IT -Security Prevention Guidelines

BY: Mahesh Singh Kathayat

MSC in Computer Engineering

1.Success of Information Security depends upon:

- Developing good basic working practices.
- Establishing procedures to ensure that they maintained.
- Creating a security-conscious atmosphere.
- Establish disciplined approach.

1.1Management responsibilities

- All senior management , and not just the computer security manager, should be sufficiently familiar with the computer systems in use.
- The role of system Administrator(SA)/ Database Administrator (DBA) must be highly computer literate to be able to administer the system in a secure and responsible manner.
- The SA/DBA access level should be restricted to the minimum number of staff.
- Computer security manager must have rights to check on the SA/DBA activities.
- The only way of establishing how a problem has occurred is to examine the logging information stored on the computer.

1.2System Administrator /Database Administrator responsibility

- People chosen for the job are absolutely reliable.
- They should be security screened
- Access to information should be restricted to that which the individual “needs to know” to do his job.
- Particularly sensitive material should be split into sections so that each section can be handled by different member of staff. or
- No member of staff should have access to all the information.
- Staff must be properly trained.
- Encourage employees to report incidents in time.
- Security and data confidentiality obligations must be included in employees contracts.

1.3User responsibilities

- Do not use any computer equipment without permission.
- Do not try to access information unless you know you are authorized to do so.
- Do not alter any information on a computer unless you know you are authorized to do so.
- Do not use the computer for personal matters.
- Do not leave a working computer unattended.
- Keep your password and user-ID confidential.
- Remember that anything done on the system using your ID and password is your responsibility.
- Do not use anyone else’s password and do not allow anyone else to use your password.
- Security and data confidentiality obligations must be included in employees contracts.

2.User Identification

- Passwords
- Smart Card
- Biometric

2.1Password System

- Be issued to an individual and kept confidential.
- Be distinct from user-ID
- Passwords must be alphanumeric and at least six characters long.
- Be changed regularly, at least every 30 days.
- Be properly managed password history list and frequently used passwords.
- P must be removed immediately if an employee leaves the organization or gives notice of leaving.
- Care should be taken with the password used for remote maintenance.
- Standard passwords which are often used to get access to different systems, for maintenance purposes ,should be avoided.

2.2Magnetic stripe card

- As its name suggests, this type of card has stripe containing some confidential information to be used together with holders code.

2.3Chip Card

- Instead of magnetic stripe, the card has built in microchip. The simplest type contains a memory chip.

2.4Biometric systems

- Make use of specific personal characteristics (biometrics) of a specific person e.g fingerprint, voice, key-stroke characteristics or the pattern of the retina.

3.Authorization

- After identification and authentication of the user(subject) there must be a function and set rules to control what object (files, devices etc) each user is allowed to access. This is the Access Control system.

4.Logging

- Most computer systems have some kind of log/
  - Systems log
  - Transaction log
  - Security system log
  - Database log
  - Application log
  - Technical log (mainly on mainframes)

4.1A proper log will answer:

- Who (user)
- When (time-date)
- Where (place)
- What (event/activity)
- Additional (additional information depending on activity)

5.Backup

- Although modern computer systems are generally very reliable, breakdowns and failures do occur.SA/DBA and users can make mistakes which lead to the accidental destruction of information. To guard against total loss of information under circumstances , it is necessary to set up procedures for making regular copies of the information on the computer system on some form of back-up media.

5.1Guidelines for the Back-up:

- Make sure that regular back-up copies are made of both data and system files.
- Back-up cycles should be of sufficient length to be of some use in future.
- 24-hour overwrite cycles are not recommended.
- Take a full back-up (both system and data) out of the cycle on regular basis and archive it off site for an extended period.
- Back-up tapes/diskettes should be kept in a safe place under lock and key and away from the computer in case of fire, flood or deliberate interference, preferably off site.
- Periodically test the back-up to ensure that the information can actually be restored in an emergency, do not wait for disaster to strike to find the backup system does not work.