The Buck Stops Here.. What should I do?

Every Corporate Manager understands that dependency of corporate business on Information and the need to secure it. But where we often differ is "Who is Responsible for the Information Security" in an organization.

For a long time, Information Security (IS) was the baby of the Information Technology (IT) Department in an organization essentially because no body else understood it. But after Enron, the advent of SOX and other legislations, it is becoming increasingly clear that the responsibility for IS reaches upto the Board of Directors because of the concept of "Vicarious Liability" of top management for maintaining "Reasonable Security Practices" in a Company.

This note explores some of the strategic changes which the top management of a company should initiate to meet the regulatory challenges that are becoming the order of the day.

[This article is contributed by Naavi, Founder Secretary of Cyber Society of India]

Changing Profile of Information Security

Traditionally, "Information Security" in IT Companies (Which includes all forms of Telecom companies and manufacturing companies using IT) has been focusing on "Prevention of Unauthorized Intrusion" into corporate information space. In practice, this translates into better management of "Computer Access" with the use of appropriate Firewalls besides physical security measures. At a slightly advanced level the "Access Security" has been extended further to using appropriate "Intrusion Detection Systems" which provide early warnings and automated security responses to potential threats. Incident management systems are a part of such an exercise as also the "Disaster Recovery and Business Continuity Plans" (DRP-BCP). This "Technical approach to Information Security" was basically a response from the IT industry to maintain "Efficiency", "Reliability" and "Quality" of the services rendered.

In the recent days, regulators at various industry levels have recognized the dependence of the society on "Information" lying inside Computer systems and accordingly are imposing statutory responsibilities on the IT industry that they need to take suitable safeguards to "Protect Information" from being misused. Such protection may be to prevent occurrence of Cyber Crimes or to protect the "Privacy Rights" of citizens. Hence the measures of Information Security which the industry was taking in its own interest, has now become an obligation under laws. This introduces "Legal Compliance" as an essential business objective of any corporate management.

Information therefore needs to be secured today not only from the point of view of "Disaster Recovery" and "Business Continuity" but also for meeting the compliance requirements. Non compliance of any legal provision results in a liability on the Company or the individual managers and therefore results in loss of revenue or loss of human resources of a company. A security approach which protects information in such a manner that it protects the company and its managers is "Techno Legal Information Security" and "Legal Compliance" is a part of this security approach.

Under the Techno Legal Information Security approach, a Corporate entity takes such measures as are required to ensure that it possesses "Defensive Legal Protection" (DLP) against liabilities as well as the "Offensive Legal Remedy" (OLR) to use the statutory provisions to recover damages from who so ever caused injury to information residing inside a computer resource.

This DLP-OLR based security is an extension of the DRP-BCP based approach and Legal Compliance is the essential ingredient of this paradigm shift in Information Security approach of industries.

Hence "Legal Compliance" is today considered a very essential part of IT industry management.

Responsibility for Legal Compliance

Most of the laws state that

> "In the event an organization is found negligent in instituting adequate Information protection measures, the organization and its executives may be held liable for offences committed with the use of the resources of the organization. In practice it means that the CEO or the Directors of the Board may go to prison for an offence committed by any one of the employees of the organization if he is guilty of neglecting his Information Security responsibilities."

The top management of the Company therefore is exposed to all IS risks and need to initiate strategic and tactical measures to "assess" and "take steps to mitigate" risks arising out of dealing with Information.

Management Challenges

In a recession hit economy, however, not all managements are capable of devoting necessary attention to the Information Security requirements. Out of them, those who have migrated from "Technical" to "Techno Legal" layer of Information security are even less.

Being a "Compliance Leader" when a majority of the industry is not much concerned about "Compliance" introduces its own challenges to a manager.

Firstly, the top management/CEO needs to carry their conviction that "Compliance Pays in the long run" and be able to meet the short term expenses in anticipation of long term benefits.

Secondly, many of the information security practices cause inconvenience to the staff members and restrict their freedom. Under legislations like HIPAA, compliance requires appropriate "Sanctions" (punishments for contraventions) to be part of the HR policies of the organizations. These issues may cause HR related disturbances in an organizations and there is a need for appropriate motivation and building of a security culture amongst staff members as a part of the management strategy.

Thirdly, there is a cost associated with compliance and it has to be incurred here and now and justified against the probability of loss occurring in future by non compliance. Like in the case of "Insurance" it is always difficult to completely justify an ROI on compliance investments and hence the CEO needs to convince a hardcore CFO about the ROI on compliance.

Fourthly, legal compliance services are an emerging service and many of the well known information security auditors are not the market leaders in legal compliance audit Hence finding resources for legal compliance audit and justifying appointment of otherwise not well known or large firms will be a challenge for the CEO.

Finally, implementation of any compliance prescriptions affects people across the organization and it cannot be considered as the responsibility of either the CTO or the IT or Legal department alone. There is therefore a challenge before the CEO in making compliance a cross-disciplinary responsibility.

Strategic Approach to Legal Compliance

In view of the many challenges mentioned above, there is a need for a well thought out strategy to convert an existing IT company with low focus on compliance to a Compliance leader.

The best way to strategies a complicated subject like Information Security is to adopt a framework and explore the requirements specific to the user's organization.

In countries like India where there are local legislations such as Information Technology Act it is necessary for managements to ensure that all legal compliance requirements as per local laws are fully conformed with even while security audit agencies focus on frameworks such as under ISO 27001 and other standards developed over a period of time by international agencies.

IISF-309 Framework

In order to meet the requirements of the Information Technology Act 2000 as amended by Information Technology Act 2008 (ITA 2008) which is the principal law applicable in India for IT users, a structured framework such as IISF-309 (Briefly described below) is a framework which meets both the national and international information security requirements.

IISF-309 framework adopts a 21 step framework which adopts the best practices from the available options worldwide. Some of the key aspects of this framework are as follows. These are in addition to the normal IS policies such as physical and logical security measures etc.

1. **Client Consent:** Whenever an organization handles information belonging to others, a letter of consent from the data subject which inter-alia becomes a disclosure of privacy and security practices adopted by the organization would be required.

2. **Employee Awareness:** Since employees of an organization are critical to implementation of any information security measures a critical part of a sound IS strategy is to create employee awareness on the needs of Information security and making every employee an "Ethical Cyber Employee". Such an "Ethical Certification" may preferably involve "Sensitization Training" and "Passing of a Test" at periodical intervals. In order to have a complete commitment of the employees it is recommended to have a signed "Ethical Declaration" from each of the employees as some of the Indian companies have adopted.

3. **Assigned Responsibility:** In order to enable appropriate corporate attention it is expected that the responsibility legal compliance in respect of Information Security requirements is entrusted to a designated "Compliance Officer". The top management will however be required to monitor the requirements at a policy making and review level.

4. **Grievance Redressal Policy:** Since the object of data protection is the "Data Subject", there is a need for the organization to institute a proper grievance redressal mechanism as a part of the IS policy. This is a recognition that even IS policy needs to be consumer oriented.

5. **Business Associates:** All Business associates who work with the organization should be bound by an appropriate agreement to be responsible for information security to the extent they handle the data belonging to the organization.

6. **Management Certification Policy:** An organization which is answerable to its stake holders such as the share holders need to ensure that the top management adds the necessary confirmation in the annual report that the IS implementation in an organization is adequate. External audit is a tool which the management may use to shore up its own certification.

7. **DLP-OLR Approach:** The entire IS approach should be oriented towards Techno Legal Information Security and should not stop at Technical security alone. Thus the Disaster Recovery and Business Continuity plans need to be extended to Defensive Legal Protection and Offensive Legal Remedy requirements.

In the above framework, the responsibility for Techno Legal Information Security is shared by all the stake holders such as Employees, Management as well as Business Associates and the Customers. It is only such collaborative approach that involves all stake holders that the objectives of Information Security can be achieved. Further the framework affords the required flexibility to enable SMEs also to adopt the necessary levels of security which mandating of other frameworks may not enable.

By initiatives such as the above specially structured information security frameworks, India is setting an example to the Information Security community for building an information security culture amongst all industry participants from an SME to a Fortune 500 company.

Na.Vijayashankar (Naavi)
www.naavi.org : naavi@vsnl.com