Sec+ 501 Get Certified Topic 9 – Implementing Controls To Protect Assets

CH 9

- You can't eliminate all risk to an organization's assets but you can reduce the impact of threats by implementing security controls
- Defense In Depth (Layered Security)
    - Security practice of implementing several layers of protection. Can't just have a firewall. Need multiple layers so if one layer fails, you can have additional layers to protect you.
- Control Diversity:
    - Use of Different security control types such as technical controls, administrative controls and physical controls.
        - Technical security controls:
            - Smart cards, encryption, access control lists (ACLs), intrusion detection systems, and network authentication
        - Physical security controls:
            - Alarm systems, locks, surveillance cameras, identification cards, and security guards
        - Administrative controls:
            - Policies, procedures, security awareness training, contingency planning, vulnerability/penetration tests and disaster recovery plans
            - User training is the most cost-effective security control to use
- Vendor Diversity:
    - Practice of implementing security controls from different vendors to increase security.
        - E.G: DMZ using 2 firewalls and the use of firewalls from 2 different vendors. [One from Cisco and other from Check Point]. If one vulnerability is discovered in one firewall, an attacker might exploit it but it is unlikely 2 firewalls have the same vulnerability.
    - User training also provides Defense in depth.

- **Remember this:**

    - **Layered Security, or Defense-in-depth practices use control diversity – implementing administrative, technical and physical security controls. Vendor diversity utilizes controls from different vendors. User training informs users of threats, help them avoid common attacks.**
- Physical security control – something you can touch. Physical security access controls attempt to control entry and exists.
    - Perimeter – Erect a fence with security guards around perimeter of land. Can installed barricades. Usually used in military.
    - Buildings – Guards and Locked door restricted entry. Includes Lighting and CCTV
    - Secure work areas –
        - Some companies restrict access to specific work areas when employees perform classified/restricted access tasks. Visitors can enter lobby and can't access internal work areas without escort.
    - Server and network rooms – Stored in areas where only appropriate IT personnel can access them.
        - Server rooms/wiring closets.
        - Common to provide additional physical security for these rooms to prevent attackers from accessing equipment.
            - E.G: Locking wired closet prevents illicit monitoring hardware such as protocol analysers
    - Hardware – Locking cabinets, Cable locks, Safes
    - Airgap – physical security control ensuring computer/network is physically isolated from another computer/network. Separates classified from unclassified networks.
- Signs – 'Authorized Personnel Only', 'No Trespassing' tell people not to enter. Usually used with additional physical security measures.
- **Remember this:**
    - **In the event of a fire, door access systems should allow personnel to exit building without any form of authentication. Access points to data centres and server rooms should be limited to a single entrance and exit whenever possible.**

- Cipher Locks –
  - Often have 4-5 buttons labelled with numbers. Employees press numbers in a certain order to unlock door.
    - E.G: Cipher code could be 1,3,2,4 to gain access
  - Can be electronic or manual.
  - Can use two numbers entered at same time instead of one in some occasions. E.G: 1/3,2,4,5 instead of 1,3,2,4,5
  - Disadv:
    - Don't identify users
    - Bad user training can cause unauthorized users to enter
    - Shoulder surfing
- Proximity Cards – Small credit card sized cards activating when close to a card reader. Usually used for Access points such as entry/exit to a building.
  - Some access control points use proximity cards with PINS for authentication.
- Biometrics - Relies on the physical characteristics of a person to identify them
  - Biometrics is considered "something you are"
  - Retina scanners, Fingerprint scanners etc.
- **Remember this:**
  - **Door access systems include cipher locks, proximity cards and biometrics. Cipher locks don't identify users. Proximity cards can identify and authenticate users when combined with a PIN. Biometrics can also identify and authenticate users.**
- **Remember this:**
  - **Tailgating is a social engineering tactic that occurs when one user follows closely behind another user without using credentials. Mantraps allow only a single person to pass at a time. Sophisticated mantraps can identify and authenticate individuals before allowing access.**
- Mantrap:
  - Area between two doorways that holds people until they are identified and authenticated
- CCTV – Closed Circuit Television

  - Video surveillance provides reliable proof of a person's location and security.
  - Cameras are connected with CCTV transmitting signals from video cameras to monitors that are similar to TVs.
  - Usually used in parking lots, entrances, exits
  - E.G: Access Log provides record of Bart entering building via Proximity card. When reviewed on CCTV Bob is entering instead. Bob can't refute the evidence that it was actually him entering causing him to be in a bit of trouble through security.
- **Remember this:**
  - **Video surveillance provides reliable proof of a person's location and activity. Can identify who enters and exits secure areas and record theft of assets.**
- Remember:
  - Only record activity in public areas.
    - Don't record in restrooms, locker rooms etc. Often illegal
    - Notify employees of surveillance
    - Don't record audio
- Fences – provide barrier around property to deter people from entering. Guards often monitor gates to authorize people who can enter.
  - Dual Gates – Allow access into one area where credentials are checked before allowing full access
- Lights – Installed at entrances of building to stop attackers from breaking in.
  - Usually used with automation, light dimmers, motion sensors.
  - Place lights high above so they can't be reached easily
- Alarms – Detect unauthorized access
  - Fire alarms through smoke/heat
  - Motion detection systems
- Infrared detection – detect infrared light, seeing difference between objects and temperatures.
- **Remember this:**
  - **Fencing, lighting and alarms all provide physical security. Often used together to provide layered security. Motion detection methods are also used with these methods to**

increase effectiveness. Infrared detectors detect movement by objects of different temperatures.

- Barricades – when fences aren't enough.
  - Bollards – short vertical posts composed of reinforced concrete and steel.
    - Often placed in front of entrances 3-4 feet apart and painted with colours to match store. Zigzagged in military.
    - Prevent thieves from driving vehicles in front of buildings and stealing everything in sight.
- **Remember this:**
  - **Barricades provide stronger barriers than fences and attempt to deter attackers. Bollards are effective barricades that can block vehicles.**
- Hardware locks – Stops free access to wiring closets and smaller server rooms and are used to restrict access.
  - For proper key management lock keys within a safe/locking cabinet
- Cable Locks –
  - Used as a theft deterrent for mobile computers and usually wraps cable around a desk, table or something heavy and plugs it into an opening in laptop created for this purpose.
  - Usually has 4 digit combo. If you remove cable lock without combo will most likely destroy laptop.
- Locking cabinets or enclosures – Used to secure equipment mounted within bays.
  - Equipment bay – size of a large refrigerator and can hold servers, routers, and other IT equipment. Usually have doors in the back and front. Admins lock these doors to prevent unauthorized personnel from accessing equipment.
- **Remember this:**
  - **Cable locks are effective threat deterrents for small equipment such as laptops and some workstations. When used properly, they prevent losses due to theft of small equipment. Locking cabinets in server rooms provide an added physical security measure. A locked cabinet prevents unauthorized access to equipment mounted in server bays.**

- Safes – prevent theft of smaller devices such as USB's, flash drives, laptops etc.
- Asset Management –
    - Process of tracking valuable assets throughout their lifecycles.
        - Reduces architecture and design weaknesses.
        - System sprawl and undocumented assets –
            - System sprawl occurs when an organization has more systems than it needs and systems it owns are underutilized.
    - Asset management begins usually before hardware is purchased.
    - RFID is used for inventory control and can track movement of devices.
        - Used to prevent shoplifting where RFID device transmits when shoplifter gets close to exit door and sounds alarm.

ENVIRONMENTAL CONTROLS

- HVAC – Heating, Ventilation and air conditioning
    - Tonnage – Cooling capacity of HVAC systems.
        - One ton of cooling = 12,000 British thermal units/hr
        - Higher tonnage HVAC systems cool larger areas or equipment generating a lot of heat.
- **Remember this:**
    - **Higher-tonnage HVAC systems provide more cooling capacity. This keeps server rooms at lower operating temperatures and results in fewer failures.**

- Hot and Cold aisles – Regulate cooling in data centres with multiple rows of cabinets.
    - Back of cabinets in one row faces back of all cabinets in adjacent row.
- HVAC includes thermostat as a temperature control and additional humidity controls
    - High humidity → Condensation of equipment → Water damage

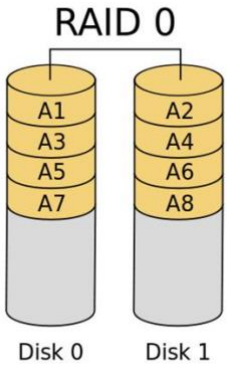
    - Low humidity → Higher incidence of electrostatic discharge (ESD)
- HVAC often integrated with fire alarm systems to prevent fire from spreading.
    - If HVAC pumps oxygen, it feeds fire so we control airflow to prevent rapid spread of fire via fire alarm systems.
    - Includes dampers to control airflow and HVAC are usually turned off when fire suppression systems detect fire.
- **Remember this:**
    - **HVAC systems increase availability by controlling temperature and humidity. Temperature controls help ensure a relatively constant temperature. Humidity controls reduce potential for damage from electrostatic discharge and damage from condensation. HVAC systems should be integrated with fire alarm systems and either have dampers or ability to be turned off in the event of a fire.**
- Fire suppression
    - Fixed Systems to control fires + portable fire extinguishers
    - Fixed system – detects fire and automatically activates to extinguish fire
        - Remove heat
        - Remove oxygen via CO_2 to stop electrical fires
        - Remove fuel
        - Disrupt chain reaction via chemicals
    - Consider safety of staff/personnel and consider alternative exits for personnel to exit if a fire occurs and proximity card readers/power stop working. This might create a vulnerability if an attacker removes power to access a secure data centre, make better judgements/decisions if can
- Environmental Monitoring:
    - Shielding – Prevents EMI and RFI (Electromagnetic Interference and Radio Frequency Interference)
        - EMI – used from motors, power lines, fluorescent lights
        - RFI – used in AM/FM Transmitters.
    - EMI shielding keeps interference out and prevents attackers from capturing network traffic
- Protected Cabling

    - Shielded Twisted Pair(STP) adds a layer of shielding inside the cable
        - CAT5e and CAT6e cables
    - Twisted pair cables such as CAT5e and CAT6 come in both shielded twisted pair (STP) and unshielded twisted-pair (UTP) versions.
    - Shielding prevents attacker from capturing network traffic and helps block interference from corrupting data.
        - Fibre-optic cables are not susceptible to induction field attacks as it uses light pulses
- Physical Distribution of Cabling
    - Physical security includes planning where you route cables and how you route them.
    - Run cables through cable troughs or wiring ducts.
        - Cable trough – long mental container 4 inches wide and high.
    - Keep cables away from EMI sources.
        - E.G: Running cables over fluorescent lighting fixtures, EMI from lights can disrupt signals on cables resulting in crappy connectivity for users.
- Faraday Cage:
    - Shielding installed around an entire room that prevents electromagnetic energy and radio frequencies from entering or leaving the room
- **Remember this:**
    - **EMI shielding prevents outside interference sources from corrupting data and prevents data from emanating outside cable. Cable troughs protect cables distributed throughout a building in metal containers. A Faraday cage prevents signals from emanating beyond the cage.**
- Redundancy: Increases reliability of systems even if they fail
    - Redundancy – adds duplication to critical system components and networks
    - Redundancy helps ensure fault-tolerance to continue operations
        - ADD:
            - Disk redundancies using RAID

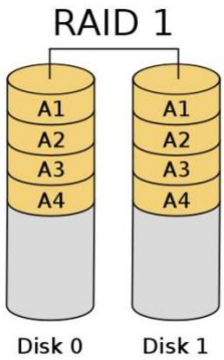
- Server redundancies by adding failover clusters
- Power redundancies by adding generators or an UPS (Uninterrupted Power Supply)
- Add Hot, Cold, Warm sites

- Single Point of Failure
  - The individual elements, objects, or parts of a system that would cause the whole system to fail if they were to fail
    - Disk
      - If server uses a single drive the server will crash if the disk fails. RAID provides fault tolerance for hard drives
    - Server
    - Power
      - Use multiple power sources such as power generators or UPS to mitigate power outage troubles
- **Remember this:**
  - **A single point of failure is any component whose failure results in failure of an entire system. Elements such as RAID, failover clustering, UPSs, and generators remove many single points of failure. RAID is an inexpensive method used to add fault tolerance and increase availability.**
- RAID – Redundant Array of Inexpensive Disks
  - Allows the combination of multiple physical hard disks into a single logical hard disk drive that is recognized by the operating system
  - Provide Fault tolerance for disks and increase system availability.
  - Are becoming much more affordable
- RAID – 0
  - Only one that doesn't provide any redundancy or fault tolerance
  - Provides data striping across multiple disks to increase performance
  - Files stored on a RAID-0 array are spread across each of the disks.

- Increased read and write performance as file is spread across multiple physical disks, different parts of file can be read from or written to each of the disks at the same time. 3 500GB drives = 1.5TB storage space.

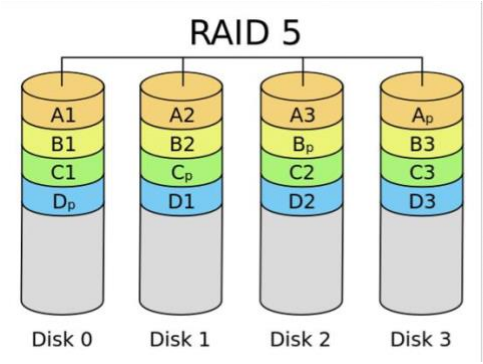


- RAID – 1
  - Provides redundancy by mirroring the data identically on two hard disks
  - Data written to one disk is also written to the other.
    If one disk fails, the other still has all data so system can continue without data loss

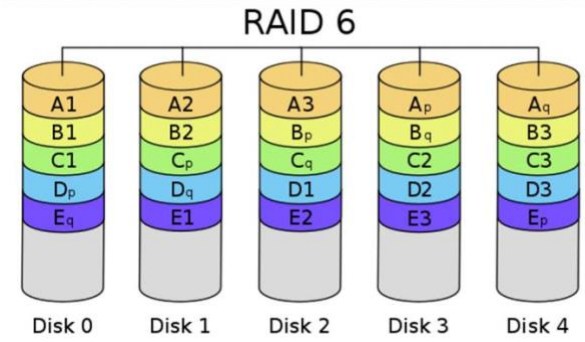


- RAID – 5/6
  - Both Provide redundancy by striping data and parity data across the disk drives
  - RAID 5 – 3 or more disks that are striped together similar to RAID-0
    - 1 drive includes parity information. This is used for fault tolerance.
      - If one drive fails, system can read information on remaining drives and determine what the actual data should be.

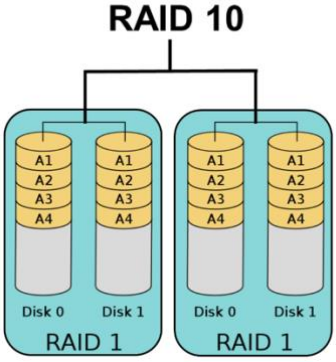
- If Two drives fail in a RAID-5 data is lost.



  - RAID 6 – Extension of RAID-5 including an extra parity block.
    - RAID-6 will continue to operate even if two disks fail.
    - Requires minimum of four disks.



- **Remember this:**
  - **RAID subsystems such as RAID-1, RAID-5 and RAID-6 provide fault tolerance and increased data availability. RAID-5 can survive the failure of one disk. RAID-6 can survive failure of two disks.**
- RAID-10 or RAID 1+0
  - Combines features of mirroring (RAID-1) and striping (RAID-0).
  - Minimum no. of drives is four. Add drives in multiples of two.
    - E.G: 2,4,6 etc.



- **Fault-resistant RAID**
  - Protects against the loss of the array's data if a single disk fails (RAID 1 or RAID 5)
- **Fault-tolerant RAID**
  - Protects against the loss of the array's data if a single component fails (RAID 1, RAID 5, RAID 6)
- **Disaster-tolerant RAID**
  - Provides two independent zones with full access to the data (RAID 10)

- High Availability – System or service that needs to remain operational with almost zero downtime.
  - Possible to achieve 99.99% uptime called 'Five Nines'.
    - Less than 6 minutes of downtime per year. Failover clusters are a common component in 5/9's.
    - Expensive
  - Distributive allocation – provides both high availability and stability
- Cluster
  - Two or more servers working together to perform a particular job function
  - Servers may also be called nodes
- Failover Cluster
  - A secondary server can take over the function when the primary one fails.
- Load-balancing Cluster
  - Servers are clustered in order to share resources such as CPU, RAM, and hard disks
- Load balancing:
  - Optimize and distributes data loads across multiple computers or networks. Usually located in the webfarm through a DMZ.
  - Can detect when a server fails.
  - Hardware based load balancer: Accepts traffic and directs it to servers based on factors such as process utilization and no. of current connections to server
  - Software-based load balancer: Uses software running on each of the servers in load-balanced cluster to balance load.
    - Uses Virtual IP
  - Some load balancers use source address affinity to direct Requests.

        - Source affinity – sends requests to same server based on requestor's IP address.
- **Remember this:**
    - **Failover clusters are one method of server redundancy and provide high availability for servers. They can remove a server as a single point of failure. Load balancing increases overall processing power of a service by sharing load among multiple servers. Configurations can be active-passive or active-active. Scheduling methods include round-robin and source IP address affinity. Source IP address affinity scheduling ensures clients are redirected to same server for an entire session. A round-robin scheduling scheme allows a load balancer to send requests to servers one after another.**

The database servers are in an active-active load-balancing configuration because web servers can query both database servers.

In an active-passive configuration, only one of the database servers would be answering queries at any given time.

Round-robin and affinity are two methods of scheduling the load balancing in an active-active configuration.

- Power Redundancies –
    - Use UPS as a fault tolerance for power and protection against power fluctuations
    - Generators provide long-term power outages.
- Backups: Require money and time
    - Full Backup
        - All of the contents of a drive are backed up o
    - Incremental Backup
        - Backs up all the data that has changed or is different since last full backup
    - Differential Backup
        - Backs up all data that has changed since last full or incremental backup.
    - Snapshot
        - Backup captures data at a point in time.
- Why are there so many different varieties of backups? Different Organisations have different needs
- **Remember this:**
    - **If you have unlimited time and money the full backup alone provides fastest recover time. Full/incremental strategies reduce amount of time needed to perform backups.**

Full/differential strategies reduce amount of time needed to restore backups.

- Testing backups
  - Validate backups via test restores.
  - Test restore – restore data and verify its integrity
  - Two tests:
    - Test succeeds – backup process works
    - Test fails – You will know there's a problem you can fix before a crisis.
  - Allows admins to become familiar with process
- Protecting Backups
  - Store them
  - Transfer them from one location to another
  - Destruction
    - Destroy unneeded backups via degaussing media, shredding or burning media or scrubbing
- Geographical Considerations for Backups
  - Off-site Backups
    - Copy of backups should be stored in a separate geographical location to protect against a disaster such as a fire/flood
  - Distance
  - Location Selection – Dependent on environmental issues.
  - Legal Implications
    - Legal implications related to backups depends on data stored in backups
  - Data Sovereignty
    - Legal implications when data is stored off site.
      - E.G: Backups stored in different country are subject to laws of that country
- **Remember this:**
  - **Test restore are the best way to test integrity of a company's backup data. Backup media should be protected with the same level of protection as the data on the backup. Geographical considerations for backups include storing**

backups off-site, choosing best location and considering legal implications and data sovereignty.

- BCP – Business Continuity Plan
  - Includes disaster recovery elements that provide steps used to return critical functions to operation after an outage.
    - E.G: Fires, Attacks, Power outages, Data loss, Hardware/Software failures, Natural Disasters etc.
- BIA – Business Impact Analysis
  - Important part of BCP. Identifies critical systems and components essential to organization's success as well as vulnerable business processes.
- **Remember this:**
  - **BIA identifies mission-essential functions and critical systems that are essential to the organization's success. Also identifies maximum downtime limits for these systems and components, various scenarios that can impact these systems and components and potential losses from an incident.**
- Privacy Threshold Assessment:
  - Helps organization identify PII within a system.
- If system holds PII → Leads to:
- Privacy Impact Assessment
  - Attempts to identify potential risks related to the PII by reviewing how information is handled. Ensure system is complying with applicable laws, regulations and guidelines.
- **Remember this:**
  - **A privacy threshold assessment is typically a simple questionnaire completed by system or data owners. It helps identify if a system processes data that exceeds the threshold for PII. If system processes PII, a privacy impact assessment helps identify and reduce risks related to potential loss of the PII.**
- RTO – Recovery time Objective
  - Identifies maximum amount of time it should take to restore a system after an outage.

- RPO – Recovery Point Objective
    - Identifies a point in time where data loss is acceptable and the amount of data you can afford to lose.

- MTBF – Mean time between failures
    - Provides a measure of a system's reliability and is usually represented in hours.
    - Average time between failures. Higher MTBF no.'s indicates higher reliability of a system/product
- MTTR – Mean Time to recover
    - Average time it takes to restore a failed system.
- Continuity of operations planning – Restoring mission-essential functions at a recovery site after a critical outage.
- Recovery site – alternate processing site that an organization can use after disaster.
    - Hot Site
        - A near duplicate of the original site of the organization that can be up and running within minutes
        - Should be operation 24/7 hours a day right after a primary site failure
    - Warm Site
        - A site that has computers, phones, and servers but they might require some configuration before users can start working
    - Cold Site
        - A site that has tables, chairs, bathrooms, and possibly some technical items like phones and network cabling
- Site variations:
    - Mobile Site
        - Self-Contained transportable unit with all equipment needed for specific requirements.
        - No set location. Provide temporary support during a disaster
        - E.G: Semitrailer with satellite dish
    - Mirrored site

        - Identical to primary location and provide 100% availability. Use real-time transfers to send modifications from primary location to mirrored site.
        - Although a hot site can be up and operational within an hour, mirrored site is always up and operational

- DRP – Disaster Recovery Plan
    - The development of an organized and in-depth plan for problems that could affect the access of data or the organization's building
    - Steps:
        - 1. Activate disaster recovery plan
            - Some disasters such as earthquakes occur without much warning. DRP is activated after disaster
        - 2. Implement contingencies
            - Move critical functions off main site.
        - 3. Recover Systems
        - 4. Test recovered systems
        - 5. After-action report
- **Remember this:**
    - **A DRP includes a hierarchical list of critical systems and often prioritizes services to restore after an outage. Testing validates the plan. The final phase of disaster recovery includes a review to identify any lessons learned and may include an update of the plan.**
- Testing Plans with Exercises.
    - Tabletop Exercise/Desktop Exercise/Structured Walkthrough
        - Coordinator gathers participants in a classroom/conference and leads them through multiple scenarios and what they should do.
    - Common elements of testing:
        - Backups
        - Server Restoration
        - Server Redundancy – If a server is within a failover cluster, test cluster by taking primary node offline. Another node within cluster should automatically assume role of this offline node.

        - Alternate sites
            - Test alternate sites such as hot, cold or warm to ensure the sites are working as desired
- **Remember this:**
    - **You can validate business continuity plans through testing. Tabletop exercises are discussion based only and are typically performed in a classroom or conference setting. Functional exercises are hands-on exercises.**