Course: Information Security Management in e-Governance

Day 2

Session 3: Physical and Environmental Security

Agenda

- Introduction to physical and environmental infrastructure elements needed for supporting IT Infrastructure management
- Information security challenges and risks related to physical and environmental aspects surrounding information security systems
- Security considerations and solutions for securing physical and environmental aspects related to Information Systems

Physical Security: so what do you check ?

- Physical access : Is there is any perimeter control for protecting against access? Is it regularly monitored or tested?
- Does access control exists to all ‘entry points’ to the facilities? Is it effective?
- Are computer program , information / documentation, data and media under secure storage?
- Does a backup power supply exists that is capable of operating the computer systems , servers , air conditioning, heating and lighting?
- Are there comprehensive instructions or procedures to be followed in case of a physical and environmental threat?

Physical Security: so what do you check ?

- Fire : Are there adequate fire precautions in the facility including detectors , alarm systems etc?
- Are all the areas kept free of combustible material ?
- Are all fire prevention and fire-fighting equipments regularly services and checked by their manufactures ?
- Has the risks from storms and other natural disaster evaluated and catered for ?

Physical and Environmental Security

- Often , ‘physical and environmental security’ is either overlooked or considered ‘boring and dry’
- Physical & Environmental security – an important aspect of information security
- Physical penetration offers the hacker or malicious user access to sensitive data with less acumen making it tempting attack method.
- Physical security of Information systems means literally their ‘physical’ protection.
- Physical threats can damage computer installations , data centers and computer networks
- e.g : e-mails should not be lost because there is a flood in the basement

Importance of Physical Security

- Most people focus on protecting *logical systems* (software that is running)
- If you cannot protect the *physical systems* (computer hardware), you cannot protect the program and data running on the hardware
  - Physical security deals with who has access to buildings, **computer rooms,** and the devices within them
  - **Protect** sites from natural and man-made physical **threats**

Physical Security Baseline Definitions

- Physical security involves measures undertaken to protect personnel, equipment and property against anticipated threats.

- Passive measures include the effective use of architecture, landscaping and lighting to achieve improved security by deterring, disrupting or mitigating potential threats.

- Active measures include the use of proven systems and technologies designed to deter, detect, report and react against threats.

Physical Security Baseline Definitions

- ISO 27001 role of physical security – Protect the organization's assets by properly choosing a facility location, maintaining a security perimeter, implementing access control and protecting equipment.

- The physical security office is usually responsible for developing and enforcing appropriate physical security controls, in consultation with the computer security management, program and functional managers, and others, as appropriate. Physical security should address not only central computer installations, but also backup facilities and office environments.

- In the government, this office is often responsible for the processing of personnel background checks and security clearances.

- What is the impact of convergence (merging IT security and physical security) on this role and how does it play into the responsibilities for physical security risk assessments and action plans?

Understand risks surrounding physical and environmental eco system

Physical Security Threats

- Weather
  - Tornadoes, hurricanes, floods, lire, snow, ice, heat, cold, humidity, etc.
- Fire/chemical
  - Explosions, **toxic** waste/gases, smoke, fire
- Earth movement
  - Earthquakes, mudslides
- Structural failure
  - Building collapse because of snow or moving objects (cars, trucks, airplanes, etc.)

Physical Security Threats (cont'd.)

- Energy
  - Loss of power, radiation, magnetic wave interference, etc.
- Biological
  - Virus, bacteria, etc.
- Human
  - Strikes, theft, sabotage, terrorism and war

Impact to the business due to these risks

Physical Security Compromise : Outcome

- Theft and fraud
- Loss of confidentiality
- Loss of privacy
- Loss of integrity
- Loss of availability

Approach to Managing physical and environmental security

If someone really wants to get at the information, it is not difficult if they can gain physical access to the computer or the physical Infrastructure !!!

Physical Security Planning

A physical security planning must address:

- Crime and disruption protection through *deterrence* (fences, security guards, warning signs, etc.)
- Reduction of damages through the use of *delaying* mechanisms (e.g., locks, security personnel, etc.)
- Crime or disruption *detection* (e.g., smoke detectors, motion detectors, CCTV, etc.)
- Incident *assessment* through response to incidents and determination of damage levels
- *Response* procedures (fire suppression mechanisms, emergency response processes, etc.)

Physical and Environmental Security Policy – Policy Sections

- The Physical and Environmental Security Policy consists of the followings
  - Physical Security
  - Environmental Security
  - Power Supplies
  - Cabling Security
  - Physical Security of IT Infrastructure
  - Clear Desk and Clear Screen..

Physical Security - Standards

Computer and Communication Rooms

- Access to computer and communication rooms should be controlled and restricted to authorised personnel who needs access to perform their duties.
- Use of authentication mechanisms (e.g. biometrics, swipe card plus PIN number, proximity cards) should be considered for computer and communication rooms housing critical information system facilities.
- Computer and communication rooms should be monitored 24 hours a day. The monitoring can be by cameras, alarmed doors and windows, people manning the rooms, or a combination of these.
- Computer and communication rooms should be equipped with doors, which are resistant to forcible entry.

Physical Security Standards
Visitors and Third Parties

- Visitors and third parties should be only allowed entry to computer and communication rooms for authorised and specific purposes only.

- Visitors and third parties should not be permitted unsupervised access to computer and communication rooms. This arrangement should exclude employees of outsourcing agencies who are responsible for owning or operating an information processing facility.

- The date and time of entry and departure of visitors and third parties and the purpose of visit should be recorded in a visitor's log.

- The date and time of entry and departure and the purpose of entry of authorised personnel (including employees of outsourcing agencies) outside normal business hours or assigned hours of work should be recorded in a log.

Physical Security Standards
Identification Badges

All authorised personnel and visitors should be required to wear some form of visible identification (e.g. employee identification badges, visitor badges) within computer and communication rooms.

- Visitor badges should be of a different colour from employee Identification badges.
- Personnel should be encouraged to question unescorted strangers not wearing visible identification.
- Reconciliation of badges issued to visitors and third parties should be done at the end of each day.

Physical Security Standards

Identification Badges

- Its the responsibility of each employee or third parties, who has been issued an identification badge to immediately report lost or stolen badges.
- The original identification badge should be taken back wherever possible (e.g. broken, damaged cards) while issuing a duplicate card.
- Identification badges should be returned by an employee, when retired or terminated, and by personnel of outsourcing agencies at the end of the contract.
- Identification badges taken from retired or terminated employees should be destroyed in a controlled manner.

Physical Security Standards

Information Storage Media

- All information storage media (e.g. hard disks, floppy disks, magnetic tapes and CD-ROMs) containing sensitive or confidential data should be physically secured, when not in use.
- Physical access to magnetic tape, disk and documentation libraries should be restricted to authorised personnel based on job responsibilities.
- Back-up media should be stored in fire resistant safes or cabinets.
- Any personal information storage media like cartridge tapes, DAT drives, floppy drives should not be allowed to brought inside computer and communication rooms.
- Any storage media (floppy drives, CDs, DAT tapes) should not be allowed out of Government premises without adequate clearances from HODs/Security Officers.

Physical Security - Standards

Offsite Facilities

- Fall back equipment and back-up media should be stored at a safe distance (e.g. an offsite location) to avoid damage from a disaster at the main site.

- The physical and environmental safeguards available at the off-site location should provide the same level of security, at a minimum, as at the primary site.

Physical Security - Standards

Security Instructions

- Long term contractors, consultants and business associates should be issued instructions on the security requirements of the site.

Security Inspections

- Security inspections should be made regularly. The inspection should cover functionality and administration.

Physical Security Standards

Major Data Centres

- The following physical security controls should be followed for major data centres in addition to the standards mentioned above:

- Major data centres and facilities housing sensitive or critical systems should be clearly separated from other areas.

- Access should be restricted through use of electronic door locks and authentication mechanisms like biometrics, swipe cards or other form of electronic cards, which should require both card and a personal code or characteristic.

Physical Security Standards

Major Data Centres

- The electronic door locks should be equipped on doors that should automatically close and which should set off an audible alarm when they are kept open beyond a certain period of time.

- The doors should be equipped with burglar alarms.

- The electronic door locks should support anti pass back mechanism (i.e. disallow entry for more than one time, unless an exit is recorded in the system), remote locking and unlocking.

- There should be audible alarm for attempted unauthorised entry

Physical Security Standards

Major Data Centres

- Electronic door locks should not be deactivated without prior permission unless needed for situations like emergency evacuation in case of fire.
- Deactivation of electronic door locks should be documented.
- Access to the security software, which validates and records the ‘swipes’ or electronic card access, should be restricted to authorised individuals.

Physical Security Standards

Major Data Centres

- The Data center and access within the facility should be monitored 24 hours a day through the use of people manning the center, CCTV and alarm systems. The cameras should be located at strategic points.

- The video surveillance recording should be retained for a minimum period of atleast 7 days for possible future playback.

- The Systems Security Administrator should review access rights on a quarterly basis.

- Security inspections should be made regularly and at least within every 6 months. The inspection routine should include access control, alarm systems and burglar protection. The inspection should cover functionality and administration.

Physical Security Standards

Major Data Centres

- Third party vendors and consultants should be allowed supervised access only. This access needs to be authorised by the Systems Administrator.

- Personal information processing equipment like laptops should not be allowed inside a major data processing centre, unless authorised by the Chief Information Officer or the Systems Administrator, in the absence of the Chief Information Officer.

- An audit trail of all access should be securely maintained and reviewed on a daily basis.

Physical Security Standards

Electronic Access Cards for Major Data Centres

- Electronic access cards should be issued to employees and personnel from outsourcing agencies in a controlled manner with approval from the Chief Information Officer or the Data Centre In-charge.
- Electronic access cards should be personal. In case if an electronic access card is lost or stolen, the concerned staff should immediately report to the Chief Information Officer or the Data Centre In-charge.
- The electronic access card, which has been reported lost, should be deactivated within 12 hours.
- The original electronic access card should be taken back wherever possible (e.g. broken, damaged cards) while issuing a duplicate card.
- Electronic access cards should be returned by an employee, when retired or terminated, and by personnel of outsourcing agencies at the end of the contract.

Physical Security

Electronic Access Cards for Major Data Centres

- Electronic access cards should be returned by an employee, when retired or terminated, and by personnel of outsourcing agencies at the end of the contract.
- Non-returned electronic access cards of retired or terminated personnel (employees or staff from outsourcing agencies) should be deactivated immediately.
- Electronic access cards taken from retired or terminated employees should be destroyed or re-used in a controlled manner.
- The expiration period of electronic access cards issued to long-time third parties (e.g. employees of outsourcing agencies) should coincide with the end of the contract period.

CCTVs

- **Def**: A Television Transmission System That Uses Cameras to Transmit Pictures To Connected Monitors
- **CCTV Levels:**
  - **Detection**: The Ability to Detect the Presence of an Object
  - **Recognition:** The Ability to Determine the Type of Object (animal, blowing debris, crawling human)
  - **Identification:** The Ability to Determine the Object Details (person, large rabbit, small deer, tumbleweed)
- **Remember: Monitoring Live Events is <u>Preventive</u> and Recording of Events is <u>Detective</u>**

Environmental Security

Appropriate controls should be established to ensure environmental exposures (fire, cyclones, water, temperature and humidity) are adequately controlled.

Purpose & Objectives

Environmental exposure to information systems is primarily due to naturally occurring events like cyclones, floods and water damage besides fire, temperature and humidity.

The Environmental Security Policy defines the minimum controls, which should be in place to reduce exposure to these environmental threats.

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- It is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards

- Environmental Security
- Fire Safety
- Cyclones
- Floods and Water Damage
- Major Data Centers

Fire Detection and Response

Fire suppression systems are devices installed and maintained to detect and respond to a fire

They work to deny an environment of one of the three requirements for a fire to burn: heat, fuel, and oxygen

- Water and water mist systems reduce the temperature and saturate some fuels to prevent ignition
- Carbon dioxide systems rob fire of its oxygen
- Soda acid systems deny fire its fuel, preventing spreading
- Gas-based systems disrupt the fire's chemical reaction but leave enough oxygen for people to survive for a short time

Fire Detection

- Environmental Security
- Fire Safety
- Cyclones
- Floods and Water Damage
- Major Data Centers

Before a fire can be suppressed, it must be detected

Fire detection systems fall into two general categories:

- manual and automatic

Part of a complete fire safety program includes individuals that monitor the chaos of a fire evacuation to prevent an attacker accessing offices

There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection

- Smoke detectors operate in one of three ways: photoelectric, ionization, and air-aspirating

•Environmental Security
•Fire Safety
•Cyclones
•Floods and Water Damage
•Major Data Centers

Fire Suppression

Can be portable, manual, or automatic

Portable extinguishers are rated by the type of fire:

- Class A: fires of ordinary combustible fuels
- Class B: fires fueled by combustible liquids or gases
- Class C: fires with energized electrical equipment
- Class D: fires fueled by combustible metals

Installed systems apply suppressive agents, either sprinkler or gaseous systems

- Sprinkler systems are designed to apply liquid, usually water
- In sprinkler systems, the organization can implement wet-pipe, dry-pipe, or pre-action systems
- Water mist sprinklers are the newest form of sprinkler systems and rely on microfine mists

Water Sprinkler System

When the ambient temperature reaches 140-150° F,
the plastic pin melts, releasing the stopper and allowing water
to hit the diffuser spraying water throughout the area

- Environmental Security
- Fire Safety
- Cyclones
- Floods and Water Damage
- Major Data Centers

Gaseous Emission Systems

Until recently there were only two types of systems

- carbon dioxide and halon

- Carbon dioxide robs a fire of its oxygen supply
- Halon is a clean agent but has been classified as an ozone-depleting substance, and new installations are prohibited

Alternative clean agents include the following:

- FM-200
- Inergen
- Carbon dioxide
- FE-13 (trifluromethane)

Environmental Security Standards Fire Prevention

•Fire Safety

•Cyclones

•Floods and Water Damage

•Major Data Centers

- All computer systems should be housed in an environment equipped with portable fire extinguishers.
- The fire extinguishers should be accessible in all areas. The distance to the nearest portable fire extinguisher should be a maximum of 25 metres.
- Fire safety equipment should be checked regularly in accordance with manufacturer's instructions. The test results should be documented.
- Hazardous and combustible materials should be stored at a safe distance from server rooms and other computer rooms. Computer supplies such as stationery should not be stored in server rooms.
- Comprehensive fire and emergency instructions should be displayed in prominent locations.

•Environmental Security
•Fire Safety
•Cyclones
•Floods and Water Damage
•Major Data Centers

Environmental Security
Cyclones

- Computer and communication rooms in cyclone prone areas should be housed in buildings, which are resistant to cyclones e.g. use of permanent cyclone shutters for doors and windows, double doors, wind resistant roof sheathing etc.

- All computer systems should be moved away from windows or glass doors when a cyclone approaches, even if the windows or doors are covered.

- All computer systems should be located on a small interior room on the first floor in cyclone prone areas. This should ensure least impact of winds and floods.

- All computer equipment should be switched off or unplugged when a cyclone approaches to protect them from power surges.

•Environmental Security
•Fire Safety
•Cyclones
•Floods and Water Damage
•Major Data Centers

Environmental Security
Floods and Water Damage

- All server rooms should be housed in an environment equipped with moisture detectors.
- Computer and communication rooms should not be located in areas susceptible to water seepage and flooding like the basement.
- Computer and communication rooms should be located in raised or elevated floors in flood prone areas.
- Adequate drainage provision should be provided to prevent water damage or flooding.
- Electrical equipment, which may have received water damage, should be checked and dried before being returned to service.

•Environmental Security
•Fire Safety
•Cyclones
•Floods and Water Damage
•Major Data Centers

Environmental Security Major Data Centres

- The following environmental controls should be followed for major data centres and for critical systems in addition to the standards mentioned above:
  - Automatic fire suppression system, in combination with fire alarms, should be installed.
  - Smoke detectors should supplement the fire suppression system.
  - Smoke detectors should be placed above and below the ceiling tiles. The detectors should produce an audible alarm when activated.
  - The surrounding walls should be non-combustible and resistant to fire for at least 60 minutes. All openings to these walls (doors, ventilation ducts, etc.) should be likewise rated at least 60 minutes.
  - Curtains, desks, cabinets and other general office materials in the data centre should be fire resistant.

•Environmental Security
•Fire Safety
•Cyclones
•Floods and Water Damage
•Major Data Centers

Environmental Security
Major Data Centres

Data centres should be housed in buildings, which are resistant to cyclones.

The following controls should be considered:

- Permanent cyclone shutters for doors and windows
- Double doors
- Wind resistant roof sheathing
- Data centres should be located on an interior room on the first floor in cyclone prone areas. This should ensure least impact of winds and floods.
- Information processing facilities should be equipped with water or moisture detectors. The detectors should produce an audible alarm, when activated.
- Data centres should be located in raised or elevated floors in flood prone areas.

Power Supplies

Information processing equipment should be protected from power failures and other electrical anomalies. A suitable electrical supply should be provided that confirms to the equipment manufacturer's specifications.

Purpose & Objectives

Information processing equipment needs to be safeguarded from power failures and other electrical anomalies.

Uninterruptible Power Supplies (UPSs)

In case of power outage, a UPS is a backup power source for major computer systems

There are four basic configurations of UPS:

- the standby
- ferroresonant standby
- line-interactive
- the true online

Uninterruptible Power Supplies (UPSs)

A standby or offline UPS is an offline battery backup that detects the interruption of power to the power equipment

A ferroresonant standby UPS is still an offline UPS

- the ferroresonant transformer reduces power problems

The line-interactive UPS is always connected to the output, so has a much faster response time and incorporates power conditioning and line filtering

The true online UPS works in the opposite fashion to a standby UPS since the primary power source is the battery, with the power feed from the utility constantly recharging the batteries

- this model allows constant feed to the system, while completely eliminating power quality problems

Emergency Shutoff

- One important aspect of power management in any environment is the need to be able to stop power immediately should the current represent a risk to human or machine safety

- Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button, prominently placed to facilitate access, with an accident-proof cover to prevent unintentional use

Power Supplies

Power Supply Standards

- Uninterrupted Power Supply (UPS) should be used to support orderly close down or continuous running of information processing equipment.
- The UPS equipment should be checked at least once in 3 months in accordance with the manufacturer's recommendations.
- All buildings should have proper earthing to prevent electric surges.

Power Supply Standards

Power-off Switches

- Two emergency power-off switches should be used, one in the computer room, and the other near, but outside, the computer room. This should facilitate rapid power-off in case of an emergency such as during a fire or emergency evacuation.

- The power-off switches should be clearly labelled, easily accessible but shielded to prevent accidental activation.

Power Supplies
Major Data Centres

The following controls should be followed for major data centres and for time-sensitive systems

- Backup UPS equipment should be used to ensure continuous running of sensitive or critical systems in case the original UPS equipment fails.

- Back-up generators should be used to ensure continued processing for critical systems in case of power failure for a prolonged period.

Cabling Security

Power and telecommunication cabling carrying data or supporting information services should be protected from interception or damage.

Purpose & Objectives

- Power and telecommunication cables that feed into the information processing facility are exposed to many environmental hazards like cyclones, floods, fire, lightning or cutting due to careless digging.
- Cables carrying data or supporting information services should be protected from interception or damage to reduce the risk of power or communication failure.

Cabling Standards

- Power and telecommunication lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.
- Network cabling should be protected from unauthorised interception or damage due to environmental hazards e.g. by using conduit or by avoiding routes through public areas.
- Power cables should be separated from communication cables to prevent interference.

Cabling Standards
Major Data Centres

The following controls should be followed for major data centres and for sensitive or critical systems

- Installation of armoured conduit and locked rooms or boxes at inspection and termination points □
- Use of alternate routings or transmission media □

Physical Security of Laptops

Policy Statement

- The physical security of laptops, as well as the security of the data residing in these systems, should be ensured.

Purpose & Objectives

- Laptops and their related components (e.g. peripherals, disk drives) are highly vulnerable to unauthorised access or theft, thereby presenting unique risks in the areas of disclosure or destruction of proprietary information.
- Laptops should be physically secured at all times to prevent unauthorised access or theft.

Physical Security of Laptops

Responsibility

- Employees to whom laptop computers are issued should be responsible for its safe custody.

Physical Security Controls

- All laptops should have a ‘power-on’ password.

- Laptops should not be left on the desk or in the work area or any other visible location overnight. It should be locked in a secure area at the end of the workday.

- The laptop or case should not be left unattended in cars.

- Laptops should not be left unattended in public places like an airport. Airport rest rooms and areas around telephones could be especially vulnerable locations.

Physical Security of Laptops

- Laptops should never be checked in as luggage, while travelling. It must always be hand carried in a briefcase or a laptop carrying case.
- Laptops should be locked inside luggage and kept out of sight, when left in hotel rooms.
- The concerned staff should file a police report immediately in the event a laptop is stolen. The staff should also notify the Systems Security Administrator and the Head of Department within one business day of the theft.

Additional Devices

- Any removable media devices, such as CD Writers, Zip drives and Tape drives, should not be added to individual laptops unless authorised by the Head of Department.

- Modems should not be added to individual laptops unless cleared and authorised by the Head of Department after consulting with the Chief Information Officer.

Clear Desk and Clear Screen

A clear desk and a clear screen policy for information processing facilities should be adopted.

Purpose & Objectives

- Information must be protected from unauthorised disclosure, modification or theft.
- A clear desk policy for papers and removable storage media and a clear screen policy should reduce the risks of unauthorised access, loss and damage during and outside normal working hours.

Clear Desk and Clear Screen
General Standards

- Computer terminals and printers should not be left logged on, when unattended.
- Key locks, power-on and screensaver passwords, or other controls should be used to protect them when not in use.
- Computer media should be stored in suitable locked cabinets when not in use, especially after working hours.
- Incoming and outgoing mail points and unattended fax and telex machines should be protected from unauthorised use outside normal working hours.
- Photocopiers should be locked or protected from unauthorised use outside normal working hours.
- ‘Top Secret’, ‘Secret’ and ‘Confidential’ information and storage media should be locked (ideally in a fire-resistant safe or cabinet) when not required.

And finally…….. Back Up your System

- Backing up your data should be a habit -Something you do automatically and consistently. Once you have completed a backup, Do not leave the backup media in the PC or even in your office. Store it in a Fire Proof media safe or an approved off-site location
- Safeguard your backup media. If that backup contains personal or confidential information, it should be protected and secured. Do not allow unauthorized access to your backup media.
- If you can't afford to lose it, then you can't afford NOT to back it up!

Your PC, Your Data, Your Responsibility !!!

Thank you…