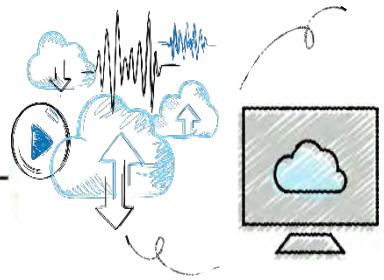
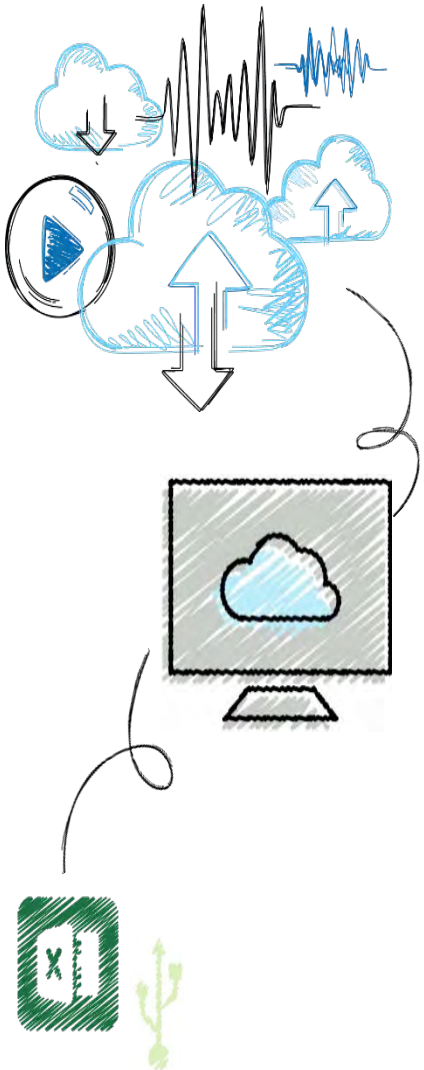
CompTIA Security+

Chapter 14

Business Continuity





Objectiaves

14.1 Describe the different types of wireless network attacks

14.2 List the vulnerabilities in IEEE 802.11 security

14.3 Explain the solutions for securing a wireless network

What is Business Continuity?

- Business Continuity
  - An organization’s ability to maintain operations after a disruptive event
- Business continuity preparedness involves:
  - Business continuity planning
  - Business impact analysis
  - Disaster recovery planning

Business Continuity Planning (BCP)

- BCP is the process of:
  - Identifying exposure to threats
  - Creating preventative and recovery procedures
  - Testing them to determine if they are sufficient
- BCP consists of three essential elements:
  - Business recovery planning
  - Crisis management and communications
  - Disaster recovery

Business Impact Analysis (BIA) (1 of 2)

- BIA - identifies business functions and quantifies the impact a loss of these functions may have on business operations
- These range from:
  - Impact on property (tangible assets)
  - Impact on finance (monetary funding)
  - Impact on safety (physical protection)
  - Impact on reputation (status)
  - Impact on life (wellbeing)
- A BIA will help determine the **mission-essential function**
  - Activity that serves as the core purpose of the enterprise

Business Impact Analysis (BIA) (2 of 2)

- A BIA can also help in the **identification of critical system**
  - That support the mission-essential function
- Identifying a **single point of failure**
  - Which is a component or entity in a system which will disable the entire system, should it no longer function
  - Minimizing these single failure points results in high availability
- Many BIAs also contain a **privacy impact assessment**
  - Used to identify and mitigate privacy risks
- **Privacy threshold assessment**
  - Can determine if a system contains personally identifiable information (PII)

Disaster Recovery Plan (DRP) (1 of 5)

- **Disaster recovery plan (DRP)**
  - Focuses on protecting and restoring information technology functions
- Written document detailing process for restoring IT resources:
  - Following a disruptive event
- Comprehensive in scope
  - Intended to be a detailed document that is updated regularly
- Most DRPs:
  - Have a common set of features
  - Cover specific topics
  - Require testing for verification

Disaster Recovery Plan (DRP) (2 of 5)

- Features
- Typical outline of a DRP:
  - Unit 1: Purpose and Scope
  - Unit 2: Recovery Team
  - Unit 3: Preparing for a Disaster
  - Unit 4: Emergency Procedures
  - Unit 5: Restoration Procedures

Disaster Recovery Plan (DRP) (3 of 5)

- Topics
  - Sequence in restoring systems (**order of restoration**)
    - Which systems should have priority and be restored before other systems?
  - What should be done if a disaster makes the current location for processing data no longer available
    - An alternative processing site must be identified
    - **Failback** – the process of resynchronizing data back to the primary location

Disaster Recovery Plan (DRP) (4 of 5)

- Testing
- Disaster exercises are designed to test the effectiveness of the DRP
- Disaster exercise objectives
  - Test efficiency of interdepartmental planning and coordination in managing a disaster
  - Test current DRP procedures
  - Determine response strengths and weaknesses
- **Tabletop exercises**
  - Simulate an emergency situation but in an informal and stress-free environment
- An after-action report should be generated
  - To analyze the exercise results to identify strengths to be maintained and weaknesses to improve upon

Disaster Recovery Plan (DRP) (5 of 5)

Feature	Description
Participants	Individuals on a decision-making level
Focus	Training and familiarizing roles, procedures, and responsibilities
Setting	Informal
Format	Discussion guided by a facilitator
Purpose	Identify and solve problems as a group
Commitment	Only moderate amount of time, cost, and resources
Advantage	Can acquaint key personnel with emergency responsibilities, procedures, and other members
Disadvantage	Lack of realism; does not provide a true test

Fault Tolerance Through Redundancy

- Fault tolerance
  - Refers to a system's ability to deal with malfunctions
- The solution to fault tolerance is to build in **redundancy**
  - Which is the use of duplicated equipment to improve the availability of a system
  - A goal is to reduce a variable known as the **mean time to recovery (MTTR)**
    - The average amount of time that it will take a device to recover from a failure that is not a terminal failure
- Redundancy planning
  - Applies to servers, storage, networks, power, sites, and data

Servers (1 of 3)

- Servers
  - Play a key role in network infrastructure
  - Failure can have significant business impact
- Clustering
  - Combining two or more devices to appear as a single unit
- Server cluster
  - Multiple servers that appear as a single server
  - Connected through public and private cluster connections
- Types of server clusters
  - Asymmetric
  - Symmetric

Servers (2 of 3)

- In an asymmetric server cluster, a standby server performs no function except to be ready if needed
  - Used for databases, messaging systems, file and print services
- All servers do useful work in a symmetric server cluster
  - If one server fails, remaining servers take on failed server's work
  - More cost effective than asymmetric clusters
  - Used for Web, media, and VPN servers

Servers (3 of 3)

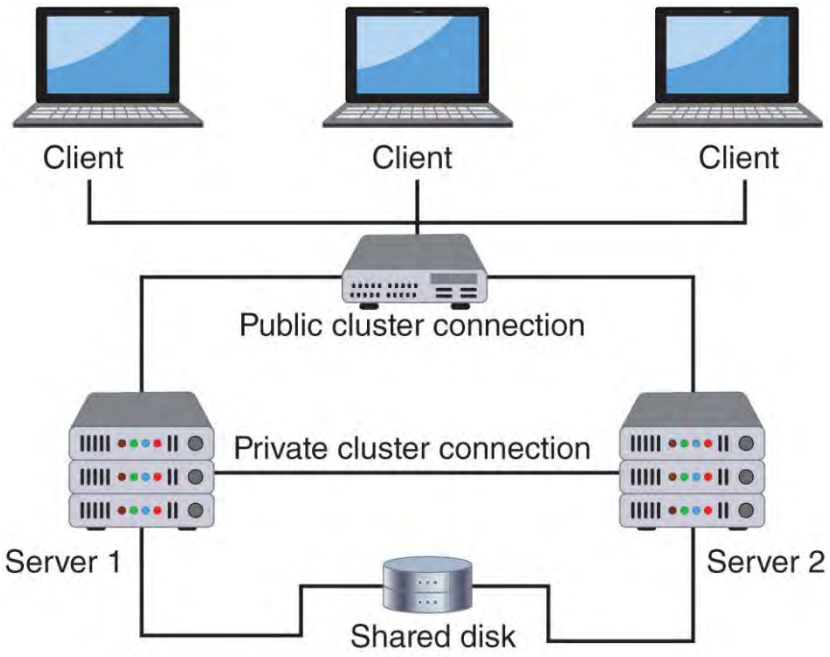


Figure 14-1 Server cluster

Storage (1 of 6)

- Storage - a trend in data storage is to use solid-state drives (SSDs)
  - SSDs are more resistant to failure and are considered more reliable than traditional HDDs
  - HDDs are often the first components to fail
  - Some organizations keep spare hard drives on hand
- Mean time between failures (MTBF)
  - Measures average time until a component fails and must be replaced
  - Can be used to determine number of spare hard drives an organization should keep

Storage (2 of 6)

- Redundant Array of Independent Devices (RAID)
  - Uses multiple hard disk drives to increase reliability and performance
  - Can be implemented through software or hardware
  - Several levels of RAID exist
- RAID Level 0 (striped disk array without fault tolerance)
  - Striping partitions hard drive into smaller sections
  - Data written to the stripes is alternated across the drives
  - If one drive fails, all data on that drive is lost

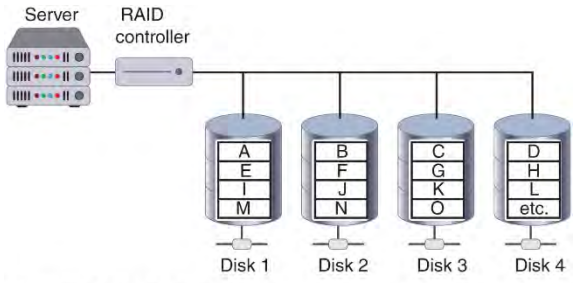


Figure 14-2 RAID Level 0

Storage (3 of 6)

- RAID Level 1 (mirroring)
  - Disk mirroring used to connect multiple drives to the same disk controller card
  - Action on primary drive is duplicated on other drive
  - Primary drive can fail and data will not be lost
- Disk duplexing
  - Variation of RAID Level 1
  - Separate cards used for each disk
  - Protects against controller card failures

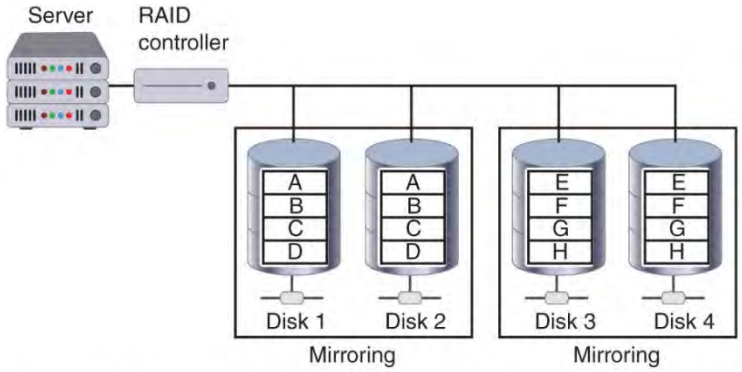


Figure 14-3 RAID Level 1

Storage (4 of 6)

- RAID Level 5 (independent disks with distributed parity)
  - Distributes parity (error checking) across all drives
  - Data stored on one drive and its parity information stored on another drive

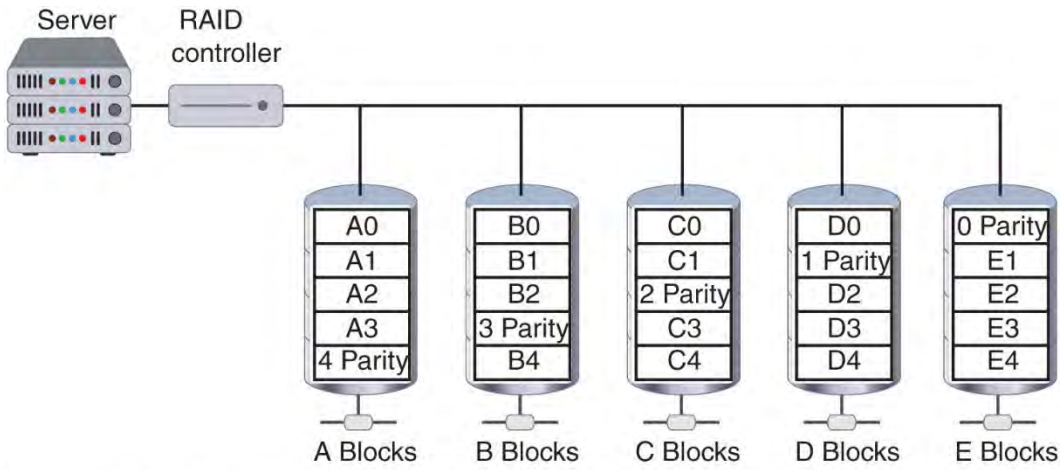


Figure 14-4 RAID Level 5

Storage (5 of 6)

- RAID 0+1 (high data transfer)
  - Nested-level RAID
  - Mirrored array whose segments are RAID 0 arrays
  - Can achieve high data transfer rates

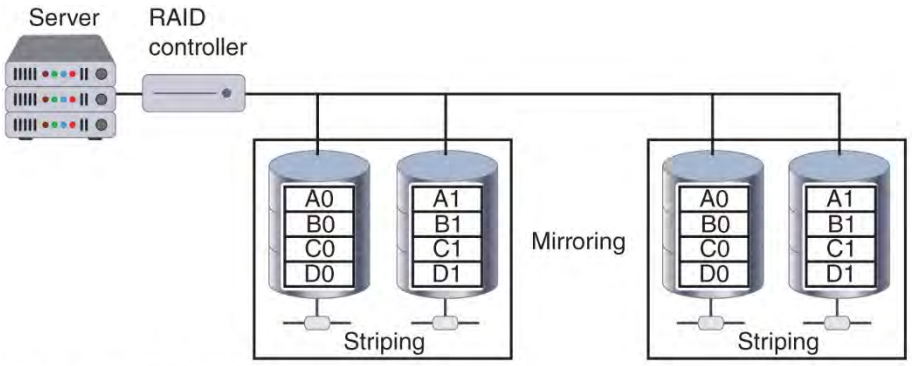


Figure 14-5 RAID Level 0+1

Storage (6 of 6)

RAID level	Description	Min number of drives needed	Typical application	Advantages	Disadvantages
RAID 0	Uses a striped disk array so that data is broken down into block and each block is written to a separate disk drive	2	Video production and editing	Simple design, easy to implement	Not fault-tolerant
RAID 1	Data written twice to separate drives	2	Financial	Simplest RAID to implement	Can slow down system if RAID controlling software is used instead of hardware
RAID 5	Each data block is written on a data disk and parity for blocks in the same rank is generated and recorded on a separate disk	3	Database	Most versatile RAID	Can be difficult to rebuild if a disk fails
RAID 0+1	A mirrored array with segments that are RAID 0 arrays	4	Imaging applications	High input/output rates	Expensive

Networks

- Redundant networks
  - May be necessary due to critical nature of connectivity today
  - Wait in the background during normal operations
  - Use a replication scheme to keep live network information current
  - Launch automatically in the event of a disaster
  - Hardware components are duplicated
  - Some organizations contract with a second Internet service provider as a backup
- Software defined networks (SDNs)
  - SDN controller can increase network reliability and may lessen the need for redundant equipment

Power (1 of 2)

- Maintaining power is essential when planning for redundancy
- Uninterruptible power supply (UPS)
  - Maintains power to equipment in the event of an interruption in primary electrical power source
- Off-line UPS
  - Least expensive, simplest solution
  - Charged by main power supply
  - Begins supplying power quickly when primary power is interrupted
  - Switches back to standby mode when primary power is restored

Power (2 of 2)

- On-line UPS
  - Always running off its battery while main power runs battery charger
  - Not affected by dips or sags in voltage
  - Can serve as a surge protector
- UPS systems can communicate with the network operating system to ensure orderly shutdown occurs
  - But, can only supply power for a limited time
- Backup generator
  - Powered by diesel, natural gas, or propane

Recovery Sites (1 of 3)

- Recovery Sites
  - Backup sites may be necessary if flood, hurricane, or other major disaster damages buildings
  - Three types of redundant sites: hot, cold, and warm
- Hot site
  - Generally run by a commercial disaster recovery service
  - Duplicate of the production site
  - Has all needed equipment
  - Data backups can be moved quickly to the hot site

Recovery Sites (2 of 3)

- Cold site
  - Provides office space
  - Customer must provide and install all equipment needed to continue operations
  - No backups immediately available
  - Less expensive than a hot site
  - Takes longer to resume full operation

Recovery Sites (3 of 3)

- Warm site
  - All equipment is installed
  - No active Internet or telecommunications facilities
  - No current data backups
  - Less expensive than a hot site
  - Time to turn on connections and install backups can be half a day or more
- A growing trend is to use cloud computing in conjunction with sites
  - Back up applications and data to the cloud
  - If a disaster occurs, restore it to hardware in a hot, cold, or warm site

Data (1 of 5)

- Data backup – copying information to a different medium and storing it at an off-site location
  - So that it can be used in the event of a disaster
- Backing up data involves:
  - Data backup calculations
  - Using different types of data backups
  - Off-site backups

Data (2 of 5)

- Two elements are used in the calculation of when backups should be performed:
- Recovery point objective (RPO)
  - Maximum length of time organization can tolerate between backups
- Recovery time objective (RTO)
  - Length of time it will take to recover backed up data

Data (3 of 5)

- Types of Data Backups

Type of backup	How used	Archive bit after backup	Files needed for recovery
Full backup	Starting point for all backups	Cleared (set to 0)	The full backup is needed
Differential backup	Backs up any data that has changed since last full backup	Not cleared (set to 1)	The full backup and only last differential backup are needed
Incremental backup	Backs up any data that has changed since last full backup or last incremental backup	Cleared (set to 0)	The full backup and all incremental backups are needed

Data (4 of 5)

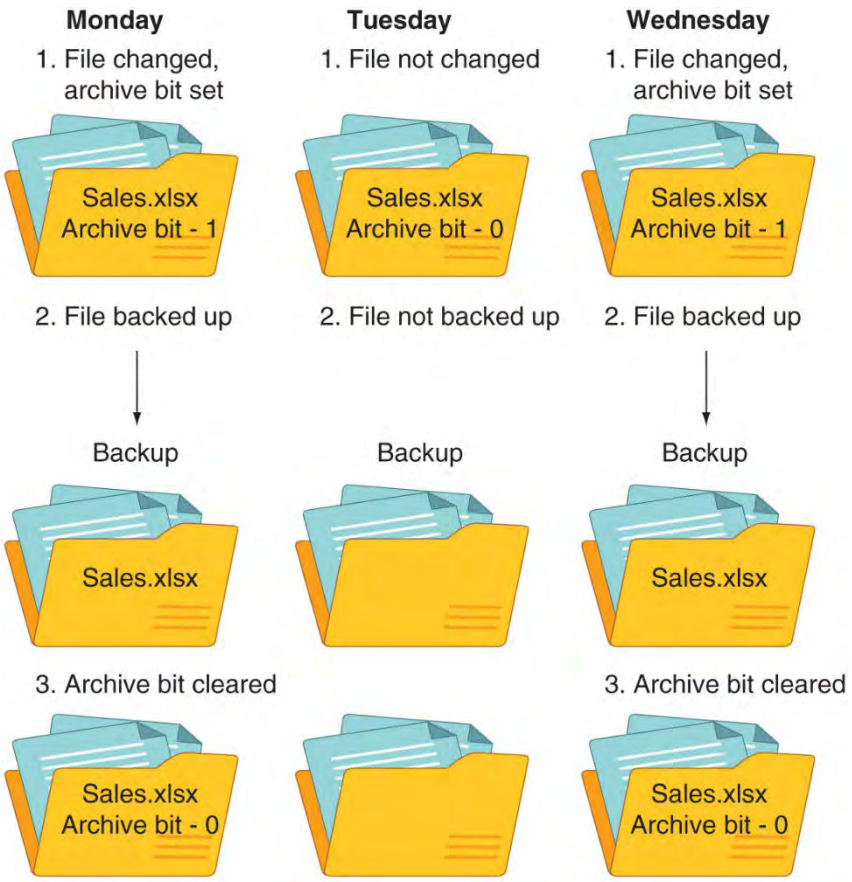


Figure 14-6 Archive bit

Data (5 of 5)

- Types of Data Backups (continued)
  - A more comprehensive backup technology is known as continuous data protection (CDP)
    - Performs continuous backups that can be restored immediately
    - Maintains a historical record of all changes made to data
    - Creates a snapshot of the data (like a reference marker)

Off-Site Backups (1 of 2)

- 3-2-1 backup plan
  - Should always be three different copies of backups on at least two different types of storage media and one of the backups should be stored at a different location (off-site backup)
- Most organizations store their off-site backups using an online cloud repository
  - These sites often use CDP to continually backup data
- There are several Internet services that provide similar features to these:
  - Automatic continuous backup
  - Universal access
  - Delayed deletion
  - Online or media-based restore

Off-Site Backups (2 of 2)

- There are legal implications of off-site backups
  - The primary issue involves data sovereignty
    - Data stored in digital format is subject to the laws of the country in which the storage facility resides
- Organizations should identify a cloud services provider whose data center locations ensure that it fully complies with all applicable data sovereignty laws

Environmental Controls

- Methods to prevent disruption through environmental controls
  - Fire suppression
  - Electromagnetic disruption protection
  - Proper configuration of HVAC systems

Fire Suppression (1 of 2)

- Fire suppression includes the attempts to reduce the impact of a fire
- Requirements for a fire to occur
  - A type of fuel or combustible material
  - Sufficient oxygen to sustain combustion
  - Enough heat to raise material to its ignition temperature
  - Chemical reaction: fire itself
- In a server closet or room that contains computer equipment
  - A stationary fire suppression system is recommended

Fire Suppression (2 of 2)

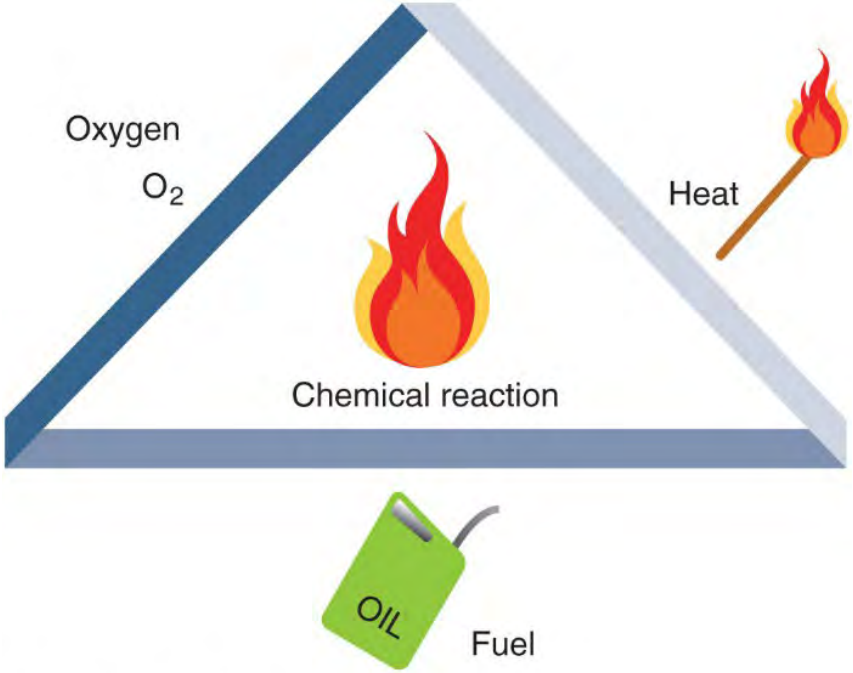


Figure 14-7 Fire triangle

Electromagnetic Disruption Protection (1 of 2)

- Electromagnetic interference (EMI)
  - Caused by a short-duration burst of energy by the source called an electromagnetic pulse (EMP)
- Electromagnetic compatibility (EMC)
  - Reducing or eliminating the unintentional generation, spread, and reception of electromagnetic energy
  - The goal of EMC is the correct operation of different types of equipment that function in the same electromagnetic environment
- Faraday cage
  - Metal enclosure that prevents entry or escape of electromagnetic fields
  - Often used for testing in electronic labs

Electromagnetic Disruption Protection (2 of 2)

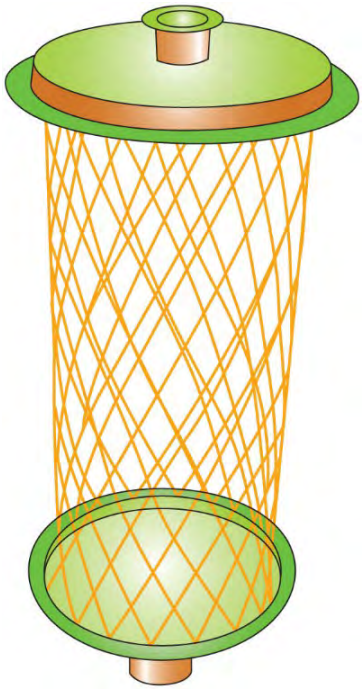


Figure 14-8 Faraday cage

HVAC

- Data centers have special cooling requirements
  - More cooling necessary due to large number of systems generating heat in confined area
  - Precise cooling needed
- Heating, ventilating, and air conditioning (HVAC) systems
  - Maintain temperature and relative humidity at required levels
- Controlling environmental factors can reduce electrostatic discharge
- Hot aisle/cold aisle layout
  - Used to reduce heat by managing air flow
  - Servers lined up in alternating rows with cold air intakes facing one direction and hot air exhausts facing other direction

Incident Response

- When an unauthorized incident occurs:
  - An immediate response is required
- Incident response
  - Involves using forensics and following proper incident response procedures

What is Forensics?

- Forensic Science
  - Applying science to legal questions
    - Analyzing evidence and can be applied to technology
  - Computer forensics
    - Uses technology to search for computer evidence of a crime
- Importance of computer forensics is due to the following:
  - Amount of digital evidence
  - Increased scrutiny by the legal profession
  - Higher level of computer skill by criminals

Incident Response Plan (1 of 2)

- Incident response plan (IRP)
  - A set of written instructions for reacting to a security incident
- Incident response process – six action steps to be taken when an incident occurs:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

Incident Response Plan (2 of 2)

- At a minimum, an IRP should contain the following:
  - Documented incident definitions
  - Cyber-incident response teams
  - Reporting requirements/escalation
  - Exercises

Forensic Procedures

- Five basic steps:
  - Secure the crime scene
  - Preserve the evidence
  - Establish a chain of custody
  - Examine the evidence
  - Enable recovery

Secure the Crime Scene (1 of 2)

- When an illegal or unauthorized incident occurs, action must be taken immediately
- Individuals in the immediate vicinity should perform damage control:
  - Report the incident to security or police
  - Confront any suspects (if situation allows)
  - Neutralize the suspected perpetrator from harming others
  - Secure physical security features
  - Quarantine electronic equipment
  - Contact the cyber-incident response team

Secure the Crime Scene (2 of 2)

- After the response team arrives, the first job is to secure the crime scene, which includes:
  - Physical surroundings documented
  - Photographs taken before anything is touched
  - Computer cables labeled
  - Team takes custody of entire computer
  - Team interviews witnesses
  - Length of time passed since the initial incident should be noted

Preserve the Evidence (1 of 3)

- Preservation of the evidence
  - Ensuring that important proof is not destroyed
- Digital evidence is very fragile
  - Can be easily altered or destroyed
- One of the first steps is for a legal hold to be issued
  - A notification sent from the legal team to employees instructing them not to delete electronically stored or paper documents relative to the incident
- Cyber-incident response team captures volatile data
  - Examples: contents of RAM, current network connections, logon sessions, network traffic and logs, any open files
- Order of volatility must be followed to preserve most fragile data first

Preserve the Evidence (2 of 3)

Location of data	Sequence to be retrieved
Register, cache, peripheral memory	First
Random access memory (RAM)	Second
Network state	Third
Running processes	Fourth

Preserve the Evidence (3 of 3)

- Use tools that allow capturing the system image
  - A snapshot of the current state of the computer that contains all current settings and data
  - Capture the current image on the screen by taking a screenshot
- Mirror image backup of the hard drive (also called a bit-stream backup)
  - Meets evidence standards
  - To guarantee accuracy, mirror image backup programs rely upon hashing algorithms as part of the validation process

Establish the Chain of Custody

- Chain of custody
  - Documents that the evidence was maintained under strict control at all times
  - No unauthorized person was given opportunity to corrupt the evidence

Examine for Evidence (1 of 3)

- After a computer forensics expert creates a mirror image of a system, the original system is secured and the mirror image is examined to reveal evidence
- Includes searching:
  - Word documents, email files, spreadsheets, cache and cookies of the web browser
- Hidden clues also can be exposed by examining
  - RAM slack, drive slack, and metadata (data about data)

Examine for Evidence (2 of 3)

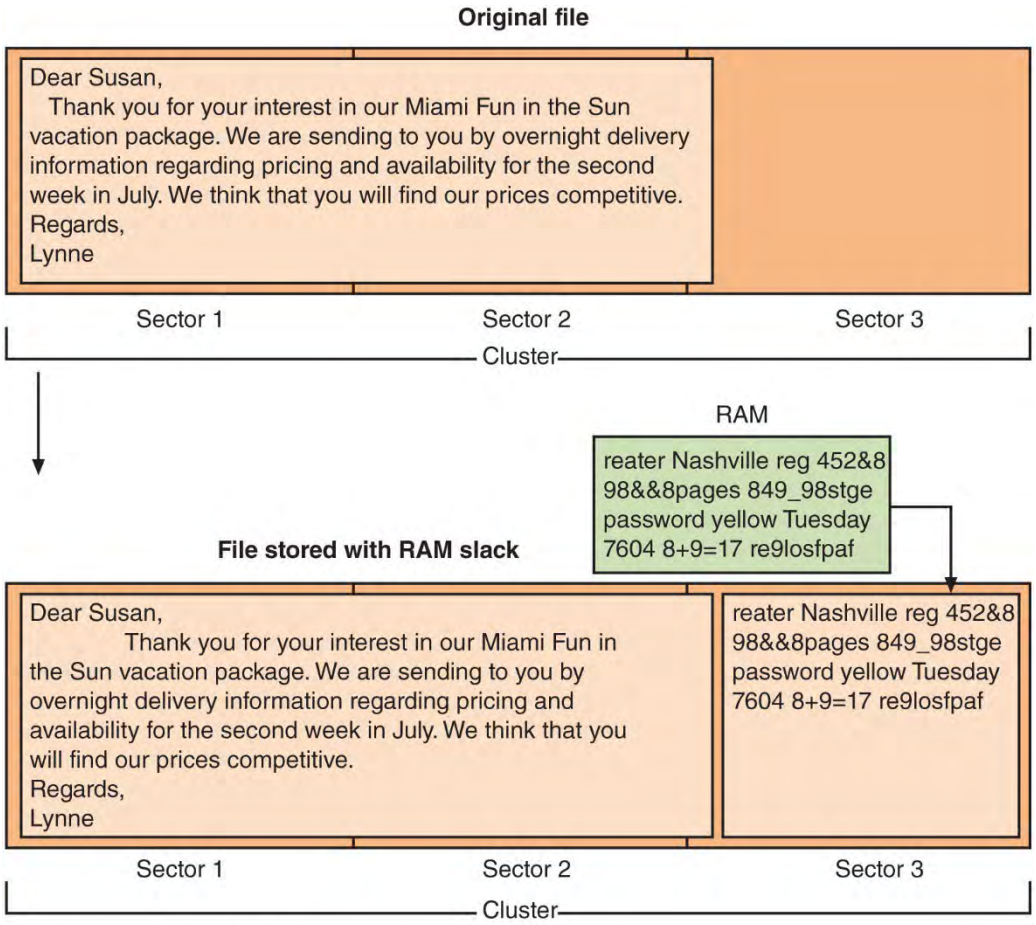


Figure 14-9 RAM slack

Examine for Evidence (3 of 3)

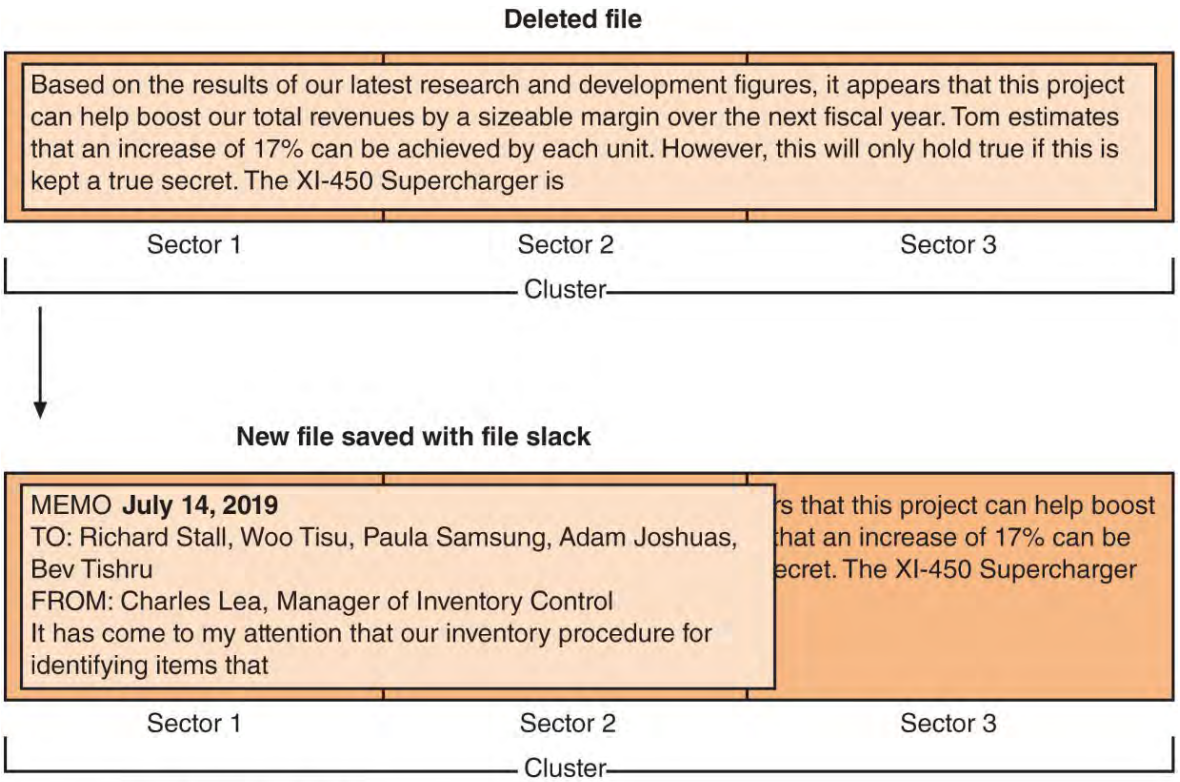


Figure 14-10 Drive file slack

Enable Recovery

- Strategic intelligence
  - The collection, processing, analysis, and dissemination of intelligence for forming policy changes
- Strategic counterintelligence
  - Involves gaining information about the attacker's intelligence collection capabilities
- Active logging
  - Maintaining active logs regarding the reconnaissance activities conducted by the attacker

Chapter Summary (1 of 3)

- Business continuity is an organization's ability to maintain its operations after a disruptive event
- In IT contingency planning, an outline of procedures that are to be followed in the event of a major IT incident is developed
- Disaster recovery
  - Focuses on restoring information technology functions
  - Disaster recovery plan (DRP) details restoration process
- A server cluster combines two or more servers that are interconnected to appear as one
- RAID uses multiple hard disk drives for redundancy

Chapter Summary (2 of 3)

- Network components can be duplicated to provide a redundant network
- Data backup
  - Copying information to a different medium and storing (preferably offsite) for use in event of a disaster
- Recovery point objective and recovery time objective help an organization determine backup frequency
- Fire suppression systems include water, dry chemical, and clean agent systems

Chapter Summary (3 of 3)

- A defense for shielding an electromagnetic field is a Faraday cage
- The control and maintenance of HVAC systems are important for data centers
- Forensic science is the application of science to questions that are of interest to the legal profession
- An incident response plan (IRP) is a set of written instructions for reacting to a security incident

Review Questions

A(n) _____ is always running off its battery while the main power runs the battery charger.

A. secure UPS

B. backup UPS

C. off-line UPS

D. on-line UPS

Review Questions

A(n) _____ is always running off its battery while the main power runs the battery charger.

A. secure UPS

B. backup UPS

C. off-line UPS

D. **on-line UPS**

Review Questions

Which type of site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running?

A. Cold site

B. Warm site

C. Hot site

D. Replicated site

Review Questions

Which type of site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running?

A. Cold site

B. Warm site

C. **Hot site**

D. Replicated site

Review Questions

Which of these is NOT a characteristic of a disaster recovery plan (DRP)?

A. It is updated regularly.

B. It is a private document used only by top-level administrators for planning.

C. It is written.

D. It is detailed.

Review Questions

Which of these is NOT a characteristic of a disaster recovery plan (DRP)?

A. It is updated regularly.

B. **It is a private document used only by top-level administrators for planning.**

C. It is written.

D. It is detailed.

Review Questions

What is the maximum length of time that an organization can tolerate between data backups?

A. Recovery time objective (RTO)

B. Recovery service point (RSP)

C. Recovery point objective (RPO)

D. Optimal recovery timeframe (ORT)

Review Questions

What is the maximum length of time that an organization can tolerate between data backups?

A. Recovery time objective (RTO)

B. Recovery service point (RSP)

C. **Recovery point objective (RPO)**

D. Optimal recovery timeframe (ORT)

Review Questions

When an unauthorized event occurs, what is the first duty of the cyber-incident response team?

A. To log off from the server

B. To secure the crime scene

C. To back up the hard drive

D. To reboot the system

Review Questions

When an unauthorized event occurs, what is the first duty of the cyber-incident response team?

A. To log off from the server

B. **To secure the crime scene**

C. To back up the hard drive

D. To reboot the system

Coming Up Next…

CompTIA Security+

Chapter 15

Risk Mitigation