**SYSTEM SECURITY:**

The measures for data protection taken by an organization reflect its awareness and attitude towards information and information technology. If top management treats computers as a de humanized, intangible, but integrity would, at best, be lackadaisical. On the other hand, if the management considers information as an important recourse and computers as an aid in decision making one would find a positive approach and involvement by the management towards security of information. This attitude naturally percolates down to the lower levels and the workers consider the computer correspondingly an enemy.

One of the best and first steps in ensuring data security is to create awareness and develop a culture within the organization towards the ways in which information can be lost/alter and what would be the consequences, of such an occurrence, to the organization and individuals.

All other steps that can be taken are:

* IT Planning: The organization must decide on policy for introduction of IT. This must be done at the highest level and should address issues such as levels of protection for various aspects of information relating to the organization.
* Selection of technology, keeping in mind obsolesces due to new innovations and necessity for at the highest relating to the organization.
* Identification of points of exposure of weak links to device means to plug them.
* Physical protection of machine and media.
* Information classification.
* Responsibility for security.
* User Training to increase security awareness and propagation of do’s and do not.
* Guidelines for creation and changes to password, etc.

Principles for ensuring security and recovery in case of breaches of security:

**PREVENTION:**

The best method is to of course stop all breaches of security before they occur. ‘Need-to-knows’ policy is an offshoot of the principle of preventions.

**DETECTION:**

However, one may try to ensure it, total security is almost impossible. The next principle, therefore, is the one must be able to detect breaches in security, whenever they occur, within the shortest possible time. This helps in damage assessment and, also, in devising further preventive measures.

**DAMAGE MINIMIZATION:**

There must be enough resilience in the system to recoup the losses, damage and become functional, by reinstating the status, at the earliest.

**PHYSICAL SECURITY:**

These involves-

* Physically bolt down the PC to a table so that it can’t be casually lifted and taken away.
* Use lockable rooms for PCs, specially those handling sensitive data. Making it a practice to lock the room when we leave.
* Keep a record of all floppies in use; do not permit alien floppies into the organization.
* Keyboard and PC locking devices can’t be fitted to the PC.

**SOFTWARE SECURITY:**

These involves-

* Use of original software for operating system, Compilers and software packages as they are bug-free, also known as “Licensed” software.
* Using correct procedures to shut down the PC so that all files would be properly closed.
* Keeping back-ups of all files.
* If we develop our own applications, we should introduce passwords to access the application.

**PROTECTION AGAINST VIRUS:**

These involves-

* Building employee awareness of the risk.
* Make system/server files “Read only”.
* Try to obtain source code for important software in use and compile it in-house.
* Check executable code, using “debug” or separate utilities to study code structure and check spaces for viruses.

**PASSWORD SECURITY:**

Only a given user, terminal or another resource can access data to which permission has been guaranteed to read, write or alter. Thus a matrix can be created to indicate which user have access to which files, records or fields. If the user request passes the matrix, he is allowed to access, otherwise he is denied access to some parts of the database.