# Information Security – Area Needing Attention for Managing Competitiveness

*Harinder K. Makkar**

**Abstract**

In the age of Information Revolution, the management of information and its security is the key concern for all organisations and nations. For sharing of information among the intended users, the systems have to be networked. With this networking the risk of unauthorized use and attacks have taken major attention of Managers.

Networks and Information are subject to various types of attacks and various products are available in the market for securing the systems. But it needs the thorough understanding of the various issues involved and proper implementation. This paper is being prepared to help the managers in understanding the various issues involved in securing the information.

## Contents of the Paper

The paper will cover the following contents:

- Information Security Issues.
- Various Types of Attacks and their counter measures.
- Information Security Policy
- Management of Security
- Security Certification and its Implementation

## Main Issues:

- Information is Wealth
- Information is being Centralized and Networked
- Moe and more dependant on IT Systems
- Security Needs to be upgraded on Continuous Basis
- Access to Networks and Information has become Easier with IP based Systems
- Need to develop Security Systems
- Secure Systems

Key Words: Information Security , Information Security Policy, Management of Security, Security Certification

## Introduction

Information is perhaps most important pie of corporate wealth. Quality information is hard to acquire and easy to lose. The good aspect of information is that now it is easy to move and easy to alter and this aspect has added insecurity dimension to information.

## 1. Information Security Issues.

Information security is an important issue, when it is put on the network. While the means to achieve security may be technical, the goals are economical. The loss of information can adversely affect the business continuity and even the image of the company. Information security is what ultimately distinguishes information that has economical value from information that does not. Add to this fact that threat to the data is increasing day by day. Security of information

* *Deputy General Manager, BSNL & Computer Faculty, ALTTC, Ghaziabad, hkmakkar@bsnl.in*

ensures the availability, integrity and confidentially of information and includes the security at all levels viz Network, OS, Application and Data.

So it a high time that we have a security policy endorsed by the higher management and get it implemented. Implementation of security policy is just not putting up data security devices and having a tight access control mechanism, it is an on going process. The security mechanism is to be continued reviewed against the failures and new threats and risks. The risks are to be analyzed and managed accordingly. The management of risk involves its acceptance, mitigation or transfer. The most important aspect is to have a security organizational set up which will do all these activities.

Information Security ensures

- Availability,
- Integrity and
- Confidentially of information

The information security set-up of any organisation has to think of security of individuals and file-level data objects and to protect the network from being launching pad of attacks by hackers. The general solution to security design problems lies in 'authentication' and 'authorisation' model, which is collectively known as access control. However access control does not provide enough security because it ignores the potential threat from insiders. Accountability steps in where access control leaves off.

A lot can be observed by just watching. Pay attention to what you can see and measure. How is it to be done? Answer lies in intercepting all transactions that involve files. Think of it as event detection. The event records are filtered and correlated at the time of capture to distinguish between OS and application activities from user-initiated data use. The audit trail is to be compressed and made temper proof and archived. Because this capture occurs in real time, the reaction can be in real time. The reaction should be risk-appropriate and may range from issuing an alarm to change in authorisation policy. The point is that you should have the event log and monitor it.

**Various Types of Attacks and their Counter Measures**

The most important threat to computer systems is from virus and worms. The first and the foremost requirement to set up secure environment is to have latest versions of software at all levels and upgrade them with latest upgradations issued by the vendors. These are the known vulnerabilities in the old versions of the software, which are mostly exploited by the hackers to attain access to the networks and the systems. Having the latest antivirus software can help a lot. Other very important aspect is to secure the network from being hacked and being used for hacking by the unauthorized persons. The network vulnerability can be tested by penetration testing methods and once vulnerabilities are known they should be plugged.

The security threats and their counter measures in this respect are published by CERT-In on their website www.cert-in.org.in. Latest security alerts and advisory are available on this site.

Security Incidents are mainly due to:

- Known Vulnerabilities
- Configuration Errors
- Virus Attacks

## 2. Information Security Policy

1.Start With a Focused Methodology
2.Evaluate the Organization's IT Infrastructure
3.Explore Departmental and IT Controls
4.Identify Gaps and Establish Controls

### *2.1 Security Policy Preparation*

- Create Usage Policy Statement
- Create A Risk Analysis
- Establish A Security Team Structure

### *2.1.1 Create Usage Policy Statements*

- Outline Users' Roles and Responsibilities
- Identify specific actions that can result in punitive actions; Actions and methods to avoid them should be articulated.
- Outline Partner Use Statement
- Outline Administrator Use Statement

### *2.1.2 Conduct A Risk Analysis*

- Identify Risk to Network, Network Resources and Data.
- Identify Portions of the Network, Assign a threat rating to each portion and apply appropriate level of security.
- Assign each network resource – Low, Medium or High Risk Level

Establish A Security Team Structure

- Team led by Security Manager and participants from each functional unit
- Each member of the team should be aware of Security policy and trained for technical requirements

### *2.1.3 Roles of Security Team*

- Policy Development – Establish and Review Security Policy
- Policy Practice – risk Analysis, Approval of Security Changes Requests, Review Security alerts from vendors and CERT, Turn plain Language Security Policy into Specific Technical implementations.
- Response – Actual Trouble Shooting and fixing of Violations.

### *2.1.4 Prevention*

- Approving Security Changes
- Changes to Network equipment that have a possible impact on the overall security of the network.
- Review the following changes:
- Any change to the firewall configuration
- Any change to ACL
- Any Change to SNMP configuration

- Any change or update in software from the approved software revision level list
- Monitoring Security of your Network

Monitoring Security of Network

- Monitor for any changes in Configuration of ‘High risk’ Devices
- Monitor Failed Login Attempts, Unusual Traffic, Changes to the Firewall, Access Grants tom Firewall, Connection setups through Firewalls
- Monitor Server Logs

Actions in Case of Violations for Analysis

- Implement Changes to Prevent Further Access to the violation
- Isolate the Violated System
- Contact ISP in an attempt to trace the attack.
- Using Recording Devices to gather evidence
- Contacting Internal Management and external agencies
- Restoring Systems
- Record the event by obtaining Sniffer traces of network, copies of log files, active user accounts, and network connections
- Backup the compromised System to aid in a detailed analysis of the damage and method of attack.
- Look for the other signs of compromise
- Maintain and Review Security Device Files and Network Monitoring Files

What needs to be done

- Secure Physical Access
- Remove Unnecessary Services
- Ensure Perimeter Security by means of Firewalls
- Ensure Proper Network Administration
- Apply Patches in Time
- Ensure an updated Antivirus Software
- Encrypt Sensitive Data
- Install Intrusion Detection System IDS

## Conclusion

Caution is the word when it comes to Information Security. In an era, when information is the power and wealth for an organisation, one cannot expect taking chances with it. Therefore, it is advisable not only to secure the physical access to the information, but also to install antivirus software, wherever required. ‘Prevention is better than cure’- goes strong in case of Information Security also, if we want to create competitiveness. Moreover Security is a continuous process, the preparedness of yesterday may npt be sufficient for today. We have to review to find the gaps and immediate action is to be taken to plug them.

**************************