CHAPTER 14

Physical Security and Biometrics

Introduction

Physical security refers to the measures taken to protect the physical environment and infrastructure that is housing the information system resources, including hardware, software, and other networking devices against physical threats such as theft, fire, water, floods, and so on.

Physical security is as important as other technical security measures that are provided for the information. Since all the system resources are placed inside a physical facility, the environment around and within this facility should be safeguarded from both natural and unnatural events. People may be thinking that having moved their infrastructure on to the cloud, they would not be impacted by physical security. It is only partially true. They may not be required to take care of physical security but somebody who provides the infrastructure facilities for the cloud needs to ensure the physical security as the servers and the infrastructure are still located in some physical facility somewhere.

Spilling water or a cup of hot coffee on the computer has the potential to destroy the electronic component of the computer and make the system dysfunctional. An unauthorized person entering into the electrical control room and switching off the power to the server room could lead to a complete shutdown of the data center. Someone can sneak into the facility and photograph or take video and hand it over to a competitor. All these are physical security related threats that need to be curtailed. Deliberate acts of sabotage or vandalism of the facility, employees stealing computers, computer accessories, confidential data, and passwords from the facility are all physical threats and need to be addressed. Natural calamities such as fire and floods, can also destroy the data including physical backup tapes inside the facility. Water leakages and power surges also represent physical threats and appropriate measures need to be taken to protect these assets.

Table 14-1 summarizes the security threats based on the CIA triad.

Table 14-1. *Security Threats Based on the CIA Triad*

Threat	Description
Physical damage	Availability
Theft	Confidentiality and Availability
Unauthorized entry to the facility	Confidentiality and Integrity
Natural Disasters (Fire, Flood, Earthquakes, and so on.)	Availability
Human Intervention (Sabotage, Vandalism, Strikes)	Availability, Confidentiality
Emergencies (Fire, Smoke, Building collapse, Explosion, Water leak, Toxic material release)	Availability

Seven major sources of physical loss have been identified as:[1]

- Temperature: Extreme variation of temperature
- Gases: War gases, commercial vapors, humidity, dry air, and so on. Examples would be transformer explosion gas, air-conditioning failures, smoke or smog, printer's liquids and toners, and cleaning liquids
- Liquids: Water and chemicals. Example would be water pipe leakages, sanitary leakages, fuel leaks, spilled drinks, acids, and chemicals used for cleaning
- Organisms: Viruses, bacteria, people, animals, and insects
- Projectiles: Tangible objects in motion such as moving vehicles, cars, trucks, and explosions
- Movements: Collapse, shearing, shaking, vibrations, and so on.
- Energy Anomalies: Electric surges, failures, magnetism, static electricity, radiation, sound, light, radio and microwaves. Examples include static electricity or carpets, cosmic radiation, explosion, and decomposition of magnetic tapes

The physical and environmental security mechanism should protect the threats either by automatic controls or driven by a set of manual processes. Normally, organizations have standard policies and procedures to protect the facility including the data/computer center:

- General management policies and procedures to secure the facility. Includes security guards, allowing visitors inside the facility after proper vetting, escorting visitors, building access, and surveillance cameras at each and every important location, both outside and inside of the facility.
- IT security policies and procedures to guard against unauthorized access to restricted areas such as server rooms, control and privileges of administrators, password policies, remote access policies, and access card privileges. Also, environmental controls required for the server/data farms/centers such as temperature, humidity, static, and dust controls.

Though physical security deals with all aspects of physical environment and other hazards, IT physical security should provide the protection of computer systems and other IT systems from the following:

- Physical damage of hardware/software as an act of sabotage, theft, unauthorized access to the server/computer rooms, or labs with the intention to damage physical assets
- Unauthorized access to server rooms/data center/labs
- Physical theft of equipment, systems, and other accessories
- Bringing personal storage devices and injecting viruses, worms, and other malicious software into the trusted networks

There have been instances of labor unions being used as a conduit by the competitors to create havoc on the premises of the target organization and physically damage the infrastructure.

Physical and Technical Controls

Physical access controls restrict the personnel access to the office buildings, labs, server rooms, data centers, or computer operation rooms where critical assets related to IT operations are operational. It should also restrict access to the locations where wiring is passing through to connect the systems, patch panel rooms, electric supply rooms, UPS rooms, the air conditioning or heating plant, data backup storage place, telephone and data lines connected area, and any other area which has IT or IT related operations.

Apart from the technical controls, enhanced corrective actions can reduce the risks. Higher levels of screening, reorganizing traffic patterns at some key locations, not displaying names of important buildings, and R&D facilities, can reduce the physical threats. Closed-circuit television cameras, motion detectors, and other devices can monitor the activities of the people and detect any intrusions.

There are a number of physical security controls available in the market that the organization should consider for implementing physical access controls both inside and outside of the facility. Some of the controls include:

- Security Guards at each of the entry and exit points
- ID cards and badges to all employees, and contractors
- Electronic Access cards for all the major doors
- Electronic monitoring and Surveillance cameras
- Metal Detectors
- Electric Fencing
- Alarms and Alarm systems
- Specialized access to computer labs, data centers, server rooms, and R&D labs
- Biometrics
- Automatic Locks and keys

ID Cards and Badges

ID cards and badges are a common method for physical access to the premises. Photo ID and digital smart cards are two common types.

Photo ID cards

Photo ID cards are simple identification cards with a photo of the personnel who is identified to provide access to the facility. Every organization provides to its employees a photo ID card for the purpose of identification and this should be worn by the employee at all times within the premises. Any violations of rules or policies within the facility by an employee can be easily identified through his/her ID.

Digital-coded cards contain chips or magnetic encoded strips on the photo ID card, which also contains all the information related to a person/employee. These types of cards are generally used in credit cards, ATM, and debit cards.

Magnetic Access Cards

Magnetic access cards are programmed by the security personnel for an entry into specific location. All the major entry and exit points of an office premise may have access points where one needs to flash this magnetic access card so that the door opens automatically. Otherwise, the access is restricted. For example, a server room or an R&D facility in the campus have special access to only few people. The door opens only when they swipe the access card at the door entrance. This will prevent any intrusions, even within the organization.

Other Access Mechanisms

Other access mechanisms that are prominently used include:

- **Wireless proximity readers** do not require users to physically swipe the card. The card reader senses the card automatically and allows the user who is in possession of the card to enter the door, which opens automatically. **Radio Frequency Identification** (RFID) technology is the one typically used by wireless proximity readers. Figure 14-1 shows one example of a RFID reader that is used for access control.

Figure 14-1. *RFID Reader*

One of the inherent weaknesses of such systems is **tailgating**. Tailgating is a method / technique used by an unauthorized person who enters the premises by following the authorized person. As soon as the authorized person swipes his/her card and the door opens and he enters the room, just behind this authorized person, another person enters before the door closes, who may or may not be authorized.

Locks and Keys

Locks and keys are probably one of the oldest access control methods ever used besides security guards. There are two types of locks:

- **Preset locks:** These are normal locks used in the houses and door locks. They are preset and the keys are fixed, you cannot change the keys.
- **Programmable locks**: These are either mechanical or electronic. A mechanical lock is generally an electromagnetic lock where a combination of numbers has to be entered to unlock. Common mechanical type programmable locks can be found in earlier labs and office doors. These are the common five-key pushbutton lock that requires users to enter a combination of numbers. This is a very popular lock for IT operations, server rooms, and so on. Nowadays, the mechanical locks have been replaced by electronic combinations, where the user is required to punch in a code on a number pad to get the access. This type of lock is known as a cipher lock or keypad access control.

Electronic Monitoring and Surveillance Cameras

Electronic monitoring controls such as Closed Circuit Television (CCTV) Cameras are used to monitor areas where either guards or dogs are not watching. These CCTV cameras may also complement the guards and the dogs. Also, the facilities are monitored 24/7 from a central location. The video footage of the CCTVs are normally recorded and stored for future investigations.

The main drawback of the electronic monitoring system is that it is a passive device. It can only monitor the intrusion but it cannot prevent intrusions. People who are monitoring the activities from the central location have to trigger an alarm in case they detect intrusion. In case the people who are monitoring the systems are not alert, intrusions cannot be stopped and later the recorded videos have to be viewed to identify the intruders and the intrusion activities.

Alarms and Alarm Systems

Alarm systems are closely related to electronic monitoring systems. But, alarms will notify whenever there is an unauthorized access. Alarms are very similar to Intrusion Detection System (IDS) that can detect any physical intrusion or any other events such as a fire, burglary, smoke, or environmental disturbance such as flooding.

Motion sensors are sensors that monitor the motion within a confined area using infrared, microwave, or optical technology. Sensors are widely used in current-day scenarios. Sensors are also additionally used in data centers to alert about temperature changes, water leakages, humidity increases, and so on.

Biometrics

We have watched in many movies how various kinds of complicated physical security measures are easily broken by intelligent planning and executing by spies and others. We have also watched in movies how various kinds of biometrics are used by military and other organizations. We have seen these biometrics systems being defeated by the severed finger of an authorized but slain officer, through static pictures of iris, through forged fingerprints. While biometrics has advanced over a period of time, additional aspects are being envisaged to be considered along with the main traits like pressure exerted or lack of pressure exerted during the fingerprint scan, and so on.

Biometrics is a technology for measuring and analyzing biological data of a human body such as fingerprints, eye retinas, irises, voice patterns, facial patterns, and hand geometry, and vascular patterns and DNA. Biometrics is mainly used for authentication purposes. Biometrics technology is used to prevent fraud, enhance security, and reduce identify theft.

There are several applications of biometrics in both government and commercial fields. Biometrics have been in use in forensic analysis for over 100 years. Biometrics have aided in criminal investigations, identification of missing children and people during disasters. Biometrics provides a higher degree of accuracy which would not be possible by human experts and has helped to solve many problems.

Governments constantly make use of biometric measures to prevent passport fraud hence preventing intruders getting inside the country by using fake VISAs and passports. Most international airports have adopted iris, fingerprint, or face recognition systems to prevent terrorists or illegal immigrants entering the country using false identity. In some developed countries, biometrics identities are included even in the driver's license (smart chips) for extra security. In India, the Aadhaar card (a unique identity for every citizen) has adopted biometric identity of all 10 hand fingerprints, face, and iris of both the eyes.

Many commercial organizations are using biometrics to protect customers' identity theft and secure commercial transactions. Most of the ATMs in developed countries have face recognition and fingerprint identity as passwords to withdraw money. Low cost biometric sensors and technology have led to the deployment of many biometric systems at ATMs, grocery stores, smartphones (iPhone 5s), laptop computers, and so on.

Apart from commercial applications mentioned above, many organizations are using biometric access control. These biometric access controls are installed and connected to door locks. When the biometric identity, such as fingerprints or retina or irises are matched with the data already captured during the enrollment process in the central database, lock systems unlock the door so that the person can enter.

Biometrics allows employees to access facilities based on the following methods:

- Acquiring data
- Extraction of features
- Encryption of template so that it is not tampered with
- Capture of data and matching
- Access is allowed or denied based on the match or no-match.

Some of the important biometric mechanisms

The biometric systems work on the basis of the behavioral traits of the users or the physical traits of the users or a mix of these.

Behavioral biometric systems use methods such as voice recognition, signature verification, keystroke recognition, gait, and so on.

- **Voice Recognition**: Voice patterns differ from person to person. The pitch value and frequency value are unique to each person and hence voice patterns are easily used for identity / authentication / verification purposes. Input voice is captured and the features are extracted from this using suitable training methods and the voice sample is stored as a template in the database. Training the voice samples is an important step. When the actual voice has to be tested, it is processed, the features out of the same are extracted and compared with the templates saved in the database. When there is a match the person is verified. Cleaning up the voice sample for noise is an important step and is carried out during preprocessing.[2]
- **Signature Patterns:** Keystrokes, the style of writing, orientation of writing, and the pressure applied while writing are the features of writing which differ from one person to the other. Hence, for a long time, banks and financial systems are relying upon the signature verification against the lodged signatures for authenticating a person or the documents signed by a person. Various government agencies also use this method effectively and extensively.

Physical biometric systems use methods such as fingerprint biometrics, facial biometrics, hand biometrics, Iris biometrics, retina biometrics, and vascular pattern biometrics.

- **Fingerprint Biometrics:** It is well known that fingerprints are most used in criminal investigations. In many countries fingerprints were taken as additional authentication to the signatures during the registration of properties, deeds, and so on. Fingerprint biometrics has almost percolated to most of the fields including companies to passport authorities to immigration authorities to many other fields. This is one of the comparatively cost effective, easy to use, and easy to implement systems available for identification and authentication or verification. The fingerprint biometrics uses the minutiae like arches, whorls, loops, ridges, valleys, and furrows which allow one fingerprint to be differentiated from the other.[2] Figure 14-2 shows an example of a fingerprint reader device.

Figure 14-2. *Fingerprint Reader Device*

- **Facial Biometrics:** Facial features like distance between two eyes; geometry of eyes, nose, lips, ears, and so on are the features used to differentiate one face from the other. Faces are captured and the facial features are extracted and used as a template. When the face is to be matched, again the same process is used to extract the features, the features so extracted are matched with the stored templates and when there is a match that means that the person is authenticated or verified. Some people have privacy reservations about this method.
- **Hand Biometrics:** Here the hand features such as size, length, width of the hand; lengths and angles of the fingers, bones, muscles, and ligaments of the hand are used to identify a person. Even the pressure applied by the hand on the scanner is one of the features that may be used.[2,3]

- **Iris Biometrics:** The use of Iris biometrics is picking up in critical and sensitive areas which require better entry controls. Iris differs from person to person significantly. Even iris may differ from left eye to right eye of the same person. Iris is the area surrounding the pupil in the eye of a human being. This is the area of the eye that determines eye color such as blue eyed, black eyed, and so on. The ring structures, furrows, and freckles pertaining to the iris are used as the features. This is easy to implement but requires specific readers and the eye has to be positioned appropriately for effective reading and is relatively costly to implement. Some people still express it as a privacy invasion.
- **Retina Biometrics:** Retina is the area within the human eye that reflects the image. This has different blood vessels flowing through it. These are captured as features as these differ from person to person significantly. This is difficult to capture as it requires appropriate lighting and exposure for a sufficiently long time span.
- **Vascular Pattern Biometrics:** Here the thickness and location of veins in a person's hand are used as features. These differ from person to person. Scanning the hand is easy and also does not involve privacy issues.[2]

How the biometric system works

Biometric system is a pattern recognition system where a biological pattern is analyzed, matched, and processed for further actions. This process has two stages:

- Enrollment stage
- Recognition stage

A basic biometric system is illustrated in Figure 14-3.

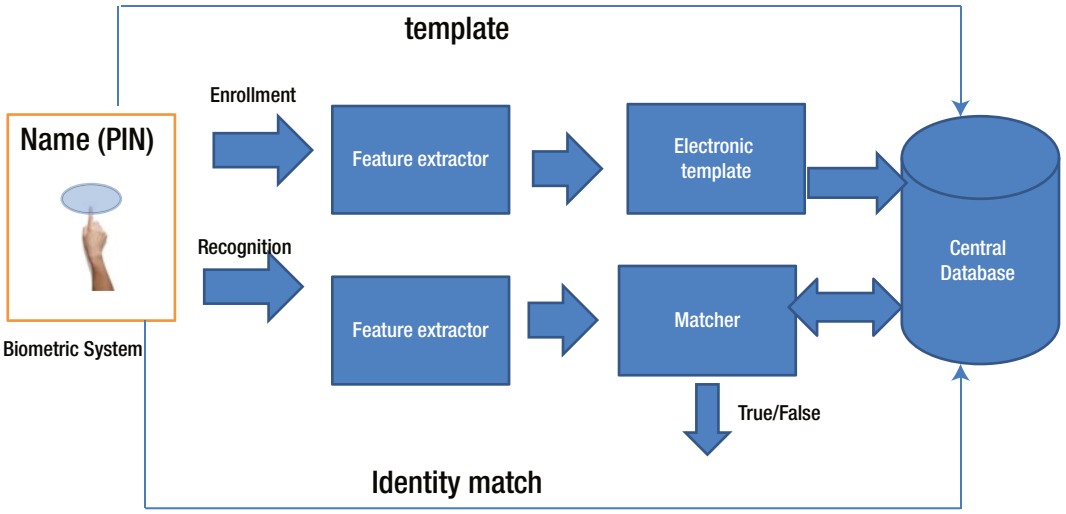

Figure 14-3. *Biometric Access System*

Enrollment

During the enrollment, a user's biological traits are captured with a scanner, camera, or appropriate reader. The captured data is preprocessed to remove any noise. The features are extracted from the captured data and the extracted features are then placed in an electronic template which is stored in a secured database in a central location for future recognition.

Recognition

During recognition, a sensor captures a user's biometric data. The data that is captured is analyzed with an algorithm that extracts only relevant features. Then this information is compared with the previously captured electronic template. If the match is found, further actions take place or else an alert is generated.

Performance of the Biometrics System

In order to be successful in commercial implementation, performance of the biometrics system has to be good. With the cost of memory and processors having come down significantly, there is more computing power available at less cost. This has propelled the usage of the biometrics systems in identification or authentication or verification processes. However, when the number of templates stored in the database increases significantly, the performance can start declining. The enrolment and matching and each of their constituent steps can take significant memory and processing time. However, as specified above, the advances in the field of computers have brought down the response time considerably.

The test of a good biometric system

A biometric system is considered good only if the following five characteristics are fulfilled:

- Unique: The feature being captured for matching purposes should be unique to each person.
- Repeatable: If again, after time lapse, the same characteristics are captured, the features extracted should be the same as that of earlier time, that is, it should be repeatable over a period of time. It should not change from one period of time to the next period of time.
- Accessible: The characteristics should be easy to be captured, such as through a simple scanner.
- Universal: Any biometrics system is not useful if it can be applied to only a portion of the target group. It should be easy to apply to all the target personnel. It should not require having some other alternative system for certain people as the system in question is not possible to be used by them.
- Acceptable: The method of biometrics should be acceptable to all. People should not have any objections about the same, like privacy related objections.

Furthermore, the following rates of acceptance and rejection by a good biometrics system should be at the minimum:

- False Acceptance Rate (FAR): A person's biometric characteristics match with somebody else's from the template database. This should not be the case as this can allow access to somebody else in the place of the genuine person. This is also known as False Match Rate.
- False Rejection Rate (FRR): A person's biometric characteristics do not match even though his feature template is already captured in the corresponding template database. This should not be the case as the person who requires genuine access may be denied access. This is also known as False Non-Match Rate.

Finally, the following rates need to be "high" for a good biometrics system:

- True Acceptance Rate (TAR): This is rate of correct match, that is, the person's identity is established correctly.
- True Rejection Rate (TRR): This is the rate of non-match correctly established, that is, if the person is falsifying the identity, that is correctly found by the biometrics system and the match is rejected correctly.

Possible information security issues with the Biometric Systems

The following information security breaches are possible with biometric systems:

- Possibility of forging the fingerprint by molding or fabricating it
- Possibility of false acceptance match
- Leakage of biometrics data may raise privacy and misuse concerns
- If not stored in encrypted mode, it may be possible for hackers to substitute the template and hence get unauthorized entry into an organization
- Possibility of the registration of a wrong person instead of a genuine person during the enrolment process without verifying the identity of the person being enrolled

It is strongly suggested that the biometrics data are not shared with others and also are not duplicated in some other systems even within the organization. Further, the biometric data has to be held encrypted so that it is not copied or replaced fraudulently by others.

Multimodal biometric system

Unimodal biometric systems, that is, biometric systems which use single characteristic like fingerprint biometrics or retina biometrics or iris biometrics have been found to have some limitations like propensity for attacks, noise in sensors, improper usage of the sensors for scanning or improper way of scanning or inadequate lighting provided (in case of iris scan), and improper exposure during retina scan leading to the noise in the traits captured for matching, and so on. Multimodal biometric systems use more than one biological trait of a person for recognition and access. For example, retina and fingerprint both can be used for establishing a person's identity. This enhances the security and also reduces the difficulties faced during recognition phase which the user experiences sometimes. It is also possible to collect data from different sensors, use different algorithms, use multiple samples, and so on.

In multimodal biometric systems the captured data can be fused at different levels and match or no-match is established. Multimodal biometric systems provide higher accuracy levels.[2]

Advantages of Biometric systems

Biometric recognition has several advantages compared to the traditional access system with simple passwords and IDs.

- Users do not need to remember passwords
- Users need not have to carry an ID card
- Unless the person is physically present, access is denied. No impersonation of identity is possible

- Biometric traits cannot be stolen or duplicated
- Biometric systems are hard to break
- Biometric systems have good accuracy
- With the advent of the computers, the declining cost of computers, the cost of the biometric systems have significantly reduced

Administrative Controls

In addition to the physical and technical controls, administrative controls are also very important from the perspective of ensuring totality and effectiveness of the controls. Some of these administrative controls are detailed in the following section.

Fire Safety Factors

Fire is an important risk each organization has to protect against. The fire risk arises from electric short circuits, gas leakage, consequential fire / fire mishaps on the premises, friction / malfunctioning of machinery leading to fire, and so on. Fire can turn uncontrollable within a few minutes depending upon the location of the fire, if not contained immediately. Fire can burn the organizational infrastructure including cabling, computers, and network equipment leading to an almost complete shutdown of the organization unless the organization has a well thought out and well-structured Disaster Recovery and Business Continuity Plans.

Some of the precautions that need to be taken to reduce the threat of fire are:

- Do not stock any inflammables like oil, old papers, and chemicals within the office premises. If you need to store them, store them separately in a secluded area and ensure that the area does not have any fire threats.
- Have smoke detectors installed at all the important places and high risk fire prone places within the organization.
- Have a good fire alarm system installed which has the capability to identify the zone in which the fire has originated and provide sufficiently audible strong alarm across the place impacted by fire.
- Have appropriate fire extinguishers installed at all the strategic and important locations within the organization, in sufficient numbers.
- Train your security guards, Emergency Response Team members, other staff members on effectively using the fire extinguishers.
- Maintain, test, and understand continued effective working of the smoke detectors.
- Ensure that the fire extinguishers have the requisite pressure maintained, the contents have not expired.
- Ensure that the electrical wiring and the switches used are of high quality and adhere to the product specifications.
- If there is an in-house canteen, ensure safe fire handling precautions. Also, have the fire extinguishers installed in sufficient numbers in that area.
- Get water sprinklers installed across the organization so that in case of huge fires the water sprinklers are activated and can control the fire.

- Train all the Emergency Response Team members in effectively handling emergency responses, effective evacuation of the employees. Carry out periodical fire-drills and ensure that the staff members understand the do's and don'ts to be followed during any fire emergency. Record the learnings of the fire drill and ensure that the Emergency Response Plans (in most of the organizations part of Disaster Recovery & Business Continuity Plans) are updated to reflect the applicable learnings.
- Ensure that the electrical earth points are well maintained.
- Emergency exits to be clearly marked and the path to the nearest emergency exit clearly specified.

During audits that we have carried out, we have discovered some of the following issues:

- Security guards and others did not know how to handle the fire extinguishers.
- Security guards did not know the priority of evacuation. When the security guards were asked, they mentioned that the computers which are costly have to be evacuated first as they are costly and surprisingly not human beings!!
- Fire Alarm Panels were not working.
- Smoke detectors were not working.
- Fire extinguishers had expired / did not have the requisite pressure.
- Fire exits were physically locked and they had a difficult time locating the key.
- Fire drills were carried out for the sake of complying with certain certifications. The learnings were not recorded and acted upon.
- Earth pits were not maintained.
- Electrical wiring was substantially old and was patched up at many places. Electrical panels were not well maintained.
- Old papers and inflammables were stored very near to the canteen area.
- Sufficient care was not exercised during the fire drills and some of the laptops were stolen by somebody when all the doors were opened automatically!!

Fire requires important consideration like other parameters by the organization. Otherwise, the organization will be at substantial risk.

Interception of Data

Data cables running within the organization, particularly in infrequently used areas, should be completely concealed so that they cannot be tampered with and to avoid the possibility of anybody fixing a monitoring / sniffing device to them. Data cables running outside the organization should be completely concealed and should be well protected so that there is no possibility of tampering by anybody.

In case of wireless devices, it should be seen that there is hardly any possibility of anybody using any rogue wireless router from outside the perimeter of the organization. The communication from the wireless devices needs to be encrypted through a strong encryption mechanism so that they are not interfered with and tampered with.

LAN points should not be normally provided in the visitor area or discussion rooms where the visitors are allowed so that there is no possibility of any visitors connecting to the LAN and manipulating the network.

Mobile and Portable Devices

Mobile phones and portable devices like laptops are highly prone to theft. Along with the theft of this system, substantial confidential data of the organization is also at risk. Particularly, mobile phones and laptops are issued to senior people within the organization and the loss of these systems can lead to substantial information security risks to the organization.

The following best practices apply to laptops:

- When not in use and needs to be left unattended, lock it to the desk using the locking cable
- While travelling, ensure that the laptop is held securely by you. Do not leave the laptop unattended at airports. Do not leave your laptop in your car when you are away from the car. Data on a laptop should be always held in encrypted form.
- Do not leave your mobile phones unattended anywhere. Ensure again that the organization has the policy to encrypt the data on the mobile. In case of loss of mobile, the organization should have the capability to wipe out the data on the mobile remotely.
- Always keep as little data as required on the mobile devices. If you are storing some content on these while not being connected to the office servers, ensure that the data is appropriately transferred back to the office servers once you are back at office or able to connect to the office servers; and delete the data from your mobile device.

As far as employee personal mobile devices are concerned, these have to be controlled as per the organizational policies. Nowadays, these mobile devices like mobile phones have high resolution cameras and have the capability to store documents and other data. Hence, a considered decision has to be taken by the organization after analyzing the risks and the benefits. If employee mobile phones are allowed to be used for official purposes, then appropriate controls as above have to be implemented so that they are not stolen placing the organization at risk. Further, employees should be strictly instructed about the do's and don'ts of the use of mobile phones within the office if personal mobile phones are allowed within the organization (e.g., not to photograph any confidential document or client sensitive data, etc.).

Visitor Control

Control over visitors is often neglected but is an important control from the perspective of physical security. Visitors normally have to be restricted to the reception area and any discussion rooms which are around the reception area but outside of the working area. If any visitor is required to come inside the organizational working area, they have to be necessarily escorted by a responsible person from the organization. Visitors should not be allowed to wander at will within the organization and have to be always escorted by a responsible person from the organization.

Visitors should be required to declare all their personal belongings including mobile phones, laptops, and pen drives. The details have to be written down in the Visitor Personal Belonging Register and have to be allowed inside the organization only on an as needed basis. Normally visitors are allowed to bring their mobile phones inside the organization. In such cases, the escort has to ensure that the mobile phones are not used to capture any sensitive document or sensitive work area. Further, while entering highly sensitive zones, they may be made to deposit the mobile phones with the security outside the area. Normally USB devices and memory cards should not be allowed within the organization.

Staff members have to follow the "clear screen" policy when the visitors are at their desk, so that even unintentionally, they do not allow the visitors to understand some sensitive information.

Chapter Summary

- We looked at the importance of physical security and at some of the threats and how they impact the information security aspects like confidentiality, integrity, and availability. We also briefly looked into the necessity of having physical security in the context of cloud infrastructure. We also looked into the need for IT physical security.
- We looked into the physical and technical controls. We described ID Cards and Badges, Locks and Keys, Electronic Monitoring and Surveillance Cameras, and Alarms and Alarm Systems.
- We explored what Biometrics is, and the different types of biometric systems in use such as behavior trait based and physical trait based systems. We looked into various behavior trait based and various physical trait based biometric system details. We explained how the biometric systems work through enrollment and recognition phases. We explored the performance of biometric systems and the characteristics of a good biometric system in detail. We looked into the security issues related to biometric systems. We then explored the value of multimodal biometric systems over unimodal biometric systems.
- We elaborated upon the administrative controls like fire safety controls, protection against interception of data, controls required over mobile and portables devices, and visitor control.