E3-E4 – CFA
IT Security

Information Sensitivity

- Information is the most important asset 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

ISO 17799:2000 defines this as the preservation of:

- Confidentiality
  - Ensuring that information is accessible only to those authorized to have access
- Integrity
  - Safeguarding the accuracy and completeness of information and processing methods
- Availability
  - Ensuring that authorized users have access to information and associated assets when required

How to Secure Information?

It involves

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

Security Attacks

Who is Attacker/Hacker?

- Internal
- External

Hacking is not difficult

Attack tools are available

- Ready made exploits
- Attack Tools (e.g.)
  - Port Scanners (Fport, Hping2 ..)
  - Vulnerability Scanners (Retina…)
  - Password Crackers (John the Ripper..)

Indications of Infection

Attack tools are available

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

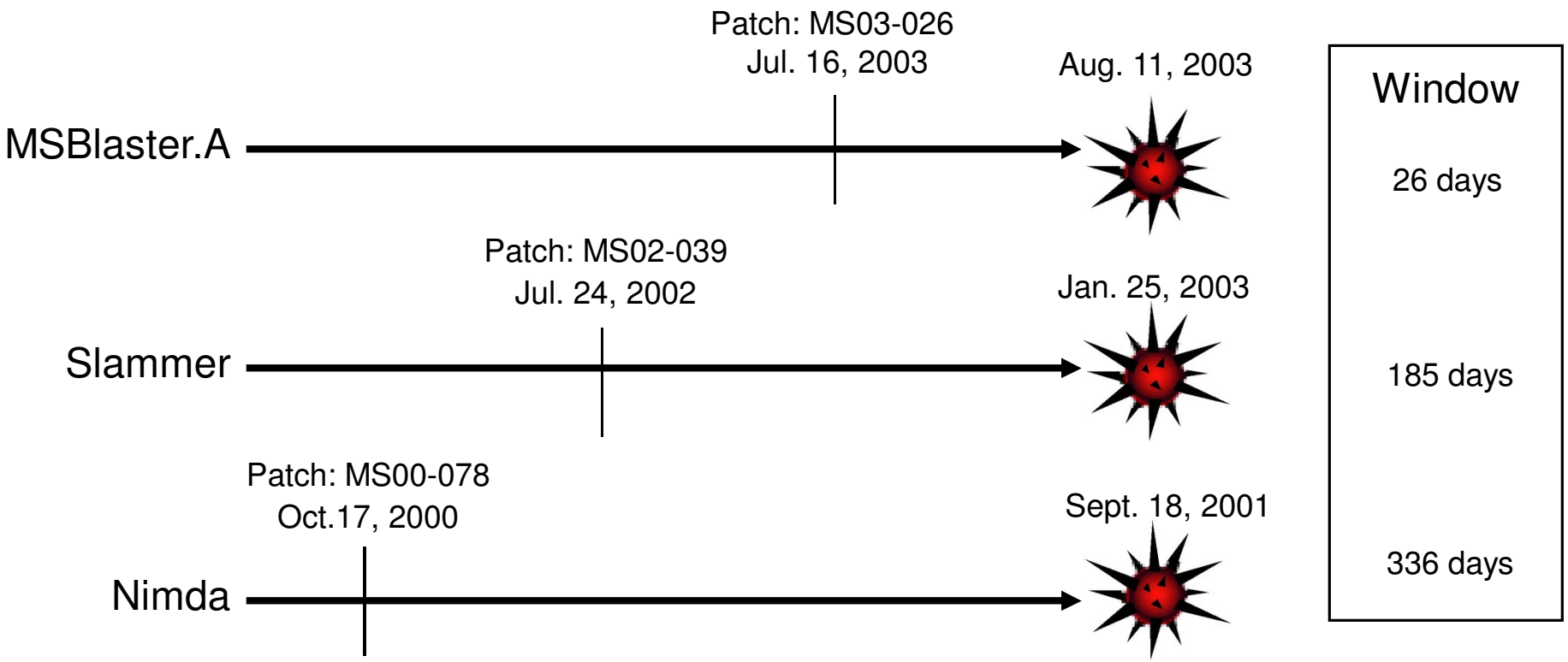
Security Incidents - Reasons

- Malware (Malicious Codes)
- Known Vulnerabilities
- Configuration Errors

Various Malicious Codes

- Virus
- Worms
- Trojan Horses
- Bots
- Key Loggers
- Adware and Spyware

Some known Vulnerability



Window of time from patch availability to outbreak is shrinking

Vulnerable Configurations

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

Information Security Management

- Start With a Focused Methodology
- Evaluate the Organization's IT Infrastructure
- Explore Departmental and IT Controls
- Identify Gaps and Establish Controls

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.

Create Usage Policy Statements

- Start With a Focused Methodology
- Outline Users' Roles and Responsibilities
- Identify specific actions that can result in punitive actions;
- Outline Partner Use Statement
- Outline Administrator Use Statement

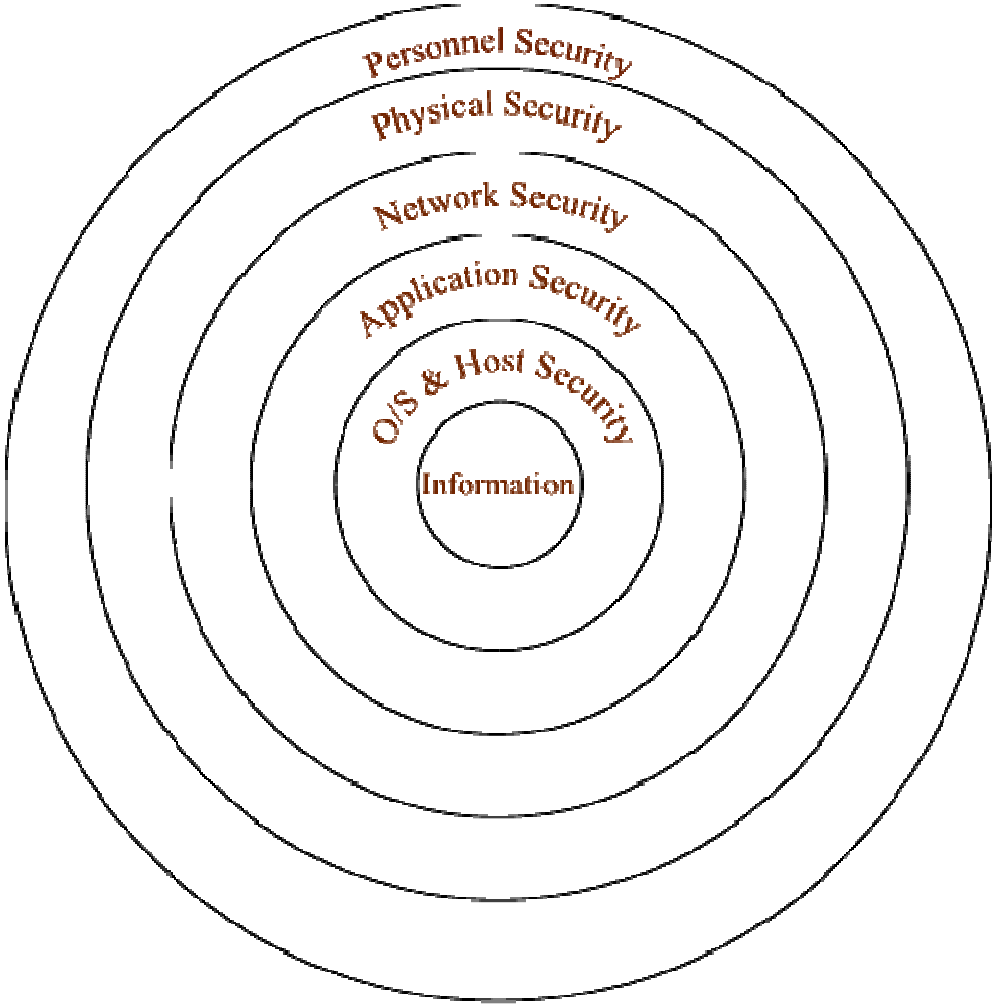
Conduct A Risk Analysis

- 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
- Identify the types of Users for each resource

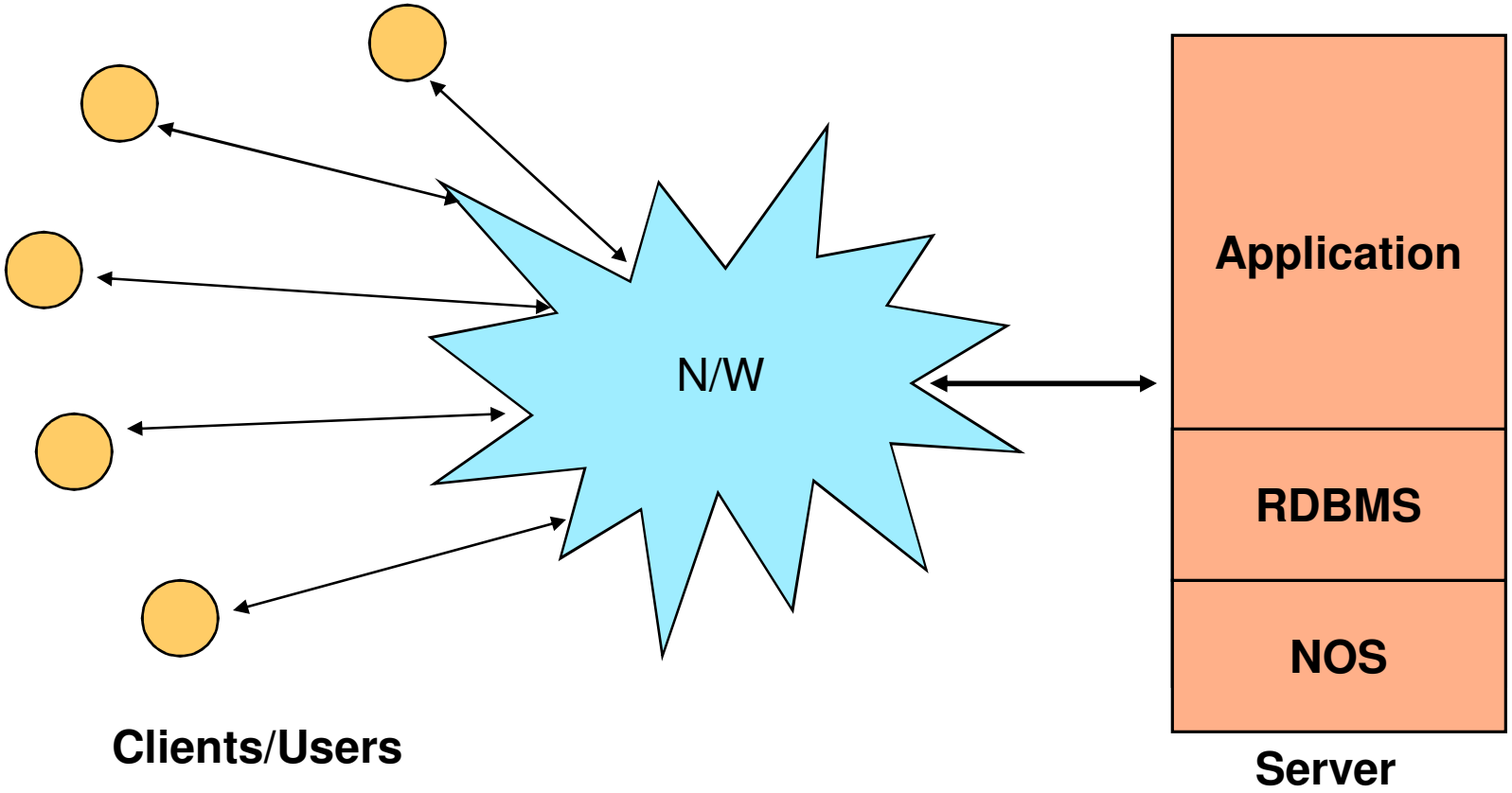
Monitoring Security of Network

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

Approach to Info Security: Defense in Depth



How to Secure Information?



Defensive Measure - OS

- Firewalls are used for Perimeter Defence
- Using Firewall Access Control Policy is Implemented.
- It controls all internal and external traffic.

Perimeter Defence

- Firewalls are used for Perimeter Defence
- 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

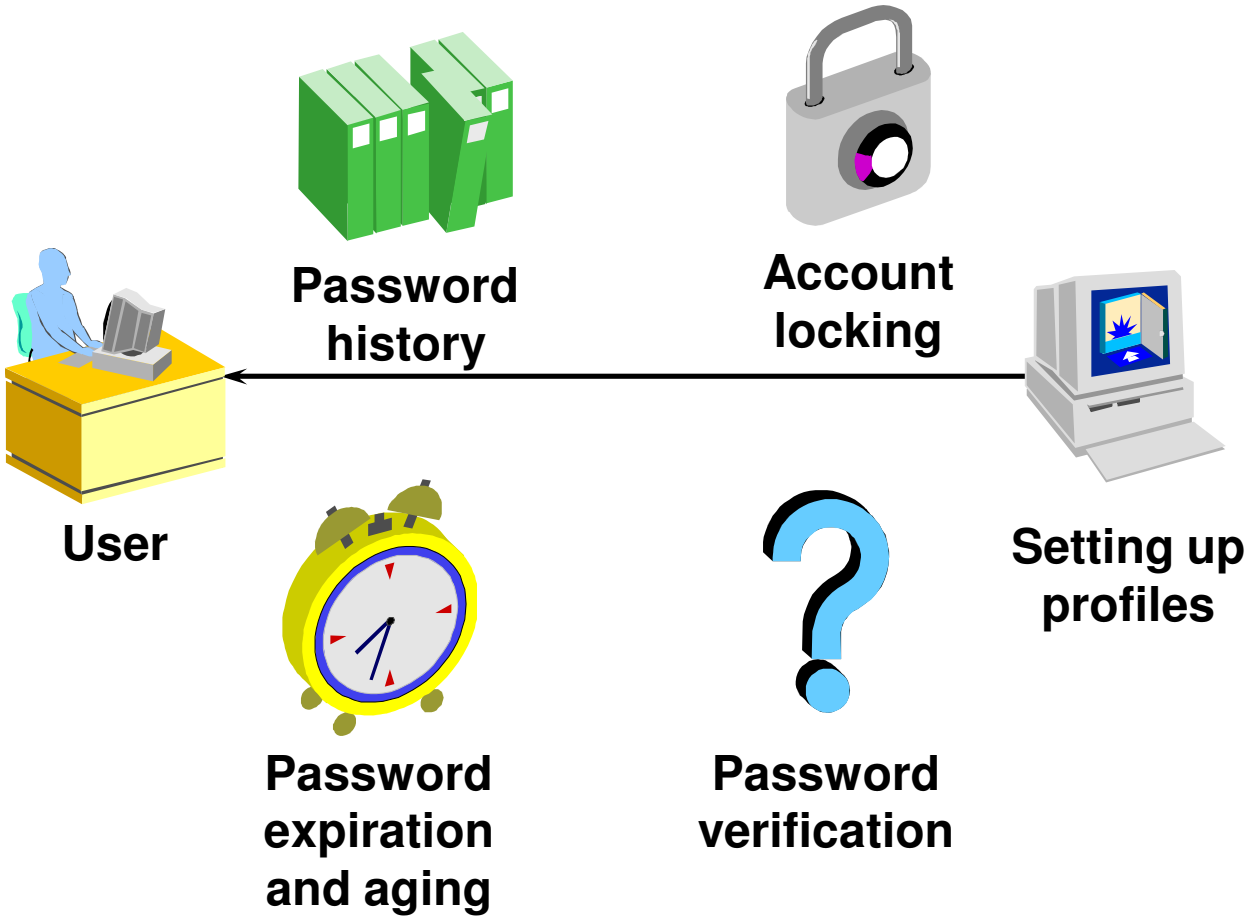
Defensive Measure – User Application

- Keep up-to-date Security Patches and update releases for Application Package
- Don’t Install Programs of unknown origin
- Precautions with Emails
- Protection from Phishing attacks
- Securing Web Browsers

Database Security Aspects

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

Password Management



Setting Resource Limits

- Number of Concurrent Sessions
- Elapsed Connect Time
- Period of Inactive Time
- Total CPU time
- Number of Datablocks

Backup and Recovery Issues

- Protect the database from numerous types of failures
- Increase Mean-Time-Between_Failures (MTBF)
- Decrease Mean-Time-To-Recover
- Minimize Data Loss

Auditing

- Auditing is the monitoring of selected user data base actions and is used to :-
  - Investigate suspicious database activity
  - Manage your audit trail
  - Monitor the growth of the audit trail
  - Protect the audit trail from unauthorized access

Summary of Action Plan

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

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:

BSNL Information Security Policy

Section A

- Information Classification and Control
- Physical and Environmental Security
- Personnel Security
- Logical Access Control
- Computing Environment Management
- Network Security
- Internet Security
- System Development and Maintenance
- Business Continuity Planning
- Compliance
- Third Party and Outsourcing Services

BSNL Information Security Policy

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.


Thank You!