UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

Lecture 12: Business Continuity

Objectives

- Define environmental controls
- Describe the components of redundancy planning
- List disaster recovery procedures
- Describe incident response procedures

Business Continuity

Business Continuity — Organization's ability to maintain operations after a disruptive event (Power outage, hurricane, tsunami)

Business continuity planning and testing steps

1. Identify exposure to threats
2. Create preventative and recovery procedures
3. Test procedures to determine if they are sufficient

Continuity of operations — Ensuring an organization can continue to function in event of natural or human-made disaster

Business Continuity

Succession Planning

Determining in advance who is authorized to take over if key employees die or are incapacitated

How?

BUSINESS IMPACT ANALYSIS (BIA)

- Analyzes most important business functions and quantifies impact of their loss
- Identifies threats through risk assessment
- Determines impact if threats are realized

Questionnaires used to prompt thinking about impact of a disaster

In-person interviews held
–Discuss different disaster scenarios
–BIA interview form helps organize information obtained from the interview

Business Continuity

Field name	Explanation
Name of Business Unit	Description of this unit's function
Employees	Number of full-time staff
Function	A brief description of the principal activities the unit performs (marketing, production, engineering, and so on)
Parent Dependencies	The names of other business units that this unit needs for its normal operations
Child Dependencies	The names of other units that need this unit for their normal operations
Technology Recovery	The critical IT functions that are needed (network services, servers, hardware, and so on)
Quantitative Impact	The financial loss to the company in the event this unit cannot function
Qualitative Impact	Any nonfinancial impact to the company (loss of reputation, loss of customers, and so on) in the event this unit cannot function
Recovery Strategy	The actions the business unit can take to recover to a normal business function (employees work from home, relocate to an alternate site, and so on)
Recovery Time	The amount of time needed to fully recover

BIA interview form

Disaster Recovery

- Subset of business continuity planning and testing
- Also known as contingency planning
- Focuses on protecting and restoring information technology functions

Disaster recovery activities:

Create, implement, and test disaster recovery plans (address redundancy and fault tolerance as well as data backups)

Disaster Recovery Plan (DRP)

- Written document detailing process for restoring IT resources
- Comprehensive in scope
- Updated regularly
- Example of disaster planning approach
  - –Define different risk levels for organization's operations based on disaster severity

Disaster Recovery Plan (DRP)

Common features of most DRP:

- Definition of plan purpose and scope
- Definition of recovery team and their responsibilities
- List of risks and procedures and safeguards that reduce risk
- Outline of emergency procedures
- Detailed restoration procedures

DRP must be adaptable

Backout/contingency option

- If plan response is not working properly, technology is rolled back to starting point
- Different approach taken

Disaster Recovery Plan (DRP)

Unit 1: Purpose and Scope—The reason for the plan and what it encompasses are clearly outlined. Those incidences that require the plan to be enacted also should be listed. Topics found under Unit 1 include:

- Introduction
- Objectives and constraints
- Assumptions
- Incidents requiring action
- Contingencies
- Physical safeguards
- Types of computer service disruptions
- Insurance considerations

Unit 2: Recovery Team—The team that is responsible for the direction of the disaster recovery plan is clearly defined. It is important that each member knows her role in the plan and be adequately trained. This part of the plan is continually reviewed as employees leave the organization, home telephone or cell phone numbers change, or new members are added to the team. The Unit 2 DRP addresses the following:

- Organization of the disaster/recovery team
- Disaster/recovery team headquarters
- Disaster recovery coordinator
- Recovery team leaders and their responsibilities

Disaster Recovery Plan (DRP)

Unit 3: Preparing for a Disaster—A DRP lists the entities that could impact an organization and also the procedures and safeguards that should constantly be in force to reduce the risk of the disaster. Topics for Unit 3 include:

- Physical/security risks
- Environmental risks
- Internal risks
- External risks
- Safeguards

Unit 4: Emergency Procedures—The Emergency Procedures unit answers the question, "What should happen when a disaster occurs?" Unit 4 outlines the step-by-step procedures that should occur, including the following:

- Disaster recovery team formation
- Vendor contact list
- Use of alternate sites
- Offsite storage

Unit 5: Restoration Procedures—After the initial response has put in place the procedures that allow the organization to continue functioning, this unit addresses how to fully recover from the disaster and return to normal business operations. This unit should include:

Disaster Recovery Plan (DRP)

DISASTER EXERCISES

Designed to test DRP's effectiveness

- Test efficiency of interdepartmental planning and coordination in managing a disaster
- Test current DRP procedures
- Determine response strengths and weaknesses

Redundancy and Fault Tolerance

WHY?

- Way to address single point of failure
- Building excess capacity to protect against failures

Redundancy planning to reduce a variable known as the **mean time to recovery (MTTR)**.

Applies to servers, storage, networks, power, sites

- Play a key role in network infrastructure
- Failure can have significant business impact

Some organizations stockpile spare parts for servers or have redundant servers

Server cluster

- Multiple servers that appear as a single server
- Connected through public and private cluster connections

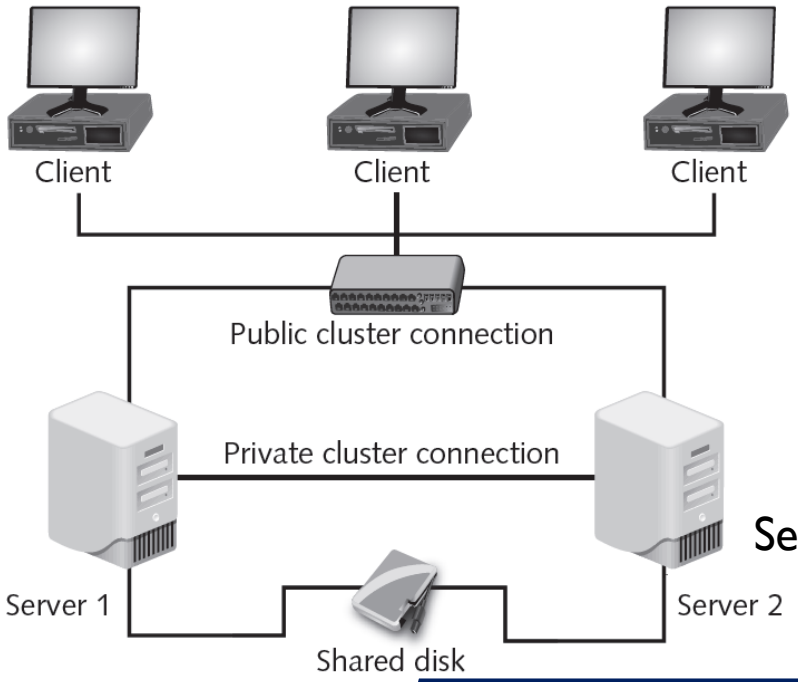
→ Asymmetric

→ Symmetric

Redundancy and Fault Tolerance

Asymmetric servers

- Perform no function except to be ready if needed
- Used for databases, messaging systems, file and print services



Server cluster

Symmetric servers

- 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

Redundancy and Fault Tolerance

STORAGE

- Hard drives
  - –Often 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

Redundancy and Fault Tolerance

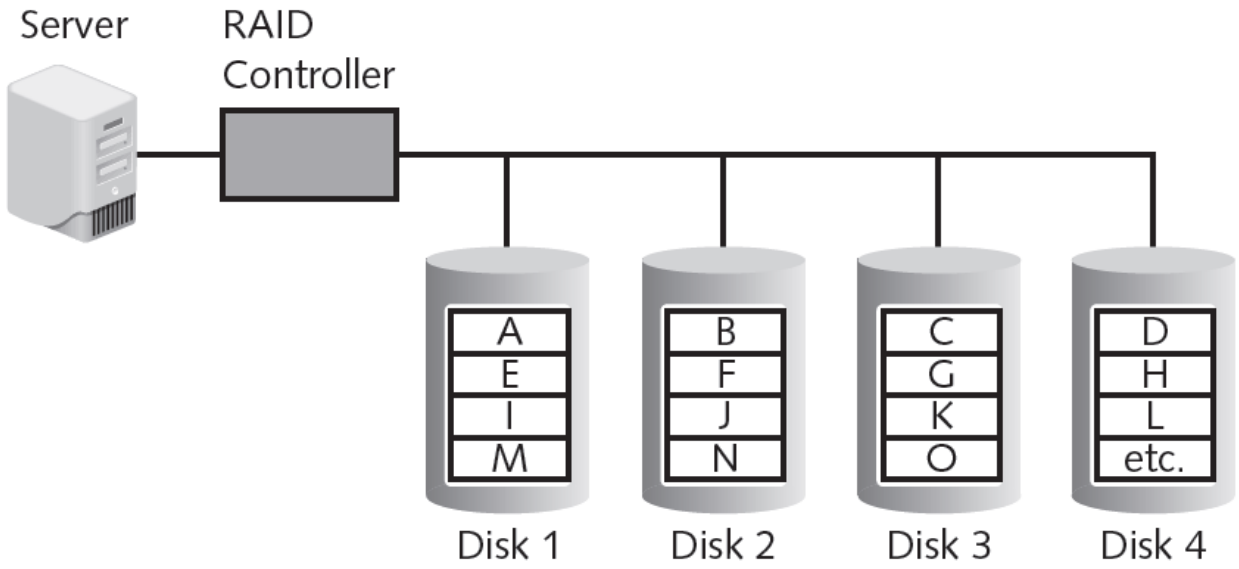
REDUNDANT ARRAY OF INDEPENDENT DEVICES (RAID)

- Uses multiple hard disk drives to increase reliability and performance
- Can be implemented through software or hardware
- Several levels of RAID exist

Redundancy and Fault Tolerance

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

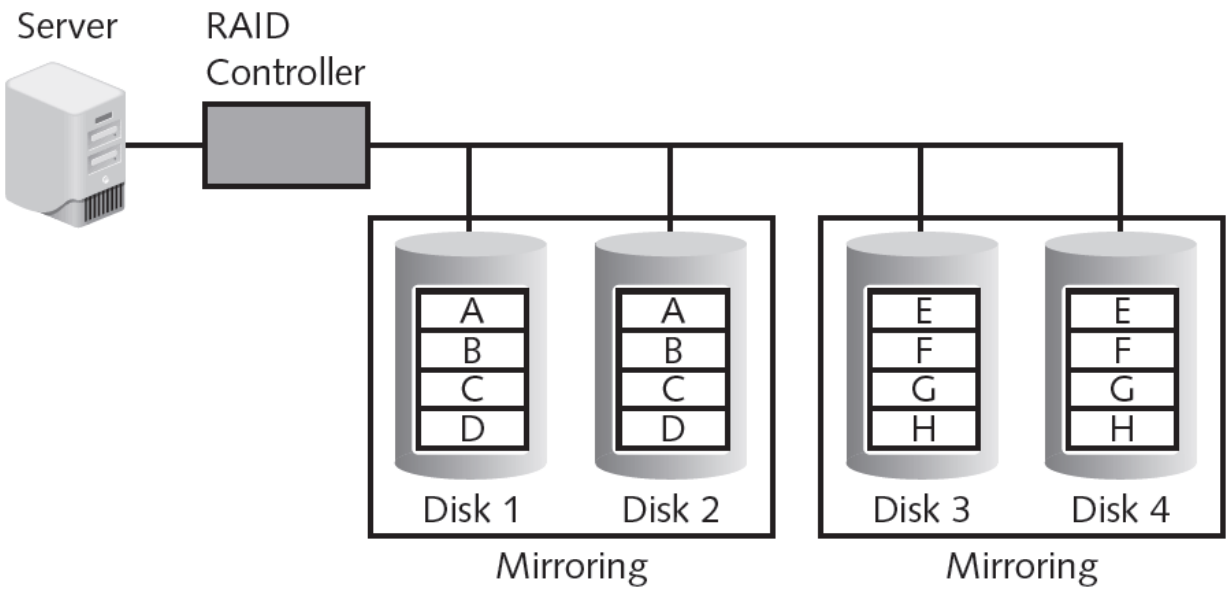


RAID Level 0

Redundancy and Fault Tolerance

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

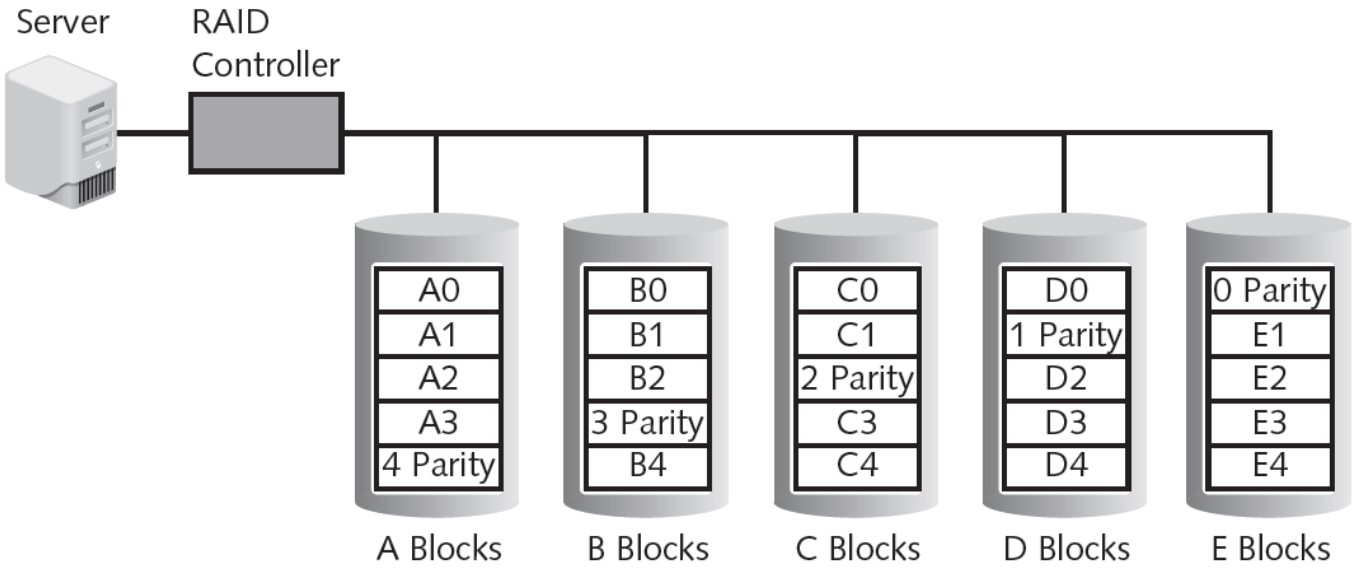


RAID Level 1

Redundancy and Fault Tolerance

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

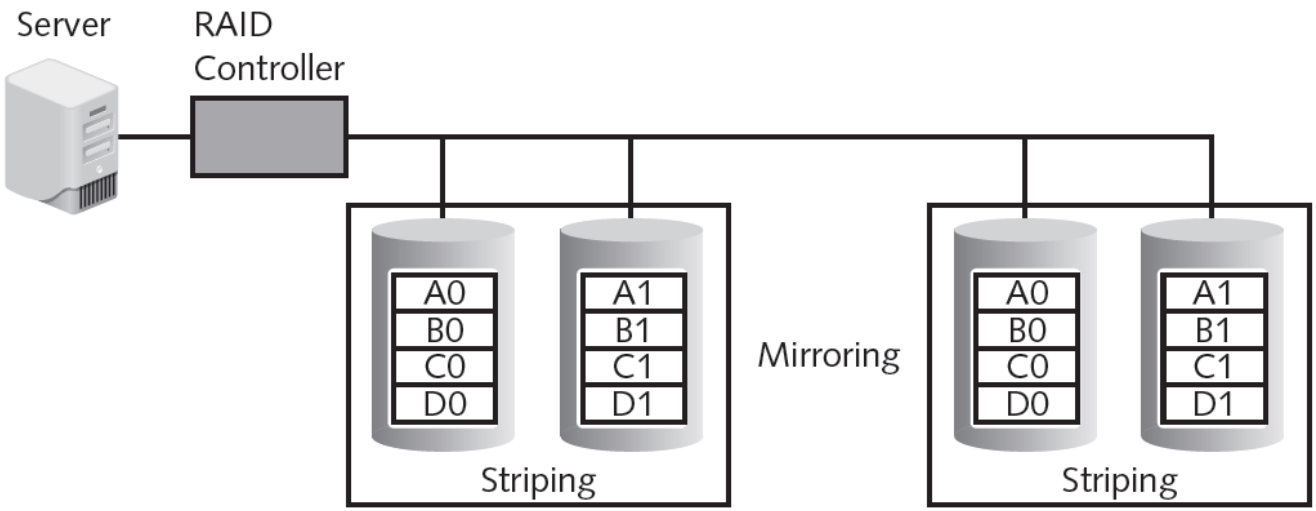


RAID Level 5

Redundancy and Fault Tolerance

Raid level 0 + 1 (high data transfer)

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



RAID Level 0+1

Redundancy and Fault Tolerance

RAID level	Description	Minimum number of drives needed	Typical application	Advantages	Disadvantages
RAID Level 0	Uses a striped disk array so that data is broken down into blocks and each block is written to a separate disk drive	2	Video production and editing	Simple design, easy to implement	Not fault tolerant
RAID Level 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

Redundancy and Fault Tolerance

RAID level	Description	Minimum number of drives needed	Typical application	Advantages	Disadvantages
RAID Level 5	Each entire 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 in the event a disk fails
RAID Level 0+1	A mirrored array whose segments are RAID 0 arrays	4	Imaging applications	High input/ output rates	Expensive

Redundancy and Fault Tolerance

NETWORK

- 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
  - –Launches automatically in the event of a disaster
  - –Hardware components are duplicated
  - –Some organizations contract with a second Internet service provider as a backup

Redundancy and Fault Tolerance

POWER

- Uninterruptible power supply (UPS)
  - –Maintains power to equipment in the event of an interruption in primary electrical power source
- Offline 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

Redundancy and Fault Tolerance

POWER

- Online 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
  - –Can communicate with the network operating system to ensure orderly shutdown occurs
  - –Can only supply power for a limited time
- Backup generator
  - –Powered by diesel, natural gas, or propane

Redundancy and Fault Tolerance

SITES

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

- –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

Redundancy and Fault Tolerance

SITES

- 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
- 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

Data Backups

- Essential element in any DRP
- Copying information to a different medium and storing offsite to be used in event of disaster

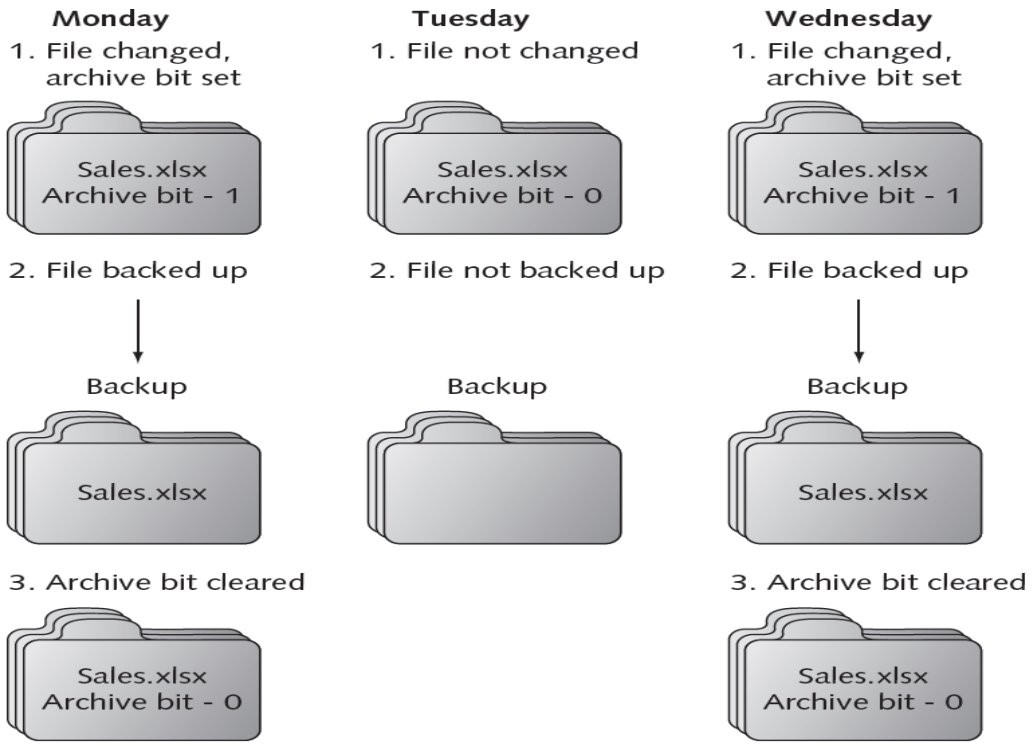
Questions to ask when creating a data backup

- What information should be backed up?
- How often should it be backed up?
- What media should be used?
- Where should the backup be stored?
- What hardware or software should be used?

Data Backups

BACKUP SOFTWARE

- Can internally designate which files have already been backed up
  -Archive bit set to 0 in file properties
- If file contents change, archive bit is changed to 1



Archive bit

Data Backups

BACKUP SOFTWARE

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

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 Backups

MAGNETIC TAPE BACKUP

- Magnetic tape backups have been standard for over 40 years
- Can store up to 800GB of data
- Relatively inexpensive

Disadvantages of magnetic tape backups

–Slow backup speed

–High failure rates

–Data not encrypted on tape

DISK TO DISK

- Large hard drive or RAID configuration
- Better RPO and RTO than magnetic tape
- May be subject to failure or data corruption.

DISK TO DISK TO TAPE

- Uses magnetic disk as a temporary storage area
- Server does not need to be offline for an extended time period
- Data later transferred to magnetic tape

Data Backups

CONTINUOUS DATA PROTECTION

- Performs data backups that can be restored immediately
- Maintains historical record of all changes made to data

Name	Data protected	Comments
Block-level CDP	Entire volumes	All data in volume receives CDP protection, which may not always be necessary
File-level CDP	Individual files	Can select which files to include and exclude
Application-level CDP	Individual application changes	Protects changes to databases, email messages, etc.

Continuous data protection types

Data Backups

Backup technology	RPO	RTO	Cost	Comments
Magnetic tape	Poor	Poor	Low	Good for high-capacity backups
Disk to disk (D2D)	Good	Excellent	Moderate	Hard drive may be subject to failure
Disk to disk to tape (D2D2T)	Good	Excellent	Moderate	Good compromise of tape and D2D
Continuous data protection (CDP)	Excellent	Excellent	High	For organizations that cannot afford any downtime

Data backup technologies

Environmental Controls

Methods to prevent disruption through environmental controls

- Fire suppression
- Proper shielding
- Configuring HVAC systems

Environmental Controls

Fire suppression

Requirements for a fire to occur
–Fuel or combustible material
–Oxygen to sustain combustion
–Heat to raise material to its ignition temperature
–Chemical reaction: fire itself

Class of fire	Type of fire	Combustible materials	Methods to extinguish	Type of fire extinguisher needed
Class A	Common combustibles	Wood, paper, textiles, and other ordinary combustibles	Water, water-based chemical, foam, or multipurpose dry chemical	Class A or Class ABC extinguisher
Class B	Combustible liquids	Flammable liquids, oils, solvents, paint, and grease, for example	Foam, dry chemical, or carbon dioxide to put out the fire by smothering it or cutting off the oxygen	Class BC or Class ABC extinguisher
Class C	Electrical	Live or energized electric wires or equipment	Foam, dry chemical, or carbon dioxide to put out the fire by smothering it or cutting off the oxygen	Class BC or Class ABC extinguisher
Class D	Combustible metals	Magnesium, titanium, and potassium, for example	Dry powder or other special sodium extinguishing agents	Class D extinguisher
Class K	Cooking oils	Vegetable oils, animal oils, or fats in cooking appliances	Special extinguisher converts oils to non-combustible soaps	Wet chemical extinguisher

Fire types

Environmental Controls

Fire suppression

Environmental Controls

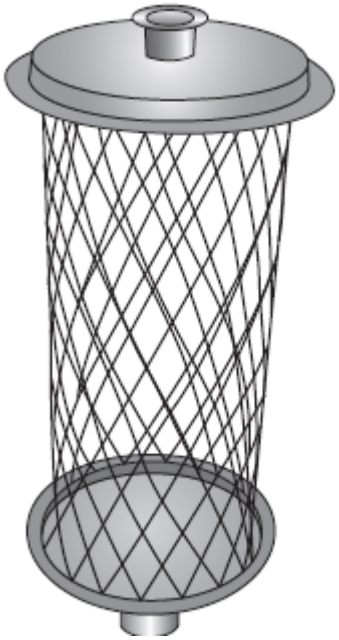
Category	Name	Description	Comments
Water sprinkler system	Wet pipe	Water under pressure used in pipes in the ceiling	Used in buildings with no risk of freezing
	Alternate	Pipes filled with water or compressed air	Can be used when environmental conditions dictate
	Dry pipe	Pipes filled with pressurized water and water is held by control valve	Used when water stored in pipes overhead is a risk
	Pre-action	Like dry pipe but requires a preliminary action such as a smoke detector alarm before water is released into pipes	Used in areas that an accidental activation would be catastrophic, such as in a museum or storage area for rare books
Dry chemical system	Dry chemicals	Dry powder is sprayed onto the fire, inhibiting the chain reaction that causes combustion and putting the fire out	Used frequently in industrial settings and in some kitchens
Clean agent system	Low-pressure carbon dioxide (CO_2) systems	Chilled, liquid CO_2 is stored and becomes a vapor when used that displaces oxygen to suppress the fire	Used in areas of high voltage and electronic areas
	High-pressure carbon dioxide systems	Like the low-pressure CO_2 systems, but used for small and localized applications	Used in areas of high voltage and electronic areas
	FM 200 systems (Heptafluoropropane)	Absorbs the heat energy from the surface of the burning material, which lowers its temperature below the ignition point and extinguishes the fire	One of the least toxic vapor extinguishing agents currently used; can be used in computer rooms, vaults, phone rooms, mechanical rooms, museums, and other areas where people may be present
	Inergen systems	A mix of nitrogen, argon, and carbon dioxide	Used to suppress fires in sensitive areas such as telecommunications rooms, control rooms, and kitchens
	FE-13 systems	Developed initially as a chemical refrigerant, FE-13 works like FM 200 systems	Safer and more desirable if the area being protected has people in it

Stationary fire suppression systems

Environmental Controls

Electromagnetic Interference (EMI) Shielding

- Attackers could pick up electromagnetic fields and read data
- Faraday cage
  - –Metal enclosure that prevents entry or escape of electromagnetic fields
  - –Often used for testing in electronic labs



Faraday cage

Environmental Controls

Heating, Ventilating and Air Conditioning (HVAC) System

- Maintain temperature and relative humidity at required levels
- Controlling environmental factors can reduce electrostatic discharge (ESD)

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

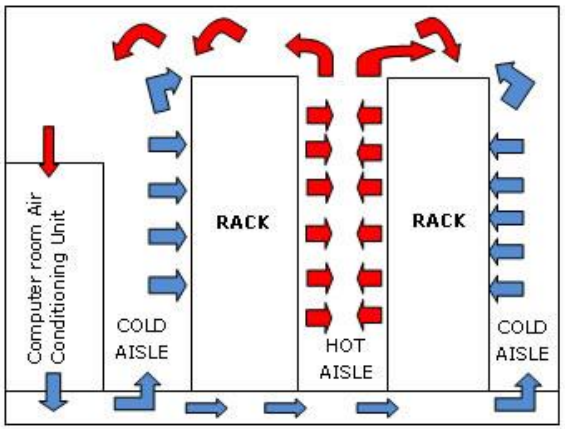


Figure A

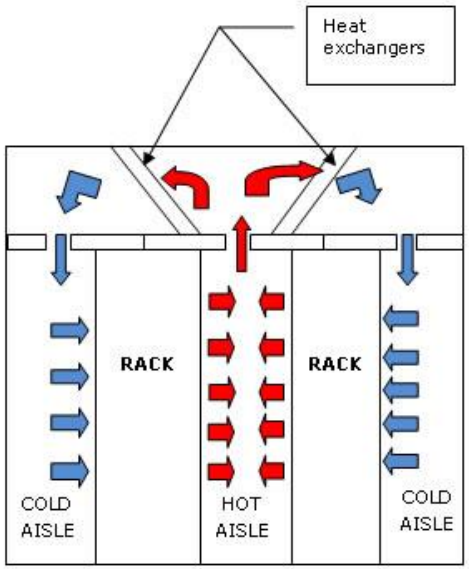
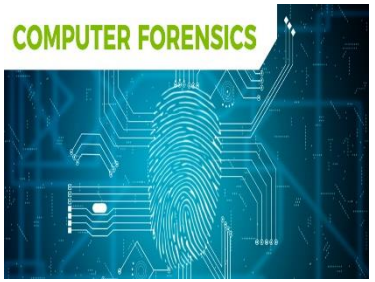


Figure B

Incident Response Procedures

- When unauthorized incident occurs:
  - –Response is required
- Incident response procedures
  - –Can include using basic forensics procedures



- Applying science to legal questions
  - –Analyzing evidence
- Computer forensics
  - –Uses technology to search for computer evidence of a crime
- Reasons for importance of computer forensics
  - –Amount of digital evidence
  - –Increased scrutiny by the legal profession
  - –Higher level of computer skill by criminals

Forensics

Basic Forensics Procedures

Four basic steps are followed
–Secure the crime scene
–Collect the evidence
–Establish a chain of custody
–Examine for evidence

- Secure the crime scene
  - –Goal: preserve the evidence
  - –Damage control steps taken to minimize loss of evidence
  - –First responders contacted
  - –Physical surroundings documented
  - –Photographs taken before anything is touched
  - –Computer cables labeled
  - –Team takes custody of entire computer
  - –Team interviews witnesses

Forensics: Basic Procedures

- Preserve the evidence
  - –Digital evidence is very fragile (Can be easily altered or destroyed)
  - -Computer forensics team captures volatile data
    - •Examples: contents of RAM, current network connections

- Order of volatility must be followed to preserve most fragile data first

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

Order of volatility

Forensics: Basic Procedures

- Establish the chain of custody
  - –Evidence maintained under strict control at all times
  - –No unauthorized person given opportunity to corrupt the evidence
- Examine for evidence
  - –Computer forensics expert searches documents
  - –Windows page files can provide valuable investigative leads
  - –Slack and metadata are additional sources of hidden data

Summary

- Business continuity is an organization's ability to maintain its operations after a disruptive event
- Disaster recovery
  - –A subset of business continuity planning
  - –Focuses on restoring information technology functions
  - –Disaster recovery plan 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
- 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