



Heinan Landa says a company whose information is not backed up might not be a company tomorrow.

All Backed Up

Disaster recovery planning keeps businesses going in face of data loss.

Maayan Jaffe
Staff Reporter

The statistics are frightening. A recent study by the U.S. Congress revealed that of companies that experience a major loss of computer records, 43 percent never reopen and 51 percent close within two years of the loss. A mere 6 percent survive over the long-term.

The question for small businesses is not how they can avoid data loss — too often they are not in control of that — but rather, what they can put in place to ensure that in the event of loss they can regain their vital information in a timely manner.

It is called “disaster recovery,” or “business continuity” planning (BCP). What that means, according to Heinan Landa, founder and CEO of Optimal Networks in Gaithersburg, is that a company assesses threats and analyzes their impact, creating plans to manage potential incidents.

When you’re talking about data loss, you are talking about everything from e-mails and documents to client,

accounting, transaction and customer tracking data, said Mr. Landa. When you’re talking about a disaster, you are talking about everything from accidentally deleting a file or e-mail to a server failure to your office burning down or even a terrorist attack.

How likely are any of these scenarios? Well, according to Dave Sobel, CEO of Virginia-based Evolve Technologies, the stats are that one in four commercial hard drives will fail within their first two years of operation. Laptop theft is becoming increasingly common. Mr. Landa said he is dealing with a client who has deleted an e-mail he wants back at least once every other day. And in his experience, out of about 60 clients, a server is down about once every two weeks.

“When people think of disaster recovery planning, they think of the grandiose, scary ones like earthquake and terrorist attack,” said Mr. Sobel. “I like to talk about those that are more likely, the minor ones — a fire in your building, theft or a hard drive

crash. Only those aren’t so minor in the scheme of things.”

Defining disaster, Mr. Sobel said, has a lot to do with the nature of the individual company. For a heating, ventilating and air conditioning company, for example, one hour of down time could cost it \$3,000 to \$5,000 in lost revenue if it is left unable to service people with air conditioners in August in Baltimore.

“And what if its customer database was wiped out?” he asked.

Backing Up

A good backup plan should have two components, said Mr. Landa. It needs to have a data recovery component and an archive component. The former is where you go to if major disaster hits. The latter is so you can quickly retrieve recently deleted e-mails or files, or find a snapshot of the server’s data before it was infected with a virus or the like.

Historically, businesses used tapes to back up their files. But tapes sometimes jam, wear out or simply don’t write the data properly, said Mr. Landa. A few years ago, information technology experts began offering disk-based backups. But disks were difficult to archive on and expensive to take off-site (which is what you want to have if your building burned down).

Then, he said, came Internet backups, which essentially allowed companies to compress their data and push it out over the Internet. This was good for disaster recovery, but it was extremely expensive (as much as \$15 to \$20 per month per gigabyte of data), and restores were slow.

However, a new combination technology recently emerged on the market that costs less and does a better job. At Optimal, they call it “dataGuard.” At Evolve, they call it “Backup Disaster Recovery (BDR) and Offsite Backup services.” But the technology is essentially the same: Via a Network-Attached Storage device, a company’s information is backed up every 15 minutes. At the same time as it’s making a local copy, it is creating a backup image to send offsite to a discreet place at night — one location on each coast. It costs only around \$3 per gigabyte per month.

“In the last nine months,” said Mr. Landa, “I’ve had 25 clients jump on this service.”

“We would be out of business if we couldn’t get our data.”

— Larry Lebow,
American Jewish Committee

Larry Lebow, IT director for the American Jewish Committee, is one of those clients. He moved the D.C. office to dataGuard and is considering implementing it in several of the organization’s other locations.

Why? “We would be out of business if we couldn’t get our data,” he said.

At Advanced Business Systems, they don’t yet use a system like dataGuard, but network technician Marcel Anton said the company has a pretty comprehensive backup system in place.

“Even if you have five pictures, you want backup,” he said. “Imagine a company that has thousands of clients. We back up every hour!”

Unfortunately, said Mr. Landa, many small businesses don’t take the time to put BCPs in place because it can require some very dedicated time on a senior level and the senior level doesn’t always have it.

The Test

Once you have a BCP, it is important to test it, cautioned Mr. Landa. He recommended testing file restoration plans on a monthly basis, server restoration plans every six months and the worst case scenario — the office is gone or you can’t get into the office — at least once, if not yearly.

Mr. Sobel told of a time he went into a local not-for-profit who was confident in its tape backup system.

“The company assured me it was changing its tapes nightly, and they were. But there was no data being written to the tapes. The backup system had not been working for at least six months,” he said. “No one had ever looked.”

It makes sense, according to the business people. And even in this economy business is good for the IT companies — “if we’re rounding into an economic recession you can afford to lose your data less,” said Mr. Landa.

But what happens if the IT company experiences disaster?

“We eat our own dog food,” Mr. Sobel said with a smile. “We use our own systems to manage our own environment.” □