Survival Planning
Are You Ready If Disaster Strikes?

93% of companies that suffer a major data loss fold within five years

By Stephenie Overman

A fire in January 2004 gave McCarty Service Systems an unwanted opportunity to test its disaster-recovery plan.

Fortunately, "We had relationships with people in the hospital industry," says CEO Bill McCarty. The reciprocal agreement meant, "We were backups for each other" in an emergency.

So when fire struck McCarty's Wood River, IL, facility near St. Louis, "We leased their plants at night. … The fire was a Tuesday night. By Saturday everyone was taken care of."

Prepared for the worst

McCarty's experience offers a primer for dealing with customers, employees, data, inventory and facilities when disaster strikes. Having a plan in place is critical—experts at a Contingency Planning & Management (CPM) conference last fall warned that four out of every 10 businesses never reopen following a disaster. Of those that do reopen, seven out of 10 close within two years.

No business can plan for every possible threat. Contingency planners advise companies to concentrate on regional threats such as hurricanes or earthquakes and on industry-specific threats, such as fire.

For McCarty Service Systems, last year's disaster was not unprecedented. "It was not our first fire. We had one in 1998," Bill McCarty says. After that, "We talked with people in the industry. Hospitals usually have to have alternative arrangements in their contracts. As a result, we were in a reciprocal agreement that helped

save the day when the second fire occurred."

After last year's experience, McCarty has a bit of hard-won advice for textile rental executives: "When you have a reciprocal agreement with someone, have your key people go over there and operate the equipment beforehand."

The company lost vehicles to the January 2004 fire, "So the first thing we did was rent trucks," he says. "The fire happened about midnight, so when employees came to work they saw they didn't

"We were able to save the computer information right away. We were able to save the hard drives and we did have backup," McCarty says. "We have a hard copy of our sales reports off premise."

have a place to work. They were notified to come back at 4 to pick up laundry."

Save data—save your company

Immediately after the fire, McCarty Service Systems received calls volunteering assistance. Companies offered desk space and an empty building for laundry sorting. There were lots of details to attend to—the empty building needed temporary heating, workers scattered at three locations had to be ferried back and forth by passenger van. Employees had to temporarily switch shifts from days to nights.

Members of employees' families worked the phones to assure customers that business would continue, he says, and delivery employees kept customers informed as they made their rounds. Consolidating the company's undamaged inventory of high-end restaurant linens was a challenge. "Drivers had some in their trucks. We were lucky we had some inventory in another building that we were able to pull and use, although some people got a larger towel for awhile," McCarty says.

Because the fire occurred in January, "A lot of our clubs were closed and we were lucky we didn't have to service them. But we were unlucky because their inventory was at our plant," he says. "A couple of places were closed for vacation and we were able to get some inventory out of there. Vendors were helpful in getting merchandise to us."

Data recovery went well, with none of the horror stories that contingency planners tell of people carefully backing up critical information—then leaving it on the premises to be destroyed along with the original.

"We were able to save the computer information right away. We were able to save the hard drives and we did have backup," McCarty says. "We have a hard copy of our sales reports off premise."

Advanced backup tools

Protecting and recovering data is critical to any business-contingency plan. Human error, natural disasters, hackers and terrorists all pose a threat in today's "always-on" business climate.

Small and midsize companies tend to think that "I don't have much data" to protect, says Bob Cramer, who spoke at the CPM conference. "But critical business data is critical business data" no matter the amount.

The questions to ask, he says, are: "How quickly do I have to recover data and how much data can I afford to lose?"

To make sure your company stays in business, you need to have assured, continuous backup with automatic, electronically based off-site protection, says Cramer, who is CEO of LiveVault Corp. And you need to be able to recover your data from anywhere, at anytime.

"The good news is that after 25 years there are now solutions that solve problems," Cramer says. "Great new technology is coming out."

Another speaker at the CPM conference, Jacob Farmer, chief technology officer for Cambridge Computer, also sees improvements in technology.

Farmer sees a trend to lessen dependency on tape "because of the

Executives who avoid preparing even the most basic disaster-recovery plan delude themselves into thinking "It won't happen to me," says Cramer of LiveVault Corp. "They think 'I never had a server crash where I lost my data, so it'll never happen to me.'"

mechanical limitations of using tape on a daily basis. The industry still regards having tape backups as a vital practice because the backups need to be both off-site and offline. The solution for smaller businesses is to back up data to a disk-based system and then to create tapes offline."

The new tools consist of disk arrays based on ATA and SATA disk drives, new backup software products, and disk arrays that have data protection functions like snapshots and replication built in. There are products like these today targeted to the small-to-midsize business marketplace, according to Farmer.

But the new solutions don't necessarily come cheap, he adds. "The trend is long term for the cost of data protection to be more than the cost of primary storage. Smaller businesses should expect their backup system to cost between half as much and twice as much as their data-storage systems."

Farmer is skeptical about outsourcing backup needs. "Backing up is one thing. Restoring is another. You must have the restoration expertise in-house or in a service that comes on-site to work for you. I would not trust that to some service over the Internet. I help

customers match needs and budgets to the right backup tools, and there are tools on the market for every size customer and situation."

Ask yourself—"What if ..."

It's Everett Griffith's job to help clients prepare contingency plans "for any catastrophe they might have." Griffith is a technical services manager with the insurance firm Haylor, Freyer & Coon, a TRSA BottomLine $ervices vendor based in Syracuse, NY, (for details, click on "member benefits" at **www.trsa.org**).

"We sit down with them and go through 'what if' scenarios. If this goes down what happens? It could be weather related, a fire, computer problems, even a medical situation," he says.

"If a business has three or four locations and one building goes down, they need to determine what they would need ahead of time. They have to find who might be able to repair equipment, whether there is another facility available they might use. Do the other plants have the capability to take on the extra work? Are there places that are easily rented? The larger they are the more they probably need a plan."

Griffith says he is especially concerned about key equipment that may take months to replace. "Many smaller businesses have only one critical piece of equipment, but that may put them down for a year. When we find we have a specialized piece of equipment we sit down with people and ask: What if? Is there another piece of equipment immediately available? How long would it take to replace the equipment?"

A related question is how easily attainable is the stock? If you are in a niche market, you must be prepared to replace supplies quickly, Griffith says.

The majority of businesses do not have disaster-recovery plans, says Griffith, so he has materials available "to take them through the process. We get most of them to take care of the basics."

Executives who avoid preparing even the most basic disaster-recovery plan delude themselves into thinking "It won't happen to me," says Cramer of LiveVault Corp. "They think 'I never had a server crash where I lost my data, so it'll never happen to me.'" Or they think a hurricane, tornado or fire won't strike.

In response, Cramer cites these statistics: 93% of companies go out of business within five years of a significant data loss and "Every state in the U.S. will suffer a natural disaster in the next two years." **TR**

Stephenie Overman is a freelance writer based in Arlington, VA.