4

Naavi

ITA 2000 GAVE LEGITIMACY

- ✖ ITA 2000 gave legitimacy to electronic documents and secured the Banking industry with the support from Judiciary.
- ✖ At the same time ITA 2000 became an important legislation that changed the legal environment of a Bank

5

Naavi

INTERNET BANKING GUIDELINES 2001

- ✖ Reserve Bank was quick to act and released a comprehensive guidelines on Internet Banking in July 2001
 - + When the country was still not having certifying authorities nor adjudicators
- ✖ By February 2003, RBI again took further steps by amending NI Act to introduce the concept of Truncated Cheques and Cheques in E-Form
 - + ITA 2000 also became applicable to Cheques for the first time

6

Naavi

BY 2008..2009....2010

- ✖ Technology environment in Banking had grown by leaps and bounds
 - + Almost all major banks are now on core banking mode
 - + Internet banking is available to customers by default
 - + Most banker-customer interactions are made through e-mails
 - + Mobile Banking is also slowly taking roots

7

Naavi

SECURITY CONCERNS

- ✖ As more and more Banks adopted technology.
 - + More and more traditional bankers became managers of digital banking environments
 - + More and more traditional customers started sporting credit and debit cards , passwords and PINs
 - ✖ Cyber Crimes in Banks started increasing.

8

Naavi

PRIORITIES CHANGED

- ✖ Pursuit of technology pushed the traditional Banking parameter of Security to the background
- ✖ Application developers hid vulnerabilities unmindful of the effect of Cyber Crimes in Banks on the social structure.
- ✖ Aggressive Banks in pursuit of higher revenue
 - + embraced technology with all its weaknesses and pushed it to the customers who were also not technically prepared to manage the increased risks

9

Naavi

ADVENT OF 2008

- ✖ Law intruded more firmly into Technology
- ✖ Mandated Information Security
- ✖ Defined Cyber Security
- ✖ Reinforced the concept of Due Diligence with
 - + Reasonable Security Practices and
 - + Data Retention norms
- ✖ Prescribed stringent punishments for non compliance

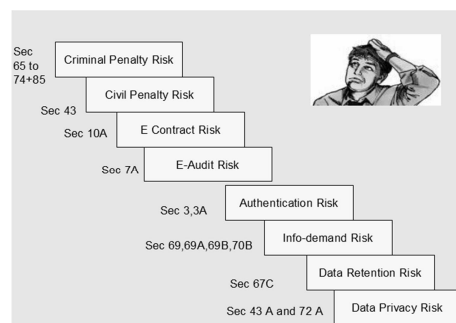
10

Naavi

AND BANKING WILL ...

.....Never be Same..here after

ITA RELATED RISKS TO BANKING



12

Naavi

ITA 2008....

✖ Data Privacy Risk

- + Requires Every Body Corporate handling Sensitive Personal Information to follow Reasonable Security Practices

- ✖ Failing which
 - ✖ the body corporate would be liable to pay compensation (no upper limit)
 - ✖ Could also lead to 3 year's imprisonment to the corporate executives who were negligent

13

Naavi

ITA 2008....

✖ Data Retention Risk

- + Section 67C
 - ✖ mandates specified data retention in specified formats

✖ Regulatory Agencies Information Demand Risk

- + Section 69, 69A and 69 B
 - ✖ empowers CERT IN with powers of interception, decryption, monitoring, blocking or demanding of data traffic information
 - ✖ Not assisting the CERT In when demanded can impose penalties on the company
 - ✖ To assist, companies need to put their compliance practices in place right now.
 - ✖ Designate a Compliance Officer whose name may have to be displayed on the website and in the annual report

14

Naavi

ITA 2008...

✖ Authentication Risk

- + Sec 3 and 3A along with Sec 5
 - ✖ mandate technical requirements of authentication of electronic documents

✖ E-Audit Risk

- + Sec 7A
 - ✖ mandates auditing of e-documents

✖ E-Contract Risk

- + Sec 10A along with Sec 4
 - ✖ mandates contractual obligations

15

Naavi

ITA 2008...

✖ Civil Penalty Risk

- + Sec 43
 - ✖ imposes civil penalties for different contraventions

✖ Criminal Penalty Risk

- + Sections 65, 66, 66A, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, 71, 72, 73, and 74
 - ✖ impose criminal penalties for various contraventions

16

Naavi

ITA 2008...EMPLOYEE CONTRAVENTIONS

✖ Vicarious Liability Risk

- + Section 85 and Section 79
 - ✖ extend contravention of any of the provisions of ITA 2008
 - ✖ by the use of any of the facilities of an organization
 - ✖ To the Company and its executives

17

Naavi

WHO TAKES THE RISK?

ITA 2008 says...

SECTION 85

SEC 85: OFFENCES BY COMPANIES.

- ✖ (1)Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is 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, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
 - + **Provided** that nothing contained in this sub-section shall render any such 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.

20

Naavi

SEC 85..CONTD

- ✖ (2)Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that
 - + the **contravention** has taken place 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 **shall also be deemed to be guilty** of the contravention and shall be liable to be proceeded against and punished accordingly.
 - + **Explanation-** For the purposes of this section
 - (i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
 - (ii) "Director", in relation to a firm, means a partner in the firm

ITA 2008 says...

SECTION 79

SEC 79: EXEMPTION FROM LIABILITY OF INTERMEDIARY IN CERTAIN CASES

- ✖ (1)Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him
- ✖ (2) The provisions of sub-section (1) shall apply if-
 - ✖ (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
 - ✖ (b) the intermediary does not-
 - ★ (i) initiate the transmission,
 - ★ (ii) select the receiver of the transmission, and
 - ★ (iii) select or modify the information contained in the transmission
 - ✖ (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)

SEC 79..CONTD

- + (3) The provisions of sub-section (1) shall not apply if-
 - + (a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act
 - + (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner
 - ✖ .Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary

23

Naavi

24

Naavi

RBI..says

INTERNET BANKING GUIDELINES..

RBI SAYS. YOU ASSUME LEGAL RISK FOR NON COMPLIANCE

- + “From a legal perspective, security procedure adopted by Banks for authenticating users needs to be recognized by law as a substitute for signature. In India, Information Technology Act 2000, in section 3(2) provides for a particular technology (Viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by Banks for authentication should be recognized as a source of legal risk”
 - × Para II (b) Internet banking Guidelines July 2001

26

Naavi

GET INSURANCE..SAYS RBI

- × “Considering the banking practice **and rights enjoyed by customers in traditional banking, bank’s liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technology failure etc needs to be assessed and banks providing Internet banking should insure themselves against such risks**” ..(Para II e) Para II (b) Internet banking Guidelines July 2001

27

Naavi

SEBI Says

CLAUSE 49 LISTING NORM

CLAUSE 49 CERTIFICATE..

- × attached to Annual Reports of listed companies..
 - + ..” these statements present a true and fair view of the company’s affairs and are in compliance with existing accounting standards, **applicable laws** and regulations”
 - × Provided by the CEO and CFO

29

Naavi

THE ROAD AHEAD

- × Conduct an ITA 2008 Compliance Audit
- × Identify Gaps in implementation
- × Initiate Compliance implementation measures
- × Get Certified for action taken
- × File with every annual report

30

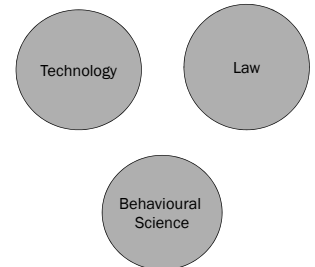
Naavi

RECOMMENDED APPROACH

THREE DIMENSIONS OF INFORMATION SECURITY

Recognize that there are three dimensions to Security.

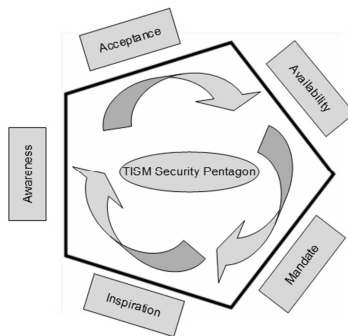
-ISO based Technology Approach
Supplemented with ITA 2008 based Legal Approach
Further supplemented with
-Behavioural Science Approach of harnessing human resources for security implementation



32

Naavi

EXPLORE..THEORY OF IS MOTIVATION



33

Naavi

USE IS REFERENCE FRAMEWORK

IS Reference Framework..IISF 309.3

Organization	Top Mgt	HR	Admin /Business	IT
Assigned Responsibility	Privacy and Security Practice Statement	Employee Awareness	Client Consent	Information Classification
Monitoring-Testing-Revision Policy	Documentation Policy	Employee Declaration	BA Agreement	Physical Access
	Audit Policy	Employee Cyber Usage Policy		Logical Access
	Web Presence Policy	Employee Media Usage Policy		Information Storage
	Hardware Policy	Employee Background Check		Information Transmission
	Software Policy	Sanction policy		Incident Management
	Grievance Redressal Policy			Contingency

34

Naavi

BE CYBER LAW COMPLIANT

....Be Protected

THANK YOU

..... QUESTIONS?

naavi@vsnl.com
9343554943
www.naavi.org