Security Products

Prepare for the Worst

By Peter Briggs · November 2007

Businesses must focus on protecting employees, key assets and inventory

Often, when people think of business continuity and disaster recovery, they immediately focus on protecting their employees and organization's key assets, such as facilities and inventory. However, in more recent years, many have become significantly more reliant on computer infrastructures and the data that is produced with these systems. Processes have become automated and storage systems have become overloaded with critical information to run businesses efficiently and effectively. Because of this reliance on electronic information, data loss can be detrimental to any company and has become a major aspect of business continuity planning.

Data loss can be caused by many different events, from hardware or system malfunctions, human error and software corruption to computer viruses and natural disasters. Surprisingly, the most common cause of data loss is hardware or system malfunctions—with natural disasters, the most publicized cause, only being responsible for approximately 3 percent of lost data.

Statistics show that U.S. businesses lose more than $12 billion per year because of data loss. Most companies believe they are properly protected, but truth be told, a majority of small and mid-sized businesses do not have air-tight backup and recovery plans in place to protect their mission-critical data if a system failure occurs.

For a business to be sustainable, it is critical that companies take data protection seriously and ensure that applications, IT infrastructure and systems are available and can continue to operate—whether a manmade or natural disaster occurs or an employee flips the wrong switch.

Management Steps In

Data backup has traditionally been a concern of the IT department. As a non-revenue generating tool, technology professionals have often had an uphill battle selling the need for disaster recovery solutions to their management. However, today, the tables have turned. With the increase in government and industry regulations, such as HIPAA and Sarbanes Oxley, the concern is often coming from upper management or even the board of directors.

There is a significant disconnect today between what a company requires for its data protection and what its IT department has actually implemented. New regulations are requiring companies to store data for a certain period of time and keep it protected from intruders and system failures. Companies also must back up their data and ensure its availability for continued business operations. For example, SOX requires companies to have systems in place that securely, accurately and reliably manage and report corporate financial data. With so many business applications affecting the company's financial information, this regulation has an impact on most departments within a company—not just finance.

Because of regulations such as SOX, auditors also are reviewing companies' technology systems, going back to the boards of directors and advising these executives that their companies need more data and system protection. In turn, management has less tolerance for downtime and lack of availability of their systems and are putting the pressure on their IT departments to put the necessary disaster recovery solutions in place.

How is Your Data Protected?

Over the past several years, most organizations have realized the importance of backing up their data and have made it a common practice. However, most businesses that have implemented some kind of disaster recovery solution think they are 100 percent protected. Most likely, this is not the case. Backup solutions are not foolproof and are resistant to failure themselves.

For example, many companies are still using tape backup solutions, which are known to have high failure rates. They back up their data and systems on magnetic tapes and store them in a safe or at an off-site location. Tapes are vulnerable to getting damaged, lost or stolen, and this approach is difficult to administer. Also, actually accessing information on a tape is extremely time consuming and inefficient. This method typically does not satisfy upper management's business continuity requirements.

In fact, according to the Gartner Group, 34 percent of companies fail to test their tape backups, and of those that do, 77 percent have found tape backup failures.

Electronic vaulting technology is one of the more popular and reliable approaches that many companies are leveraging today to back up their data. Using the Internet to perform disk-to-disk backup, there are no tapes to transport or store, and data is encrypted and automatically transferred to an off-site data center. Once the company's data is transferred over the vaulting technology, it then regularly identifies and backs up only incremental changes to the data, making it a much more efficient process.

Backup is Not Enough

Backing up data is critical—there is no doubt. However, data that is backed up but not easily accessible essentially has no value. If a system failure occurs, and data and applications are backed up to another system or location—the recovery of that data is vital for business continuity.

There are now disaster recovery solutions that perform disk-to-disk restoration of data to standby servers, enabling businesses to be operational much more quickly than with traditional methods. With electronic vaulting, data is automatically transferred to an off-site data center, where files can be easily accessed through a standard Web browser. A typical recovery is completed in less than 10 hours, which will satisfy the requirements of most companies. Because electronic vaulting is an Internet technology, there is virtually no capital outlay, and it is easy to set up and straightforward to use.

There also are solutions that provide even more immediate access to data to suit the needs of more fast-paced businesses. High-availability solutions are typically monthly subscription fee programs that create "mirrors" of mission-critical data and systems. If a disaster occurs, the company will be able to access the replicated version of its IT environment via the Internet within a desired recovery time. Several high availability solutions offer this service in less than two hours.

Finding the best solution depends on the business and how reliant it is on its computer systems. A hospital or financial institution needs real-time backup and recovery and cannot survive without its computer systems. If a patient-record system fails, the hospital will not be able to be efficient. If a credit card system fails and customers are unable to make purchases, a financial institution will most likely lose clients, and retailers may experience a reduction in sales.

However, a manufacturer whose payroll system is shut down most likely can continue operations for a reasonable period of time before it begins to affect business. Every business is different—each has its own processes and various industry or government regulations with which it must comply. Therefore, there is no one solution that fits all. Companies need to evaluate their business and determine their own recovery time objectives to ensure sustainability.

Find a Partner

Statistics show that 60 percent of companies that lose their data will shut down within six months of the disaster. Clearly, business continuity and disaster recovery planning is not something to take lightly.

As computer systems have become much more complex, more businesses are hiring IT service providers to keep up with the ever-changing technology marketplace. There are always new and better solutions being sold and new issues that businesses must address. By partnering with IT experts, small and mid-sized businesses can focus energies on business operations that will help them grow and succeed.

There are specific companies that specialize is business continuity planning and others that perform data protection and recovery. These experts can thoroughly evaluate a business, its processes and the industry and government mandates that affect operations. They will help develop a detailed business continuity plan and determine which solutions best fit the business' needs.

About the author

Peter Briggs
Peter Briggs is the president of SafeData. He also is a member of the New England Disaster Recovery Exchange.