Disaster Recovery: Are you Prepared? (Post 9.11)

A Fortis™ and File Magic® 5 Series White Paper

About Westbrook Technologies

Westbrook Technologies' flagship document management products, Fortis, Inflo, PowerWeb and File Magic, are currently assisting thousands of customers in 40 countries streamline business processes and work smarter. Partners and customers commend Westbrook Technologies' software suite for its ease of use, scalability and strong contingent of professionals that ensure success out of our Branford, Conn.-based headquarters. For more information, contact Westbrook Technologies at 1-800-WHY-FILE or +1-203-483-6666. E-mail address: Publicrelations@westbrooktech.com.

Copyrights, Legal Notices, Trademarks and Servicemarks

Contents

Introduction

Since September 11, the IT industry has been buzzing with the term Disaster Recovery. While the concept has been around for many years, Disaster Recovery has a different connotation today. As business technology and software applications have advanced, Disaster Recovery has come to mean more than simply the ability to get your systems back online after a power outage. Companies are now expected to recover from unforeseen disasters, and retrieve contracts, memos, invoices, signatures and all other critical documents with minimal interruption. They can accomplish this with the help of an electronic document management system from Westbrook Technologies, whereby all documents can be digitally scanned and stored.

This article focuses on the concepts of Disaster Recovery, why it is important to implement a Disaster Recovery plan that incorporates Westbrook Technologies' products, and what should be done to be properly prepared in the event of a natural or man-made disaster.

There is little doubt of the importance of an effective backup plan if a natural or man-made disaster destroys your business records. Many companies, however, still have yet to implement a Disaster Recovery plan, believing that the chance of it happening to them is too slim. The reality is that an organization may declare a disaster for a number of reasons, including:

- Extreme weather conditions (e.g., Hurricane Floyd, which brought the eastern United States to a standstill in September 1999)

- Prolonged power or communications failure (e.g., the difficulties faced by enterprises and individuals in New York after the World Trade Center attack)

- Robbery or other criminal activity (e.g., the theft of credit card numbers from CDNOW and other e-commerce sites)

- Civil unrest (e.g., the disturbances at the World Trade Organization conference in Seattle in 2000 and the Group of Eight summit in Genoa in 2001)

- Terrorist acts

Research firm Gartner estimates that two out of five enterprises that experience a disaster go out of business within five years. In some cases, the disruption of normal business operations causes customers to lose confidence in the enterprise's viability. In other cases, the financial cost of recovery is simply too great.

There are several components of a Disaster Recovery plan, such as rotation of copied files to an off-site location, regular system backup, and routine testing of the backup plan. An electronic document management system such as Fortis or File Magic 5 Series is an essential element of any Disaster Recovery plan, transforming your paper into durable electronic files.

It's important to develop a basic plan for your entire company. Consider all key system components including hardware, networks, software and the key personnel that maintain these systems. Discuss Disaster Recovery plans with your IT consultants. Westbrook Technologies' worldwide Partners are available to review your business processes and determine an appropriate strategy to prepare for an emergency. In addition, Westbrook

Technologies offers customized software support contracts, last-minute on-site support, system backup consulting, Disaster Recovery plan reviews as they relate to our products, and customized administration education for key personnel.

Critical Components

By understanding the core components of Westbrook Technologies' document management systems, you can then begin to formulate how to backup the records stored there. The three core components that must be evaluated as part of an effective Disaster Recovery plan are the database, the documents, and the software.

Database

Both Fortis and File Magic support the use of multiple databases. The database is the central location where the meta, or index, data is stored. This is the data that describes the documents and is used for retrieving the documents. As the database grows in the number of records it contains, so does its value. That is, it becomes worth more due to the effort put into creating it. It is a cumulative process, and large databases can cost millions of dollars to build from a time and effort point of view.

Documents

All Westbrook Technologies products store documents external to the database. The database only stores a system field that contains a pointer to the file location on the network or storage device. Each database has a unique set of corresponding documents. Documents are uniquely numbered and automatically partitioned into subfolders for organization and efficiency. By far, the document archive becomes the largest over time. That is, a letter-sized document scanned at 300 DPI is usually between 30–50 KB. Therefore, a 1 million record database consisting of 2-page documents would require 95 GB of storage space.

Software

Fortis and File Magic are typically installed in a multi-user network environment. The software configuration is made up of program files, the system preferences, and the database engine. The program files are the executable programs that allow our products to run. System preferences are configured at the time of installation and adjusted periodically by the system administrator. They include information on In Baskets, User Accounts, Archive locations and security options. The database engine processes user requests and retrieves the requested record(s) from the database.

The Costs

Westbrook Technologies is often called upon to help salvage accounts that have no Disaster Recovery plan for their document management system. This was more common 10 years ago, when document storage took a tremendous amount of disk space as a percentage of what was typically available. Additionally, storage space was expensive. In the early 90s, the cost for storage space was over one dollar per MB. As such, only the database was backed up, and documents or images were omitted from the backup schedule.

While the capabilities of modern backup solutions have dramatically increased in the last 10 years, there are still many users that fail to properly back up their critical components. This

may be the result of not understanding the key components, or they may be under the misconception that everything is stored internally to the database. In all cases, if no backup exists or the backup is incomplete or damaged, little can be done by anyone to help recover the key system components and return the system to working order.

As stated earlier, with each document that is added to a Fortis or File Magic system, the system becomes more valuable. To calculate the system's value purely from a cost perspective, add the cost of the software, hardware, scanners and peripherals, the cost of hardware and software support, and a percentage of salary for scanner operators and personnel that index documents into the system. Be sure to include a portion of overhead for each full time person as well as employee benefits, etc.

A typical Fortis 10-user system, including three scan/index operators, will cost nearly $200,000 in the first year of operation. With this configuration, 10,000 documents per week can be captured. At the end of a year, the system will contain roughly 500,000 documents. That's 40 cents per document. Except the cost of the software and scanners, which have become inconsequential, subsequent years are similar. This means at the end of five years, the system will contain over 2.5 million documents and will be worth almost $1 million.

The Plan

As you can see, the value of the document management system becomes significant with each passing day. And users ask, how often should I back up my system? This is a legitimate question with many different answers depending on how the system is used. The simple answer is: you only need to backup as frequently as you can afford to lose. That is, if you don't mind losing a week's worth of work, you only have to back up once a week.

The *minimum* that must be done is a backup of the critical components described earlier. A simple plan would be to back up the database daily, back up the program components once a week in the full backup, and back up the document archive based only on what has been changed or added daily.

A robust backup plan would include a weekly full backup of the entire system, including the documents, and moving backup tapes to an off-site location.

A complete plan would not only include a proper backup plan, scheduled rotation, and testing of the backup once it is complete, but it would also include key elements of a Disaster Recovery plan. A complete plan should address the "what if?" scenarios. Depending on how urgently you need to access your documents, several things can be done. As long as you have an off-site backup, you could move to a new location, restore the tapes, configure the workstations and conceivably be up and running within a few days.

A quality backup solution to all key system components is essential. Without that, disaster or not, you are living on borrowed time. Every day, Westbrook Technologies receives reports of crashed hard drives, failed RAID controllers and electrical damage to servers. Whether it is a major disaster or a localized problem, your valuable database and documents may be gone forever.

In addition to ensuring your system is properly backed up, there are several steps that can be taken to make sure your system runs smoothly. They include:

Overall Network Health

Ensure your network operating system is running properly. There are a variety of software and hardware solutions that can keep the system up in the event of a problem, and they can also automatically log the problem and notify key personnel in the event of an error. Regular maintenance by qualified network administrators is a must.

Quality Components

Choose only certified and industry recognized hardware and software components. Select hardware from reputable manufacturers that is under warranty. Ensure the vendor understands the nature of the applications to be implemented on the components they provide.

Properly Supported Hardware and Software Solutions

Maintain proper support levels for each of the key system components. In this fast-paced industry, companies are bought, sold and go out of business every day. If any critical components change, be sure to replace them or update the contact and support contracts for the related products.

Proper Administration Education

Only authorized Westbrook Technologies personnel can perform installations, configurations, and system changes for our software. Our document management software is specialized and requires a different level of understanding due to its customized nature. As document management software is not yet a mainstream solution, many IT workers don't fully understand the ins-and-outs of every system. If you choose not to use authorized personnel for this task, we encourage you to enroll in a Westbrook Technologies End-User Administration course that covers the basics for administering our document management solutions. See our Web site for details on this course.

Conclusion

The best defense is to be prepared for the worst, so that nothing will be a surprise in the event of a problem. With today's technology, it's no longer sufficient to simply get your systems back online after an emergency occurs. Empower your business to recover critical records almost immediately and don't miss a beat by implementing a smart plan that incorporates Westbrook Technologies' software and services.