# BACK UP AND RESTORE

In today's 24/7 information-centric society, consumers, small businesses and large enterprises have become increasingly dependent on stored data. At home, as well as in business, data is an asset that, like family heirlooms and valuable corporate assets, must be protected. Consumers are likely to store email, personal financial data, music and priceless family photos and videos on their hard disks, while businesses store data that is essential to their very survival on file servers and employees' computers. How many businesses could survive without email and access to CRM, inventory records or ERP systems?

And yet, it is estimated that about 6 percent of users lose their data each year.

## Reasons for Data Loss

There are many reasons why consumers and businesses experience data loss:

- Hard drive failure – Whether it's within one year or in 5 years, hard drive failure is inevitable.
- Hardware failure – Failures of other hardware, such as hard drive controllers or memory, can cause data corruption.
- Improper system shut-downs – Data can be corrupted when systems are improperly shut down, due to a power failure, or because a user simply pressed the power-off switch before properly shutting down the operating system.
- Computer viruses and malware – Some studies report that up to 7 percent of data loss is attributable to computer viruses and malware.
- Disasters and on-site losses – Site-related data loss can occur due to power surges, fire, flooding, earthquake and theft.
- Disgruntled employees – Sadly, much loss comes at the hands of companies' own employees. Disgruntled employees may intentionally delete files, format their hard disks or attack server-based data that they routinely access to do their jobs.
- Human Error – Even happy employees can be responsible for data loss if they accidentally delete files or spill a cup of coffee that results in a computer failure.
- Theft and loss – Many lost or stolen laptops are never found, and all of its important data is gone, too.

Proper backup can minimize the impact of data loss that occurs due to any of these reasons.

## What is Backup?

In simplest terms, a backup is a copy of the data stored on a hard drive that is used to restore data in the event that a loss occurs. There are good reasons to create backups:

- You have the ability to restore files if they are ever accidentally deleted or corrupted.
- You can recover from disasters as diverse as floods, fire, virus attacks or equipment failure.

However, creating backups can be a daunting task. Each day businesses create massive amounts of data and store it on hard drives and servers throughout the organization. To ensure that a backup copy of the data is always available, a solid strategy is required—one that employs back-up systems that are appropriate to the organization's needs.

## Choosing an Appropriate Backup Strategy

A good backup strategy may be designed to optimize the use of backup storage resources or to reduce recovery times and quickly restore business operations in the event of a disaster. And others must be designed to ensure compliance with industry mandates or state and federal regulations, such as HIPAA (which governs patient privacy and records retention for the healthcare industry) and the Sarbanes-Oxley Act of 2002 that governs the financial services industry.

Whatever the backup need, there exists a wide range of methods for backing up data, as well as many choices of media on which to store backups.

## Backup Methods

Different types of backups can be performed to secure data. Each offers advantages, as well as disadvantages, and the various types can be combined to fit into a backup strategy to fill the particular needs of the enterprise or organization.

### *Full Backup*

As the name suggests, a full backup copies all files and folders from a hard drive or file server to a target repository, such as a tape drive or external hard drive, where the backup data will be stored. The advantage of doing a full-backup is that it minimizes the time required to restore data in the event of a hardware failure.

Full backups, however, can take a significant amount of time. Depending on how much data needs to be backed up and the speed of the backup device, the "backup window" in some environments may not be long enough to capture all of the data.

Full back-ups can also consume a significant amount of storage capacity. For file server-based backups, backup software designed specifically for the server operating system is required in order to properly backup system data that is not stored as a file or folder. Examples include metadata information, such as file permissions, groups, owners and Access Control Lists.

Open files also present challenges. Large database files, for example, are always open and are subject to constant updates. And, large files can take a significant amount of time to backup. In order for a database backup to be usable, it needs to be a snapshot of the entire database rather than a sequential backup created by reading through the file. Server backup software is designed specifically to backup databases while they are still online and usable by clients.

### *Incremental Backup*

An incremental backup only captures changes that were made in files after the previous backup was made. For instance, if a full backup is performed on Monday at midnight, an incremental backup performed at midnight on Tuesday will only capture changes that were made to files in the 24 hours that preceded it. Similarly, an incremental backup run at midnight on Wednesday will only capture changes made to files after the midnight Tuesday backup was run.

Incremental backups take less time to perform and use fewer storage resources since they record only the changes and not a full record of all files. The disadvantage occurs when files need to be restored. If a full restoration is needed, the process must start with the last full backup that was done, and then all of the incremental changes that were backed up since that time must be recovered. If a backup plan calls for weekly full backups and daily incremental back-ups, a full system restore could require restoration of up to six incremental backups in addition to the full backup. Depending on the size of the organization, this can be considerably time consuming and may not be the best backup strategy in a time sensitive environment

***Differential Backup***
Differential backups are similar to incremental backups except that they backup all the changes since the previous full backup. The advantage that a differential backup has over a full backup is that it takes less storage space and less time to restore if data loss should occur. A differential backup does require more space and time than an incremental backup. However, in the event of data loss, a full restoration would only require the restoration of the most recent full backup and the most recent differential backup. As compared to restoring a full backup with multiple incremental backups, this reduces the amount of time before files are fully restored and users are back in operation.

***Real-Time Backups***
In some business environments, such as the processing of credit card transactions, there is a requirement for real-time or near real-time backup of data. This can be accomplished by "mirroring" the data, or saving a copy in real-time onto a second server or storage device. Backup applications for such settings are often operating system specific, detecting changes as they are made to files on the primary server in order to update the backup server.

***Disk Image Backups***
Disk image backups are most often used for disaster recovery. A disk image backup uses disk imaging software to create a complete snapshot of a hard disk and store it in one or more files, depending on the operating system. In the event of data loss, the image includes virtually everything needed to restore the files to a new disk. All partition information, boot sector information, as well as the operating system, applications and data can be easily recovered – often in as little as one or two mouse clicks.

The chief advantage of this type of backup is that it avoids the so-called "bare metal restore" in which all systems and files must be re-installed from scratch. In the event of a disaster such as a hard drive failure, re-creating a system from incremental or differential backups could be a daunting task. At a minimum, the operating system and well as the backup/restore software would have to be installed. For client systems, where many of the backups are file and folder-based, original application installation media must be found, re-installed, and like the operating system, updated to the latest versions. Without an image-based backup, a bare metal restore could take in excess of 20 hours to complete.

Disk imaging software is widely available for both clients and servers at affordable prices but disk-imaging should not be considered a complete backup solution. Rather, disk images should be taken at scheduled intervals as part of an overall backup strategy that also includes full backups as well as incremental or differential backups.

## Storage Media
Data can be backed up to tape drives, CDs or DVDs, USB flash drives, direct-attached USB flash drives, network attached storage (NAS) devices or the Internet. As with backup strategies, each media selection offers advantages and disadvantages.

***Tape Drives***
Because of the relatively attractive ratio of cost per Gigabyte, tape drives have been a traditional choice of many IT departments for backing huge amounts of data. Tape is a sequential media and, although write speeds to tape can exceed those of writes to disks in some cases, locating and restoring files from tapes can be more time-consuming than restoring files from disk-based backups. Automated robotic tape-changing mechanisms can reduce the work of tape rotation and managing large numbers of tapes.

***CD or DVDs***

These optical media types offer relatively limited capacities (700 MB and 4.3 GB respectively) but have the advantage of being inexpensive. New Blue Ray high-density DVDs offer double the capacity of traditional DVDs. The most common CD-R and DVR-R formats can be written to only once and their volumes closed to prevent future changes. Write-once media is required by federal regulations for archival storage for some industries. There has been some discussion about whether or not CD-R and DVD-R media types are appropriate for long term archival purposes because of their relatively short life span. Inexpensive aluminum-based CDs can have a life span that is relatively short. However, some media manufacturers offer premium, gold-based media that is certified for archival use. Serialized, certified archival media is also available for the medical industry.

***USB Flash Drives***

With capacities ranging up to 32GB, flash drives offer a convenient, if not inexpensive, way to backup data. Many consumer-oriented flash drives lack encryption. Since it is fairly easy to misplace or lose a flash drive, these are generally inappropriate for business use. However, some companies offer drives with automatic 256-bit encryption as well as models that are FIPS 140 level 2 compliant for federal government use.

***Direct-attached USB Drives***

Recent advances in technology have expanded the capacity of single disks to 2 TB and have pushed the prices of USB/Firewire direct attached external devices down to about $200. Devices that are 1 TB are available for less than $100. These devices offer a large amount of storage at a reasonable cost. They are easy to connect and they provide rapid recovery times, but they may become damaged if they are moved to be stored off-site.

***Network Attached Storage***

Network Attached Storage (often referred to as NAS) devices are special-purpose dedicated storage servers that plug into a local Ethernet network and offer shared storage to network clients. NAS products, such as Buffalo's TeraStation 5000N family of storage solutions targeted at small to medium enterprises. TeraStation 5000N products have a complete range of access control capabilities to allow or deny access to data and integrate seamlessly with Microsoft's Active Directory as storage devices. Advantages of using a TeraStation 5000N, either as a backup storage device or as primary storage, include:

- Deployment Ease – Guided by installation wizards, non-IT personnel can add shared storage capacity to a network in as few as 15 minutes.
- NAS hard drives – All TeraStation 5000N devices use NAS hard drives, which run cooler, reducing power consumption and result in lower operating costs and longer average lifetime
- Linux-based – Having a Linux-based operating system, TeraStation 5000N devices are immune to viruses and rarely require upgrading or patching.
- Windows Storage Server® 2012 R2 – All TeraStation 5000N WSS devices are shipped with this Microsoft software, which allows for data deduplication and DFS Replication
- RAID-enabled – TeraStation 5000N offers fault tolerance through RAID (redundant array of inexpensive drives) configurations. In a fault tolerant RAID configuration, data is written to multiple drives, such that no data will be lost in the event of a single drive failure.
- Hot-swap Drives – TeraStation 5000N devices also support "hot swap" capabilities (the ability to remove a defective disk without powering down the device). With hot swappable disks, a defective disk in an array can be replaced with zero downtime.

- Real-time Replication and Failover Support – Each TeraStation 5000N can be backed up to another TeraStation or to attached USB storage devices. Scheduled backups or real-time replication between multiple TeraStation devices offer a backup framework to backup local and remote offices.
- Desktop and Rackmount form factors – The TeraStation 5000N series provides both desktop and rackmount solutions, providing the option to choose what best suits your business' needs

Buffalo's Replication feature provides easy and high performance data replication from one Buffalo NAS device to another Buffalo NAS device over the network or the Internet. With replication, rest assured that your important documents are always and immediately backed up onto another device on the network.

***Internet Cloud-based Storage***

The increasingly fast broadband speeds available to both consumers and enterprises have produced an entire industry of companies offering online backup services. Many of these online backup service providers offer geographically redundant storage in data centers that are staffed 24/7 by IT professionals. Corporate data is encrypted prior to transmission to the storage providers, so while these providers may store a company's data, they do not have access to it. Online storage can be a viable backup option for small to medium businesses that do not have a dedicated IT staff to help manage the backup process. Importantly, online storage ensures that mission-critical data is stored off-site so that data is not lost in the event of a disaster, such as a fire or flood.

## Backup Strategies

Developing a comprehensive strategy for backing up and restoring data is not a simple task. The different backup types must be considered as well as the appropriate storage media types. In some industries, federal requirements for data security, privacy and records retention can also be an important factor to consider when developing a backup strategy. For many businesses, a combination of backup types, storage media and offsite storage strategies will be the best solution to prevent data loss.

This paper has introduced the basic types of backup methods, as well as commonly used backup media. Further considerations for preventing data loss include:

- A backup strategy should employ a multi-tiered approach. File and folder-based backups are fine for protecting a few valuable files, but they are not adequate if an entire hard disk fails. Disk imaging programs, available for both computer and server platforms, can quickly restore data, operating systems and all installed applications.
- Choose backup software with flexible scheduling capabilities to perform regular backups. A scheduler eliminates the need to remember to manually start a backup. Most software has the flexibility to schedule regular full backups, as well as incremental or differential backups.
- No matter what media is used, copies of backups should be stored off site. Whether it is a simple plan of rotating USB drives to another location each week, sending media to a company that specializes in media storage and record retention or using an online storage provider, it is important to store mission-critical data in multiple physical locations. In the event of a disaster, off-site storage can make the difference between survival and going out of business.
- Test backups should be done periodically by restoring data to an alternate location. Without testing a backup by restoring it, there is no way to ensure the backup is working.

For more information about Buffalo Americas, visit www.buffalotech.com.