Cyber Security & Internet Technology Laws in India

By
Naavi
(LBSIT on 24th Feb 2011)

1 Naavi

What is Cyber Security?

- There could be different Perspectives
  - IT professional's Perspective
  - Law Enforcement Perspective
  - Netizen perspective
  - Managerial Perspective

2 Naavi

IT professional's Perspective

- Security is an Extension of "Quality"
  - Technical perspective
  - It's Voluntary
  - Non compliance is not punishable but required to meet quality standards
    - Technical perspective of information security ends with DRP and BCP

3 Naavi

Law Enforcement Perspective

- Security is an obligation to the society to prevent crimes
  - Both to the Netizen as well as the service providers
  - It is a Mandate
  - Non compliance could result in loss of money or imprisonment
    - Security in the end means conviction of the offender

4 Naavi

Netizen's Perspective

- Security is part of the service offering
  - If I am told that I can keep a deposit in the Bank and will get 15% p.a. return but there is a one in 10,000 chance that my money will be wiped out by a Phishing fraud
    - I may not like to avail the service at all
- Lack of security in service is therefore "Deficiency of Service"
  - Security in the end means recovery of loss

5 Naavi

Managerial Perspective

- Security is a business necessity
  - I want my information to be secure from being stolen, compromised, altered or blocked from genuine users
  - In the unlikely event of a security breach, I donot want to be saddled with any liability, civil or criminal
    - Security perspective ends with Defensive Legal Protection (DLP) and Offensive Legal remedy (OLR)

6 Naavi

How does Indian Law address these different perspectives of Security?

- Mandate security but yet leave scope for managerial discretion
- Protect Consumer rights
- Provide protection against vicarious liabilities on corporate executives?
- Provide support to law enforcement to investigate and prosecute without unreasonable barriers
  - ITA 2008 addresses these requirements with reasonable efficiency

7 Naavi

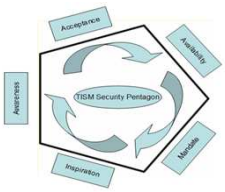
Recommended Approach to Security

- Three Dimensional Approach
  - Security is an outcome of
    - Technical Aspects
    - Legal Aspects
    - Behavioural Science Aspects of people

8 Naavi

Theory of Information Security Motivation

- Security Pentagon Model of Motivation built on five parameters
  - Awareness
  - Acceptance
  - Availability
  - Mandate
  - Inspiration



9 Naavi

Internet is a platform..

- Internet is a "technical platform" that facilitates
  - Communication
  - Data Storage
  - Data Processing
- Used for
  - Social Networking
  - Entertainment
  - Education and Information Sharing
  - Governance
  - Commerce etc

10 Naavi

Providing a "Secure Platform"

- Requires
  - Understanding the cyber laws and incorporating compliance of laws into our software and the service
  - Identify Cyber Crimes and provide relief to victims
  - Understand where and how to collect cyber Evidence, and how to present it to the Judiciary.
  - Identify managerial requirements in Cyber Law Compliance
  - How to educate the next generation to help them prepare for facing the digital world

11 Naavi

The Risks Ahead

- E Mails have become the "Address" for people
  - Can be used not only for sending birthday greetings but also legal notices
- Websites/Blogs have become "Means of Digital Expression"
  - Can convey marketing messages and can also create warranties and liabilities associated therewith
  - Facebook can not only create contacts but also deface reputations

12 Naavi

More the use, More the Risk

- Our money in Banks
- Our property documents in the Registrar's office
- Our ID in the UID office
- Our personal Reputation on the web
- Our confidential information with Tax authorities..etc
  - Lack of security may hurt us in many ways

Some Examples

- Defacement of websites
- BOI website
  - Virus on visit
- Spam and Denial Of Service
- Phishing
  - Bank accounts
  - Employment
- Forgery on the Web
  - Credit Card/Bank transactions
- Reputation loss
  - Tampered profiles on Orkut, Face book
    - Terrorists are using all these offences to further their objectives
    - Enemy countries are using all these offences to conduct cyber wars

Netizen's Ask..

- Can we have
  - Risk free Internet Presence?
  - Anonymity?
  - Pseudonomity?

How does Law address these issues?

- By providing legal recognition for electronic transactions
- By defining basic norms for usage of IT and making contraventions punishable
  - Civil and criminal liabilities
- By making intermediaries and service providers adopt certain security provisions and making "negligence" punishable with vicarious liabilities
- By facilitating technology tools for security and providing infrastructure support
- By providing implementation support though appropriate law enforcement and judiciary systems tailored for the cyber law regime

Legal Recognition

- Sec 4: Electronic Documents
  - Exception as per Sec 1(4)
    - Bill of Exchange/Promissory Notes
    - Will, POA, Trust
    - Documents of transfer of interest in immovable properties
- Sec 5: Digital/Electronic Signature
- Sec 11: Attribution
- Sec 13: Time and Place of Message

Civil Liabilities

- Civil Liabilities
  - Sec 43: 10 types of contraventions
    - Unauthorized
      - access/download/virus/damage/disruption/denial of access/assistance/charging another person/diminishing value/concealing,destruction
  - Sec 43A: Sensitive Personal Information to be protected with Reasonable Security Practice

Criminal Liabilities

- Sec 65-Deletion of data/evidence
- Sec 66- 10 different offences linked to Sec 43
- Sec 66A-e-mail harassment, Phishing
- Sec 66B-stolen devices
- 66C-Identity Theft
- 66D-Impersonation
- 66E-Voyerursim
- 66F-Cyber terrorism

19 Naavi

Criminal Liabilities

- Sec 67-obscenity
- Sec 67A-Obscenity-sexually explicit material
- Sec 67B-Child pornography
- Sec 67C-Retention of data
- Sec 69-Interception
- Sec 69A-Blocking of websites
- Sec 69B- Data Traffic
- Sec 70-Protected Systems
- Sec 71-Misrepresentation-digital signature
- Sec 72-Confidentiality
- Sec 72A- Privacy
- Sec 73: Misrepresentation-digital signature
- Sec 74: Fraud-digital signature
- Sec 84A
- Sec 84B

20 Naavi

Intermediary liabilities

- Sec 79
  - Intermediaries
- Sec 85
  - Companies and Company executives

21 Naavi

Technology tools

- Digital Signature
  - PKI based
- Electronic Signature
  - Open to other technologies

22 Naavi

Law Enforcement and Judiciary

- Sec 75-Jurisdiction
- Sec 80-Police Powers
- Sec 84B-Abetment
- Sec 84C-Attempt
- Sec 46-Adjudication
- Sec 57-CAT

23 Naavi

Law Enforcement and Judiciary

- Sec 65B of Indian Evidence Act
  - Electronic Evidence as can be seen converted into printed copies

24 Naavi

Cyber Security is now legally defined

- Cyber Security Defined [Sec 2(nb)]
  - Protecting information, Equipment, devices, communication device and information stored there in from
    - Unauthorized access, use, disclosure, disruption, modification or destruction
- Reasonable Security Practices
- Due Diligence
- Sec 70B-CERT In powers

25 Naavi

Summary

- ITA 2008 defines several offences for the purpose of protecting the cyber environment
- Supports with innovative options for evidence provision
- Mandates security for service providers
  - If we know what is there in ITA 2008 and comply as a society, we may have a more secure Internet experience

26 Naavi

Role of Technology Students

- Understand technical aspects of Cyber Law
- Understand Cyber Security and Cyber Forensics
- Apply Security at work
- Develop Cyber Law Compliance products
  - Eg: E-Audit Tool

27 Naavi

Thank You

Naavi@vsnl.com
www.naavi.org

28 Naavi