



Business continuity plans should be multi-layered and expandable

November 7, 2005

Takeaway:

A business continuity plan may start with a backup solution, but it doesn't end there. And the more your company grows, the more important it becomes to develop a comprehensive continuity strategy that can scale to keep up with your growing need to have important data and resources available at all times.

You spent big bucks on a backup solution -- tape, disk-based or hybrid -- so you figure you're covered if disaster strikes. Your data is safe. But is it really? And does it even matter, if your employees, partners, and customers don't have a way to easily access that data after a hardware meltdown or a natural disaster? A good backup solution is an important part of an effective business continuity plan, but it's only one component.

As your company grows, it becomes more and more important to have a comprehensive strategy in place that will allow you to continue operations as normally as possible whether you lose a single hard disk, a server, or an entire building housing your network infrastructure. That's why your business continuity plan needs to be multi-layered and able to expand in scope as your company grows.

Components of a multi-layered business continuity plan

There are several important issues to address when mapping out your business continuity plan, including:

- Data backup
- Hardware redundancy

- Software failover
- Continuity of network connectivity
- The human factor

Data backup

You can think of data backup as the core component of your plan. After all, hardware can be replaced, operating systems and applications can be reinstalled, and new network connections can be established -- eventually. On the other hand, data collected or created by your users may be unique and difficult or impossible to recreate exactly.

A good data backup solution depends on the amount of data generated and how often it changes. Daily backups may suffice for small companies, whereas larger companies that produce a high volume of data may need to back up data several times per day, or on a continuous basis. Tape or disk, or a combination of the two, can be used for backup.

Another option is a backup service, such as [Acme Data, LLC](#), that allows you to back up your data to a remote location across the Internet. Off-site backup is a crucial part of any backup strategy that has business continuity in mind, since backup tapes or disks stored on-site can be destroyed along with the original data if a flood, fire, tornado, or other natural disaster occurs. On the other hand, data stored in a remote location may be difficult to access and restore if you lose your Internet connection. Thus, we recommend a combination of on-site and off-site backup.

An alternative for off-site backup storage is to physically move a copy of each day's backup to another location. In a small company, this may mean the owner or IT manager takes the backup disk home with him/her every night. In a larger company or one with high security concerns, the backup tapes may be transported via armored car to a vault.

Hardware redundancy

If a server goes down, you can lose money and productivity if you have to wait for a new machine or component to be purchased and configured. As the company (and IT budget) grows, you should plan to purchase critical servers in pairs and configure them identically at initial setup. You can then either keep the "spare" in reserve in case of failure, or implement server

clustering with failover so that when one of the pair goes down, the other automatically takes over for it without virtually no downtime.

Software continuity

Server clustering allows you to create a "mirrored" server that has the same software as the primary server, and either mirrors the data or shares a connection to the data storage array.

If you run Windows 2000 Advanced or Datacenter Server or Windows Server 2003 Enterprise or Datacenter edition, you can use Windows' built-in clustering services. However, in Windows Clustering, the cluster members (nodes) must be located near one another because they use SCSI connections to storage resources. For best protection, members of a server cluster can be located in different physical locations. Solutions from vendors such as Veritas and NSI allow mirroring of cluster servers to remote sites.

Your business continuity plan should also take into account availability of client software for accessing resources. The larger your company, the more workstations will be involved. One way to ensure that clients will have the proper software to do their jobs, even if they have to work from different machines in a different location, is to use an Application Service Provider (ASP) or have users run applications on a terminal server rather than installing the application software on individual client machines.

Network connectivity availability

Access to data and software may not be all that employees need to get their work done. More and more, an Internet connection is necessary to perform necessary tasks. And of course, if you run e-commerce sites your sales will depend on the availability of an Internet connection.

You can ensure continued Internet connectivity by purchasing two or more Internet connections. Software solutions such as Rainfinity's [RainConnect](#) and hardware solutions such as Xincom's [Twin WAN](#) series can be used to provide failover when one connection fails. As a bonus, many of these products also aggregate the bandwidth of your multiple Internet connections, giving you a bigger "pipe" when both connections are up and running. As the company grows, you can add more and faster connections. For example, a small company may aggregate two DSL lines or a DSL line and a cable connection. Larger companies can often use the same consolidation/failover product to aggregate multiple T-1 or T-3 lines.

Firewalls, routers and other internal network components can also be purchased with failover capabilities.

The human factor

Don't forget the human factor in putting together your plan. In case of a true disaster, some of your personnel may be temporarily or permanently out of commission. If the network administrator is the only one who knows the passwords that are necessary to get a critical server back up and running, time (and business) can be lost. Responsible password management can make emergency personnel transitions smoother.

Important passwords can be stored in a safe off site, to which a trusted party (also off site) has access. Cross training of IT personnel ensures that you don't run into a situation, for example, in which Joe is the only person who knows how to boot the Exchange server.

As the company grows, these practices should become more formalized and administrative responsibilities should be shared and delegated to avoid focusing all control in the hands of one person.

White Papers

[Enabling Effective Decision Making](#)

[Gartner Report--Dynamic Volume Expansion: Not All Arrays Are Created](#)

[Equal](#)

[Real-Time Business Intelligence and Data Integration as a Strategic and Critical Component](#)

[Gartner Update--CIO Update: Server Consolidation Offers Range of Benefits](#)

[Enabling Operational Business Intelligence With Real-Time Data Integration Solutions](#)

Additional Resources

[Tech Toolshed](http://www.techtoolshed.com)

<http://www.techtoolshed.com>

[Learning CD-Roms](http://fasttrack.techrepublic.com)

<http://fasttrack.techrepublic.com>

[Quick Reference Charts](http://quickref.techrepublic.com)

<http://quickref.techrepublic.com>

[TechRepublic's Catalog](http://www.techrepublic.com/catalog)

<http://www.techrepublic.com/catalog>

[Copyright](#) ©1995- 2003 CNET Networks, Inc. All Rights Reserved.

Visit us at www.TechRepublic.com