

# SAFE

These days, computers store everything from staff schedules to patron payments. What happens if the system crashes?

| by Julie Sturgeon

# KEEPING

**P**aul Chisholm has seen it so many times before. People dumfounded that all the data their computer had been showing them just moments ago — time sheets, staff records, patron information — is gone.

“[People] think it will never happen to them,” says the CEO of Mind SHIFT Technologies in Boston. “Or, if so, they can go back to paper record keeping,” he says. “But the world is getting pretty complex now.”

And computer data is not nearly as secure as many would like to believe. A natural disaster could erase it in a nanosecond. Someone could walk out the door with a laptop or a server after hours. Even a temporary setback — say the business down the street experiences a steam pipe explosion — could separate the staff from its vital data and shut down operations for several days.

As a first line of defense, many professionals keep their servers in their own locked rooms. They also may back up the data every week, with incremental saves throughout the day and every night.

Unfortunately, not everyone is so diligent about backing up files and securing IT equipment, which could leave a facility in the lurch if the unexpected were to happen.

The procedures required to back up computerized systems and secure technology are painless and the rewards endless. Here are some issues to keep in mind when evaluating the security of your high-tech assets.

## Seeing the light

Getting companies to recognize the value of the data their computerized systems contain often is the first step in formulating a solid backup plan, experts say. In fact, protecting this data is so important that many insurance companies which carry business' errors-and-omissions policies want to see good data backup plans in action.

“The insurance companies probably won't insure you for various types of business losses incurred by not having a good backup,” says Jennifer Walzer, CEO of BackUpMyInfo.com based in New York.

Yet backing up is like insurance, says Dana Friedman, CEO of Dragonfly Technologies, a small-business computer consultancy also in New York. According to Friedman, you have to scare people with the potential loss rather than sell them on the gains.

But for the more positive-minded, backups mean you never have to say goodbye to your efforts. It's also far more affordable than bringing in a data-recovery expert to extract what they can from damaged computers, Friedman notes.

So what's the hang-up? When Walzer digs into a company's backup history, many times she gets the runaround. The owner says the controller is in charge, the controller says it's the office manager's responsibility. As a result, no one has backed up files for several quarters.

Chisholm often finds other human errors at work, too: Someone stays late to catch up on paperwork and therefore overrides the automated backup procedure, for instance.



### Storage options

The country's widespread failure to backup can be chalked up in part to the fact that computer users aren't well-educated on the topic, Friedman attests.

"People think they are prepared because they made a copy on a thumb drive," she says. Yet the size of those miniature drives alone means they are easily lost or broken, which makes them a fine choice for data transfer, but a poor option for permanent storage.

More advanced businesses prefer tape drives or disks to hold their myriad files. Consultants recognize these tools as an acceptable recovery solution, but they're quick to warn companies of the drawbacks, too. For one thing, tape corruption means 20 percent to 30 percent of backups fail, Chisholm points out, though technological improvements continually drive that rate lower.

"You really have to have the discipline in your business so that

someone comes in today and checks the files from last night to make sure it backed up properly," he notes.

Second, the data on a tape drive typically isn't encrypted. If someone steals your hardware and its customer information, you could be in big trouble for compromising credit card numbers and other financial records, Walzer reminds.

**Computer data is not nearly as secure as many would like to believe. A natural disaster could erase it in a nanosecond. Someone could walk out the door with a laptop or server after hours. Even a temporary setback — say the business down the street experiences a steampipe explosion — could separate staff from its vital data and shut down operations for several days.**

tell a computer, 'OK, restore me' because it doesn't work that way. [Aquatics professionals] are busy — they don't have time to play Russian roulette trying to restore everything properly," Walzer says.

On the other hand, in a true emergency, getting files back as

On top of that, troubles can arise if your computer has a virus. If you replicated everything onto that tape, you no longer have a secure copy to work from.

Finally, restoring that stored data to the company laptops isn't as easy as it seems. "You can't

*continued on page 16*

## CHOOSING WISELY

Like any industry, the range of services in the off-site backup and storage business run the gamut. Dana Friedman has seen most of them.

“We are approached by vendors of every shape and size, hawking every type of product or service one could possibly imagine, including off-site backup. Not only do they not offer support, but sloppy execution in the backup process,” says Friedman, the CEO of Dragonfly Technologies, a small-business computer consulting firm based in New York.

How can you avoid becoming a victim of your safety net? For starters, the quality companies still believe in human interaction. For instance, these firms will send you a monthly report and actually go over it with you, pointing out, for example, when too many employees leave open particular applications that prevent proper backups.

“I’ll tell you, 99.9 percent of online data backup companies offer no support. So, though they’re very affordable, you’re on your own to figure out everything,” points out Jennifer Walzer, CEO of BackUpMyInfo.com, which is based in New York. She suggests retailers ask these questions before signing a contract:

■ **Is my data encrypted?** It’s important that these companies give you the ability to log on any time, use a simple password and download your files in a readable format. The encryption should be on their end in case an outsider hacks into your system.



■ **Can you handle my data load?** If you’re just looking for replication of “QuickBooks” files, Word documents or the occasional spreadsheet, most places offer adequate space. If you have an exchange server for e-mail and are running SQL databases for client information, the typical consumer backup service may be over its head.

■ **Who are you?** While their Web sites may be impressive, the firms you consider to handle backing up your data should have a few credentials under their belts. Someone who started their backup business yesterday in their basement probably isn’t stable enough to entrust with your facility’s future.

— J.S.

soon as possible is key, “and so having something on site for that purpose isn’t the worst idea in the world,” Friedman says.

Others prefer an off-site backup route because it removes the data from harm’s way in the case of a natural or man-made disaster. “You should not be able to touch, feel or hug your data,” Walzer says. “Look at what happened during Hurricane Katrina. A lot of business owners backed up on magnetic tapes for the week, took them home, and lost them in the floods like everything else.”

Not to mention, electronic, off-site backups also may be scheduled in the middle of the night without human intervention.

An off-site solution is usually priced by

the amount of data you store. Smaller operations should expect to pay between \$8 and \$12 per gigabyte, which translates into \$200 to \$500 a month. The number of times you back up the information is unlimited, Chisholm says, so it’s not unusual for his clients to do as many as six daily routines, as well as one monthly and one quarterly backup.

Of course, if the advantages of tape and off-site make sense, there’s no reason you can’t choose both, Friedman says.

#### Worth saving?

A final challenge is deciding what is and is not worth backing up. Most experts agree: If it’s important to your operation, it’s worth saving.

Just don’t take the phrase “full backup” literally. For example, there’s no reason to waste gigabyte space backing up common software such as “Microsoft Word,” which exists on disks in every big-box electronics store in the country. Save your space to store the documents you created in Word instead.

But whatever you do, don’t procrastinate.

“We are relying on computers more and more today,” Walzer says. “I can’t stress it enough.”

Aquatics professionals work hard to build their facilities. “Why in the heck should they decide to skip out on protecting one of the most important assets of their whole world?” she adds. ■