[This is part of a special Disaster Planning section from the November 2006 issue.]

Among other things,
a disaster recovery plan covers the data, hardware and software critical for a business to restart operations in the event of a natural or human-caused disaster. It should also include plans for coping with the unexpected or sudden loss of key personnel, although it is not covered in this article. Rather, the focus here is on data protection.

Definitions of Disaster Recovery & Business Continuity Planning:

- Disaster recovery in information technology is the ability of an infrastructure to restart operations after a disaster. While many of today's larger computer systems contain built-in programs for disaster recovery, standalone recovery programs often provide enhanced features. Disaster recovery is used both in the context of data loss prevention and data recovery.
- Business Continuity Planning (BCP) is a methodology used to create a plan for how an organization will resume partially or completely interrupted critical function(s) within a predetermined time after a disaster or disruption.
BCP may be a part of a larger organizational effort to reduce operational risk associated with poor information security controls, and thus has a number of overlaps with the practice of risk management.

Many different risks can negatively impact the normal operations of an

- System and/or Equipment Failures
- Human Error
- Computer Viruses
- Legal Issues
- Worker Strikes

In the '80s, you might have owned a few fireproof cabinets in which to store your paper files in case of a natural disaster. In the '90s, you graduated to computer systems with electronic files such as Word and Excel files and utilized one of the above mentioned disaster recovery techniques. When the century turned, we were introduced to new technologies that were meant to consider the disparity of paper and electronic documents. This software is referred to as document management, and here are some typical questions firms should be asking when seeking a document management system:

- Storage. Where will we keep our documents? How much can we spend to store them?
- Retrieval. How can people find needed documents? How much time can be spent looking for them?
- Filing. How do we organize our documents? How do we ensure documents are filed appropriately?
- Security. How do we protect against the loss, tampering or destruction of documents? How do we keep sensitive information hidden?
- Archival. How do we ensure the readability of documents in the future? How can we protect our documents against fires, floods or natural disasters?
- Retention. How do we decide what documents to retain? How long should they be kept? How do we remove them afterwards?
- Distribution. How do we get documents into the hands of people who

need them? How much can we spend to distribute the documents?

the concept is to combine your electronic data with your scanned paper files so that all the information (say for a client file) is in one place (e-mails, spreadsheets, tax return, workpapers, engagement letter, etc.). By the nature of ending disparately stored information, you have a much easier task of considering disaster recovery on a central storage repository.

As you create a virtual filing environment for both electronic documents and scanned documents, there is the looming question of applying protection for your firm's information through redundant backup of your now central repository system. The summary below will give you a few important definitions and some good options for combining a document management system with good disaster recovery
protection.

———————————————————

Document Management & Disaster Recovery Options:
There are two types of document management systems offered in the market.

1. **Internal.** Server database and document storage is locally at your firm location.
2. **Hosted/ASP.** Server database and document storage is outsourced to reside at an outside location (should be a level 4 facility).

In either model (internal or hosted), you should have, at a bare minimum, the following:

- Mirrored Server. Protect you from hardware failure.
- Redundancy. Off-site backup.

In the hosted model, you are already accomplishing offsite backup into what

LLC in Dallas, Texas (www.Acct1st.com).

Technology