WRS
web resource solutions
Monthly Newsletter

Better Safe than Sorry – Backup and Recovery for Small Businesses
October, 2010, by Bill Spallino

"*Many backup because they have seen the dark side of failing to do so, blessed are those that backup who have not seen! — T.E. Ronneberg*. The topic of system backups isn't very sexy. But the one thing certain about computer systems is that eventually they will fail. And, while computers and data storage media are themselves relatively inexpensive, your data is priceless, and protecting it is a must.

The only safeguard you have against a catastrophic data loss is maintaining good backups. This month's newsletter will cover the importance of backing up your data, identifying critical data, developing a sound backup strategy, and various methods to effectively back up data.

"Any company that experiences a computer outage lasting for more than 10 days will never fully recover financially"

Why Is Backup Important?

As an IT consultant, one of the first things I look at when evaluating a new client's IT infrastructure is the company's backup and recovery strategy. It amazes me how regularly I find that this important, if mundane, function is overlooked. This is a disaster waiting to happen.

The first question I ask is, "How long can your company function without access to its critical IT systems?" The answers vary, but usually translate into, "Not very long." A company's exposure to critical data loss is generally a function of how reliant the company is on its systems to conducting business. If your answer is similar, then protecting data should be an important topic to you.

The impact of critical data loss can be enormous. One study reports that any company that experiences a computer outage lasting for more than 10 days will never fully recover financially and that 50 percent of companies suffering such a predicament will be out of business within 5 years [1]. Let's look at some other sobering statistics:

- 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster.
- 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately.
- 31% of PC users have lost all of their files due to events beyond their control.
- 34% of companies fail to test their backups, and of those that do, 77% have found back-up failures.
- Simple drive recovery can cost upwards of $7,500 and success is not guaranteed.
- It takes 19 days & costs $17,000 to retype 20 megabytes of sales data. Recreating 20 megabytes of accounting data takes 21 days and costs $19,000.

- 70% of small businesses reported that a single incident of data loss would be considered significant and costly. [2]

As you can see, the cost of failing to adequately protect your company's data can be high, even a death sentence. The thing that is truly heartbreaking about data loss is that it's completely preventable and made all the more so because protecting your data can be so easy and affordable.

What to Backup?

Now, a detailed explanation of how to conduct an exhaustive data-criticality study is beyond the scope of this article, but there are some rules of thumb. Data needs to be categorized by its Criticality, Volatility, and Retention requirements. Criticality is determined by measuring the impact of losing it. Volatility is a function of how often it changes. Regulatory Retention requirements will vary by industry.

Additionally, you want to backup *everything* at least once. Then, create additional backups of other data matched to how often it changes (for more on this, see "Backup Methodology," below). As a rule, data that changes daily should be backed up at least daily, data that change monthly at least monthly, and so on. To zero in more closely on what you need to backup, it's helpful to look at some of the types of risks your data face.

"*The thing that is truly heartbreaking about data loss is that it's completely preventable and made all the more so because protecting your data can be so easy and affordable*"

Assessing Risks

Planning for only one type of failure will almost guarantee that you get nipped by another type of threat (see *Figure 1*). For example, you may have backups that protect against hardware failure, but did you think about human error? Or, what happens if the office is flooded or burns down? In addition to physical threats, what types of regulatory retention requirements does your company face? Failure to keep the necessary data to support your IRS returns can be disastrous, successfully defending a lawsuit may depend on your ability to reproduced historical records, and email retention requirements are ever changing, just to name a couple of examples. Let's look at some of the areas that need to be studied when creating a backup and recovery policy:

Hardware Failure

Look at your system at large, its various hardware components, and the data stored there. Internal hard disk drives are an obvious component, but you may have others that are important as well. Remember, the average life span of a common hard drive is 3-5 years and they often give no warning when they're about to give out.

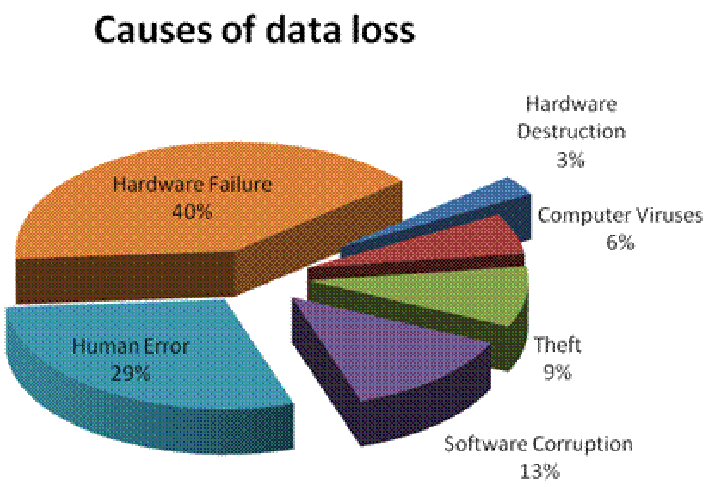

Figure 1 - Causes of Data Loss

Applications

Even small business-oriented applications rely on databases of one type or another to store critical business data. While fast and generally reliable, they are subject to corruption for a variety of reasons. They are also prone to errors introduced by users.

Human Factor

What types of mistakes can you or your employees make that could translate into a critical loss of data from your company? Also, beyond just critical loss, accidentally deleting certain files can take hours to recreate – protecting them can save time and money later.

Regulatory Retention Compliance

Requirements in this area vary by industry. You need to make sure you can resurrect important information for local, state, and federal agencies, as well as other governing bodies that oversee your industry. Also, email has become an important data type whose backup must be managed properly for compliance purposes.

Disaster Recovery

As discussed above, a catastrophic event, like a fire or flood, can doom your business if it takes your data with it. Backups for this purpose need to include the minimum amount required to put your business back to its pre-crisis state. To have it available, it of course needs to be stored somewhere offsite.

"Conduct a study of the risks your data face. Planning for only one type of failure will almost guarantee that you get nipped by another type of threat."

Also, remember to include backups of the installation media for any of the critical applications you use to operate your business and that they match the data; a five year-old version of your accounting application probably won't function with your current data. You must also have available any special equipment needed to access the data. For example, tapes made on an

older tape backup device may be unreadable with new equipment – unusable backup media is worse than not having any, because it provides a false sense of security.

Backup Media

Tape was once the king of backup media, but with the low cost of hard disk and broadband Internet connections, there are a number of newer options available. Storage companies are now marketing single and multi-bay devices that house removable hard drives. Smaller companies often use USB Flash drives and/or optical media (CD/DVD) and larger companies have begun using Virtual Tape Libraries (VTL), which function like tape, but exist on hard disk.

Also, a whole industry has sprung up around Internet-based "cloud" backup services. These services, from companies such as Mozy, Carbonite, and Iron Mountain, provide a small program that sits on your computer and creates backups, over the internet, to disk drives at the provider's remote location.

In most cases, you'll find that companies operate a hybrid of these media types. For example, hard disk may be used to protect against drive or application failure, but off-site versions might exist on tape or cloud backup. Smaller companies may use Flash drives in combination with CD.

A word of warning: many companies market those external USB backup hard drives that plug into a computer on your network and promote them as a "backup solution". While this beats no backup at all, it is not recommended that this type of drive be considered as the *sole* backup medium. When you open up one of these devices you'll find inside just another disk drive, as prone to failure as any other drive. We've seen a lot of heartache result in companies that held a false sense of security from believing that one of these drives was sufficient to meet all of their backup needs.

Backup Rotation

More important than the media is the schema used to rotate "units" of storage (i.e. one tape, one CD, one hard disk, etc.). Perhaps the most common and easy to understand rotation method is the "Grandfather-Father-Son" technique. Daily backups, or "Sons," are promoted to "Fathers" or weeklies, which in turn are promoted to "Grandfathers" or monthlies. One or more of copies of these are in turn taken off-site for disaster recovery purposes (see *Figure 2*).

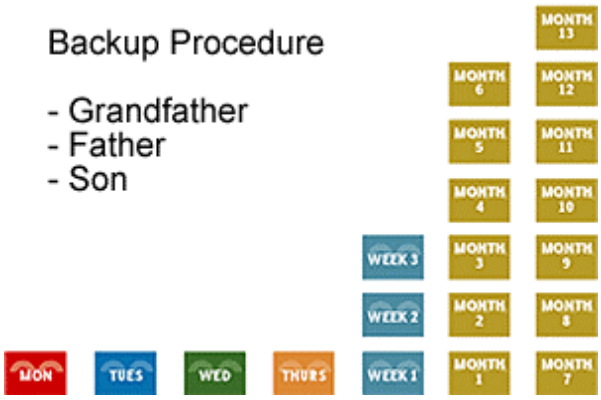

Figure 2 - GFS Backup Procedure

While a Full backup is generally preferable, it can mean a much larger amount of backup media be used. So, deciding upon which method to use will center on the availability of media for backups and the turn-around time demanded by the business environment.

Backup Methodology

In addition to identifying the data you need to back up and rotating backup media, it is important to decide on the methodology or style of backup you'll use. There are three basic types: Full, Differential, and Incremental.

- **Full**: This methodology transfers a copy of all data within the scope of the backup, regardless of whether the data has been changed since the last backup was performed.
- **Differential**: This methodology backs up all files changed since the last full backup, regardless of whether they have been changed since the last backup operation of any kind.
- **Incremental**: Here, only those files that have changed since the last backup operation of any kind (full, differential, or incremental) will be transferred to the backup medium.[3]

Essentially, the choice is between the speed of making backups versus the speed of recovering data. A Full backup backs up everything as it sits, while the other styles start with a Full backup, then backup only files that have changed. The Differential and Incremental styles of backup require that the last Full backup be restored, then brought up-to-date by adding the other partial backups.

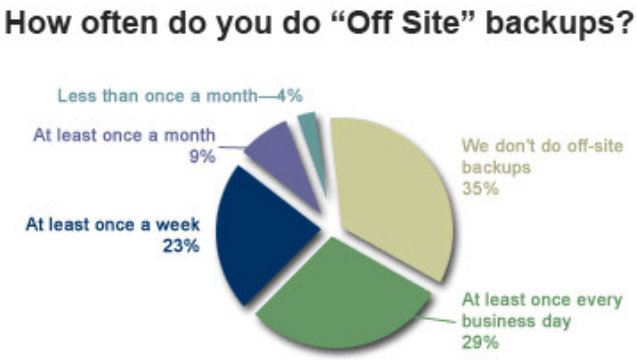

Figure 3 - Survey of companies' off-site backups practices.

Recovery

If there is one recurring flaw that we find in many backup strategies, other than not having one, is the failure of companies to test their recovery process. It's amazing how many times we've seen elaborate backup efforts that have failed because backups were not usable when needed or the necessary data wasn't available. It is imperative that backups be tested regularly for viability. Waiting to test data backups until they're needed is a form of "Russian Roulette" that you don't want to play.

Disaster Recovery and Off-Site Backups

While Disaster Recovery (DR) (also known as Business Continuity) is a separate topic onto itself, it should be an important consideration in your overall backup strategy. Despite its technical sounding name, DR is merely an "insurance policy" against a catastrophic event that could put your company out of business.

The DR plan you decide to implement will need to take into account a host of factors, but in all cases will include storing at least the minimum of data needed to conduct business offsite. (For a rudimentary discussion of Disaster Recovery, see http://www.ehow.com/disaster-recovery-

planning/ - for a DR success story in the aftermath of hurricane Katrina, see http://searchcio.techtarget.com/news/1122305/Katrina-IT-lessons-in-disaster-recovery).

Conclusion

Keeping your data safe requires recognizing your data's importance and putting into action a solid backup and recovery plan. Whether you operate a small "mom and pop" shop or a large enterprise, the motivation for keeping usable backups, made at appropriate intervals, is vital. Failure to address this important area has doomed innumerable companies to bankruptcy – don't let yours be one of them.

[1] http://gbr.pepperdine.edu/033/dataloss.html
[2] http://www.rbs2000.com/index.php?cat_id=103&nav_tree=179,103
[3] http://articles.techrepublic.com.com/5100-10878_11-1040176.html

About the Author – Bill Spallino is the President and CTO of Web Resource Solutions, a leading Web & Application Development and IT Management consultancy located in Orange County, California. Bill is a 30-plus year veteran of the Information Technology industry, and has served as a developer, network and systems administrator, project manager, and CIO for large corporations like Heinz, Transamerica, and Nissan, as well as numerous smaller concerns.

Web Resource Solutions specializes in assisting small and medium-sized businesses in developing applications, managing IT infrastructure, and conducting business on the Internet, including implementing backup and recovery and business continuity plans. If you're interested in protecting your business against the ravages of critical data loss, contact us about a Free Evaluation. We can show you how you can develop an enterprise-class backup and business continuity strategy on a small company budget.

www.webresourcesolutions.com.