Organizational Security

Prof. Dr. Eşref ADALI

www. Adalı.net

Concerns


Data
Confidentiality
Sources
Integrity
Reputation
Availability

Development of Security

Policy of Security : The importance of security may vary depends on organization. While data are important for a company, reputation is more important for others.

Standards : There ara some national or international security standards. Organization should be satisfied to these standars. For example if a bank is not stisfy them, its operaion will be stoped.

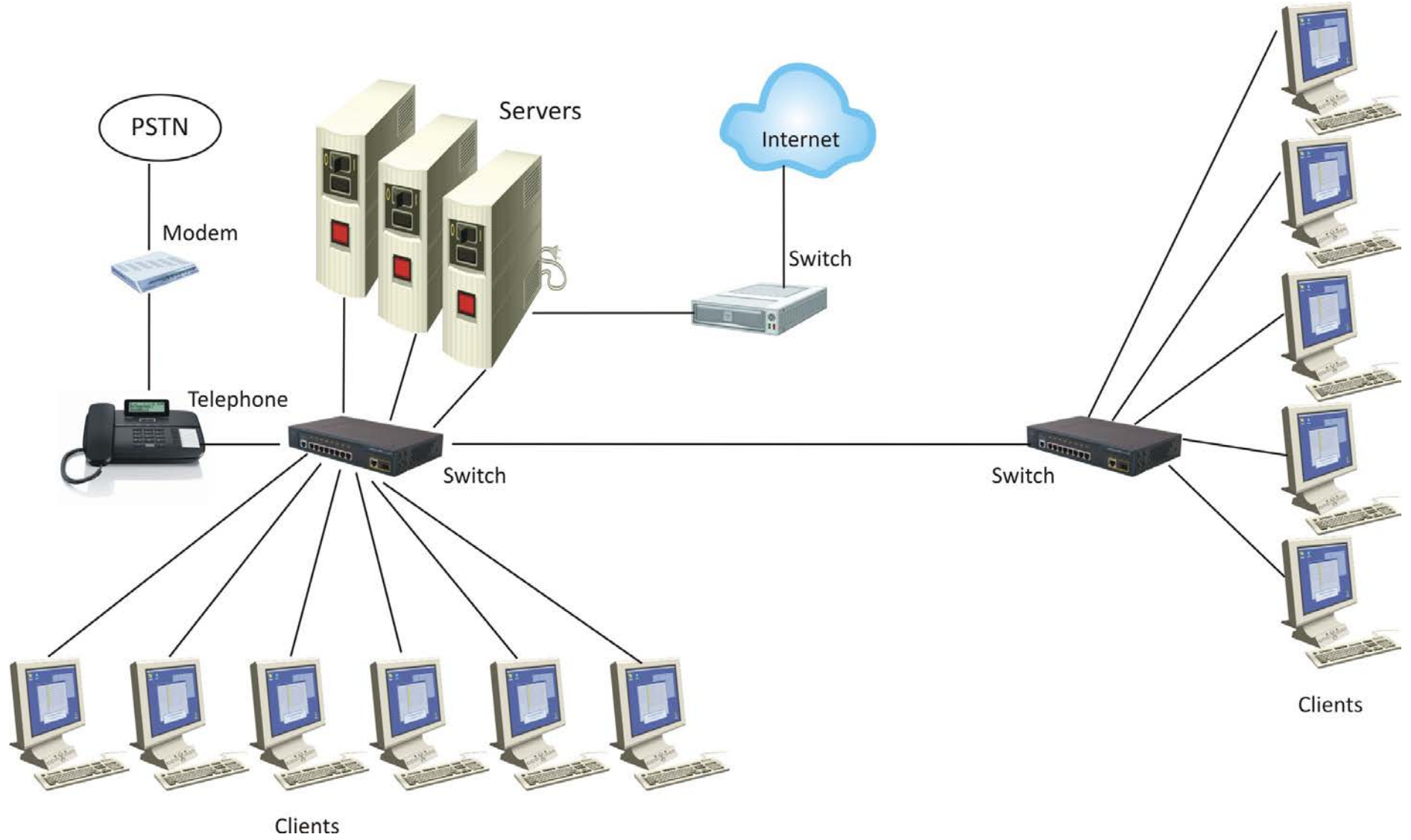
Principle : Each organization should have some security principle. These principle are proposal for policy of organization

Process : Process are explain step of action about security, shuch as necessary protection, what will do against to attack.

Duties of Security Department

Examination and Planning

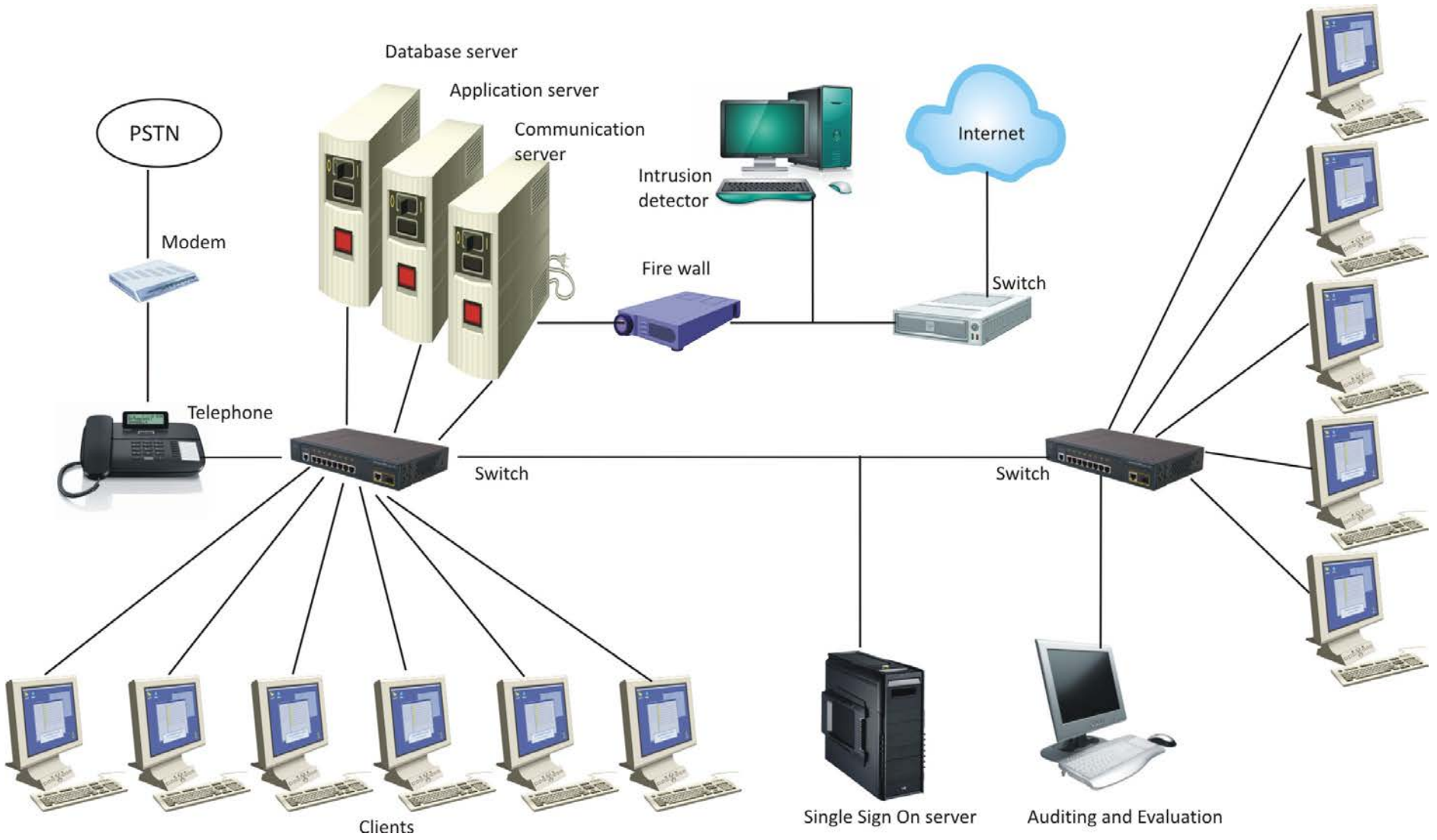
- Current situation of IT system must be examine in terms of security
- In order to make IT system make a new plan



Application

Some necessary devices are added to IT system which are:

- Intrusion detector
- Fire wall
- Single Sign on Server
- Auditing and Evaluation Server



Auditing

Auditing and logging for each user:

- Logging and logout time to system in working hour
- Logging and logout time to system out of working hour
- Logging and logout time to system from out of organization
- Logging and logout time to software that user has the right to access it
- The time and numbers of try to access a software that user has not the right to access it
- Logging and logout time to database that user has the right to access it
- The time and numbers of try to access a database that user has not the right to access it
- The IP of user

The results of auditing must be written on log file

Evaluation

Evaluation system analysis the auditing log file and prepare a report.

Authorization and Delegation

Top management : Responsible for all sources and data of organization

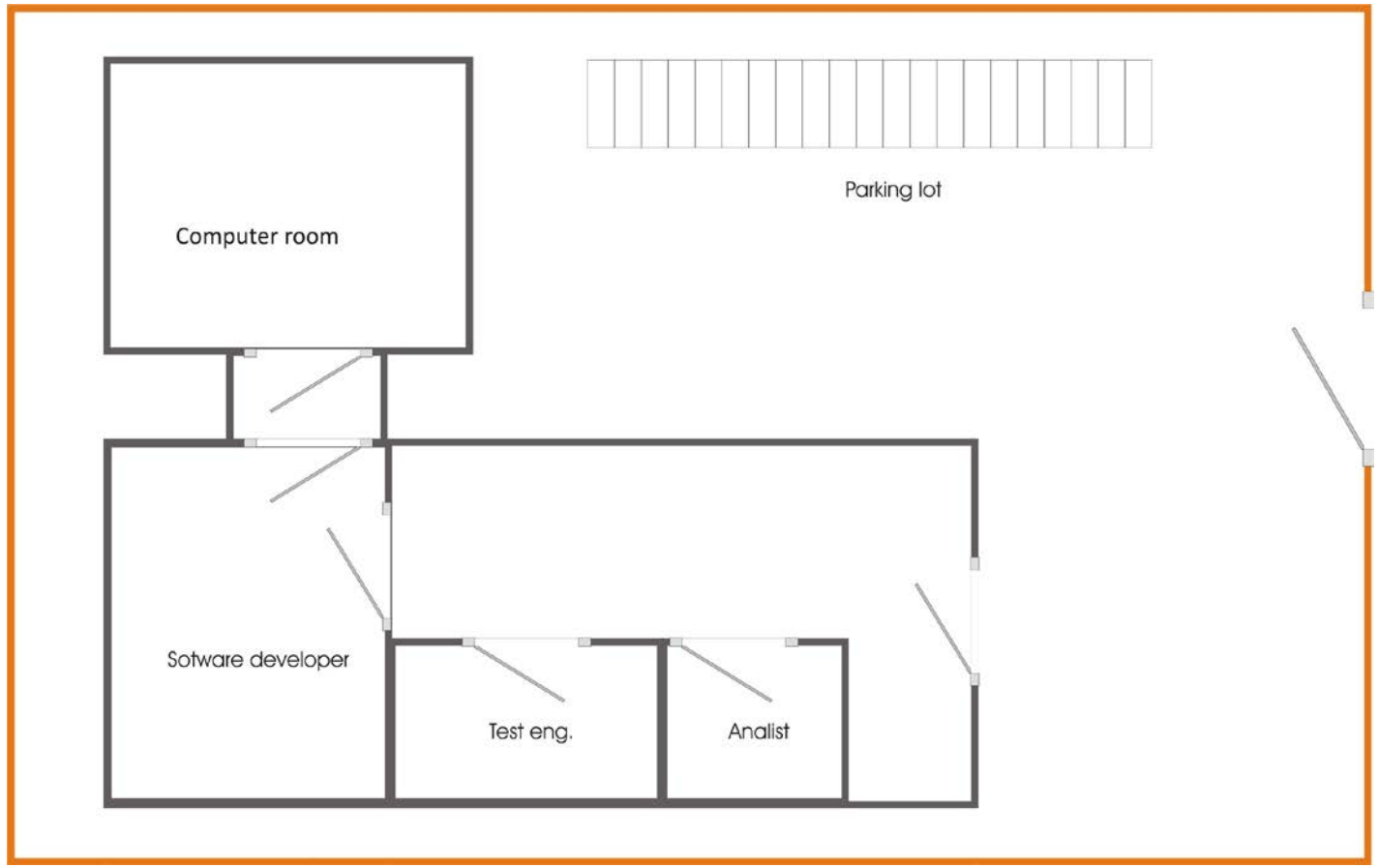
Manager of IT Security : Responsible to carry out IT security according to policy of organization

Users : They have to work according to process of organization

- They promise to obey the rules of organization
- Keep in secret the ID and password
- Turn of the computer when work is ended
- Inform the manager if see any unusual event
- Keep the door close for security
- Obey all laws and regulations
- Careful about secret document and data

Physical Security

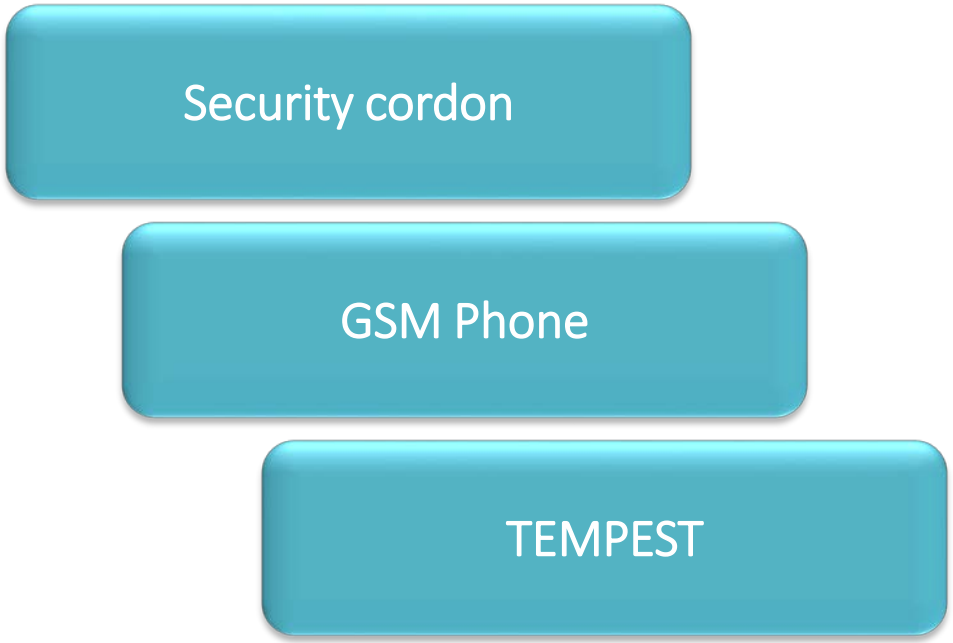
- Computer room must be midpoint of organization
- Floor must me solid
- Only one door access
- Door must be fire proof
- No false floor or ceiling
- No windows
- The walls must be concrete shear Wall
- One electricity panel
- Fire detection and holon base extinguisher system must be installed
- Has own air condition system which has high level filter.
- Has surveillance camera



Door System

- Control by warden (3 shifts)
- Can open by badge
- Baffle gate

Additional Cares

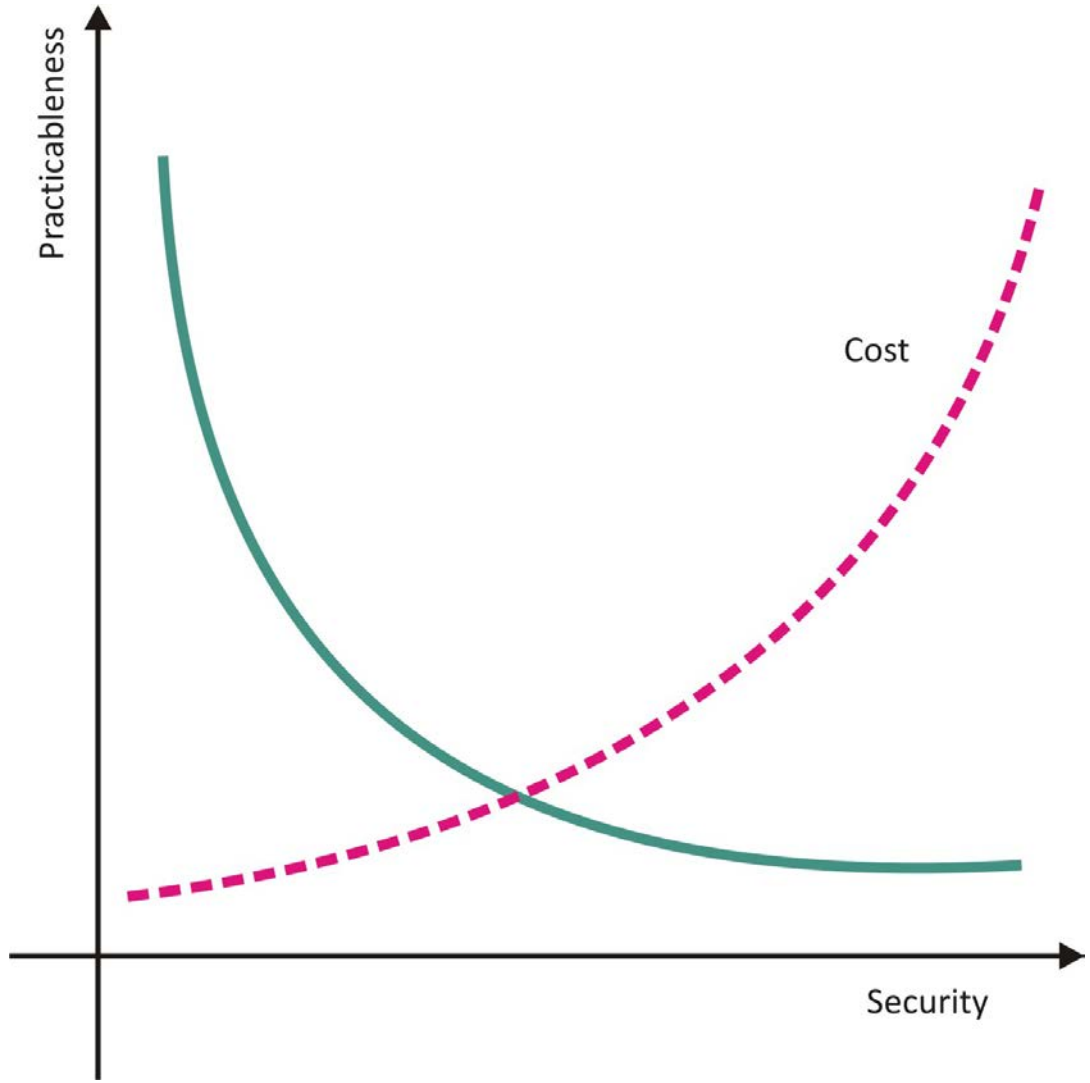


Backup and Disaster Center

- Backup of data must be taken frequently
- Backup must be saved out of computer room
- A mirroring data base system should be used
- A disaster center is needed for higher security

Cost of Security

- Which entities must be protected?
- What are importance degree of each entity?
- From where attack come ?
- Why attacks come ?
- Who will attack ?
- What is the probability of corruption ?
- What will be cost of corruption as far as financial and reputation are concerned?
- What will be the cost of recovery of system
- What is the cost of small corruption?
- What is the cost of big corruption?



Physical Connection

- Coaxial cable
- Twisted pair cable
- Fiber cable
- Wireless connection