Information Security Issues

CC Faculty
ALTTC, Ghaziabad

Information Security

- Information is perhaps most important pie of corporate wealth
- Quality information is hard to acquire and easy to lose.
- Information Nature : Easy to move and easy to alter and this aspect has added insecurity dimension to information.

Information Security

- Vital if Information is on Network
- 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

What is Information Security

It ensures

- **Availability,**
- **Integrity and**
- **Confidentially of information**

What is Information Security

It involves

- The security at all levels viz
  - Network
  - OS
  - Application
  - Data

Information Security

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

Security Policy Preparation

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

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

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

Conduct A Risk Analysis ....contd

- Identify the types of Users for each resource
- Users – Admn, privileged, Normal Users, Partners, Others

Conduct A Risk Analysis ....contd

System	Description	Risk Level	Types of Users
ATM switches	Core network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Network routers	Distribution network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Closet switches	Access network device	Medium	Administrators for device configuration (support staff only); All others for use as a transport
ISDN or dial up servers	Access network device	Medium	Administrators for device configuration (support staff only); Partners and privileged users for special access
Firewall	Access network device	High	Administrators for device configuration (support staff only); All others for use as a transport

Conduct A Risk Analysis ....contd

DNS and DHCP servers	Network applications	Medium	Administrators for configuration; General and privileged users for use
External e–mail server	Network application	Low	Administrators for configuration; All others for mail transport between the Internet and the internal mail server
Internal e–mail server	Network application	Medium	Administrators for configuration; All other [illegible]
Oracle database	Network application	Medium or High	[illegible] system administration; Privileged users for data updates; General users for data access; All others for partial data access

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

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.

Prevention

- Approving Security Changes
- Monitoring Security of your Network

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

Important Guidelines

- Change Passwords to Network Devices on a routine basis
- Restrict Access to network Devices to an approved list of personnel
- Ensure that current software levels of network equipment and server environments are in compliance with security configuration requirements.

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

Response

- Security Violation
- Restoration
- Review

Actions to be Taken in Case of Violations

- 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

Actions in Case of Violations for Analysis

- 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

Security Incidents - Reasons

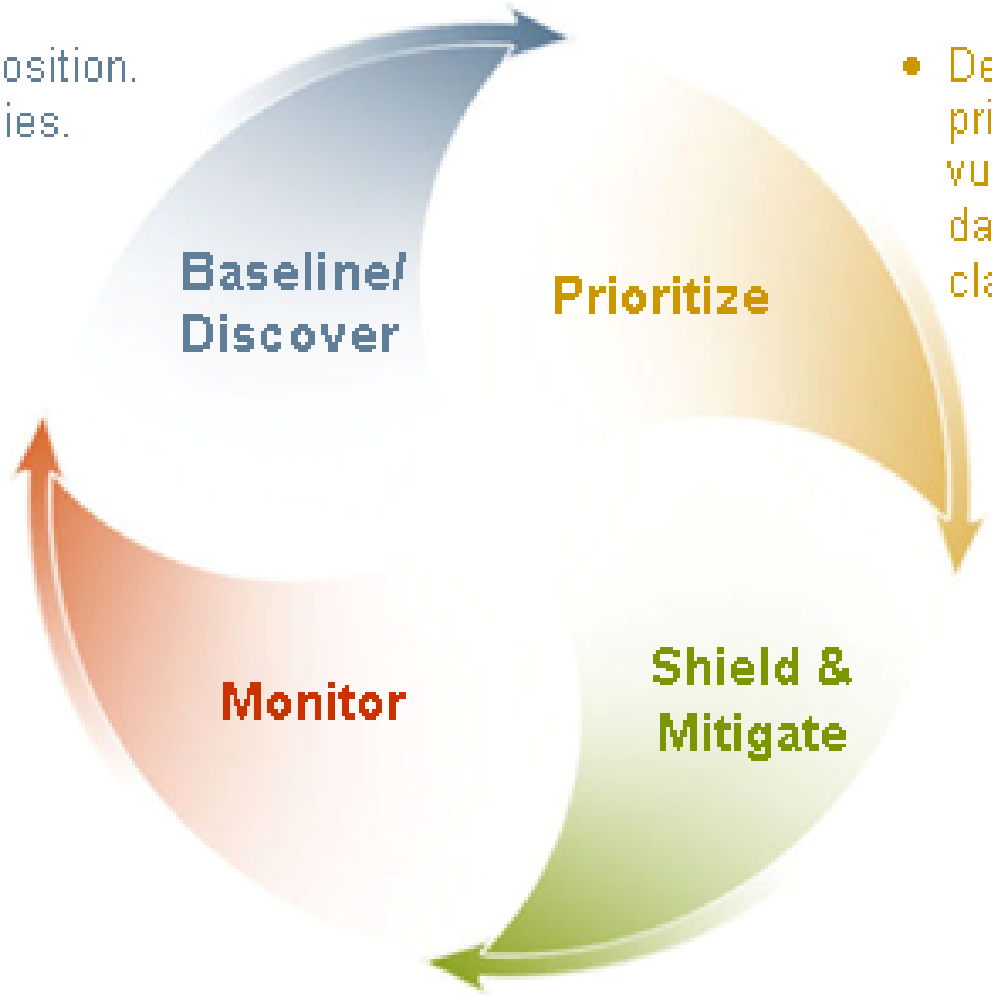
- Known Vulnerabilities
- Configuration Errors
- Virus Attacks

What Needs to be done

- Secure Physical Access
- Remove Unnecessary Services
- Perimeter Security
- Proper Network Administration
- Apply Patches in Time
- Antivirus Software
- Encrypt Sensitive Data
- Install IDS

Vulnerability Management Lifecycle

- Establish "as is" position.
- Identify vulnerabilities.
- Develop ideal baseline.



- Determine risk and prioritize based on vulnerability data, threat data, and asset classification.

Thanks!