STAR Watch

Statewide Technology Assistance Resources Project

A publication of the Western New York Law Center, Inc.

Volume 10 Issue 1 January-February 2006

How Good Are Your Backups?

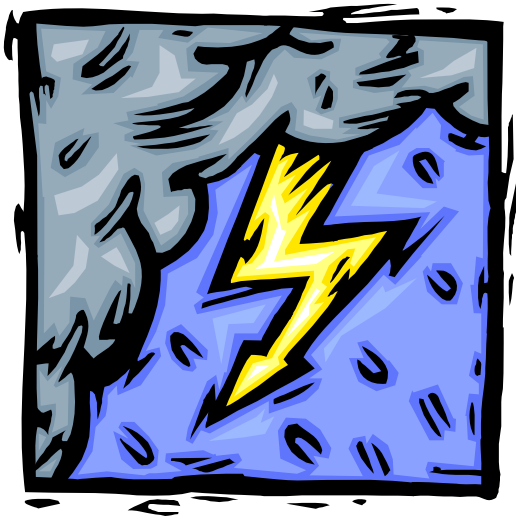
In today's IT world, there is a backup solution to fit organizations of every size from single-workstation offices to organizations with multiple offices, hundreds of workstations, and multiple file servers. There is a backup solution to fit every wallet, ranging in price from a few hundred dollars to tens of thousands of dollars. Backing up data could be as simple as burning all important data to a CD, or as complex as a fully automated backup to tape with multiple magazine-fed autoloading tape drives. Any backup system is a good system if it does what it was intended to do.

Although backup hardware and software will fail on occasion, usually that does not cause any major problems. In our experience, virtually all unrecoverable catastrophic data losses involve multiple human errors or omissions.

So, how much data would your organization lose if your file server has a catastrophic failure? I'm sure that there are many Executive Directors out there who are absolutely certain that, for their organization, the answer is "None". Their certainty is based on the following:

- The latest backup hardware and software was installed recently. It has the latest and greatest features.
- The consultant(s) who set everything up gave assurances that "Everything important is being backed up. Just make sure that the backup program doesn't have any errors when it runs."
- No one on staff has ever reported that any backups have had errors.

In this issue…



Things may not be as good as you think…

Experience has pointed out some flaws in this logic. It may seem silly to ask the following questions, but the answers are not always what is expected. Sadly, all of the questions in this section were suggested by the unfortunate experiences of others…

- **Is it possible that the backup program is not generating error messages because it hasn't been running**?

  Most backups are scheduled to run in the wee hours of the morning so they will be finished before the arrival of staff. If the scheduling mechanism fails to start the execution of the backup program, it won't run. If it doesn't run, there is no backup.

- **If the backup program has been running successfully, is it backing up all data that should be backed up?**

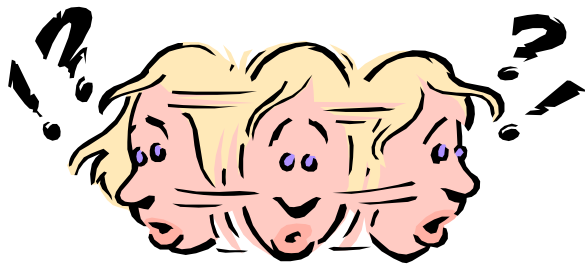
  Many times, new applications get installed, but no one changes the backup to include the application and its associated data.

- **Who made the decision about what data is to be backed up**?

  Unless literally everything is backed up every time the backup is run, it is important that key personnel in all of the functional areas of the organization be consulted regarding data that should be backed up. IT personnel should have input into these decisions, but the final decision should rest with the persons held responsible for getting the work done.

- **Has anyone ever checked the backups to verify that all of the data that is supposed to be backed up is on the backup?**

  The point of backing up data is to be able to recover from a data loss. If the data isn't on the backup tape, it can't be recovered. Many backup programs can be set up to produce a log that lists all of the files/folders contained in the backup. Whenever the backup procedure is changed, this log should be created and reviewed to be sure that all of the intended files are being backed up.



- **Whose responsibility is it to make sure that the backup ran successfully?**

  It should be a staff member who is expected to be in the office every day, not an outside consultant.

- **If that person is not in the office, to whom does the responsibility transfer?**

  People take vacations, get sick, or have personal emergencies that cause them to be absent from the office.

- **Do both of these people know that they have this responsibility?**

  Too many times, everyone assumed that the staff members knew that they had this responsibility-- so no one ever told them.

- **Do these people understand how important this task is?**

  It needs to be crystal clear to staff members charged with backup responsibility that this is an important ongoing daily task. Then, the responsible person must be given the time to perform this task daily.

- **Have these people received any training?**

  If no one knows how to ensure the proper operation of the backup software, then there is no assurance that the backup is running properly. If no one knows how to run the backup or look for problems, then problems won't be found until it's too late.

- **In the event of a loss of data, do these people know how to restore the lost data from the backup?**

  Even if the data is securely stored on the backup, if no one knows how to get it back onto the file server, what good is it?

- **Where are the backups stored? Or, are they just left lying around?**

  In the event of fire, an unprotected backup will be rendered unusable in less than 30 seconds. In a file cabinet, it may survive a few minutes. In a fire-resistant document safe, it could last for several hours. A backup that goes home in a staff member's brief case would survive the total destruction of the office.

- **Have the backups been clearly labeled?**

  If backups are not identified as to date of backup and contents, it may not be possible to figure out which one to use to restore data.

- **Are any of the backups stored off-site in case the office is inaccessible?**

  In the event of fire, flood, or other catastrophe, it may not be possible to get into the building to retrieve

backups for days or weeks. And when they are finally retrieved, they might be damaged. Without this data, you could be out of business. Backups stored at an off-premises location could allow you to start the recovery process.

- **How old are these off-site backups?**

  After the disaster passes, getting an organization back on the air is critical. A lot can change in a week, so imagine how much data could change in a month. Many organizations have off-site vault space for backups, but only swap out media once a month because it takes too much time to do it once a week. Is month-old data even usable? Back to a previous suggestion: A backup that goes home in a staff member's brief case would be stored off-site—and it would probably be more current than the data stored in the off-site vault.

- **Is all critical data in a place where the backup program can access it (to back it up)?**

  Is there any critical data squirreled away on someone's workstation? Is there a good reason for it to be there? Many times, sensitive financial/ confidential information is not stored on the network. It is kept on the workstation of the person responsible for administering it. If the workstation fails and the data hasn't been backed up, that data might be gone forever. If the office is involved in a disaster, it is almost a certainty that the data is gone forever. All critical data should be backed up. To do that, it must be in a place where the backup software can access it. If it is decided that certain types of data should not be stored on the network, it still needs to be backed up.

Doing things right…

Formulating and implementing a strategy for backups is not a trivial task. It will require time and input from all staff levels in the organization, not just the IT support staff. The folks in IT may know <u>how</u> to run the backup, but the decisions about <u>what</u> to backup requires input from the rest of the organization. Beyond that, deliberate steps need to be taken to make sure that the decisions made are translated into a clear plan of action that can be easily monitored for compliance and individuals held responsible for non-compliance. This will not be the most exciting project that anyone has ever worked on. The work is tedious, detail-oriented, and a bit sobering. It is about planning for the survival of your program when the worst happens.

Microsoft Announces Plans for Internet Explorer 7

Responding to user concerns about security and functionality of Internet Explorer, Microsoft has announced that a Beta version of Internet Explorer 7 is available for downloading. According to a Microsoft spokesman, the beta version of IE7 was released to allow end-users to provide feedback before releasing the final product.

This new version of IE is loaded with new features and multiple significant changes. Here are just three that we feel are the most important.

Tabbed Browsing

IE7 lets users view many different websites at one time — all within one organized window. Launch IE7 and the user's home page opens in the first tab. To view additional sites without losing the information from the first site, click the "new tab" button in the toolbar and then navigate to the new site. All previously-opened pages stay open in their respective tabs.

Closing tabs is also easy. Click the close button that appears on the right side of the selected tab and that tab is removed.

Search

With the built-in search box, users can search the web at any time without having to open a search provider page. Search results are displayed in a separate tab. Navigating to any of the sites in the search result list will open additional tabs. This allows users to compare the information from several sites by clicking on the desired tabs, rather than navigating back-and-forth between the sites. Users will be able to specify which search engine should be used by default.

Security

While browsing the web, IE7 automatically monitors computers to protect them from unwanted and malicious programs that might be installed on the workstation as a result of surfing the web.

It will also alert users to potential "phishing" sites — sites that look legitimate but actually are designed to capture personal information.

It will also be easier to see which sites provide secure data exchange, giving users more confidence when shopping or banking online. Internet users will be able see whether the site they are visiting has a valid secure sockets layer (SSL) certificate or if there are irregularities in the certificate information. The "Phishing Filter" will warn of suspicious sites that might attempt to collect personal information.

When will IE7 be available?

The release date for the final product hasn't been announced. For those who have to have it now, a beta version can be downloaded. Just remember: This is a work in progress. This is an unsupported product and there are no guarantees that it is bug-free. But, if you still want to try it, go to:

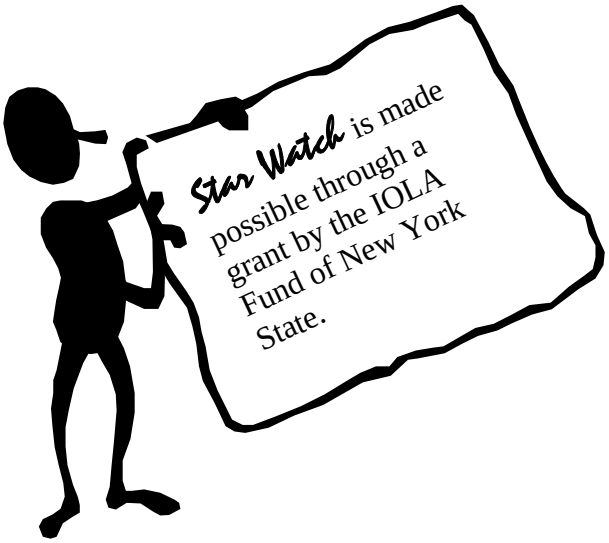
http://www.microsoft.com/windows/IE/ie7/ie7betaredirect.mspx

WNYLC Web Statistics For January 2006

Total Hits	349,991
Total User Sessions	61,868
Average Hits/Day (Mon-Fri)	14,001
Average user Sessions/Weekday	2,280
Number of Pages Viewed	130,052
Avg Number of Pages /Day	4,064
Number of Documents Viewed	72,731
Accessed Using Internet Explorer	90%
Accessed Using Netscape	4%

Operating Systems Used:

Windows XP	56%
Windows 2000	14%
Windows 98	7%
Windows ME	1%
Windows 95	<1%
Windows NT	<1%
Macintosh	<1%
Linux/Unix	<1%



WHO WE ARE

Joe Kelemen - Attorney
Kathleen Lynch - Attorney
Tom Karkau - Programmer

Wnylc@wnylc.com

716-855-0203

www.wnylc.net

Western New York Law Center, Inc.
237 Main Street, Suite 1030
Buffalo, New York 14203