# Information Security

*Deepak Rai* & Shikha Rai***


## < EXECUTIVE SUMMARY >

◆Today, everything has been transformed into bits & bytes. There is nothing concrete, everything is in cyberspace. But the economy still faces the threats of theft, fraud, politics etc. The world is still a nasty place where threats can come anytime from anywhere without warning and without leaving any evidence. The wealth targeted now being – Information – which reiterates the importance of information security system in an organisation.

The Information Systems Security for any organisation is now not an IS or IT departments' issue alone but rather a business issue. The information system needs to be provided security not only with respect to external users but also with respect to the persons who are not authorised to access the data internally.


Personal Computers, Local Area Networks, Wide Area networks, Extranets, Internet …. Boundaries fading …. Information exploding …. Welcome to the brave new world - where data is mined, data is warehoused, information is processed and knowledge marts provide business intelligence at a premium. Most of today's financial assets float on the web and are held virtually. Consider the mountain of information that is moved every time an ATM is accessed or stock is bought and sold on the web. It is unbelievable.

Everything in bits & bytes. Nothing concrete, everything in cyberspace. But, this New Economy still faces the threats of the Old economy – theft, fraud, politics …. The world still is a nasty place; where threats can come anytime from anywhere without warning and without leaving any evidence. The wealth targeted now being – Information. With multiple connections into Corporate Networks – Mobile employees, partners, suppliers, customers & public; the need to be open for 'e-business' 24*7*365 and the accelerated speed of deployment of new technologies has made organisations vulnerable to security issues. Hacking is no longer rocket science, hackers' tools are freely available on the net and techies love trying out their programming skills by hacking Networks just for kicks.

Apart from the outside threats, threats from insiders are on the rise. Ignorance, Carelessness, disregard for Security policies and malicious intent could be the factors for security breach by an insider. The case of former FBI agent Robert Phillip Hanssen, who was convicted for spying for Russia, is an extreme but prime example of how insiders can take advantage of their access and authorizations. Hanssen manually and electronically stole information from the FBI for his own financial gain, and he did it for more than 15 years without trouble because he was a trusted insider.

Information Systems Security for any organisation is not an IS or IT departments' issue alone; it is a business issue. Business leaders need to understand and own the process of Security because compromise of any Information system would impact employee productivity, corporate image, consumer & stakeholders trust; besides the financial loss. Therefore IS security needs ownership starting from the Boardroom.

**Member of the Institute*
***HOD (IT-Canon India Pvt. Ltd.)*
*The views expressed herein are the personal views of the authors and do not necessarily represent the views of the Institute.*

For any organisation to start drafting a security strategy following questions need to be asked:

What is at Risk?

Financial assets, Technology, Design and Patents, Market Share and customer intelligence: What part of the business activity is such as to be so germane to the functioning of the organisation that it could impact the organisation.

How hard will someone try to get at it?

How much will it hurt, if someone succeeds?

How much am I willing to pay to prevent myself from getting hurt?

These are questions which would need to be pondered over and reacted upon.

Experts on IS recommend the 'Threat & Risk assessment methodology'. This is a detailed plan for identifying and analysing each information access point and processing centre on an empirical basis. Based on this a matrix is designed to understand the cumulative threat and the impact of that threat.

Threat and Risk exercise is essentially divided into three parts viz. identifying important assets, analysing risk levels and proposing a risk mitigation plan. The whole activity is completed in six steps as detailed under:

1. Identify important information assets
2. Collect vulnerability Information for Identified Assets
3. Analyze Threats & Risks for these Assets with respect to Vulnerabilities Identified
4. Assess Administrative and management Procedures and Processes for these Assets
5. Check compliance with IS regulations
6. Draft a mitigation plan to protect these Assets in a cost effective manner

**1. Identification of critical assets**

For identifying which Information assets are important to an organization, Key business process owners, information asset owners and users need to be consulted/ interviewed based on the following three parameters;

a. Availability of Information Systems : Business impact due to system breakdown or non-availability for any other reason.
b. Confidentiality of Data: Data getting revealed to unauthorized person inside or outside the organization.
c. Integrity of Data: Data getting modified or deleted in an unauthorized manner.

This information would help in compiling the risk index for IT assets and prioritize them based on their importance to the organisation.

**2. Vulnerability Assessment**

The purpose of vulnerability assessment is to investigate likely threats including but not limited to intentional and unintentional events caused by human error, system design weaknesses, lack of software updates, environmental threats, and operational/administrative threats e.g., inadequately trained employees.

During vulnerability assessment, system-specific and generic information technology threats in all components of IS infrastructure e.g., communications, data network, compute systems, application systems, personnel, physical security etc are identified.

**3. Threat & Risk Analysis**

Mathematically, Risk can be presented as a function of vulnerabilities detected in a particular system, importance (sensitivity) of that system to business functions and visibility of the system across an organization or beyond.

Therefore risk can be represented as the following mathematical equation:

$$\text{Risk } (R_i) = \text{Visibility Rating } (V_i) + \text{Sensitivity Rating } (S_r) + \text{Vulnerability Rating } (V_r)$$

Because it is prohibitively expensive and probably impossible to safeguard information and assets against all threats, security practice is based on assessing threats and vulnerabilities and the degree of risk they present and selecting appropriate, cost-effective safeguards.

**4. Assess Administrative and management Procedures and Processes**

This includes all the controls for accessing the assets which have been identified: for instance the Network and Applications user access rights, Backup and restoration procedures, Disaster recovery procedures, Change controls, Physical security, system logs monitoring etc.

**5. The security strategy of any organisation should be guided by the IS regulations.**

The BS7799 is on date used as the standard for Security guidelines. The IT Act 2000 applicable in India provides a legal and regulatory framework for promotion of e-commerce and covers security procedures for electronic records & digital signatures, on-line contracts, definitions of computer crimes and their penalties.

The main aspects of the IT Act 2000 are:

Extends to the whole of India

Electronic contracts will be legally valid

Legal recognition of digital signatures

Digital signature to be effected by use of asymmetric crypto system and hash function

Security procedure for electronic records and digital signature

Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities

Controller to act as repository of all digital signature certificates

Certifying authorities to get License to issue digital signature certificates

Various types of computer crimes defined and stringent penalties provided under the Act

Appointment of Adjudicating Officer for holding inquiries under the Act

Establishment of Cyber Appellate Tribunal under the Act

Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court

Appeal from order of Cyber Appellate Tribunal to High Court

Act to apply for offences or contraventions committed outside India

Network service providers not to be liable in certain cases

Power of police officers and other officers to enter into any public place and search and arrest without warrant

Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller

The IT Act enables:

- Legal recognition to Electronic Transaction / Record
- Facilitate Electronic Communication by means of reliable electronic record
- Acceptance of contract expressed by electronic means
- Facilitate Electronic Commerce and Electronic Data interchange
- Electronic Governance
- Facilitate electronic filing of documents
- Retention of documents in electronic form
- Where the law requires the signature, digital signature satisfy the requirement
- Uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records or documents
- Publication of official gazette in the electronic form
- Interception of any message transmitted in the electronic or encrypted form
- Prevent Computer Crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in Electronic Commerce and electronic transaction

The IT Act 2000 is an important facilitator of bringing ecommerce with all its functional utility within the reach of the common man and also the risks associated with it. The deterrents provided in the enactment are various punishments. Since the enactment is recent there are not too many case laws. The usage of technology would help in evolving the judicial precedence which would dictate operating practices. In the meantime caution would be the watch word.

**6. Drafting of Risk Mitigation Plan:**

The Risk Mitigation plan would be a comprehensive plan based on the TRA report, Administrative policies & procedures under practice and guided by the IS regulations.

The Plan would address the following:

A. Physical security of the Information assets: The physical locations of the assets/ the selection of the facility and the areas. Depending on the criticality of the NOC (Network Operating Centre) or the Data centre, the physical access needs to be defined – starting from elementary lock & key to biometry. Fire protection of the assets, water proofing of the facility and insurance of the facility and assets are also important.

B. Operating System Hardening : Operating System vendors are continuously posting patches/ service packs on their sites. These are often bugs or security holes which have been patched. Exploiting Operating system known vulnerabilities are by far the most commonly used way of entering corporate networks. As soon as a vulnerability is found, patches/ fixes are posted on the Microsoft or other O/S vendor sites. These are invariable required to be checked for compatibility with the applications that are running in the organisation. A constant vigil needs to be kept on the patches that are released and a system of validating the patch with the existing applications, though a tedious process needs to be incorporated within the days schedule and strictly followed. This is a simple and a very effective solution for medium risk organisations and databases. System Administrators also need to be aware that there are a

number of default services which are bundled into any OS. These are often not required and tend to compromise the security of the entire network. Unnecessary services like FTP Publishing Server, SMTP Service, WWW service can be exploited apart from wasting vital system resources like processing power and physical memory.

C. Access Rights on various systems & Applications
Proper user profiling and tight access control mechanism over network access, services, applications and data files is extremely essential. Access rights should be reviewed periodically for employees who have left the organisation or for accounts which are invalid.

D. Network architecture covering Firewalls, Intrusion Detection Systems (IDS), DeMilitarised Zone (DMZ).

Firewall is a protective shield to the organisational network allowing only authorised people into the domains into which they are authorised to access and also to limit and monitor access of inside users to outside services basically http. Firewall rule sets need to be configured very carefully.

1. Firewall rule sets for all firewalls should be in following order:
   - —Stealth rule to be the first rule
   - —The destination ports need to be defined explicitly.
   - —anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)
   - —User permit rules (e.g. allow HTTP to public web server)
   - —Management permit rules (e.g. SNMP traps to network management server)
   - —Deny and Alert (alert systems administrator about traffic that is suspicious)
   - —Deny and log (log remaining traffic for analysis)

Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.

Firewall administrators and Managers should monitor any attempts to violate the security policy using the audit logs generated by the application level firewall.

Intrusion Detection System look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. Attack signatures should be updated regularly and network administrators should diligently monitor the logs and fine-tune the IDS settings.

De-militarised Zone (DMZ) is a must for an organization that wants to host web-enabled services. The DMZ contains devices accessible to Internet traffic Web (http) server, FTP server, SMTP servers etc. DMZ sits between the internet and the internal Network's line of defense (Firewall, IDS etc.) and even if one of the services in the DMZ gets compromised the internal network remains unharmed.

E. Data encryption

Data encryption is essentially the conversion of data into a garbled mass which can only be deciphered with the use of a key. This key is known to the desired user. Encryption is essential to maintain confidentiality. Confidential data whether on the Desktop or on file server or being transmitted across the Internet needs to be protected and depending on the level of confidentially should be password protected, digitally signed and/or encrypted.

Internet usage and business models which are dependant on the internet have to use encryption of data. The process involves securing a connection between the user and the database of the organisation so that the data that flows through this pipe is not sniffed. Besides this there is also the need to identify the user and ensure that only the desired person is accessing this gateway.

Web servers that serve on-line transactions like Banking, e-commerce, ticket booking etc. and are linked with payment gateways are ideal candidates to focus on encryption of the credit card numbers and customer data getting transmitted on the Internet.

SSL(Secure Sockets Layer) protocol embedded in both the popular browsers Netscape & Internet Explorer use public keys to encrypt data for transmitting private documents over the Internet. This connects the user site to the central site from where the data is being pulled and the transactions happen. Once the connection is established the identity of the user is identified by the Public key.

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

PKIs integrate digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

F. Digital Signatures A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the indi-

vidual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are a number of different encryption techniques to guarantee this level of security.

G. Policies & Procedures Refinement: The policy and procedures for the entire organisation need to be very strictly followed. Password protection/ usage of email/ content classification/ internet usage/ using of FTP sites etc need to be monitored. Behaviour of individual employees should be passively monitored because any intrusive behaviour usually starts of with very small and seemingly harmless violations. Just the fact that the organisation is serious about even the harmless intrusions or minor violations sends a message through the organisation that which inhibits such behaviour. Examples of this could be browsing unwanted sites/ downloading information/ uploading harmless information/ sending or receiving bulky emails not commensurate with the work at hand etc. A good supervisor is generally able to detect signs of irregular behaviour well in time. Such monitoring should be encouraged within the organisation with the subtle message that this monitoring is not an intrusion on any ones privacy but an essential act for preserving the organisation.

Besides this the policies should be dynamic and respond to the situation as desired. A periodic review and upgradation of the policy and the infrastructure is very essential.

H. Security Awareness in the Organisation: Employees should be made aware of their role in the security domain of the organisation. Procedures need to be simple and such that are easy to understand and follow. As far as possible these should not inhibit the normal work practice. Periodic information dissemination in readable formats is a must. A formal review of the extent of the knowledge of the procedures should be done. This would log the extent of the awareness within the organisation.

I. Disaster Recovery & Business Continuity: The procedure and organisational effort at disaster management is directly related to the importance of the data and the time which the organization can wait for getting the information back in case it is hit by disaster. From simple back ups to complex duplicating of servers to archival of information and transactions the data recovery and storage procedure can be a major cost centre. Largely depends upon the risk perception and the need for immediate recovery. A financial institution for example could ill afford a disruption in its web transactions so much so that it would impact its business very adversely in a very short time indeed. Hence banks have elaborate procedures for data duplications which is done at multi-locations across geographies and time zones. Data storage procedures are also very complex in such situations. The design of the Disaster Recovery Plan would largely depend upon the Threat Risk Analysis and appropriate budgeting could provide a near fail safe solution in this case.

**Implementation of the Security Strategy**

The best laid out plan is only worth the paper on which it has been written until it has been implemented. The seriousness with which the management and the business addresses this issue would depend upon the organisation itself. A new inclusion to the CXO list these days, is the Chief Security Officer (CSO). To draft & implement a security policy, a qualified person preferably a CISA (Certified Information Security Auditor) or a trained BS7799 professional would be recommended. Outsourcing the security planning and management is also a recommended alternative where in-house expertise is not available.

Finally like all other things in the IT domain the life of the present security arrangement is as short-lived as the constituents that it seeks to protect. The substratum which needs to be protected is under continuous evolution. So the security policy too must evolve continuously. Upgradation of the systems and the scale would also be essential if the organisation is growing and the IT technology is helping it to accelerate on its path. Therefore it is advisable to budget for growing expense on the security systems – perhaps in excess of the budgets for the IT itself. The more the business model of any organisation starts to leverage the IT enabled services the more acute the requirements for its functioning in a fail safe mode get enhanced. A database which is servicing 100 clients and a database which is serving 1000 clients needs a higher scale of investment on security even if the backend technology use is the same. And if the users on any such platform are on the increase it is an indication that the business model is succeeding. Acceleration of the expenditure on security would therefore have to be on two clear aspects: Investments in protecting a larger network and insulation against obsolescence. Growing businesses put pressure on investments and the decisions to go to what extent to protect data is a tricky one. There can be no formula for a standard plan on this and would vary according to the circumstance of the situation. An increasing awareness and an underlying discomfort that the business is at risk is an essential ingredient of every successful web enabled environment. ■