Information Security for Indian Organizations
An Approach Paper

Why do we need Information Security?

To most professionals, the reasons would seem obvious. Financial losses, loss of business reputation are the ones that come to mind immediately. But organizations need to appreciate other key factors that drive the need for information security. The Indian Penal Code defines theft as "Whoever intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft". So the key to theft is transfer of possession of an asset from one person to the other (to the thief). Information theft, however, does not necessarily move the possession of your information to someone else. You could be accessing and using the information on a regular basis for your business and at the same time the "information thief" could also be accessing your information. You would never realize that the reason you were losing prospective customers to competition was not because the competition had a better product; the competition could simply be having access to your information interchange with the prospective customer! Another aspect that organizations tend to overlook is the information security obligations, both explicit and implicit, arising out of their contract and agreements with vendors and customers. But the one aspect that rarely comes to mind when talking about Information Security is the legal obligations that organizations have to protect key information. Yes, the Information Technology Act 2000, which is the law of our country obligates organizations to implement Information Security measures. Few organizations are aware of the Information Technology act; fewer still understand the obligations that the various provisions of the act place on organizations. Organizations listed on stock exchanges are required to submit a quarterly compliance report to SEBI, stating that they are complying with all laws and regulations, signed by the top management. How many of such signatories are even aware of the Information Technology Act, let alone being assured of its compliance by their organizations, is anybody's guess.

OK, so we now know why we need Information Security. But how does an organization go about achieving this? The first step to Information Security is to identify where the organization's information resides.

What do we seek to protect?

Information is the life line of every organization. Information is generated, processed and accessed at every level, both laterally and vertically, in the organization. It is a vital resource for the organization's efficiency and growth. The organization's information resides in various mediums across all locations. In Information Security parlance, we term these mediums as Information Assets. So the first step to securing information is to identify all the vital information assets of the organization across all mediums. Most organizations tend to look primarily at computer systems as their information assets and this it is probably correct since almost 80% of an organization's information in current times would be residing on computer systems. However, the non-computer based information assets, which may constitute only 20% of the information assets, could be of significant value. It is said that the formula of Coca-Cola, which is the multi-billion dollar global company's single most valuable asset, is stored not on any computer system but on a piece of paper in a vault! Further, an organization needs not only to identify it's information assets but also understand how these are being stored, accessed, processed and destroyed. Does every organization ensure that old reports and printouts of emails, for example, are shredded? What would be the impact if the printout of a earlier version of a quotation falls into a competitor's hand?

By now, we have identified our key information assets. The next step would be to understand from what or whom do we need to protect these information assets.

What is Information Risk?

Security and Risk are two faces of a coin. Why do we have fire extinguishers in our organizations? Because we know that we run the risk of accidental fire! On the same lines, what risks do an organization's information assets face? When one speaks of Information risks, the first picture that pops up in the minds of most professionals is that of a person sitting on a remote computer at 3.00 am in the morning, attempting to access your servers to steal and/or destroy your vital data. While this is very much a possibility, most organizations would leave it to their "IT folks" to take appropriate measures. But how many times does the term Information risk bring up in your mind the picture of an electrician correcting the switch near your table and walking away with a copy of your customer agreement lying on your table? Rarely, would be the answer in most cases. When identifying information risks, an organization needs to take a comprehensive view of all possible information risks. This is achieved by identifying the components of information risk viz. Threat Sources, Threats, Vulnerabilities and Controls. Discussion of components of information risk is too technical and that is not the intent of this paper. Organizations need to understand the importance of assessing and identifying information risks in order to secure their vital information assets.

The next step to information security is to plan how to mitigate (reduce or eliminate) risks to information assets.

Planning Information Security

Organizations need to decide what control measures they intend to put in place in order to mitigate risks to their information assets. These controls could be physical controls such as locks, security guards, biometric access controls or logical controls such as restricting database access to authorized personnel. For each risk, organizations need to identify the current controls in place and the additional or new controls recommended. A key point to note is that no risk, whether information risk or risks we face in real life, can be completely eliminated. Unless one completely eliminates an activity and thus eliminating the risk associated with the activity, some element of risk, termed residual risk, will always remain. When deciding what controls to implement, an organization should take into account various factors. Some of these factors are: Value of information asset being protected vis-à-vis cost of controls for protecting the asset, the requirement that controls should not restrict or hamper business operations since business efficiency and growth are the basic reasons for which information security is being implemented, and proper assessment and acceptance of residual risk. Also, controls should be assessed ad determined in an iterative manner, assessing the residual risk during every iteration till it reaches a level that is acceptable to the organization.

This paper has been published by Information Guardians in the interests of Information Security awareness. For more details, please visit our website www.infoguard.in. For any queries or to avail of our services, our contact details are: Email: sales@infoguard.in Telephone: 09820739183

With this, the organization has completed Information Risk Assessment. It has identified its key information assets (including mediums on and location where key information of the organization exists), it has assessed possible risks to its information assets, has identified appropriate cost-effective control measures it has decided to implement in order to mitigate the risks and is aware of and accepts the residual risks remaining after such controls are deployed. The next step is to implement these controls to accomplish Information Security. This is accomplished by means of an Information Security Policy.

Implementing Security: Information Security Policy

Organizations publish policies to communicate to their employees, vendors, contractors, customers their principles of operations and ethics. Human Resources policies communicate the work ethics, employability criteria, etc for employees. Organizations publish policies to ensure transparent dealings of employees with vendors and contractors (e.g. Non-acceptance of “gifts” beyond reasonable value). Information Security Policy is the document that an organization publishes to communicate to their employees and business associates the organization’s stand on protecting vital information of the organization. Section 43 of Information Technology Act 2000 states “Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.” . An Information Security Policy is the proper vehicle for implementing and maintaining “reasonable security practices and procedures” . Information Security Policy differs from other policies such as Human Resources Policy in the structure and form. An Information Security Policy generally is comprised of: (1) Overall Policy statements of approach to Information Security (2) Individual policies in specific domains, stating what is allowed and what is not allowed in the organization (usage of USB drives being an example) (3) Standard Operating Procedures detailing the procedure for implementation of the policy (For example, where USB drives usage is restricted to prior approval, the procedure for obtaining such approval, executing the approved usage and closure of the one-time approval) (4) Work Instructions: As stated earlier, generally 80% of an organization’s information resides on computers systems. Most organizations deploy multiple technologies (Windows, Unix, etc.). The technical implementation of a particular procedure detailed in a Standard Operating Procedure will differ depending on the technology. (For example, the procedure of disabling USB ports is different in Unix and Windows). Work Instructions detail the implementation of a Standard Operating Procedure in a specific technology environment. (5) Forms: Paper or electronic forms should be deployed to capture every transaction occurring under Information Security Policy domain, from initiation of a request, through its approval, to its execution. Forms are the basis for auditing Information Security Policy implementation.

Once an organization has developed the Information Security Policy, it needs to ensure effective implementation of the same for ensuring security of information assets. Some critical factors that determine success or failure of an Information Security Policy implementation are (1) Properly designed controls that do not hamper business operations (2) Communicating the Information Security Policy, the need for the policy, the importance of adhering to the policy and the penalty for non-adherence, needs to be widely and effectively communicated across the organization (3) Adequate training to users and implementers of the policy.

Implementing a vibrant Information Security Policy is the key to successfully protecting key information assets of the organization while complying with statutory and legal requirements. Like any other business process, the true effectiveness of the policy and consequent benefits can be derived by an organization only through regular review of the implementation. This is accomplished through regular audits of the Information Security policy.

Auditing Information Security

Organizations that have an in-house audit team should conduct internal audits of Information Security. The frequency and scope of such audits would be driven by the size of the organization, the size and skill sets of the audit team, etc and such internal audits could be limited in scope. Organizations should conduct an annual external audit through an appropriately qualified agency. Such audit would be comprehensive in scope and would highlight lacunae in framing as well as execution of the Information Security Policy. External auditors, if appropriately qualified, would also add value to the audit by highlighting areas that need to be reviewed in light of the changed laws and regulations. For organizations conducting business overseas, a qualified auditor would also bring to the table his knowledge of Information Security requirements of the foreign country that need to be adhered to by the Indian organization.

Like ISO 9001, is there a globally accepted standard for Information Security?

Most organizations and professionals are aware of the ISO 9001 standard for Quality Management Systems, published International Standards Organization (ISO). ISO has published ISO 27000 as the globally accepted standard for Information Security Management Systems. The ISO 27000 family comprises of the certifiable standard 27001 along with a set of guidelines (27002, 27003, 26004, 27005) covering areas such as Information Risk Management, Risk Assessment and Treatment, Information Security Management Systems Measurement and Control Objectives identifying control requirements in almost all areas of Information Technology operations. The Information Technology Rules (notified in April 2011) to the Information Technology Act, under the heading of "Reasonable Security Practices and Procedures" state that an organization that has implemented IS/ISO/IEC 27001 shall be deemed to have complied with reasonable security practices and procedures. It is pertinent to note that this is the only standard stated by name in the Information Technology Act 2000.

A note about the authors of this document

This note has been prepared by Information Guardians for creating Information Security awareness and is aimed towards Indian organizations and Information Security requirements within the Indian regulatory and legal framework.

Information Guardians offer a suite of Information Security Management Systems. These include Information Risk Assessment, Information Security Policy development and implementation, Information Security Audits, Training and implementation of ISO 27001, pre-certification audit for ISO 27001. We also offer short seminars on Information Security and Information Technology Act 2000. Visit our website www.infoguard.in for more details or give us a call on 09820739183.