In today's hi-tech era, Information Technology and business have critical relationship. Big businesses are heavily dependent on the strategic management of IT for its success and survival. IT has potential to be driver of economic wealth but it also carries great risk. Thus, a well-structured Information Risk methodology is must.

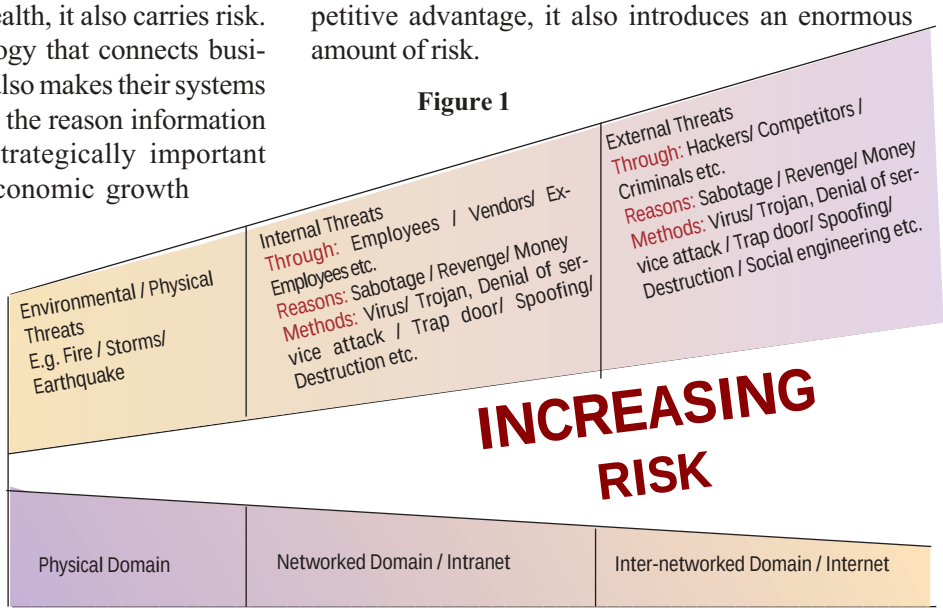
How to manage information risk

—Kavita Gorwani

In this era of globalisation, where Information systems have become the part of key business process and an ever larger percentage of the market value of enterprises has transitioned from the tangible (inventory, premises, plant, machineries, equipment etc.) to the intangible (information, expertise, reputation, patents, knowledge, etc.), we simply cannot deny the strategic importance of Information and Information assets in managing the enterprise. While IT has potential to be the driver of economic wealth, it also carries risk. The same information technology that connects business to the global market place also makes their systems vulnerable to attack. This is for the reason information security is becoming more strategically important everyday for sustainability, economic growth and future health.

There once was a time when a computer occupied an entire building and security was limited to the locking of door and engaging the guard. Today, much better functionality, more features and significantly enhanced computational capabilities are even available on a hand-held computer. But it was not the size, which changed the security concerns; it was the time when computers started talking to each other when networking, multi-sharing, multi-programming, multi-processing and Internet came into the picture. Information technology forever transformed the way all businesses operate, the way the communication and innovation takes place and most importantly the way value is delivered to the customers. It has opened the doors to new markets at a faster pace. While it offers tremendous opportunities and competitive advantage, it also introduces an enormous amount of risk.

Figure 1



The author is a Member of the Institute. She can be reached at gorwanik@rediffmail.com

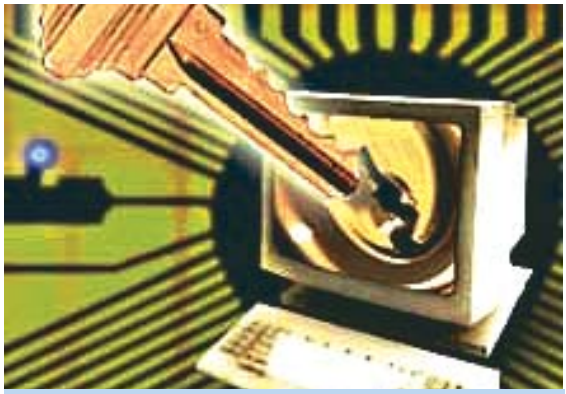
As organizations leverage computer networks and the Internet to transform the enterprise and to enable increasingly global and dematerialised transactions, board and senior management must understand the new risks introduced by opening their critical business systems and data to public and global Internet. (See Figure: 1)

Failure to manage information security is likely to be a root cause of the negative experiences many boards have had with Information Technology. IT has handed out some gruelling lessons to those that leveraged it to move data farther and faster then ever before. One of those lessons compels the need for greater concern over information Security.

Information Security: Challenges

Security in any system should be commensurate with its risks and Information Systems are not the exception. Failure to achieve Information security goals can result from a variety of challenges including lack of concern over technological issues, treating information systems not more than a calculator, information overload, abdication of oversight responsibilities, inadequate training, concentration on immediate problems and service delivery issues, supporting unbudgeted and unplanned issues while delaying and even postponing the planned issues etc.

Too often, the security failure is explained by not implementing appropriate risk management strategies which further results into business losses, damaged reputations, inefficiencies or weakened competitive positions.



Even with the implementation of most stringent safeguards, the information systems may suffer a disaster. Business continuity planning is a comprehensive term covering business resumption planning, disaster recovery planning and crisis management.

Information Risk Management: The Process

The risk is the uncertainty or chance of loss or injury, which is one of realities of life. **Information Risk Management** is the process of identifying information assets, assigning appropriate values, identifying threats to those assets, measuring or assessing risk and then developing strategies to manage it. (See Figure: 2)

Information Risk Management: Role of IS audit

IS audit has an important role in the entire process of information risk management. Effective IS audit covering information risk audit determines capability of organisation to get its goals.

- by providing assurance as to the security of IS resources that are critical in support of business objective,
- by enabling well informed risk management decisions, and
- by assisting management in accrediting the information assets and functions on the basis of the supporting documentation resulting from audit

To ensure the effectiveness of risk management techniques in place, the IS auditor should

- review IS policies, procedures and standards to ensure their alignment with overall organizational policies and objectives,
- review the organisation chart to ensure that it enables an organisation to set responsibilities for enforcing security controls and undertaking recovery tasks,
- review the access control procedure to ensure that access to information resources is on 'need to know- need to do' basis and access is controlled by adequate logical and physical access control procedures,
- interview few people in organisation to determine level of security awareness and effectiveness of training imparted,
- review the classification of data and allocation of responsibilities to maintain its integrity, confidentiality and availability
- examine various application system controls and OS level controls including input, processing and output controls, user access controls etc.,
- ensure that exceptional transaction are properly reported by the system and are handled accordingly,
- ensure that backup is taken regularly and is kept off-site also,
- ensure all access violations are reported timely, and
- review the service level agreements to ensure that they include provision for security in case of outsourced services.

Effective IS audit procedures enable an organisation to balance costs of security measures and achieve gains in job competence by protecting information resources that support its mission.

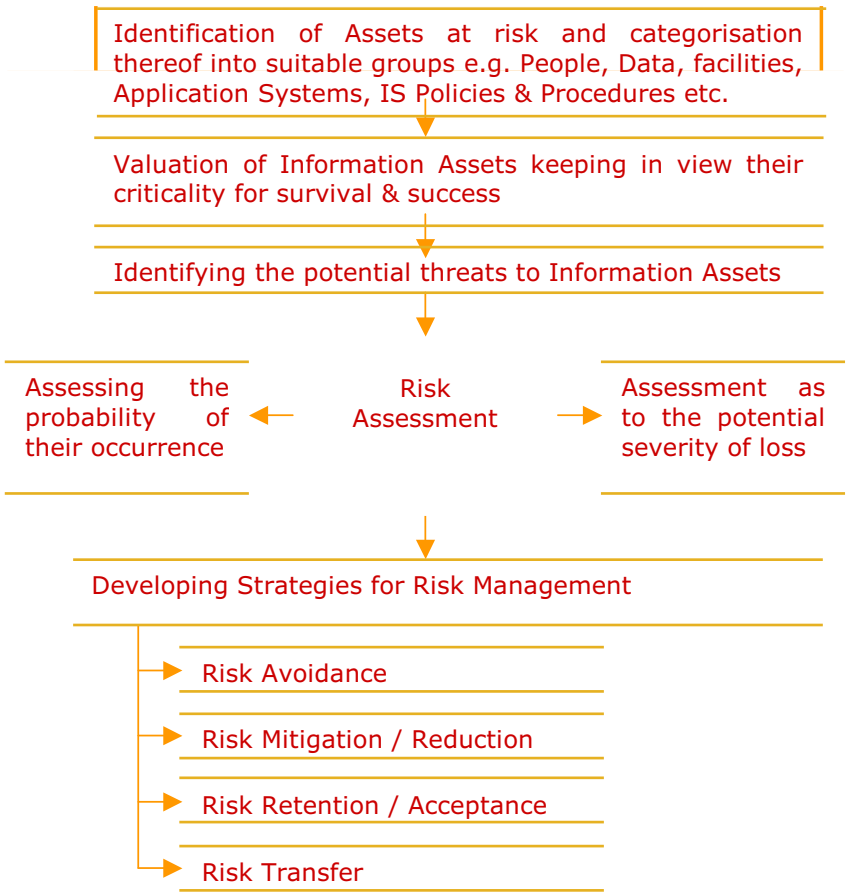


Figure: 2

Step 1: Identification of Information Assets

The first step in the information risk management process is to identify the information assets in support of critical business operations. The assets could fall under different groups which are:

Physical/Tangible Assets

- People e.g. End users, analysts, programmers etc.
- Hardware e.g. mainframes, minicomputers, microcomputers, storage media, printers, communication lines, concentrators, hubs and switches etc.
- Facilities e.g. furniture, premises etc.
- Documentation e.g. printed forms, manuals, system and database documentation, IS policies & procedures

Conceptual Assets

- Data, Information
- Software - Application Software (Application Packages for accounting, payroll, sales etc.) and System Software (Operating system, utility programs, compiler, communication software, DBMS etc.)

Step 2: Valuation of Information Assets

The assets so identified and grouped in the previous step are categorized into different classes, which are:

The Information Risk Management is regarded as the process of identifying information assets, assigning appropriate values, identifying threats to those assets, measuring or assessing risk and then developing strategies to manage it.

Critical: The information assets, which determine the survival of business and it is impossible to run business without them would fall under this category

Essential: The assets which are important for business success and survival but without which business can run for some period

Normal: The assets without which business can run for an extended period of time though inconveniently

The above analysis and categorisation of information assets will enable an organisation to focus on high impact assets.

Step 3: Identifying the threats

Threats can be defined as anything that contribute to the interruption or destruction of any service / product. Various threats can be grouped into environmental, internal and

external threats. (See Figure: 1)

Step 4: Information Risk Assessment

Once the assets and corresponding potential threats have been identified, experts are contacted to review the system for weaknesses that can be exploited and the likelihood of those being exploited. As a result, appropriate corrections shall be made to the system, if required. Immediate action may not be taken to correct some identified vulnerabilities but the process will at least analyse these vulnerabilities, document and recognize them for subsequent risk management decisions.

The process of Risk Assessment includes not only assessment as to the probability of occurrence but also the assessment as to the potential severity of loss, if risk materializes. This will assist in determining the appropriate risk mitigation strategy, the residual risk and investment required to mitigate the risk.

Step 5: Developing Strategies for Information Risk Management

Once risks have been identified and assessed, the strategies to manage the risk fall into one or more of these four major categories:

Risk Avoidance: Not doing an activity that involves risk. Involves losing out on the potential gain that accepting the risk might have provided

Risk Mitigation/Reduction: implementing controls to protect IT infrastructure and to reduce the severity of the loss.

Risk Retention/Acceptance: Formally acknowledging that the risk exists and monitoring it. In some cases it may not be possible to take immediate action to avoid/mitigate the risk. All risks that are not avoided or transferred are retained by default.

Risk Transfer: causing another party to accept the risk i.e. sharing risk with partners or insurance coverage.

In ideal information risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurrence is handled first, and risks with lower probability of occurrence and lower loss are handled later.

Major Risks and Security Controls

Depending on the nature of risk and likelihood of its occurrence, security controls may differ. Major risks and corresponding control measures are:

Error Risk

The possibility of error cannot be ruled out completely even in the highly automated environments with fewer manual controls and fewer manual interventions. However, to minimise the possibility of errors, an organisation should ensure the adequacy of input, processing and output controls.

Input controls ensure that only valid and authorised transactions are entered and accepted into the system. These controls include various accuracy and completeness checks incorporated in the application design like limit checks, sequence checks, range checks, reasonableness checks, logical relationship and interdependency checks, existence checks, check digit, batch controls etc.

Processing and data file control procedures ensure the completeness, accuracy and validity of data on a file / database unless changed as a result of valid and authorised processing. These controls also ensure that only authorised processing occurs to the stored data and include manual recalculations, run-to-run totals, audit trails, exceptional reports and transaction logs, reconciliation and balancing, parity checks, internal and external labeling etc.

Output Control Procedures provide assurance as to the consistency, accuracy and validity of data/information delivered to users by implementing controls over the distribution of printed material, storage of soft copies and hard copies of documents containing sensitive information at a secured place, reconciliation, balancing etc.

Fraud Risk

To minimize the possibility of fraud, an organisation should

ensure that

- the security requirements are defined, data owners are identified and roles and responsibilities are adequately described,
- access to resources is on 'need to do – need to do' basis and sufficient segregation of duties is in place,
- all program change / system development requests are authorised and all changes and system developments are adequately tested to ensure the adequacy of control procedures,
- information assets are kept at the secured location and adequate physical and logical access control procedures are in place. Physical access control procedures include bio-metric devices authenticating users identity based on a unique measurable attribute like palm traits, hand geometry, iris, retina, fingerprint, voice etc. Logical access controls include logon Id and password, single sign on for all resources etc.
- programs are kept in the secured libraries,
- proper reconciliation and checking procedures are in place to ensure the accuracy of data conversion / migration process at the time of implementation of new system,
- encryption and integrity checks are applied to the critical data being transmitted over the network,
- access to public network is authorised and effective firewalls and intrusion detection systems are in place,
- users are trained to maintain the password secrecy by not sharing the password with others and by protecting password

IS audit has an important role in the entire process of information risk management. An effective IS audit covering information risk audit determines the capability of an organisation to accomplish its goals.

from public sight,

- user Ids are unique and those not in use are deleted promptly. There is a check on the maximum number of trails for entering the password and maximum period of inactivity,
- the concept of maker-checker is in place i.e. the transactions are authorised by an appropriate authority
- backup is taken regularly and it is kept at a secured place, and
- the information assets are protected by an adequate insurance cover.

Disclosure Risk

Disclosure risk may arise from the access of confidential data on a system/ network either through the hacking, eavesdropping, inadvertent broadcast of data across the network, improper disposal of data etc. For the mitigation of disclosure risk, an organisation should ensure that:

- confidential data/information is identified and the severity of loss by their unauthorized disclosure is assessed,
- assignment of access privileges is done on 'need to know – need to do' basis,
- access to data/ information is controlled by adequate logical access controls,
- Storage media is kept at a place adequately secured by physical access controls,
- data in transit is adequately secured by encryption and access to encryption algorithm is adequately secured,
- responsibility for printed reports and their distribution and preservation is fixed,
- procedures to restrict the release of confidential data for testing are in place, and
- storage media is demagnetised before removal/disposal.

Organisation Risk

Organisation risk may arise from improper role definitions, lack of efficient IT staff, insufficient segregation of duties, lack of security awareness, inadequate job descriptions etc.

To manage the organisation risk, an organisation should enforce the implementation of a formal organisation chart that ensures the well-defined job descriptions, roles and responsibilities and sufficient segregation of duties. IS policies and procedures should be developed in alignment with overall business policies and objectives.

Outsourcing Risk

To manage the risk associated with outsourcing of IS processes, an organisation should, first of all, document the outsourced process and identify the control points.

There may be a situation where any internal business process relies on the output generated by the outsourced process. In such a situation, inadequacy of controls on the outsourced process may adversely affect the efficiency of dependent processes. Therefore, standards should be set for the outsourced process to which the vendor must confirm. The security controls on the outsource process should meet organizational standards. The services offered from time to time should be monitored. It should be ensured that the vendor has adequate contingency arrangements covering hardware, software, building, staff etc.

Disaster Recovery and Business Continuity

Even with the implementation of stringent safeguards, the information systems may suffer a disaster. But it must be possible to recover the operations and mitigate losses. Business continuity and disaster recovery plans enable a business to continue operation in the event of a disruption.

Business continuity planning is a comprehensive term covering business resumption planning, disaster recovery planning and crisis management. While business resumption planning covers the operational aspects of business continuity plan, disaster recovery covers the technological aspects to minimise risk and continue operations in the event of disaster. Crisis management aims at the overall management of crisis in a timely and effective manner by minimizing the damage to organisation and continuity of critical business operations.

The business continuity planning process can be divided into following phases:

Phase 1 – Business Impact Analysis

This phase is extremely critical for the development of a Business Continuity Plan as this is where the key business processes, their dependencies and interdependencies are identified and documented, criticality of Information resources in support of critical business processes is established and the impact a disaster will have upon the business is identified and quantified.

There are a number of ways to conduct Business Impact Analysis including but not limited to questionnaires, interviews, workshops and analysis of documentation.

This phase includes a number of tasks:

- Obtaining clear understanding of organizational culture, the environment in which it operates and associated risks
- Identifying critical business processes, their dependencies and interdependencies
- Identifying the information resources in support of critical business processes
- Establishing the criticality of Information resources
- Identifying and quantifying the risks to critical information resources

Determining the critical recovery time period for information resources i.e. the maximum allowable downtime (MAD) within which business operations must be resumed before the significant or unacceptable loses are suffered

Determining the impact to the organisation in the event of a disaster, e.g., financial loss, loss of reputation, brand damage etc.

Phase 2- Developing Recovery Strategies

The next phase in the business continuity plan is the development of various recovery strategies, analysing them and determining the most appropriate strategy for recovering from a disaster. The objective of this phase is to identify the recovery strategies that are low risk and cost-effective and ensure the timely recovery for all critical processes.

Recovery Strategies for physical Information Processing Facility

In case of disasters that damage the primary physical facility, the off-site backup hardware facility is required to continue the operations. The various options are:

Hot Site: Ready to operate site with compatible hardware and operations facilities available at site. Hot site is used for the recovery of critical business processes for which its high cost can be justified. It is intended for emergency operations of shorter period.

Warm Site: This is a partially configured site with all facilities except the main computer. This is less expensive than the hot site. IT can be activated within several hours.

Cold Site: Cold site is suitable where organisation can tolerate some recovery time. Cold site has basic environment for operating an information processing facility. It is least expensive. Its activation may take several weeks.

Duplicate Information Processing Facilities: These are dedicated self-developed sites providing for the backup of critical business operations. To ensure the availability of duplicate IP facility in the event of disaster, it should be ensured that

- the duplicate IP site is not susceptible to same natural disaster as the primary IP facility,
- the hardware and software at the duplicate site are compatible with those at primary site,
- if capacity is enhanced at primary site, it should also be given effect at the backup site, and
- testing of backup sites should be performed at regular intervals

Reciprocal Arrangements: The arrangement entered into between two or more organisations with similar IP facilities whereby they promise to provide IP facility to each other when disaster strikes.

Recovery Strategies for telecommunication network disaster

To maintain the critical business processes, IP facility's business continuity plan should also provide for telecommunication network disaster recovery methods, which serve to protect the network and reduce the severity of loss arising from several disastrous events unique to telecommunications like central switching office disasters, communication software glitches and errors, cable cuts, security breaches. These various methods are:

Redundancy: It provides for surplus capacity with a plan, which can be used when primary telecommunication facilities become unavailable. E.g. in case of LAN, having an additional cable through an alternate route for use when primary cable is damaged, providing multiple paths between routers etc.

Alternative Routing: It involves routing information through an alternate medium without affecting the route for transmission. The examples include using a dial-up circuit as an alternative to leased lines, couriers/ posts/ Facsimiles as alternatives to e-mail etc.

Diverse Routing: It involves routing information via a different route without affecting the medium i.e. routing information through split cable facilities or duplicate cable facilities.

Long-haul Network Diversity: It aims at ensuring long distance network availability. It involves a provision for automatic re-routing to a different carrier if original network damages.

Last-mile Circuit Protection: It involves use of a different local carrier to carry the traffic in the event of a local communication disaster.

The plan should also cover key information about the organisation's insurance. It should be ensured that all assets and possible risks are covered in insurance like IS facilities and equipments, cost of business interruption, extra expenses incurred for recovery, fidelity, resident data and data in transit, documentation, media etc.

Phase 3 - Development of the Recovery/Continuity Plan

The phase aims at developing and documenting the recovery processes in a form that is appropriate for execution under emergency conditions. There are a number of steps to be taken, including:

- Selection of the most appropriate tool for the formation and maintenance of the continuity plan
- Determining the recovery tasks, their sequence and timing
- Preparing different teams including emergency action team, emergency management team, damage assessment team, security team, network recovery team, transportation team, relocation team etc. and assigning responsibilities for various tasks
- Defining the escalation processes.
- Identify and listing key contacts

Phase 4 - Testing of the Recovery/Continuity Plan

The objective of this phase is to develop a comprehensive and effective test plan and implementation thereof to ensure that the business continuity plan will work as designed. The test plan and implementation thereof also reveals the deficiencies in the emergency, backup or recovery plan or in the preparedness of organisation in the event of disaster. Therefore, BCP should be tested regularly to provide an assurance that the organisation will survive the disaster.

Phase 5 - Maintenance and Update of BCP

This phase is an important part of the risk management. The phase aims at developing strategies to maintain the Business Continuity Plan in a state of readiness.

Conclusion

The Information Risk Management is a key aspect of modern decision making for all industries. The universal need to make informed, realistic and justifiable decisions in the face of uncertainty is the driver for increased information risk management activities in most of the organisations.

A well-structured and effective information risk management methodology not only helps management identify appropriate controls for providing the mission-critical security capabilities but it also determine its survival and prosperity. ■