
Chapter 13
Business Continuity
Objectives

• Define business continuity
• Describe the components of redundancy planning
• List disaster recovery procedures
Business Continuity

• Business continuity is the process of assessing risks and developing a management strategy to ensure that the organization business can continue if case of a disruptive event (electrical outage or as catastrophic as a hurricane).

• Business continuity management is concerned with developing a **business continuity plan** addressing how the organization can continue in the event that risks materialize.

• Business continuity is a critical element for all organizations
  – However it remains sadly lacking.
  – Many organizations are either unprepared or have not tested their plans.
Redundancy Planning

• One of the primary ways to ensure business continuity is to use redundancy planning
  – Which involves building excess capacity in order to protect against failures
• Redundancy planning can involve redundancy for servers, storage, networks, power, and even sites
Servers

• A crash of a single server that supports a critical application can have a significant impact

• **Single point of failure**
  – The loss of one entity would adversely affect the organization

• One common approach is for the organization to design the network infrastructure
  – So that multiple servers are incorporated into the network yet appear to users and applications as a single computing resource
Servers (continued)

- **Server cluster**
  - The combination of two or more servers that are interconnected to appear as one

- There are two types of server clusters:
  - **Asymmetric server cluster**
    - A standby server exists only to take over for another server in the event of its failure
  - **Symmetric server cluster**
    - Every server in the cluster performs useful work
Servers (continued)

Figure 13-3  Server cluster
Storage

- **Mean time between failures (MTBF)**
  - Refers to the average (mean) time until a component fails, cannot be repaired, and must be replaced
  - Calculating the MTBF involves taking the total time measured divided by the total number of failures observed

- **Fault tolerance**
  - The ability to endure failures
  - Prevents a single problem from escalating into a major failure
  - Can often be achieved by maintaining redundancy
Storage (continued)

• A system of hard drives based on redundancy can be achieved through using a technology known as RAID.

• RAID (Redundant Array of Independent Drives)
  – Uses multiple hard disk drives for increased reliability and performance.

**RAID, is a technology that provides increased storage functions and reliability through redundancy. This is achieved by combining multiple disk drive components into a logical unit, where data is distributed across the drives in one of several ways called “RAID levels”.**
Networks

• **Redundant network**
  – “Waits” in the background during normal operations
  – Uses a replication scheme to keep its copy of the live network information current

• Virtually all network components can be duplicated to provide a redundant network

• In addition, some organizations contract with more than one Internet Service Provider (ISP) for remote connectivity
Power

• Uninterruptible power supply (UPS)
  – A device that maintains power to equipment in the event of an interruption in the primary electrical power source

• Two primary types of UPS
  – Off-line UPS
  – On-line UPS

• UPS systems can also communicate with the network operating system on a server
  – To ensure that an orderly shutdown occurs
Power (continued)

• A UPS can complete the following tasks:
  – Send a message to the network administrator’s computer, or page or telephone the network manager to indicate that the power has failed
  – Notify all users that they must finish their work immediately and log off
  – Prevent any new users from logging on
  – Disconnect users and shut down the server

• Because a UPS can only supply power for a limited amount of time, some organizations turn to using a backup generator to create power
Sites

• Redundancy can also be planned for the entire site itself

• **Hot site**
  – Generally run by a commercial disaster recovery service
  – Allows a business to continue computer and network operations to maintain business continuity

• **Cold site**
  – Provides office space but the customer must provide and install all the equipment needed to continue operations
Sites (continued)

• Warm site
  – Has all of the equipment installed but does not have active Internet or telecommunications facilities, and does not have current backups of data
Disaster Recovery Procedures

• **Disaster recovery**
  – Procedures and processes for restoring an organization’s IT operations following a disaster
  – Focuses on restoring computing and technology resources to their former state

• **Disaster recovery procedures** include planning, disaster exercises, and performing data backups
Planning

- **Disaster recovery plan (DRP)**
  - A written document that details the process for restoring IT resources
    - Following an event that causes a significant disruption in service
  - Comprehensive in its scope, a DRP is intended to be a detailed document that is updated regularly
- All disaster recovery plans are different
### Planning (continued)

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Description</th>
<th>Impact Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Central computing resources</td>
<td>The Computer Services building and central computer room which houses the campus servers and routers, and serves as the primary hub for campus electronic and voice communications and connectivity</td>
</tr>
<tr>
<td>Level 2</td>
<td>Campus network infrastructure and the telephone public exchange</td>
<td>Central telephone services, 911 emergency services, network infrastructure and services, and cable plant</td>
</tr>
<tr>
<td>Level 3</td>
<td>Risks specific to unique applications or functionality</td>
<td>File and print services, student records, e-mail, Web, student residential network, technology enhanced classroom support, and student computer labs</td>
</tr>
</tbody>
</table>

**Table 13-5**  Sample educational DRP approach
Planning (continued)

- Most disaster recovery plans address the common features included in the following typical outline:
  - Unit 1: Purpose and Scope
  - Unit 2: Recovery Team
  - Unit 3: Preparing for a Disaster
  - Unit 4: Emergency Procedures
  - Unit 5: Restoration Procedures

- It is important that a good DRP contains sufficient detail
COMMUNICATIONS ROOM

The purpose of a communications room is to provide a central point of contact and coordination. This telephone equipment in this room will include:

- Three wired telephones
- Four full-charged cellular telephones
- One satellite telephone

Media communications in this room will include:

- One television
- One standard radio
- One police radio
- One citizens band radio
- One DVD player/recorder

This room should be isolated from other functional areas and only authorized personnel will be allowed to enter.

**Figure 13-8** Sample excerpt from a DRP
Disaster Exercises

- Disaster exercises are designed to test the effectiveness of the DRP
- Objectives of these disaster exercises:
  - Test the efficiency of interdepartmental planning and coordination in managing a disaster
  - Test current procedures of the DRP
  - Determine the strengths and weaknesses in responses
Data Backups

• Data backup
  – Information copied to a different medium and stored at an offsite location so that it can be used in the event of a disaster

• Five basic questions that should be answered:
  – 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 (continued)

- Backup software can internally designate which files have already been backed up
  - By setting an archive bit in the properties of the file
- Backing up to magnetic tape has been the mainstay of data backups for over 30 years
- **Grandfather-father-son backup system**
  - Divides backups into three sets: a daily backup (son), a weekly backup (father), and a monthly backup (grandfather)
Monday
1. File changed, archive bit set
   Sales.xlsx
   Archive bit - 1
2. File backed up
   Tape backup
3. Archive bit cleared
   Sales.xlsx
   Archive bit - 0

Tuesday
1. File not changed
   Sales.xlsx
   Archive bit - 0
2. File not backed up
   Tape backup
3. Archive bit cleared
   Sales.xlsx
   Archive bit - 0

Wednesday
1. File changed, archive bit set
   Sales.xlsx
   Archive bit - 1
2. File backed up
   Tape backup
3. Archive bit cleared
   Sales.xlsx
   Archive bit - 0

Figure 13-9 Archive bit
## Data Backups (continued)

<table>
<thead>
<tr>
<th>Type of Backup</th>
<th>Description</th>
<th>How Used</th>
<th>Archive Bit After Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup</td>
<td>Copies all files</td>
<td>Part of regular backup schedule</td>
<td>Cleared</td>
</tr>
<tr>
<td>Differential backup</td>
<td>Copies all files since last full backup</td>
<td>Part of regular backup schedule</td>
<td>Not cleared</td>
</tr>
<tr>
<td>Incremental backup</td>
<td>Copies all files changed since last full or incremental backup</td>
<td>Part of regular backup schedule</td>
<td>Cleared</td>
</tr>
<tr>
<td>Copy backup</td>
<td>Copies selected files</td>
<td>Copies files to a new location</td>
<td>Not cleared</td>
</tr>
</tbody>
</table>

*Table 13-6  Types of data backups*
<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>31</td>
<td>1 Jun</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Son</td>
<td>Son</td>
<td>Son</td>
<td>Father</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Son</td>
<td>Son</td>
<td>Son</td>
<td>Father</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Son</td>
<td>Son</td>
<td>Son</td>
<td>Father</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Son</td>
<td>Son</td>
<td>Son</td>
<td>Father</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td>1 Jul</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Son</td>
<td>Son</td>
<td>Grandfather</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 13-10**  Grandfather-father-son backup system
Data Backups (continued)

• **Recovery point objective (RPO)**
  – The maximum length of time that an organization can tolerate between backups

• **Recovery time objective (RTO)**
  – The length of time it will take to recover the data that has been backed up

• An alternative to using magnetic tape is to back up to magnetic disk
  – Such as a large hard drive or RAID configuration
  – This is known as **disk to disk (D2D)**
Data Backups (continued)

• D2D offers better RPO than tape
  – However, as with any hard drive, the D2D drive may be subject to failure or data corruption
• Disk to disk to tape (D2D2T)
  – Combines the best of magnetic tape and magnetic disk
  – Uses the magnetic disk as a temporary storage area
• Continuous data protection (CDP)
  – Performs continuous data backups that can be restored immediately
Data Backups (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Protected</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block-Level CDP</td>
<td>Entire volumes</td>
<td>All data in volume receives CDP protection, which may not always be necessary</td>
</tr>
<tr>
<td>File-Level CDP</td>
<td>Individual files</td>
<td>Can select which files to include and exclude</td>
</tr>
<tr>
<td>Application-Level CDP</td>
<td>Individual application changes</td>
<td>Protects changes to databases, e-mail messages, etc.</td>
</tr>
</tbody>
</table>

*Table 13-7*  Continuous data protection types
## Data Backups (continued)

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

*Table 13-8  Data backup technologies*
Summary

• One method for ensuring business continuity is to use redundancy planning
• Power redundancy can be attained by using an uninterruptible power supply (UPS)
• Disaster recovery is defined as the procedures and processes for restoring an organization’s IT operations following a disaster
Resources