BUSINESS CONTINUITY: PLANNING FOR THE UNTHINKABLE

In today's 24/7 business economy, no company can risk catastrophic data loss. Whether it is due to fire, flood, lightning, theft or human action, the results can be devastating. A study done by Pepperdine University in 2003 pegged business losses due to data loss at $18 billion per year. But data loss often means much more than financial loss to the business; it can mean the loss of the business itself.

According to reports from the National Archives & Records Administration in Washington (NARA), 50 percent of companies that lost their data centers for 10 or more days filed for bankruptcy immediately and 93 percent filed for bankruptcy within one year. It is little wonder, then, that most large companies today allocate at least 2 percent of their total IT budgets to disaster recovery planning.

For small to mid-sized enterprises that lack the staffs and budgets to quickly marshal resources and restore operations if disaster strikes, the statistics are even more sobering. A survey conducted by the University of Texas found that 43 percent of businesses that are forced to close because of catastrophic data loss never reopen and 51 percent close permanently within two years; only six percent can be expected to survive the long haul.

Catastrophes—Large and Small

Catastrophic data loss results from numerous causes. The Federal Emergency Management Agency (FEMA) reports that fire is the most common devastating natural disaster to befall businesses, annually accounting for damages that rise into the billions. Water damage that occurs during the fire-fighting effort only compounds the risk to data and can be more dangerous to electronic assets than the fire itself.

Far more common, however, is data loss that occurs every day. The Pepperdine study estimated that only 3 percent of data loss occurs as a result of natural disasters. The far more common "disasters" are everyday threats resulting from hardware failure, software corruption, virus attacks and human activities.

The IT research organization, Computer Economics, has estimated that business losses due to virus attacks alone grew from $500 million in 1995 to $14.2 billion in 2005. And, sadly, some of the most devastating attacks have come from within. Consider the case of a former engineer at the Federal National Mortgage Association (Fannie Mae) who, after being fired from his job, was arrested on charges of designing malware to "destroy and alter" data on the company's 4000 servers. Experts believe that, if another engineer had not discovered the crime shortly after the code was planted in 2008, the attack would have idled the mortgage giant for at least a week.

The Ponemon Institute, a Michigan-based research center focused on data security, has suggested that, during this time of elevated staff turnover due to economic turmoil, as many as 70 percent of American businesses will experience data theft at the hands of current or former employees.

Nevertheless, according to a CSI/FBI report on business losses due to data loss found that the majority of incidents, some 39 percent, are due to non-malicious activities. Malware is often introduced by the uncontrolled use of iPods, PDAs and USB flash drives that employees use to carry from work to home and back again. And even the most well-meaning employees inadvertently delete files, reformat hard disks or introduce viruses or malware to their employers' computer networks.

Recovering lost data is an expensive proposition. The cost of recovering and restoring files on even a single PC hard drive can easily top $7500 if backup copies of the data are not available. The number quickly rises to staggering proportions if the loss extends across the network to the company's file servers.

Business Continuity Planning

Given the cost of recovering files, prudence in advance of disaster seems in order. As the Pepperdine study concludes:

"Since the technologies available to back-up data are often reasonably priced, cost does not necessarily present a stumbling block in preventing permanent data loss. … A saying that precedes the advent of the computer is appropriate here: an ounce of prevention is worth a pound of cure."

The speed with which a company is able to return to normal, or near normal, business operations following a catastrophic event depends, in large part, on the attention it gives to continuity planning long before such an event occurs. Business continuity guidelines from both FEMA and the Department of Homeland Security urge you to respond to disaster before it strikes. It is not a question of what you must do to be in business. It is a question of what you must do to *stay* in business. It should include:

- Redundant systems with up-to-date backups of all mission-critical applications and data files. These should be accessible via the Internet so that employees can access them from remote locations.
- Digitization of paper archives to provide easy-to-duplicate backup copies of all essential records.
- Multiple electronic backups of archives for compliance with regulatory mandates.
- Offsite storage of mission-critical files and important archives to ensure their continued existence if the company servers are destroyed.
- Work-at-home support for employees who are unable to get to the office.
- A succession plan for key personnel.
- Cross-training to assure all personnel possess the skills to cover necessary jobs.
- Identification of secondary sites from which business could be conducted if disaster strikes the primary site.
- A communications plan to maintain close contact with key customers, suppliers through times of emergency.

The first five points are essential survival tactics for any business. Even if the business is not in a location that is subject to natural disaster or terror attacks, it is important to guard the business against catastrophic data loss and to provide work alternatives and succession if key employees become seriously ill, disabled, or worse.

Digital Preparedness

In the data center, business continuity means readying for data loss of any sort. That means having the tools and a strategy for backing up digital assets, including operating systems, applications, device drivers, and all system and application updates and patches, as well as mission-critical data files. These include email, accounting records, customer information, and all archives of files whose retention is mandated by state and federal regulations.

Not only should these files be backed up, they should be backed up to media that accommodates the business's need of them and stored off-site to protect against loss due to site-related disasters such as fire, water and earthquakes or theft. Archives, for instance, require a media that is primarily designed for longevity

and not necessarily for speedy retrieval. Mission-critical data and applications, those that are routinely accessed each day in the course of doing business, should be stored on a media and in a format that enables easy restoration and ready access.

In the event of a disaster such as a virus attack, hard drive failure, theft or total destruction of a company's file server, re-creating a system from scratch can be a daunting task. At a minimum, the operating system and well as the backup/restore software must 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. This so-called Bare Metal Restore could take in excess of 20 hours, on average, to complete. Clearly the time involved is especially disabling to small to mid-sized businesses that lack the IT staff to perform the task. Recovery may not even be possible if the business has misplaced the original installation disks or relies on older applications that are no longer available in the versions that the business was using. Professional recovery services can help but, besides the expense, they may be unable to recover all of the files and the software files that can be recovered may be corrupted and unable to operate normally.

Devising an appropriate backup plan to protect business continuity begins with determining business needs and resources.

- What files should be backed up?
- To what type of media should they be backed up? How often should they be backed up?
- Where should data backup and archive files be stored?

Assessing Needs

It goes without saying that a business should back up all of the files needed to run the business. But what, exactly, does that involve? When asked about necessary files, business people tend to think of the data files they work with daily and overlook the system files, applications, patches and drivers that provide the platforms and software engines needed to access and work with those files. An appropriate backup strategy should protect all of them. Backup software can be configured to produce daily backups of data files as well as periodic full and differential backups of the contents of an entire hard disk to ensure current (or relatively current) copies will be available if needed.

An assessment should be made of the business's archival needs. What information should be archived? How often and to what media? The choice of media is critical when archiving data in an industry that is obligated to meet compliance standards, such as those set by the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Acts (HIPAA). Traditional magnet media deteriorates over time and durable optical media is often necessary. Multiple copies, stored off-site in diverse locations, ensure that if one or more sets of data files in destroyed, alternate copies still exist. The media choice can be critical to businesses that deal with compliance and regulatory requirements as traditional magnetic media tends to deteriorate over time. If long-term or permanent archiving is required, considerable attention should be given to the choice of media. Tape, the traditional long-term storage and archiving solution in many IT departments, provides an inexpensive way to back up huge amounts of data but it is a sequential media that does not easily accommodate the retrieval of specific files. It also deteriorates in a few years. Lifespan is also an issue with other inexpensive magnetic media, including CDs and DVDs, although some media manufacturers offer premium optical and gold-based media that is certified for archival use.

A good backup strategy should protect critical databases, operating systems, applications, data files, wikis, blogs, instant messaging and email across all servers and operating systems. It is important, too, to have a

means to test the integrity of backed-up data to ensure working copies will be available when needed. A reporting system that collects data about the integrity of the backup as the backup is being done—and that sends alerts in the event of a failure—should be implemented. A robust reporting system that not only issues alerts when a backup fails, but also provides data regarding the cause of the failure, allows the business to readily address problems that may complicate data restoration later.

In addition to on-site electronic backups that enable quick recoveries if individual files are deleted or users are struck by a virus, provisions should be made to back up files to off-site devices. If disaster should strike, the same event that destroys primary data assets is also likely to wipe out the backups. Instead, arrange for off-site storage at a location that can be easily accessed in a timely manner.

Providing Solutions

Many small- to medium-sized companies choose Network Attached Storage (NAS) devices, such as units from the Buffalo TeraStation™ 5000N family, to provide data redundancy for business continuity and disaster recovery. The TeraStation 5000N family of storage solutions, which ship with installation wizards and software to schedule automatic backups, provides an ideal option for small offices that lack IT staffs to configure complex redundant networks and backup schemes. Commonly used as backup servers, TeraStation 5000N devices enable data from multiple computers to be backed up across a network to a central location. Additional TeraStation 5000N units can be added to a network as needed to provide high capacity storage, quick transfer rates for speedy recoveries and full encryption to ensure optimum security for data files stored in off- site locations where the business does not control physical access. TeraStation 5000N NAS solutions are available in capacities ranging from 2 TB to 48 TB.

TeraStation 5000N devices include several built-in backup features. Client software, provided with each TeraStation, enables clients to automatically backup their computers. TeraStation has a built-in feature that allows it to backup data to another TeraStation or to a locally attached USB storage device. Scheduled backups can be configured as full backups, incremental backups or differential backups. These Buffalo products also support real-time replication between one or multiple TeraStation 5000N units, making them ideal for real-time redundant onsite or offsite storage of mission-critical data.

Many offices have begun establishing “virtual” infrastructures that support redundant systems in off-site locations to shield their data resources from disaster. A completely redundant system that employees can access via an Internet connection allows work to continue in the event of an evacuation or destruction of the network. Employees can access the tools and files they need to be productive from their homes if they are unable to get to the office. Files stored on a TeraStation 5000N device are readily remotely accessible via Buffalo's web interface or via FTP. This enables the company to continue operations even when roads are impassable and employees cannot get to the job site.

Depending upon the size of the business and its IT budget, a backup plan may involve the installation of redundant systems that allow a business to mirror files and applications on a secondary system so that, if one fails, the other can continue operating with no noticeable interruption to the business. These mirrored networks essentially provide identical secondary systems that capture changes in system and data files as they are made, writing copies to the primary and secondary systems at the same time, to ensure that a fully operable, up-to-date network can always be accessed by users with little to no interruption in business activity. Enterprise backup software can be configured to automatically save a copy of every change made to data so an up-to-date copy of the data can be restored at any time.