

Building a Backup Strategy for SMBs

WHITE PAPER

Dantz Development Corporation

Overview

Over the past few decades, the amount of data stored on business computers has grown at an astronomical rate. Today many small and midsize businesses (SMBs) now have databases, file servers, and e-mail systems containing constantly changing data that is crucial to day-to-day business operations. If a company loses this data, business grinds to a halt.

It is essential for SMBs to have a reliable backup and restore strategy to guard against data loss. Unfortunately, SMBs are caught in a squeeze. Most backup strategies are either relatively unsophisticated solutions designed for home users or overly complex solutions geared toward large corporations. Low-end solutions designed for individual computer users do not provide the advanced features that SMBs need to protect vital business data; and enterprise-level solutions often require far more IT resources than SMBs have at their disposal.

SMBs need to find a middle ground between these extremes in order to adequately protect business data. They need a backup strategy that can protect all their data while remaining easy to set up and run with minimal IT resources. The following guidelines can help SMBs establish a reliable backup strategy to safeguard the integrity of data and guarantee quick, easy, and accurate restores.

Using Business-Class Backup Software

Low-end backup software, drag-and-drop strategies, mirroring, and disk duplication do not provide business-class data protection. These strategies sometimes provide adequate protection for personal users with minimal data, but they have a number of flaws that make them unsuitable for business-class backup and restore features.

These strategies simply write over the files and folders previously existing on the backup media, erasing all previous backup data and creating one restore point. The problem with having only one restore point on the backup media is that problems such as virus infections, inadvertent file deletions, and unnoticed file corruptions that are not discovered prior to performing a backup are propagated to the backup media. Past versions of files are lost, and the computer cannot be returned to a prior point in time.

Additionally, drag and drop is a flawed data protection strategy because it depends on end users to transfer important information at regular intervals from their desktops and notebooks onto a backup server. However, end users back up sporadically, if at all. And few employees know where all of the important files and settings of their computer reside.

Business-class backup software overcomes the limitations of low-end backup software. SMBs need to select software that protects all business-critical data and individual computer settings. It needs to be easy to set up, run on a schedule, and keep data protected by automatically adjusting its operations. And it needs to provide multiple restore points by saving several past versions of files, folders and computer settings.

Protecting Everything on the Network

SMBs need to select business-class backup software that protects more than just files and folders. Backup software needs to protect all the computers on a network, work with the most popular operating systems, and back up all the data necessary to restore a computer in the event of a failure.

- **Servers, desktops, and notebooks**

Some backup strategies protect only file servers and business-critical application servers, but according to a Gartner study, 40-80% of a company's vital data resides on desktops and notebooks. Notebook computers present a special challenge. Because companies often issue notebooks computers to their executives and strategic planners, notebooks often contain a business's most vital information. But notebooks are often not connected to the network during scheduled nightly backups, which means they can remain unprotected for extended lengths of time. A complete backup strategy needs to protect servers, desktops, and notebooks by recognizing them when they appear on the network.

- **Applications, settings, and drivers**
Protection also needs to encompass the operating systems, device drivers, applications, application settings, and user settings on the computers in a network. When a computer fails, restoring the operating system, applications, and settings can be a time-consuming process. IT personnel can spend countless hours loading application CDs, re-installing applications, and re-configuring settings. Plus it can be extremely difficult or impossible to identify and locate applications that were previously downloaded over the Internet.
- **Heterogeneous networks**
Having multiple operating systems on a network can also present a challenge. Backup software needs to protect the computers that run popular Windows, Macintosh, Linux, and Solaris operating systems.

Ensuring Fast Backups and Accurate Restores

Full backups copy all of the files and folders each time a backup occurs. Full backups provide accurate restores because they make an exact copy of every file and folder selected for backup. However, full backups are time consuming, require a lot of backup media, and provide few restore points. To save time and backup media, backup software often performs incremental or differential backups that capture only files that are new or that have changed after an initial full backup.

Although incremental and differential backups save time and backup media, restoring from them is a complex process that almost always results in flawed restores. Problems will occur because the data from the initial full backup is returned to the hard drive followed by data from the incremental or differential backups. This process returns previously deleted, moved, or renamed files and folders. For example, if a working file had been moved three times, renamed, and then deleted, the restore could return five different versions of that file when an accurate restore would not have returned it at all.

The only way to get the benefits of incremental or differential backups and still have 100% accurate restores is to select backup software that scans the hard drive prior to performing a backup, creates a list of the files and folders present, and stores that list on the backup media. Later, the software uses the appropriate list to guide the restore, returning only the exact files and folders that existed at that particular point in time.

Automating Backups

Automating common backup tasks can greatly reduce the amount of time and energy that must be spent performing daily backups, but implementing automated backups is not always easy. Care must be taken to make sure that automated backups run reliably and protect all the computers on a network.

Automated backups do not protect desktop computers that are turned off or mobile computers that are disconnected from the network during scheduled backups. Additionally, if backup windows are limited and large amounts of data are transferred, most backup software has time to back up only higher priority computers before time runs out. For these reasons, some computers can go unprotected for extended periods, even with an automated backup system.

SMBs need to select backup software with a built-in self-adjusting scheduler that recognizes computers that were not backed up. The scheduler assigns those computers a higher priority for the next backup. With an automatic scheduler controlling the backup process, IT personnel can devote their time to more important tasks, rather than spending time each day adjusting backup scripts. Notebooks would also be adequately protected, as they would be recognized when they appeared on the network and then prioritized for backup.

Protecting Backup Media from Disaster

SMBs need to make at least two copies of the backup media and store one in a secure, offsite location to guard against catastrophic events such as fire, flood, earthquake, or other disasters that might destroy the onsite backup media. Rotate onsite/offsite backup media at regular intervals. Select software that doesn't

need to perform a time-consuming full backup each time offsite media is brought onsite. This will significantly speed up the process.

Conclusion

A reliable backup strategy is built on business-class backup software that delivers easy-to-use, reliable backups and allows accurate restores and recovery from disaster. Backup software needs to provide complete protection for all your computers, applications, settings, and operating systems. It must save time by performing fast incremental or differential backups while at the same time delivering 100% percent accurate restores. And it needs to utilize automated backup technology, which allows small and midsize businesses to protect data without requiring extensive IT resources or unnecessary expenditures to train employees in complicated backup and restore procedures. As part of any backup strategy, remember to keep a copy of the backup data offsite in a secure location to guard against disaster.