Disaster Avoidance: A Key to Business Continuity

- Keeping the Doors of Business Open
Disaster Avoidance: A Key to Business Continuity

- Natural Disasters

In 1992, Hurricane Andrew completely leveled thousands of South Florida businesses.

The storm caused nearly $25 billion in damages. This summer, the National Oceanic and Atmospheric Administration predicts one of the most active and intense hurricane seasons in history.
Disaster Avoidance: A Key to Business Continuity

- Unnatural Disasters

In 2002, Hurricane Arthur completely demolished one South Florida business.

Arthur in purchasing picked up some "discounted" servers and lost your corporate data. All your corporate data.

Guess what?
42% of corporate data loss is caused by hardware malfunctions.
Disaster Avoidance: A Key to Business Continuity

- Unnatural Disasters

In 2002, Hurricane Sally cut a swath through one South Florida company that's still being felt today.

Sally, your office manager trashed some "extra" files. Unfortunately, Sally's definition of "extra" is your definition of "accounting."

Guess What?
30% of corporate data loss is caused by human error
Disaster Avoidance: A Key to Business Continuity

- Unnatural Disasters

In 2002, Hurricane Kyle thoroughly thrashed one South Florida corporation, before heading north and fading away somewhere near Long Island.

Kyle, in network administration, installed faulty data storage software (along with a password only he knew). Today he's no longer with your company. Unfortunately, neither is your data.

Guess What?
13% of corporate data loss is caused by software failure.
Loss of Email

- The average user sends 34 emails a day.
- The average user receives 99 emails every day.
- You have a 75% chance of losing email at least once this year.
- Another 14% will likely experience a major planned outage due to system or hardware upgrade or maintenance.
Loss of Email: Economic Impact

- A 5,000 person health care provider lost $3M during an 8 hour outage due to loss of power.
- A 2,000 person national law firm CIO estimates that a recent email outage cost the firm $100K per hour in lost revenue and productivity.
- Last year five financial services firms were fined a total of $8.25M for failure to protect and preserve email communications.
- A national financial services firm lost $6M from a virus-related email outage.
Protection of Passwords

May 4, 2008 – Nearly 67% of 272 people surveyed in downtown San Francisco gave their computer password to a complete stranger in exchange for a free cup of coffee. This study conducted by VeriSign showed that 70% of people who would not give up their password gave significant clues about their password such as spouse’s name, anniversary date, etc.
Top 5 Causes of Disasters

Based on a survey of 582 disaster events by Disaster Recovery Journal.

• Power Outage 15.6%
• Hardware Error 13.2%
• Fire 10.8%
• Flood 10.0%
• Earthquake 9.1%
Top Causes of Disasters

Analysis of Disaster Causes

- Power Outage: 15.6%
- Hardware Error: 13.2%
- Flood: 10.8%
- Earthquake: 9.1%
- Hurricane: 9.0%
- Software Error: 7.6%
- Bombing: 6.7%
- Water (Flood): 6.5%
- Network Failure: 3.9%
- Contamination: 1.8%
- HVAC Failure: 1.2%
- Forced Evacuation: 1.2%
- Hardware Error: 1.2%
- Burst Pipe: 1.4%
- Fire: 0.9%
- DR Test Failure: 0.5%
- Riot: 0.6%
- Delayed Relocation: 0.6%

Other causes include Power Outage, Hardware Error, Flood, Earthquake, Hurricane, Software Error, Bombing, Water (Flood), Network Failure, Contamination, HVAC Failure, Forced Evacuation, Hardware Error, Burst Pipe, Fire, DR Test Failure, and Riot.
5 Levels of Disaster Avoidance

- Tape Backup
- Offsite Data Storage
- Cold Sites
- Hot Sites
- Active Load Balancing
Disaster Recovery

- How long would it take you to recovery from a disaster or other unplanned event?
Proactive Preparation and Protection

Average Disaster Recovery Time

- 0 - 24 Hours: 20%
- 25 - 48 Hours: 17%
- 49 - 72 Hours: 11%
- 73 - 120 Hours: 15%
- 121 - 264 Hours: 6%
- 265 - 336 Hours: 9%
- 337 - 720 Hours: 12%
- 721+ Hours: 10%
Level 1 Preparation: Tape Back-up

Answer the following questions to determine your level of preparedness:

• How often do you do a complete vs. incremental back-up?
• Are you backing-up workstations along with servers?
• What will you do if your tape drive fails?
• What will you do if your host or server fails?
• How often do you rotate your tapes?
• How often do you do a sample restore to test the data?
• How often do you replace your media?
• Where do you store your tapes?
Level 2 Preparation: Off-Site Storage

Answer the following questions to determine your level of preparedness:

- How often do you ship tapes off-site?
- How quickly could you retrieve these tapes?
- Have you inspected the location where they are kept?
- Is your media in an environmentally controlled facility?
- What will you do if your tape drive fails?
Level 2 Preparation: Off-Site Storage

- A new industry is forming – off-site data storage onto remote servers & hard drives
- Backup your servers and your workstations
Level 3 Preparation: Cold Sites

- Cold sites are empty, environmentally controlled computer rooms available on a subscription basis.
- Usually contracted for a period of 1 – 5 years.
- Equipment is not provided as part of the service.
- Major players: SunGard, Comdisco and IBM.
- Target customers:
  - Traditional raised floor, legacy data customers.
  - Insurance companies often contract for cold sites.
  - Call centers are beginning to contract for cold sites.
Level 3 Preparation: Cold Sites

Answer the following questions to determine your level of preparedness:

- How many subscribers does your cold site contract?
- How many simultaneous customers will the site support?
- Do you have a plan to relocate the equipment?
- Do you have a vendor on call to replace the equipment?
- How quickly could you replace your equipment?
- Are your employees fully briefed on cold site procedures?
- Do you have a disaster recovery plan?
- Have you tested your DR plan?
Level 4 Preparation: Hot Sites

- Hot sites are operational ready data centers offering specific hardware platforms for immediate availability
- Usually contracted for a period of 4 or more years
- Costs are based on the equipment provided
- Most hot sites limit the disaster mode use to eight weeks
- Target customers:
  - Traditional raised floor, legacy data customers
  - Financial companies often require hot sites.
Level 4 Preparation: Hot Sites

Answer the following questions to determine your level of preparedness:

- How many subscribers does your hot site contract?
- How many simultaneous customers will the site support?
- Do you have a plan to relocate your operations?
- Do you have a plan to notify your customers?
- Are your employees fully briefed on hot site procedures?
- Do you have a DR plan?
- Have you tested your DR plan?
Level 5 Preparation: Active Load Balancing

- Technology today supports multiple active data centers.
- The data is load balanced between 2 or more data centers.
- The Internet is used as an alternative transport medium.
- Provides a business model offering up to 100% up-time.
- The Internet is used to provide access to:
  - Diversely located employees
  - Customers
  - Vendors
  - Business partners
Level 5 Preparation: Active Load Balancing

Answer the following questions to determine your level of preparedness:

- Can your business afford down time?
- How much money does your business lose per hour of downtime?
- Will your operations sustain the loss of a data center?
- Are your data centers in diverse climates and locations?
- Does 100% up-time increase customer satisfaction?
- What is your competition doing for disaster recovery?
- Have you tested your DR plan?
Disaster Recovery & the Internet

Can the Internet be used as a Disaster Recovery tool?
### Internet as a Content Delivery Tool

Average U.S. Internet Usage, Combined Home & Work, Month of November 2009

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Nov-09</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions/Visits per Person</td>
<td>51</td>
</tr>
<tr>
<td>Domains Visited per Person</td>
<td>86</td>
</tr>
<tr>
<td>Web Pages per Person</td>
<td>2,603</td>
</tr>
<tr>
<td>PC Time per Person</td>
<td>66:28:44</td>
</tr>
<tr>
<td>Duration of a Web Page Viewed</td>
<td>0:00:57</td>
</tr>
<tr>
<td>Active Digital Media Universe</td>
<td>195,149,922</td>
</tr>
<tr>
<td>Current Digital Media Universe Estimate</td>
<td>234,372,000</td>
</tr>
</tbody>
</table>

Source: The Nielsen Company
Top 10 Reasons DR Plans Fail

10. DR is just too expensive!
   “We simply can’t afford to test DR.”
   Integrate DR into standard operations where possible.
   Make an informed decision: spend money or accept risk
   How long can you operate in DR mode?
   What is your return to normalcy plan?
   Do you have a DR plan for your DR site?
Top 10 Reasons DR Plans Fail

9. Who will be there to recover?
   - Tough topic to consider, but look at New Orleans.
   - Redundancy in roles: Each team member understands key responsibilities
   - Need comprehensive documentation/training
   - What is the access to the DR plan?
   - How will you communicate during recovery?
Top 10 Reasons DR Plans Fail

8. Your backups don’t work!
- Tape is still the #1 recovery method.
- Will you have access to a compatible tape drive during recovery?
- Poor tape management: rotate media
- Failures of nightly backup
- Monitor / manage your backups
Top 10 Reasons DR Plans Fail

- 7. Your DR plan doesn’t address the right risks
- What constitutes a disaster?
  - 36 FEMA declared “Major Disasters” in 2005 (as of 10/10/05)
  - 67 FEMA declared “Emergency Declarations”
  - 29 FEMA declared “Fire Management Assistance Declarations”
- How much insurance do you need?
- Rank risks against business impact
- Weigh event probability vs. cost vs. impact
  - Risk = Probability
Top 10 Reasons DR Plans Fail

6. You lack clearly defined DR roles
- Coordination is critical (chaos is a given)
- Identify the processes and workflows needed
- Identify the teams involved
- Understand points of intersection and handoff
Top 10 Reasons DR Plans Fail

5. Your recovery goals can’t be achieved

- Set realistic objectives
  - Recovery time objectives need to be established
  - When does the clock start?
  - Set recovery point objectives as well

- Can your infrastructure support your goals?
  - Limits of tape-based recovery
  - Cost vs. objectives
  - Technology requirements / limitations
  - DR site considerations

- Technology options
Top 10 Reasons DR Plans Fail

4. You don’t do DR tests
   Or… you don’t test the right things
   End-to-end testing to production
   Server centric vs. application centric
     • Address application interdependencies
   Site considerations
     • Hot vs. warm vs. cold
   Finding & fixing bugs is a GOOD thing
Top 10 Reasons DR Plans Fail

3. Your DR plan is not up to date

DR planning lifecycle
- Should be a part of all other life cycle planning

Continuous process
- DR maintenance should be an integral part of change management
- Areas most overlooked in change management:
  - Backups
  - DR
Top 10 Reasons DR Plans Fail

2. You don’t really have a DR plan

- Elements of a DR plan
  - How will employees communicate?
  - Where will employees go?
  - How will employees keep doing their job?

- Detail actions BEFORE, DURING & AFTER

- Detailed system and device recovery

- Assign owners & key contacts for each activity

- Sequence the events
  - Identify dependencies
  - Prioritize recovery
Top 10 Reasons DR Plans Fail

1. Business and IT are not in sync

Who sets DR policy?
- 71% of companies only involve IT staff in DR strategy

Business continuity vs. disaster recovery
- 38% of companies integrate a BC/DR plan

The challenge of alignment
- Understand actual business requirements
- Set and meet realistic expectations
- Ability to meet critical needs
Take a ways

At the conclusion of this seminar you should:

• Be able to articulate the basics of disaster preparedness and business continuity plan.
• Understand the importance of aligning business goals and technical capabilities
• Prepare the outline for DRP/BCP discussion.
• after this disaster recovery presentation, you should be able to understand the critical components of any IT disaster recovery plan that are essential in preventing data loss that can impair a business’s ability to operate