IN THIS ISSUE:
~ Disaster Recovery

COMING NEXT MONTH:
~ Storage - Drives

ReadyNetGo .... News

November 2003 **http://www.readynetgo.net** **610-856-0990**

TIP OF THE MONTH

The Windows Key

Most keyboards made in the last several years come with a Windows key, and sometimes also with an Application key. Try these keyboard shortcuts for extra speed and productivity.

Display the Start menu: *Windows*

Open the Run dialog box: *Windows-R*

Minimize all: *Windows-M*

Undo minimize all, tile horizontally, tile vertically, or cascade: *Shift-Windows-M*

Open Help: *Windows-F1*

Open Windows Explorer: *Windows-E*

Open Find/Search Files or Folders: *Windows-F*

Minimize all and undo minimize all: *Windows-D*

Open Find/Search Computer: *Ctrl-Windows-F*

Open System Properties sheet: *Windows-Break*

Prepare for Disaster Before It Happens

There is no way to plan for all of the bad things that could happen in the world. It is better to be prepared. After all, how much downtime can your business afford? Two months ago brought us the second anniversary of 9/11, a massive blackout across the US and Canada and Hurricane Isabel. We felt it would be a good time to discuss Disaster Recovery Plans.

Disaster Recovery is salvaging data stored on damaged media, such as magnetic disks and tapes. There are a number of software products that can help recover data damaged by a disk crash or virus. In addition, there are companies that specialize in data recovery. Of course, not all data is recoverable, but data recovery specialists can often restore a surprisingly high percentage of the data on damaged media.

The primary objective of a Disaster Recovery Plan is to enable an organization to survive a disaster and to reestablish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame.

There are four critical components of a successful Disaster Recovery Plan:

1) **FAULT TOLERANCE** – *The ability of a system to respond gracefully to an unexpected hardware or software failure*.

There are many levels of fault tolerance, the lowest being the ability to continue operation in the event of a power failure. Many fault-tolerant computer system mirror all operations - that is, every operation is performed on two or more duplicate systems, so if one fails the other can take over.

2) **BACKUP** - *To copy to a second medium (a disk or tape) as a precaution in case the first medium fails*.

A backup is the only foolproof means to prevent data loss from viruses, human error, or catastrophes. In addition, it is the most cost effective means to store your mission critical data off site or in multiple locations. A backup plan requires a media rotation scheme and a reliable backup software application. No matter how reliable the system, data cannot be restored that has

been deleted, overwritten or corrupted. One of the cardinal rules in using computers is to back up your files regularly and test your backups to ensure that they will be accessible in case disaster strikes.

Even the most reliable computer is apt to break down eventually. Many professionals recommend that you make two, or even three, backups of all your files. To be especially safe, you should keep one backup in a different location from the others.

Ensure that network hardware configurations and network server backups are performed as a routine part of operations and that these backups are stored in an organized fashion off-site.

3) **INVENTORY** - An important component to any recovery plan is an equipment inventory. At a minimum this should include:

- a listing of all equipment by type and model number;
- associated software packages, with version number and License Keys;
- date of purchase; and
- original cost

The original software media (or a copy) should be kept off-site along with license information. Only one copy of the software is needed off-site as long as a copy of each license is off-site as well.

4) **A DOCUMENTED RECOVERY PLAN** - Maintain a detailed Recovery Plan with specific written procedures that have been tested.

Disaster recovery planning is not a two-month project, neither is it a project that once completed, you can forget about. An effective recovery plan is a live recovery plan. The plan must be maintained current and tested/exercised regularly.

A Disaster Recovery Manual should be established and kept off-site. At the very least it should include the following:

- systems to be recovered and detailed procedures for how to recover them
- server configuration information;
- workstation configuration information;
- emergency call lists of all personnel;
- vendor and outside support personnel call lists;
- hardware lists and serial numbers;
- software lists and license numbers;
- network schematic diagrams;
- equipment room diagrams;
- contract and maintenance agreements;
- special operating instructions for sensitive equipment;
- Documentation (Procedure Manuals)

Specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

There are many companies that provide off-site storage for a monthly fee which includes pick up and delivery of backup tapes, a storage container, vault space and a disaster recovery box to store software, licenses, the disaster recovery plan etc. If your budget doesn't allow this luxury use a business partner, supplier, a customer or a friend.

For more information on developing your Disaster Recovery Plan please contact our office.