

B(IT)² INFOSOURCE

A collaborative publication of the top small business IT Consultants in San Diego

FOURTH QUARTER 2002

INSIDE THIS ISSUE:

VIRUS UPDATE	2
WHAT IS RAID?	2
INTERNET SECURITY	3
TID B(IT)S	3

SPECIAL POINTS OF INTEREST:

- Test your internet speed speedtest.dslreports.com
- Online Technology for Long-Distance Meetings/Sales Calls myplaceware.com
- The Ultimate Small Business Resource www.chamberbiz.com

Backup and Recovery...the most important ROI you will ever evaluate.

As we reflect on the one-year anniversary of the tragedies of 9/11, disaster preparedness is a topic that should be thought about by all businesses. Disasters can come in all sizes ... no matter how hard we try, there are some events that are out of our control and others that just aren't reasonable to try to control.

There are many aspects of disaster preparedness; this issue of B(IT)² Infosource will touch upon data backup and recovery. Speaking from experience, data backups are very often not thought about until after disaster strikes.

How Important Is Your Data?

Not all files on your system are created equal; some data can easily be recreated while other data can not. Bookkeeping files are more important than temporary internet files. You can reinstall Excel from CD, but you can't recreate a spreadsheet without a good backup. Important files may be text documents, spreadsheets, pictures, music files—anything that would be difficult or impossible to replace.

Why backup?

No matter how stable a system is, and how well it is maintained, you cannot guarantee that your data will be safe if it exists in only one place. The risk of data loss is much greater than most people realize.

It doesn't matter what kind of hardware you have; if you don't have a good, reliable, and restorable backup of your critical data, you will lose important data ... it's just a matter of time.

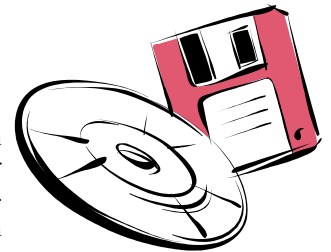
Some of the very real reasons you may lose your data include:

Hardware failure is the most common reason for losing data. Because the hard drive contains all your programs and data, an unrecoverable hard drive failure would require a restore from your backup. Using RAID on your system can help keep your system running.

A power loss at the wrong time can result in the loss of files and could result in file system

corruption which prevents your server from booting. Using an uninterruptible power supply can prevent this from happening and could also prevent hardware failure from power surges.

It is estimated that at least 50% of all businesses that experience data loss will be severely impacted and their business will suffer. How important is your data? Hopefully after thinking about some of the issues discussed in this issue of B(IT)² Infosource, you will review your company's disaster preparedness plan and evaluate where you are. The question isn't whether disaster planning is worth it, but how much is it worth? How much risk are you willing to assume? **B(IT)² ◀ John Fredette, Fredette Systems IT**



As mentioned previously, file system corruption can result in data on the hard drive becoming damaged, and in some cases result in data loss. Using an IT professional regularly to maintain the disks properly with system scans and defrags as well as consistency checks on RAID arrays will help minimize chance of file system corruption.

Human error may be one of the most common causes of data loss ... an accidental deletion could cause the loss of a file or folder that isn't noticed missing for several days. Or if the wrong file is deleted, it could prevent the system from starting. Using properly configured access rights and user privileges, as well as keeping your server in a locked room can help minimize data loss through human error.

New Virus infections are occurring almost daily. A virus can easily cause the loss of data and cause damage as a result of removing the virus from the system. Using a good antivirus

(Continued on page 2)

(Continued from page 1)

application in your environment can minimize the impact of viruses on your system.

The physical elimination of your system though natural disaster or theft would require you to recover all your data from a backup ... this is a reason you should keep a copy of your backup off-site.

What should you do?

Make sure:

- you have a backup and restore strategy, performing periodic trial restorations to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up with software verifications.

- to perform backups every day so that the restored data is as current as possible.
- to back up the entire volume. It is more efficient to restore the entire volume in one operation when you need to be up and running quickly.
- to create a backup log for each backup and review it daily.
- to keep at least three pieces of the media and rotate it. As an extra precaution, keep one of these offsite.

Talk with an IT professional about your disaster recovery. Your IT professional can automate your backup routines and provide you with different backup options.

B(IT)² ◀ John Fredette, Fredette Systems IT

**Computers are
useless. They
can only give
you answers.**

-Pablo Picasso



What is RAID?

RAID (Redundant Array of Independent Disks) allows you to link multiple hard disk drives together and write data across them as if they were one large drive.

There are several levels of RAID, and each RAID level has different advantages in term of performance, redundancy and capacity. The two most common RAID levels are 1 and 5.

In RAID 1 configurations, data on one disk is duplicated on a second disk. This is called mirroring. RAID 1 must be configured on a two-disk array and the total capacity of the disks is reduced by 50%. If either of the two disks fails, data is available from the duplicated disk. Choose RAID 1 if high availability and performance are important, but cost is not a major concern.

RAID 5 provides good overall performance and data protection with minimum loss of storage capacity ... the total capacity of the disks is reduced by one disk. RAID 5 must be configured with at least a three-disk array. If one of the disks fails there is no data loss or system interruption because the data can be rebuilt on a new drive. Choose RAID 5 if cost, availability, and performance are equally important.

B(IT)² ▶ John Fredette, Fredette Systems IT

Virus Update:

Yes, unfortunately the KLEZ virus is still out there. If KLEZ is a word you've never heard of, shoot me an email and I will send you a prize.

Here's a couple of facts you may not have known about this famous virus:

- KLEZ is both a worm and a virus.
- You cannot be infected with the KLEZ virus if you do not open the infected attachment. However, you might still be spreading virus. The worm part of KLEZ is activated simply by opening the email, or even just by having "preview mode" turned on in Outlook. It searches the Windows address book, ICQ database, and all local files for email addresses and sends an email message to these addresses with itself as an attachment. The "From:" line of the message is also randomly chosen from email addresses that the worm finds on the computer. This means that people could be receiving infected messages that look as though they are coming from you!

For example, Linda Anderson is using a computer that is infected with W32.Klez.H@mm. Linda is not using an antivirus program or does not have current virus definitions. When

W32.Klez.H@mm performs its emailing routine, it finds the email address of Harold Logan. It inserts Harold's email address into the "From:" portion of an infected message that it then sends to Janet Bishop, among others. Janet then begins sending Harold nasty messages accusing him of emailing her a virus, but when Harold scans his computer, his virus protection software does not find anything, because of course, his computer is not infected!

- Antivirus software makers have estimated 2000 new infections daily of the KLEZ virus.

- A British security group estimates that 1 in every 300 email messages holds a variation of KLEZ. KLEZ has also been disguised as an immunity tool. DON'T BE FOOLED into opening an attachment that tells you it will make your computer immune to the KLEZ virus. The only protection is to have up-to-date virus protection software with the most current virus definitions!

*Information collected from PCWorld magazine and Symantec's virus encyclopedia. Please email John@Fredette-it.com for answers to your virus questions.

B(IT)² ◀ Anna Luksich, Kaiser & Associates

Internet Security - a starting place

This Center for Internet Security (CIS)- a not-for-profit cooperative organization assisting network users and operators, and their insurers and auditors to reduce the risk of significant disruptions of electronic commerce and business operations due to technical failures or deliberate attacks.

The Center for Internet Security's mission is to help organizations around the world effectively manage the risks related to information security. CIS provides methods and tools to improve, measure, monitor, and compare the security status of your Internet-connected sys-

tems and appliances, plus those of your business partners.

CIS is not tied to any proprietary product or service; it manages a consensus process whereby members identify security threats of greatest concern, then participate in development of practical methods to reduce the threats. This consensus process is already in use and has proved viable in creating Internet security benchmarks available for widespread adoption.

<http://www.cisecurity.org/>

B(IT)² ◀ Clifford Kaiser, Kaiser & Associates

Why Outsource IT?

Millions of dollars are lost struggling with implementing and maintaining complex technologies, moving from legacy systems to the Web, fragmented infrastructure and lack of skilled IT staff. Outsourcing ensures competitiveness and increases your ROI.

In IT deals, many buyers think price is the determining factor, but if you're dealing with a high-quality provider, it's the people and the cultural fit that really make the difference. **B(IT)² ◀**

TIDB(IT)S:

What type of Backup Device should I use for my Small Business?

There are wide range of devices available to use for backup and the appropriate device will depend on your system configuration.

Are you using a server?

The recommended backup device for servers is a tape system. Tape backup systems range in cost from a few hundred dollars to thousands of dollars. With additional cost you typically get more capacity and faster speeds.

The tape drive for most small businesses is a "DAT" tape drive. These devices run \$800-\$1100 (plus tapes), are fast, and can store up to 40 Gigabytes of data.

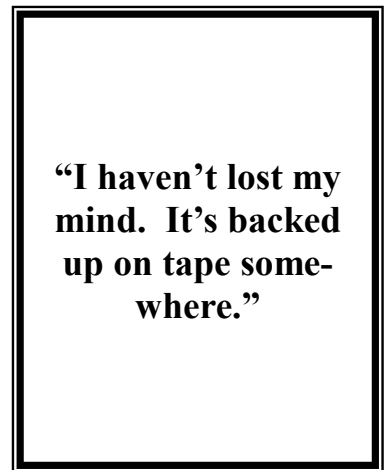
What to use for stand-alone PCs

With stand-alone PCs, if you have less than 650MB to backup, use a CD-RW or the new 750MB Zip Drive. The disks are re-writable, so you can set up a disk rotation, re-using the disks after a certain time period.

If you have more data then 650-750 MB to backup, the next step is a "Travan" tape drive.

"Travan" tape drives cost a few hundred dollars, so they are affordable, and can store up to 20 Gigabytes of data. The tape media is more expensive than DAT running \$25-35 each.

B(IT)² ◀ Dave Peiser, Peiser Solutions



DID YOU KNOW?

Holding down the **Alt** key and pressing the **Tab** key lets you switch quickly between programs that you have opened on your desktop.

Fredette Systems & IT Consulting

John Fredette has had over 15 years of proven professional experience in the technology industry. He specializes in Microsoft products and his forte is systems engineering and network design/implementation as well as systems administration and end user applications.

Previously John has held positions as Senior Systems Engineer with WinResources Computing, IT Operations Manager with Pacific Technology Services and Field Service Engineer with Wheb Systems.

Mr. Fredette holds a Bachelors of Science degree in Computer Information Systems and an Associate in Science degree in Electronic Engineering Technology as well as being a Microsoft Certified Professional and Certified NetWare Administrator.

John has an ongoing commitment to expand his industry knowledge, and to share this knowledge with interested audiences



(760) 758-1973
Professional On-Site
Computer and Networking
Services

Serving San Diego, Orange County and Temecula

support@fredette-it.com
www.fredette-it.com