

DISASTER RECOVERY

JOURNAL

September 1st, 2002

Time Is Money When Recovering Lost Data

By Frank J. Real

What Is The Value of Your Organization's Data?

Time is of the essence when recovering your company's lost data. While you are impatiently waiting for your IT department to recover your data, your customers may be contacting other vendors. Just-in-time manufacturing and the global digitalization of information have put a premium on timely services, and consequentially, a premium on rapid access to digital data. Rapid access to data is a distinct competitive advantage in this marketplace. Gone are the days when a business could wait for days while their data is found, or worse, reentered into their computers. According to a Needham & Company investment analysis, a common benchmark among IT managers is that one cent of data backup is worth \$2,500 of data re-entry.

Data loss can result from a wide variety of causes, including human error, equipment failure, database corruption, hacking, computer viruses, and various other external disasters. According to a recent study by Internet security firm Riptech, corporate computer security breaches increased by 50 percent last year. In the same study, 41 percent of the companies in the study experienced "critical" attacks on their information. Systematic and cost-effective backup and archiving (storage of infrequently accessed information) of data stored on client/server networks have become essential.

How Should Backup Data Be Stored?

In the past, the most frequent protection from data loss was to back up data onto a tape and take the tape offsite for storage. In the event of data loss, a company would bring the tape back, reload it on a computer, and find the data on the tape. As all MIS personnel know, this is not as easy as it sounds. Tape backups are error-prone and labor-intensive, and still must be moved offsite for disaster recovery. Human error plays a larger role than it should in this process. People often forget to back up the data to a tape, or they are simply too busy to spend the necessary time for backup. If they back up to a tape, the tapes are usually rotated, and any virus or accidental deletion on one tape will quickly end up on all tapes.

In addition, the data on these tapes are almost always unencrypted. If the person in charge of backup takes these tapes off site, the company's proprietary data may be sitting in a glove compartment or apartment unencrypted. This is certainly not a good way to protect confidential information.

Even if data has been religiously backed up to a tape, tapes are difficult to work with in a disaster-recovery setting. The quality of tapes can erode after time, threatening the integrity of the data stored on them. They are also highly prone to environmental concerns, such as temperature and humidity. Finally, there is a physical problem presented with the cumbersome nature of tapes. Tapes and the machines that hold them take up valuable space in an office and are simply difficult to work with when the time comes to use them.

Eighty percent of recovery is simple file or folder recovery. Recovering data via tape is similar to storing needles in a haystack and then bringing the whole haystack back to locate one particular needle. Wouldn't it make more

sense to store the needles separately so that they can be recovered individually?

Example:

John, the accountant, makes a number of changes to an Excel spreadsheet he has been working on for several days. He hits the "Save" button and not the "Save As" button. Almost instantaneously, he realizes that he has made a mistake and all of his spreadsheets are incorrect. What are the possible ways to recover from this?

1. He can redo the spreadsheet but this will take a long time, and there is a risk he will make additional mistakes while reentering the data.
2. He could contact the MIS department, have them locate a tape(s), and start looking for an old copy of the spreadsheet. The old copy may or may not exist, depending on how the tapes were used and stored. Also, as is true many times, the spreadsheet may not have been backed up correctly to tape. With no standardized backup test, it is possible that this error would go unnoticed.
3. He could contact MIS, and within seconds they could recover data from an electronic vault, which has kept encrypted data offsite on a server.

The best option is point 3, recovering data from the electronic vault. The data can be recovered faster than any other methodology, and it is safer than any other system currently available. Bottom line: you are back in business much more quickly.

Electronic Data Storage: Why Now?

Several forces over the last few years have interacted to make offsite electronic data storage a viable alternative to tape backup, including:

- A decrease in bandwidth cost
- An increase in bandwidth speed
- A decrease in storage equipment cost
- An increase in labor costs

Small- To Medium-Sized Companies Missing The Boat

Large companies such as Fortune 500s have large MIS departments and millions of dollars to spend on equipment and staffing. Most of their money ends up with staffing, since it has been estimated that the cost of data storage equipment is only about 10 percent of the total costs of data storage. Personnel costs make up the other 90 percent of the cost of data storage. Data storage requires employees with expertise in the following areas: storage hardware, storage software, different software platforms, and transmission of data (telecommunications).

Ninety percent of businesses in the United States have fewer than 100 employees and do not have the expertise on staff to keep current on data storage technologies. Most companies in the United States have not put much thought into how they store their data, and more importantly, how long it would take to recover their data in the event of data loss.

What Can Small- To Medium-Sized Businesses Do?

The best solution is to outsource data storage to a company that can provide the required expertise and maintain data in a secure environment. Preferably, this company will be an outside group that has had security procedures audited by a third party.

The key data recovery issues for a company are: how quickly the company can resume operations in the event of data loss of any kind, and whether data is being adequately protected. If they were honest with themselves, most companies would not know the answer to these questions. They have no idea how long it would take

them to recover data and they have no idea how safe their data is.

How To Select A Storage Service Provider

The best way to address the issue of data storage and recovery is to contact a storage service provider. Storage service providers have the technical expertise to address these concerns. They can provide offsite data storage and rapid recovery for companies of any size.

A company should select a storage service provider that addresses its needs. The service provider should offer a rapid recovery methodology and the data must be stored in a secure environment. The storage service provider should have had a procedural audit by a third party, preferably a large auditor to ensure the security of all data. Also, it is very important to visit the storage service provider and meet the personnel, look at security features, and ask to run a pilot program to see if there is a good fit. The analysis required in selecting a storage service provider is the same as in deciding to outsource any other critical function. Do we have the expertise in house or is it more cost-effective to hire outside experts who can stay current on technological developments?

Save On Insurance

If you are looking at changing your backup and recovery process, you should contact your insurance agent/underwriter and discuss whether you can receive a reduction in your business continuation insurance. Often these premiums are based on the time needed to resume operations after a disaster. If you can shorten the recovery time and prove this to the insurance underwriter, you should get a reduction in your premium.

Conclusion

The most important criterion in your data security decision is the amount of time needed to recover from a data loss event. The reason computer data is backed up is to have it available when needed. Therefore, it only makes sense to go with a method that provides for quickest recovery and is cost effective. Offsite electronic data storage is the answer for most companies. Remember, when you need to recover lost data, time is money. Tick ... tick ... tick....

Frank J. Real is the chief executive officer and one of founders of DataGuard Group, LLC. DataGuard provides computer data recovery services for small, medium and large companies and nonprofit organizations. Real has extensive experience in tax, finance, law and accounting, with a particular emphasis in designing, structuring and implementing new business ventures for both new and on-going enterprises.

© Copyright 2002 Systems Support Inc. All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of System Support Inc. is prohibited.