



# Moving Forward, Backing Up

by Jo Day and Kevin Day

**H**er name was Susie. She worked for a mid-sized planning firm, and she had a problem. With each passing day, she noticed that data seemed to be randomly missing from their contact management system. “It’s been happening for the past week—can you help?”

I had a sinking feeling when I asked Susie about her tape backup schedule and she replied, “We use seven tapes, one for each day of the week.” I shook my head—this meant if the data had been missing for more than seven days, it was gone forever.

Susie’s company had made a mistake that a lot of planning firms make. They were thinking about their backup system the wrong way. What they really needed was to move forward with how they backed up.

There are two primary reasons for backing up your data—disaster recovery is one of them and, unfortunately, it is the one that gets all the press. Sure, if your office gets hit by a hurricane, fire or large iguana, you want to get your practice up and running ASAP.

But this is only half the story. Think about how you explain risk mitigation to your planning clients.

A spouse’s death can have a catastrophic impact on a family’s financial well-being, but the risk of that happening is considerably less than the risk of job loss or disability during a client’s lifetime. A client who thinks they are covered because they have life insurance is missing the bigger picture.

Likewise, a catastrophe that wipes out all of your data is much less probable than the primary reason to perform backups: to protect against the much more likely event of “incidental” data loss. In short, planning to

“The only thing worse than not having a backup is **thinking you do, and being wrong.**”

protect against incidental data loss is the most important thing you can do to avert disaster.

In the grand scheme of things, catastrophic data loss is easy to deal with—you know when a catastrophe has happened, and you can take steps to recover. Incidental loss, where data is destroyed without your realizing it, is much worse.

This can happen when a user accidentally (or intentionally) overwrites or erases a file. Another cause of incidental loss is when your hard drive has a hiccup that corrupts a file while you are saving it to disk. In Susie’s case, a combination of a hard drive hiccup and a backup schedule that didn’t protect against incidental loss nearly resulted in disaster for her and her firm.

## Rules to Live By

The only thing worse than not having a backup is thinking you do, and being wrong. Simply put, the last thing you want to find out when you have to recover data is that your backup hasn’t been working. Tech-savvy planners will make sure they never wind up in this situation by following a few simple rules:

**Use a backup schedule that protects you from both catastrophic and incremental loss.** A backup schedule known as “progressive cyclical backup” ensures protection of your data while minimizing the cost of backup media. This schedule uses 13 tapes and

allows you to recover data from any day in the past week, any week in the past month, any month in the past quarter, any quarter in the past year, and any year. You can download the 2003 version of this schedule from our Web site at [http://www.trumpetinc.com/Downloads/tapesched\\_2003.pdf](http://www.trumpetinc.com/Downloads/tapesched_2003.pdf).

To make it even easier to use, I keep a copy of the schedule taped to the front of the computer that runs our backups.

**Every day, check the status of the previous night’s backup.** Configure your backup system software to provide a status report each time it runs. Each day, look at the status report for the following:

- The date of the backup report to ensure you are looking at the results for last night
- Any error messages and research them
- The compressed data size against the total uncompressed space available on each tape to ensure you aren’t running out of backup capacity.

**Monthly, test restoring files from backup to a temporary location.** I talk to planners all the time who admit they have never tried to recover a file from their backup system. This is not something you want to teach yourself when you urgently need to recover data that has become corrupted. This also helps you avoid situations where a tape or disk has failed but the backup software was not able to detect it.

Document the process of restoring data from your backup system, and keep a copy

next to the backup computer itself, as well as in your disaster recovery manual (you *do* have a disaster recovery manual, don't you?).

Also, use a different tape for each monthly recovery test.

**Password-protect media.** It is much more likely that a backup will be lost or stolen than your server. I am continually surprised at how many people install security systems on their offices, but don't take steps to ensure the security of their data if a backup falls into the wrong hands. The solution is simple: make sure you use the password protection feature available in most backup software applications.

**Take media offsite every day.** To protect against catastrophic loss (I knew we'd get to catastrophic loss eventually), make sure you always have your most recent tape offsite. This may seem obvious, but it's easy to overlook, especially if you work from a home office. If your home and office are one and the same, send your backup to work with your spouse each day, and have them swap it for the previous day's media.

When taking media offsite, be sure to handle it so it won't be damaged—that is, don't put a tape or zip disk into a purse that has a magnetic clasp, and don't leave any backup media in a car that is exposed to hot or cold temperatures.

## Good Backup Options

Many different types of media are available to use for backups, and others have already written extensively about them. For a general overview of the media options available, I like the guide at <http://www.pcguides.com/care/bu/method.htm>. The only options that aren't covered at this Web site are recordable DVDs (still a young technology and probably not a viable option for another six months or so) and Internet backup solutions.

I haven't heard enough feedback from firms using Internet-based backup solutions to say whether this is a viable alternative for planners. Most of the solutions I have seen

are bundled with full-service remote administration packages that are only appropriate for firms with 50 or more employees. If you are using an Internet backup service, please let us know your experience.

While you are considering your options, make sure you can get all of your data onto a single medium. Experience shows that planners who try to save money by spanning multiple CDs or performing incremental backups ultimately pay a much higher price because they don't back up as often and have difficulty locating the exact file they are trying to recover.

Another tip: In most cases, you only need to back up data (not applications). Backing up the operating system and applications can make recovery from a catastrophic failure quicker, but catastrophic loss happens so rarely that it is probably not worth upgrading to a larger capacity backup system to accommodate it.

On a final note for those of you who are storing scanned images, the Securities and Exchange Commission in 2001 published final rules on backup and storage requirements for planners going "paperless." You can take a look at these at <http://www.sec.gov/rules/final/ic-24991.htm>.

## Why Removable Hard Drives Are Not a Good Backup Option

Prices on removable hard drives are dropping quickly, and many planners look to them as a potential backup option. Removable hard drives are fantastic for catastrophic data recovery, but fail miserably when it comes to incidental data loss. After all, if you constantly overwrite a removable hard drive with your "live" data, corrupt files can overwrite good files, resulting in lost data.

Unless you are willing to purchase enough removable hard drives to implement a backup schedule that protects against incidental loss, don't rely on these drives as your only means of backup. That said, removable hard drives are an excellent com-

plementary backup technology that can help get your business up and running quickly in the unlikely event of catastrophic loss.

## Conclusion

Susie got lucky. We found that her hard drive had started failing on the previous Tuesday. Because she called on a Monday, we were able to recover an uncorrupted version of the troublesome database file. One more day, and the file would have been gone for good.

Her firm has since changed to a progressive cyclic backup schedule, and they are much more comfortable with their ability to recover from incidental loss.

Susie was very lucky to have learned about protecting against incidental loss, without the hard lesson of losing her data. I suggest that you learn from her experience as well.



*Jo Day and Kevin Day are principals of Trumpet Inc. in Phoenix, Arizona. They provide technology consulting and services to financial planning firms via the Internet. They can be contacted at [info@trumpetinc.com](mailto:info@trumpetinc.com) or <http://www.trumpetinc.com>.*

