Chapter 9

Implementing controls to protect access

horizontal line

# Security layers

Security needs to be implemented in vendor-diverse layers. This ensures that the vulnerabilities for each system are different, making it difficult for an attacker to exploit all of them

Security training for users is one of the most important layers

# Physical security controls

* Perimeter
* Buildings with additional controls
* Secure work areas
* Server and network rooms, with security controls to prevent unauthorised access
* Hardware, e.g. cabinets/locks
* Airgap, which ensures that a comp/network is not connected to another comp/network
* Signs

# Door lock types

# Cipher locks

A PIN must be entered. However, this has a risk of shoulder surfing or brute force attacks. To prevent these, some codes have numbers which must be entered at the same time, e.g. 1 and 3

# Door access with cards

Proximity cards activate a door when they are waved in front of a card reader.

# Biometrics

Some can provide identification and authentication using a database.

# CCTV

CCTV must only be recorded in public areas, and employees must be notified of this. Furthermore, they must not record audio.

# Fencing, lighting and alarms

They can be used as deterrents, and also to detect illegal entry. IR detection can also be used, which detects movement by detecting different temperatures. Bollards are steel poles that prevent a criminal form driving a truck through the building.

# Asset management

An effective asset management policy can help reduce:

* **Architectural and design weakness**, by making sure that purchases go through an approval process.
* **System sprawl and undocumented assets:** System sprawl is when an organization has more resources than it needs

# Environmental controls

Environmental monitoring allows admins to see whether the controls are keeping up with the demands of the data centre

# HVAC

Heating, ventilation and air cond systems enhance availability of systems. This is important in places such as data centres, where machines will overheat within seconds if AC fails. Higher tonnage HVAC systems provide more cooling capacity

# Hot/cold aisles

Help regulate the cooling in data centres, by putting servers front-to-front and back-to-back. This creates hot and cold aisles. A HVAC system would have a thermostat as temperature control, and humidity controls. High humidity can cause condensation and water damage, and low humidity can cause ESD, electrostatic discharge.

# HVAC and fire

HVAC systems should respond to fires by reducing oxygen flow and activating fire alarms. They should also have the ability to be turned off.

# Fire suppression

Fire can be combated by removing heat, oxygen, fuel and using a fire extinguisher. Employees should also be able to leave without any ID cards/authentication

# Shielding

Protects against EMI and RFI. EMI shielding can keep interference out and prevent attackers from capturing network traffic

# Protected cabling

CAT5e and CAT6 come in shielded twisted pair (STP) and unshielded twisted pair (UTP) versions. **The shielding prevents an attacker from capturing network traffic.**

# Protected distribution of cabling

Cables should be out of sight and access, such as through a false ceiling or through the floor. Cables should be kept out of the EMI sources.

# Faraday cage

A room that prevents signals form emanating beyond the room. They can also provide shielding against EMI and RFI.

**Redundancy and failure**

Redundancy adds duplication to a critical system and provides fault tolerance

# SPOF

Single point of failure. Examples include:

* Disk: RAID (redundant array of inexpensive disks) can provide fault tolerance for disks
* Server: Failover clusters can increase availability
* Power: Generators and UPS (uninterruptible power supply) = fault tolerance

# Disk redundancies

RAID-0: 2+ disks used. Files stored on RAID-0 array are spread across each of the disks, so pats of a file can be written/read at the same time

RAID-1: Uses 2 disks, with data replicated between disks. If each of the disks has a separate disk controller, it removes a single point of failure

RAID-5: 3+ disks. If one drive fails, data can be read from the other one to see what is missing RAID-6 is an extension, where the subsystem till continue to operate even if 2 disk drives fail

RAID-10: Combines RAID-1 and 0 features

# Server redundancy

Failover clusters can provide high availability, where active nodes take over form inactive, failed nodes through heartbeat connections.

# Load balancers for high availability

Can be hardware or software, and balances load between systems on a network by scaling out and adding additional servers to a load balancer (Scaling up is increasing processor and memory)

They send new requests to to servers in a round-robin fashion, where the servers pass on the requests to other servers. The load balancer then detects the load on the servers and sends new clients to the least used server.

Source affinity sticks users to a specific server for the duration of their sessions.

A software-based load balancer uses a virtual IP

# Data backups

# Full backups

Backs up all data, but consumes time and money. However, it is the easiest to restore.

# Differential backups

Start with full backup, and then data that has changed since the last full/differential backup is backed up. It requires the restoration of the full and most recent differential backup.

# Incremental backup

Starts with full backup, and then data which has changed since the last full backup is backed up. It would require the restoration of several different backups

# Snapshot backup

Captures the data at a moment in time, commonly used in VMs.

# Testing backups

The best way to test the integrity of a backup is to restore it and see if it is the same as the data you backed up.

# Protecting backups

Includes:

* **Storage**: Clearly identifying the data, and providing physical security
* **Transfer**: Data should be protected during transfer
* **Destruction**: They should be destroyed safely, e.g. shredding/burning, or scrubbing by writing 0s and 1s to the media

# Geographic considerations

* **Off-site backups**: They should be stored offsite to protect against geographic disaster
* **Distance**: it depends on the company goal, so they can either have it close for easy access or far for security
* **Location selection**: Should be selected based on environmental considerations
* **Legal implications:** If data includes PII then the backups need to be prevented according to government laws
* **Data sovereignity**: if data is stored in another country, it can be subject to additional rules and regulations.

**Business continuity elements**

# Business impact analysis concepts

**BIA** is a part of **BCP** (business continuity plan) and identifies critical systems and vulnerable processes. It also provides management with valuable info so they can focus on critical business functions in a scenario of system failure.

# Impact

BIA evaluates various scenarios such as attacks/natural disasters, and the possible outcomes. It attempts to identify the impact of these scenarios, such as loss of data/life/profit.

# Privacy impact and threshold assessment

**Privacy threshold assessment** is a questionnaire completed by admins, and helps identify PII in systems, and then a **privacy impact assessment** identifies potential risks related to PII and how the info is handled, ensuring that it complies with guidelines and rules.

# Recovery time objective

RTO is the max amount of time it can take to restore a system after an outage. It indicates the maximum amount of down time that is acceptable to a business

# Recovery point objective

RPO identifies a point in time where data loss is acceptable, e.g. if management want to be able to recover data from at least the previous week, then the RPO is one week.

# MTBF vs MTTR

They are used to predict potential failures

**Mean time between failures:** MTBF, provides a measurement of a system’s reliability and is represented in hours. It also provides the average time between failures. Higher MTBF gives a more reliable system

Mean time to recover: MTTR, gives the average time to restore a failed system.

# Continuity of operations planning

Focuses on restoring mission-essential functions at a recovery site after an outage

# Recovery sites

Alternate processing site that can be used after disaster

# Hot site

Operational 24/7 and can take over functionality should the primary site fail. However it is expensive to maintain.

# Cold site

Requires power and connectivity, but not much else. The organisation has to bring the rest when they activate it. It is the cheapest, but hardest to test

# Warm site

A compromise between hot and cold sites.

# Site variations

**Mobile site**: A self contained, transferable unit with all the equipment needed for specific requirement

**Mirrored site**: Identify to primary site and provide 100% availability. Hot site can be up and operational within an hour, but a mirror site is always operational

# Order of restoration

After an outage is finished, functionality needs to return to the primary site. This is done by returning the least critical functions first, so that undiscovered problems will appear and can be resolved without affecting critical functions

# Disaster recovery

Part of a Disaster Recovery Plan (DRP). There are multiple DRPs within a BCP, and they prioritise systems that should be recovered depending on criticality. The phases of a Disaster recovery process are:

1. Activate the disaster recovery plan
2. Implement contingencies: Recovery plan may require implementation of alternate site
3. Recover critical systems: DRP documents which systems to recover first
4. Test recovered systems: May include comparing functionality with primary site baseline
5. After-action report: Review of disaster.

# Testing plan with exercises

Testing validates that the plan works as decided. Tabletop exercise is a formal discussion, including the team member’s responsibilities and roles.

Functional exercises provide the opportunity to test in a simulation environment. Testing includes:

* Backups: tested by restoring the backups
* Server restoration: Server is rebuilt using a test system without touching the live system
* Server redundancy: this can be tested by taking a primary node offline, so another node can replace it
* Alternate sites: This can be tested by moving some functionality to the other sure and seeing if it works

**ACRONYMS**

SPOF: Single point of failure

RAID: Redundant array of inexpensive disks, providing fault tolerance for disks

BIA: Business impact analysis

BCP: Business continuity plan

RTO: Recovery time objective, max amount of time it can take to restore a system

RPO: Recovery point objective, a point in time where data loss is acceptable

MTBF: Mean time between failures, the higher this is the more reliable the system

MTTR: Mean time to recover, average time needed to restore system after failure