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

The world changed forever on September 11, 2001. Our inherent sense of security and stability was shaken as we watched the chaos and terror created by a small number of people as they flew airplanes loaded with passengers and fuel into buildings full of people. I doubt if the concept of disaster recovery was something that the average worker or business spent much time thinking about before that day.

On September 12, 2001, it was at the top of every corporate and small business agenda. Put down this magazine and look around at your office. Imagine all of it being gone in a flash.

A fire, a bomb or a tornado. Gone.

All of the paper. All of the computers. Everything.

Our first reaction to insecurity is to create a plan. Thus, in the months and years after September 11, 2001, a great many companies spent a great deal of money on Disaster Recovery Plans. The plans were simple in scope. Assume the total loss of your primary business site. What steps would you need to take (and how long would it be) before you could "recover" from such a disaster.

Millions watched as paper and dust flew into the streets of Manhattan as the Twin Towers collapsed. What was not fully understood was that not only did people and property cease to exist as the horror unfolded before our eyes, but entire businesses were being irrevocably damaged.

Again, think of your office. Every computer, every backup disk and CD, every

the years who said that they made backups each day and stored them in a file cabinet or desk drawer in the office. Thus, the same fire that destroyed all of the computers also took out the tapes or disks.

Let's talk about backups. Most people are lazy or casual about backups. They are diligent at first, but when they see that the time spent appears to be wasted, they go from daily backups, to weekly, to monthly to "I'm not sure when I last ran a backup."

Another great question to ask is, "When did you last test your backups?"

Have you ever gone to the vault, pulled out a tape of "Year End 2004," and verified that you could read that tape? When you upgraded your computers in 2005, did you make sure that you could still read those old tapes? Do you even know how to restore data from an archive without destroying your good current
data?

What about all of your software? Do you have all of the original licensed disks and codes? Have you been backing up programs and updates along with your data? Could you restore all software
and data to a brand new machine and get back to work? Would you have to repurchase
and reinstall software? What if the versions of the software programs that you are using are no longer being sold or supported?

Astonishingly, most people are clueless as to the complexity of the design and procedures necessary to keep your data safe via a backup process. The real disaster comes after they realize how unprepared they were.

As it turns out, the time to actually recover from a disaster in which all

What if every paper document in your files was destroyed? How would you recover?

We also should not forget one of the most critical assets that your business contains — your colleagues and employees. If the unthinkable happens (the loss of an employee), can your firm continue? Is there anyone in your office who is the only person that knows something important and necessary to continuing
operations? Are you sure that all key knowledge is spread among others? Are things documented well enough that a replacement could come in and quickly pick up the responsibilities and work of a lost resource?

A Disaster Recovery Plan should address all of these issues. You should, within hours of the disaster, begin to execute a set of planned steps to get your business running again.

1. Check the status of all of your people. If any are lost, move designated replacements into key positions via your succession plan or hire new people.
2. Activate your plan for a backup work site.
3. Arrange to have the backup tapes brought to your new work site.
4. Get enough computers and printers delivered to the new site, and bring up the network and communication lines.
5. Restore everything from the backups (software and data).
6. Regenerate all paper files from other sources (clients and storage).
7. Communicate to customers, press and community that you are coming back.

How long do you think that all of this would take?
Even a strong, well-planned, well-executed Disaster Recovery Plan could take weeks to months to bring you back to a stage where you could actually run your business. Are you depressed? Is there a better way? Are there things that small to medium businesses could do to mitigate these risks? Actually, there is.

The solution resides in a rethinking of the concept of Disaster Recovery itself.

framework in which a fault in any area can be "tolerated." What do I mean by this? Simply stated, you remove as many "single points of failure" from your operation as possible. The simplest way to accomplish this is to build two complete offices, copy all paper records and have a copy at each site, staff each site with "clones" of all of your key people, and make sure that you have two compete (separate) IT systems that contain all of your up-to-date data.

You are probably thinking that this is not a realistic scenario. Okay, I admit that the cloning of key people is a bit too far out of the box, but what about the other issues?
Building a fault-tolerant technology infrastructure was once reserved for only the largest of companies and government agencies. Just a few years ago, it would have been unreasonable to suggest that you buy a second server as a "hot" standby machine and set it up at a second facility with a separate IT staff to support it.

What has changed?
In the last few years, a large number of very high-end "Managed Hosting" companies have entered a new market. For a very small fee ($200 to $400 per month), they will provide you with a server in a 24/7 high-tech data center, manage it for you and give you access to storage as required. These centers are all over the world and can even offer asynchronous replication to other data centers (admit it, you've never even considered asynchronous replication or even used it in a sentence before).

Thus, it would be possible for you to set up your network so that all live data and copies of your programs reside not only in your office, but at a Managed Hosting site somewhere else in the world. The cost for this type of a setup

is much lower than you think and should be thought of as premiums on a "business

Take the following as an example: You prepare taxes in your office. All of the data and the software also exists on the hosted server. Overnight, a fire destroys your office. All of the data and programs are available to you the next morning via the Internet on the managed site! You could go to Best Buy, purchase a few computers and a wireless hub, and continue to do business while your office is still smoldering! You could even tell your staff to meet you at Starbucks and have a temporary office for the cost of a few Lattés.

If you also went to the trouble of digitizing each of your mission-critical papers using a scanner and an electronic file cabinet type of a product, this same fault-tolerant setup would give you access to all of the documents that are stored electronically on the managed host! Rather than having to find tapes, find a tape reader (not a trivial task), and restore key information, you would be fully operational within minutes!

This mode of operation is really part of a step toward "virtualizing" your office anyway, a trend that has existed in the market for years. By running applications and storing documents on remote servers, you will not only be moving toward a "no down time" model for business continuity, but you will enable your staff to work from home when they cannot get to the office (illness, family stuff or weather). This will even allow for the retention of key staff that might be forced to move to another city when their spouse is relocated.

As to the cloning of your people, that is still a few years off. But what you can do is document mission-critical processes and make sure that there are no pieces of your business that are only understood by one employee. By documenting
processes, you will be building both a succession plan and a business continuity process. Thus, a disaster that takes out key people will be less difficult to

recover from since you will not be losing unique domain knowledge along with

a plan. If you think that you will just work it out when a disaster strikes, think again. That is why they are called disasters!

Dr. Bodner is VP of Global Architecture and Standards for Proquest Business Solutions (www.pbs.proquest.com).

Technology