ITA 2008- The Road Ahead for IS Professionals

By
Naavi

Presentation delivered at ISACA, Bangalore Chapter on April 18, 2009

The developments in the IT field in the last few years have brought Information Security to the forefront of IT business management.

In the early days, Information Security was a cover against the technical mishaps that could destroy information. This required appropriate back ups solely because the system may get corrupted due to multitude of reasons including bugs in software.

Then in the early days of Cyber Crimes, it was the "Script Kiddies" who were out to show their expertise by hacking into corporate systems and leave their stamp of expertise in the form of defacement of a website or a corporate document. The intention at this stage was not either a commercial gain or fundamentally malicious. At this stage the requirements of Information security was extended to maintenance of simple Firewalls to prevent unauthorized intrusions through IP filtering etc. Some first generation viruses were also used by the script kiddies and IS professionals needed to use appropriate anti virus software.

Gradually, the cyber criminals sought financial benefits in their hacking activities and focused on theft of information, corporate espionage etc using more sophisticated tools. There were organized crime syndicates which acted at different levels such as "Identity Theft", "Hacking", "Denial of Service Attacks", "Creation of exploits that could be used at a later time for extortion" etc.

At this time, in order to protect the E-Commerce and the E-Economy, it became necessary for law to intervene and place deterrents in the form of punishments for offences. As a result Cyber Crime laws started emerging in different countries which made Cyber Crimes punishable. Since Cyber Crimes arose due to "Security Breach Incidents", there was a close link between the Crimes and the security implementation. Law not only punished the offender, but it also raised the issue of "Assistance" and "Complicity" and brought in third parties within the network of law. The law also recognized the concept of "Vicarious Liability" and "Need to practice Due Diligence". This brought Information Security professionals and corporate executives also within the long arm of the law both as compliance officers as well as possible offenders themselves.

At the same time, a new generation of Information Security Professionals in the form of "Security Auditors" emerged as Trusted third party examiners of the Information Security practices and certifying them as adequate. These were the "Information Security Auditors".

At this stage itself, some far thinking Information Security specialists started recognizing the need for Cyber Law Compliance as a part of Information Security practice.

However, the Core community of Information Security Professionals focused only on hardening of the security aspects and did not adopt legal compliance as a part of security. As a result while "Information" was protected in most cases of security breach, the "information Security owner" was left to face the consequences of the termporary security breaches both in terms of "Reputation Loss" as well as "Liability to third parties".

Though the professionals could restore lost data through effective DRP and BCP implementations, the owners did not have ability to protect themselves against legal claims nor enable them take legal action against outsiders who caused the loss.

It has slowly dawned on the Information Security community that if Technical Security is fortified with Legal Compliance, the resulting "Techno Legal Information Security" would provide what can be called DLP-OLR protection.

The DLP-OLR (Defensive Legal Protection-Offensive Legal Remedy) protection means that as a result of the security breach incidence, the information owner would be able to defend himself from liabilities and also take legal action against outsiders to recover its losses.

In the recent days, law has also been hardened with the requirement of "Legal Compliance" as a part of "Information Security Practice" being made mandatory. This trend has been seen in US laws such as HIPAA, GLBA, SOX etc.

Now the Indian law is also following a similar trend and in ITA 2008, there has been an attempt to prescribe several aspects of Information Security as a part of law.

While ITA 2000 was enacted with an objective of E-Commerce Promotion, ITA 2008 (ITA 2000 as amended by Information Technology Amendment Act 2008) has focused on "How to make the Cyber Space Secure". In view of this the Information Security industry in India has undergone a major shift in focus which has to reflect in the activities of the community of Information Security Professionals.

While the Information Security professionals in the industry have to incorporate Legal Compliance into their Technical security infrastructure, the Information Security auditors will also have to become "Techno legal information security auditors". In practical terms it may mean that in future, Information Security Teams must have Cyber Law specialists as part of the team.

The Key Elements of ITA 2008 Compliance

The first aspect we may note about ITA 2008 is that it provides a legal definition for "Cyber Security" under Section 2(nb) and sets up an apex Information Security Agency

in India under Section 70(B). This Cyber Security Regulatory Agency which may be called the "Computer Emergency Response team" (CERT) will prescribe guidelines for information security, monitor its practice, have powers to order penalties etc.

The Act through the rules to be notified will notify "Data Retention Norms", "Traffic Data Storage requirements" , "Reasonable Security Practices" etc. It will also have powers to intercept, monitor, Block, decrypt data in the hands of the Intermediaries and IT Companies if required.

Some of the important sections and their implication on compliance are as follows:

Section 43A requirements

Under Section 43A responsibility has been cast on Companies for Data Protection and to create a liability in case the Company is "negligent in implementing and maintaining reasonable security practices and procedures"

For the purpose of this section, "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 the time being 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.

For the purposes of this section, "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.

The Government is expected to define "Sensitive Personal Information" and it is the responsibility of "Body Corporates" to ensure that reasonable security practices are followed.

The IT and ITES industry should therefore first examine their SLA and in its absence examine if there is any law that directly affects their activities. If neither are there, then the security practices to be specified by the Government as a follow up of ITA 2000 would be followed. In the event SLA makes a mention of security practices as defined in

Data Protection Act or HIPAA or GLBA etc, then that will take precedence over any other security practice.

Section 67C requirements

Section 67 C prescribes that 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"

Contravention of this section has criminal consequences and

> Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

An Intermediary is also a member of the IT industry and the definition in Section 2(w) is wide enough to include many service providers.

The definition states:

"Intermediary" for this section 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.-

It is clear that a very large number of IT companies come under the scope of the section 67C.

We are awaiting the notification regarding the time for which specified information needs to be preserved under this section. It could be one year in the minimum and six to seven years at the outer end.

What is important to note is that any alleged non compliance could expose the Company and its executives to the penal provisions of this section as well as section 65. Since this is a "Cognizable" offence, any "Inspector" of Police can now start questioning the CEO of a BPO if he is preserving the information in tact etc.

Section 72A requirements

Section 72A provides criminal liabilities for not protecting data. According to this section

-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

Further, under Section 85, the liabilities that fall on a company under this section will extend to any officer in charge of business or director etc unless "Due Diligence" is proved.

Section 79 requirements

Section 79 provides certain immunity from liability to “Intermediaries” which however is subject to certain preconditions such as

That the Intermediary

(a) 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

(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 expeditiously removes or disables access to that material on that resource without vitiating the evidence in any manner

Section 69, 69A and 69B requirements

Further the powers that the Central Government or the State Government exercises under the sections 69, 69A and 69 B also imposes liabilities on a Company which needs to be addressed during compliance.

Under Section 69, 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 direct any agency of the appropriate Government

to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource and any any person who fails to assist the agency shall be punished with an imprisonment for a term which may extend to **seven years** and shall also be liable to fine.

Under Section 69A, the Central Government or any of its officer specially authorized by it in this behalf may

block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource and any intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to **seven years** and also be liable to fine.

Under Section 69 B, The Central Government may, monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource and 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.

Additionally, any Company would be required to set up reasonable precautions to prevent contravention of Section 43 or any other sections of the Act failing which the Company may be accused of the contravention directly and also make its executives liable because of Section 85.

It would therefore be necessary for Companies as well as Information Security Auditors to develop appropriate "Techno Legal Information Security Standards" that would meet the requirements as per the Act.

Naavi's Cyber Law College has developed one such standard in the form of an "Information Security Framework" titled IISF-309 with the following 7 basic principles, further expanded into 21 compliance specifications.

Basic Principles:

1) Designate a Cyber Law Compliance officer
2) Initiate training of employees on Cyber Law Compliance
3) Introduce sanction procedures in HR policy for non compliance
4) use authentication procedures suggested in law
5) Maintain data retention as suggested under Section 67C
6) Identify and initiate safeguard requirements indicated under Sections 69 and 69A, 69B
7) Initiate global standards of data privacy on collection, retention, access, deletion etc

21 Compliance Specifications of IISF-309

Specifications of IISF-309

Number	Description	Level 1	Level 2	Level 3
IISF 1	**Client Consent**	A letter of consent to be obtained (in a form acceptable under ITA 2008) on behalf of every data subject from the data vendor to outsource the data as per the Privacy and Security Practice Statement, a copy of which must be made appropriately available to on the website. Every version of the statement from the date of inception of the Policy shall be archived and the vendor is notified of any changes subsequent to the date of consent with an option made available to the vendor to refuse the changes.	Same as Level 1	Same as Level 1

IISF 2	**Employee Awareness**	Every Employee of the Organization shall be made aware of the information privacy and security policy of the organization as contained in the Privacy and Security Policy Statement (PSPS) and other initiatives undertaken by the Organization towards its implementation. The employees shall also be adequately trained in the use of any software or hardware devices used for the implementation of the policy. Every employee shall undertake a "Test of Awareness" at least once each year and the performance documented in the employee service records.	Same as Level 1	Same as Level 1
IISF 3	**Employee Declaration**	Every Employee shall sign a declaration of Ethics in duplicate agreeing to abide by the requirements as required under the PSPS a copy of which is kept along with the service records of the employee. One copy is returned to the employee.	Same as Level 1	Same as Level 1
IISF 4	**Assigned Responsibility**	The responsibility for Privacy and Information security compliance shall be allocated to an official who shall provide periodical compliance reports and certificates to the management every month. The official may be holding any other responsibility additionally.	Same as Level 1	Same as Level 1

IISF 5	**Employee Background Check**	Every employee's background is verified with reference to the documentary evidences submitted during the time of his employment in the application.	In addition to level-1 requirements the background is verified with reference to the "Referees" indicated in the application with written with reference to the "Referees" indicated acknowledgements duly verified for correctness.	In addition to level-1 and level 2 requirements, the H R manager shall provide a declaration to the management that the background verification has been completed as required
IISF 6	**Information Classification**	Information handled by the organization shall be classified appropriately on the basis of its sensitivity. The classification tag shall enable assignment of designated employee force for access on a need to know basis and management of access privileges	Same as Level 1	Same as Level 1
IISF 7	**Employee Cyber Usage Policy**	The employees will be bound by an ethical declaration and subject to a self impose discipline as defined in the security policy documents.	In addition to level-1 requirements, the employee activities on the Internet would be fully monitored and logs archived for both real time and post event audit. Any violations will be suitably recorded and sanctions invoked.	In addition to level-1 and level 2 requirements, the employees will be allowed to use Internet only to the extent of pre-defined business purpose and a suitable firewall controlling access will be used.
IISF 8	**Media Usage Policy**	The employees will be bound by an ethical declaration and subject to a self imposed discipline as defined in the security policy documents	In addition to level-1 requirements, restrictions would be imposed on the use of external media and laptops to reasonably prevent unauthorized copying of data.	In addition to level-1 and level-2 requirements, employees will have access to data only through a remote access environment from thin clients and no data would be permanently storable in the local machines except under specific authorizations and in a secure manner

IISF 9	**Sanction Policy**	Appropriate sanctions will be imposed for violations of any of the security policies with the sanctions being commensurate with the nature of violations.	In addition to level-1 requirements, suitable clauses would be introduced in the employee contracts and NDAs to be signed by the employees.	In addition to level-1and level 2 requirements, NDAs are obtained both at the time of employment and at the time each major assignment is handled.
IISF 10	**Privacy and Security Practice Statement**	Organization will develop a detailed Privacy and Security Policy Statement which would be approved by the Board and signed by the CEO and CTO. The statement would be adequately communicated to all the employees as well as the clients and business associates of the organization. A copy should be made available through the website of the Company. The organization may develop different versions of the statement for the public and internal use as the management may find it necessary.	Same as Level 1	Same as level 1
IISF 11	**Physical Security**	Organization shall have appropriate policies and procedures to ensure that only authorized persons will have access to the working area containing IT assets including the Wireless perimeters. An appropriate documentation would be maintained for guest access provided.	In addition to level-1 requirements, the access points shall be monitored by appropriate electronic access monitoring devices.	In addition to level-1 and level 2 requirements, the entry and exit of authorized persons to the work area would be linked to the attendance and any anomalies recorded as a security breach incident.

IISF 12	**Logical Access Security**	Policies and Procedures shall be implemented for ensuring that access to any IT device is made available only with appropriate access authentication such as Passwords. Appropriate measures shall be initiated for ensuring that a strong password policy is maintained across the organization.	Same as level 1	Same as level 1
IISF 13	**Information Storage Security**	Policies and Procedures shall be appointed to ensure that information under storage is accessible only by authorized persons on a "Need to Know" basis.	In addition to level-1 requirements information under storage is kept in encrypted for. .	In addition to level-1and level 2 requirements, access shall be backed up by data integrity control, audit trail monitoring and archival.
IISF 14	**Information Transmission Security**	Transmission of Information into and out of the systems would be monitored by a suitable Firewall and appropriate polices and procedures shall be implemented to ensure that viruses and other malicious codes are filtered effectively.	In addition to level-1 requirements, appropriate audit trail would be maintained and archived to ensure future reference if required. All confidential mails shall be appropriately encrypted.	In addition to level-1 and level 2, requirements all outward mails likely to cause any liability to the organization shall be digitally signed by the sender.
IISF 15	**Hardware/Software Policy**	Policies and Procedures shall be put in place to ensure that any hardware or software or hardware used by the organization is certified by the supplier to be free from known security vulnerabilities.	In addition to level-1 requirements, Policies and procedures shall be put in place to ensure that Hardware and Software used by an organization shall be tested by a third party security auditor and certified to be free of known security vulnerabilities.	In addition to level-1 and level 2 requirements, Policies and Procedures shall be put in place to ensure that Hardware and Software used by the organization is backed by a source code audit certificate from a third party.

IISF 16	**Web Presence Policy**	Policies and Procedures shall be put in place to ensure that the domain name, hosting facilities and content used by the organization is adequately protected against malicious attacks, unauthorized alteration and IPR infringement. Suitable Privacy Policy and Disclosure Documents indicating the identity of the owner of the web content shall be provided on the website of the organization.	In addition to level-1 requirements, the web content is monitored by the organization at periodical intervals and self certified for data integrity.	Same as level 2
IISF 17	**Grievance Redressal Policy**	The organization shall designate an official as "Security Grievance Resolution Officer" (SGRO) to be the single point contact person accountable for handling all disputes related to the information security and contact details of such a person including e-mail and physical address is provided on the website.	In addition to level-1 requirement, the organization shall also designate an external person of repute as an "Ombudsman" to resolve the disputes which cannot be resolved by the SGRO.	In addition to level-1 and level 2 requirements, the organization shall also set in place an arbitration mechanism to handle disputes which are not resolved by the Ombudsman.
IISF 18	**BA Agreement Policy**	Policies and Procedures shall be put in place to ensure that the Information security responsibilities of an organization shall also be followed by any external agency which is provided access to the protected information by a suitable contractual arrangement with appropriate indemnity provisions.	Same as level 1	Same as level 1

IISF 19	**DLP-OLR Policy**	Policies and Procedures shall be put in place by the Organization to maintain incident monitoring system and an appropriate Disaster Recover and Business Continuity Plan to meet any contingencies arising out of security breach incidents.	In addition to level-1 requirements, appropriate evidence archival systems shall be maintained to ensure capability for "Defensive Legal Protection" against any liability claims that may arise on the organization	In addition to level-1 and level 2 requirements. appropriate evidence archival systems shall be maintained to empower the organization to launch "Offensive Legal Remedy" procedures
IISF 20	**Policy Documentation**	The organization shall retain all Policy documents related to information security for a period of a minimum of 3 years either in print or electronic form. Data which is part of a security breach incident, is kept indefinitely.	Same as level 1	Same as level 1
IISF 21	**Management Certificate/Audit Policy**	The operational management shall submit a certificate of compliance of information security to the Board of Directors once a year recording there in the observed short comings and how they are proposed to be remedied with appropriate implementation schedules.	In addition to level-1 requirements, the Board of Directors shall incorporate a certificate of compliance of information security in the annual report to the share holders of the Company recording there in the observed short comings and how they are proposed to be remedied with appropriate implementation schedules.	In addition to level-1 and level 2 requirements the Board of Directors shall incorporate a certificate of compliance of information security in the annual report to the share holders of the Company recording there in the observed short comings by an external auditor, the management's perceptions and how the management proposes to meet the audit suggestions.