

Physical Security for Computer Centers

Ralph Earl

Ralph F. Earl Associates, Inc.

Bryn Mawr, Pennsylvania

Web Page-www.ralphearl.com

Tel: 610 896 4433

Fax: 610 896 2134

Confucius

551 B.C.

- “When the perfect order prevails, the world is like a home shared by all. -----
- Villains such as thieves and robbers do not exist. The door to every house need never be locked by day or night. These are the characteristics of an ideal world.”

Physical Security Program for Information Systems

- Policy and procedures identify purpose and responsibilities.
- An element of site security and life safety.
- Protection of areas with high sensitivity and highly critical operations.
- Relates to location, physical construction, technical systems and human resources.

Components of Physical Security for Computer Center

- Access Control Systems.
- Intrusion Detection Systems.
- Closed Circuit Television (CCTV).
- Fire/Smoke Detection and Suppression Systems.
- Emergency Power and Lighting.
- Water Leak Detection.
- Monitoring Environment Humidity/Temperature

Use of Physical Security Procedures & Systems

- Identify and assess threats and vulnerabilities to Computer Center and occupants.
- Evaluate existing security systems and level of site security.
- Determine type and level of systems and personnel required.

Considerations for Security System Applications

- Construction of Computer Center. Windows, ductwork, dropped ceilings.
- Location and number of access points to Center. Doors, elevators, stairways.
- Personnel authorized access. Employees, contractors, temporary staff.
- Budget

Problems and Weaknesses

- Access by “Tailgating.”
- Lack of system, procedures or personnel to monitor access.
- Personnel disregard access control procedures.
- Insufficient access controls for sensitive areas within Computer Center.
- Lack of procedures for administrative action for violations.

Administration of Access Controls for Computer Center

- Uniformity in background investigation requirements. Employees and Contractors.
- Identification card program.
- Visitor controls.
- Accountability for introduction and removal of equipment and inventory items.
- Coordination with Facility's Security Office.

Fire Prevention, Detection and Suppression

- Systems meet local code and insurance requirements.
- Fire detection system in place. Ceilings, air ducts and raised floor.
- Fire extinguishing systems have automatic activation capability.
- Maintenance program in effect.

Fire Prevention, Detection and Suppression

- Conduct emergency fire drills.
- Procedures for “Hot Work.”
- Maintain clear paths in emergency egress areas.

Emergency Plans and Procedures

- Bomb threats.
- Medical emergencies.
- Threats against employees.
- Natural Disasters and Accidents.

Emergency Lighting and Backup Power Sources

- Sufficient power and lights for orderly and timely shutdown of computer equipment and operations.
- Test emergency sources.
- Y2K potential power problems and public utilities.
- Confirm documentation procedures for temporary shutdown.

Computer Center Security Audit

- To assure equipment, personnel, operations and related areas controlled and protected.
- Adequacy of insurance coverage.

Sample Layout

