CHAPTER-10

INFORMATION SECURITY

Information Security

Introduction

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.

Need of Securing Information

Information is most important asset for any organization especially for a telecom operator. All our revenue comes from some information only. Besides revenue if there is loss of information all our processes can come to a standstill and it will result in interruptions. It takes lot of efforts to build up information, but the small negligence at any level can result in loss of information. 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 during security incidents besides revenue, the image of the company is also at stake.

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 ongoing 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.

Meaning of Secured Information

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.

Reasons of Security Incidents.

Security Incidents may occur due to any lapse or negligence, but they are mainly due to:

- Malicious Code Attacks
- Known Vulnerabilities
- Configuration Errors

Indications of Infection

A system infected with malicious codes will have following symptom(s):

- Poor System Performance
- Abnormal System Behavior
- Unknown Services are running
- Crashing of Applications
- Change in file extension or contents
- Hard Disk is Busy

There can be various types of malicious codes like Virus, Worms, Trojan Horses, Bots, Key Loggers, Spyware, Adware etc. The solution against these is to have good anti-virus software. The anti-virus software should be updated in routine so that it is effective against new malicious codes.

Vulnerable Configuration

The Configurations of the systems are Vulnerable because of

- Default Accounts
- Default Passwords
- Un-necessary Services
- Remote Access
- Logging and Audit Disabled
- Access Controls on Files

We should ensure that these vulnerabilities are removed from the systems.

Security by Monitoring

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 riskappropriate 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.

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

Security has to implemented at all levels i.e. Network, NOS, Application and RDBMS.

Security of Network: Firewalls are used for Perimeter Defence of Networks. Using Firewall Access Control Policy is implemented. It controls all internal and external traffic

Security of OS/NOS:

- Keep up-to-date Security Patches and update releases for OS
- Install up-to-date Antivirus Software
- Harden OS by turning off unnecessary clients, Services and features

Security of Application

- Keep up-to-date Security Patches and update releases for Application Package
- Preventing usage of unauthorized and unsafe software
- Precautions with Emails
- Protection from Phishing attacks
- Securing Web Browsers

Security of RDBMS

For securing data the following are needed:

- User Access Control
- Password Policy Management
- Managing Allocation of Resources to Users
- Backup and Recovery
- Auditing

BSNL Information Security Policy

BSNL has formulated its Information Security Policy and circulated for its implementation during December 2008. The BISP consists of two sections:

Section A

This provides the directives and policies that would be followed in ICT facilities within BSNL to provide secure computing environment for BSNL employees and business to run. The policies are formulated around 11 domains of security. These are

S#	Domain
1	**Information Classification and Control**
1.1	Data Owners
1.2	Information Classification
1.3	Information Labelling & Handling
2	**Physical and Environmental Security**
2.1	Physical Security
2.2	Environmental Security
2.3	Power Supply
2.4	Cabling Security
2.5	Security of the Information System Equipment
2.6	Physical Security of Laptops
2.7	Clear Desk and Clear Screen Policy
3	**Personnel Security**
3.1	Security during Hiring, Transfer and Termination
3.2	User Responsibilities / Accountability
3.3	Security Awareness & Orientation Sessions
4	**Logical Access Control**
4.1	User Access Management

S#	Domain
4.2	User Responsibilities
4.3	Desktop/Laptop Logical Security
4.4	Usage of Sensitive System Utilities
5	**Computing Environment Management**
5.1	Identification of Hardware
5.2	Emergency Procedures / Privileged Accounts
5.3	Documented Operating Procedures
5.4	Incident Management Procedures
5.5	Segregation of Duties
5.6	Security of System Documentation
5.7	Computer Virus Control
5.8	Disposal of Media
5.9	Configuration Management
6	**Network Security**
6.1	Network Management Controls
6.2	Network Devices
6.3	Remote Access
6.4	Network Diagnostic Tools
7	**Internet Security**
7.1	Internet Use
7.2	E-mail Security
7.3	Firewall Security
8	**System Development and Maintenance**

S#	**Domain**
8.1	Controlled Environment
8.2	Change Request
8.3	Source Code Management
8.4	Version Controls
8.5	Testing
8.6	Retention Requirements
9	**Business Continuity Planning**
9.1	Contingency Planning
9.2	Backup and Recovery Procedures
10	**Compliance**
10.1	Use of unauthorised software
10.2	Purchasing and regulation of Software Use
11	**Third Party and Outsourcing Services**
11.1	Risk Assessment
11.2	Access Control
11.3	Security Conditions in Third Party Contracts
11.4	Security Conditions in Outsourcing Contracts
11.5	Service Level Agreements

Section B

This provides the technical solution support to the policies mentioned within the policy document. It is intended to allow policy makers and architects within BSNL to prepare solutions around the various security requirements as proposed in Section A.

All BSNL employees are to implement BISP and Violation of these Policy Standards may result in immediate disciplinary action.

Summary of Action Items

- Classy the information and according handle it.
- Secure Physical Environment and Access
- Remove Unnecessary Services
- Secure and Properly Administer Network
- Secure Perimeter
- Apply Patches in Time
- Install Antivirus Software
- Prevent usage of unauthorized and unsafe software
- Make Contingency Plan and Backup Data
- Encrypt Sensitive Data
- Proper Monitoring

Conclusion:

Caution is the word when it comes to Information Security. In an era, when information is the power and wealth for an organization, one cannot expect taking chances with it. Therefore, it is advisable not only to secure the physical access to the information, but also to manage the security as organizational initiative by implementing BISP. ‘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 not be sufficient for today. We have to review periodically to find the gaps and take immediate action to fill them.