# BUSINESS PERFORMANCE
# ADVANTAGE

**Plus** LLC
**CFO**
Partners In Growth

*Our mission is to provide information and strategies to business owners and managers for improvement in the effectiveness of its business management so that key objectives can be realized.*

**CFO Plus, LLC**
**Ted Hofmann - Principal/Senior Consultant**
**John Morre - Principal/Senior Consultant**
**Linda Panichelli - Principal/Senior Tax Consultant**

**1450 Grant Avenue, Suite 102**
**Novato, CA 94945-3142**

**Home Office: 415-898-7879**
**Toll Free 866-CFO-PLUS or 866-236-7587**

**Email:   thofmann@cfoplus.net**
**          jmorre@cfoplus.net**
**          lpanichelli@cfoplus.net**

**Web:    www.cfoplus.net**

## Backing Up is Hard to Do

Imagine tomorrow that you go to your office, and all the computers are there, but there is nothing on any of their hard drives. If that doesn't send a shiver down your spine, just keep reading.

A survey paid for by Iomega, makers of the popular Zip drive, shows that most people don't back up their data.

*According to the survey, 41 percent of computer users do not personally back up their data. More than two-thirds (69 percent) of home computer users and nearly half (46 percent) of work computer users personally back up their data only once a month or less often, or they never back up their data.*

Iomega has a vested interest in selling Zip drives to back up your data, so the phrase "personally back up their data" gives me pause: most larger businesses rely on their Information Technology (IT) or Management Information Systems (MIS) department to back up data, regardless of where it lives.

But my gut tells me that they're not far off the mark in smaller companies where MIS/IT is the function of one person (office manager, tech guy, owner).

**A Cautionary Tale**
A well-run organization (about 30 employees) I know recently turned off their Microsoft Exchange 5.5 server (ironically, to upgrade the uninterruptible power supply for the server). When they turned it back on, the hard drive would not spin up. And, uh-oh: the backup doesn't want to restore. Off to DriveSavers *(http://www.drivesavers.com)* in Novato, California for their expert help in recovering "lost" hard drive data. Of course, that expertise comes at a price: $3,800 for a DVD containing the recovered data. A painful experience, without a doubt. Now, you might ask, "What went wrong with their backup procedure? Shouldn't they just have been able to restore the system from their last backup?" To make a long story short, in the process of upgrading other system software, the backup process had stopped working some time back, although not in an obvious fashion. The missing link here was actually testing the recovery procedure on a regular basis.

Believe me, I know how scary it actually is to test your belief that something works (e.g. unplugging the UPS from the wall while the server is live). But would you rather find out when it's just a controlled test, or when it's absolutely critical that things work as advertised? 'Nuff said.

Regardless of how many computers your business owns, a "reasonably current" copy of mission-critical data (customer data, accounting files, ...) must be stored off site. Your definition of "reasonably current" may be daily, weekly, or monthly, depending on how often you add customers or close your books. The trade-off is the amount of data lost if catastrophe occurs. If you have a single Windows computer and a decent network connection, you may want to consider using @Backup *(http://www.atbackup.com/)*. For $99 a year, you can store up to 100 megabytes (MB) of data, with convenient, automatic nightly backup and other features (500 MB costs $299 annually). This may actually be a cost-effective solution for larger groups if it avoids the cost of additional personnel. Additional benefits include off-site backup (in case the building burns down) and accessibility from anywhere (in case you need that PowerPoint presentation on your office machine). But it does require Windows (95, 98, NT, or 2000) and a recent version of Internet Explorer or Netscape to operate. This may be a great answer for your home office. The growing size of computer hard disks complicates the backup problem. For complete system backups, the only real alternative is tape. It's cost-effective and can be stored off-site. Tape comes in different formats (DAT, DLT, Exabyte, LTO, QIC, Travan, yikes!), but DAT (Digital Audio Tape) and DLT (Digital Linear Tape) are the ones you should consider. For reliability purposes, avoid QIC and Travan tape drives. CD-R, Zip drives, and diskettes are best suited to storing small groups of files.

## Backing Up is Hard to Do (cont.)

In a small workgroup situation, the best answer is to have a central file server with a tape backup unit. If you have a bunch of computers, without a network, this is one of the best excuses to add networking to your office, along with a central file server. A file server does not have to be complex: devices such as the Quantum Snap! *(http://www.quantum.com/Redirect/snap+main.htm)* are easy to install. The shortcoming of the Snap! (which surprises me), is that it doesn't have any attached backup facility - you have to back it up to another machine over its network connection.

You can set things up so that users store their work on the server (make it the default file location in applications such as Microsoft Word). Alternatively, you can use the server to automatically back up remote PCs.

I suspect that most of my readers will turn to the individual or organization that maintains their computer and network infrastructure for help with their backup policy. In that case, here are the important things to ask:
- Is our backup procedure documented?
- Do we have an off-site backup? How current is it? Where is it stored?
- Is valuable data stored on individual user computers? If so, how is it backed up? Don't forget things like e-mail folders, documentation, contracts, contact lists, and calendar data.
- Who is responsible for making sure data is backed up? Are they aware of their responsibility and what it entails? Who covers when they're away?
- Have we tested our recovery procedure? Recently?
- How do I know that backup is taking place?
- How automatic is the backup process?

For those do-it-yourselfers, you may find these articles on a painless backup strategy *(http://windows.about.com/library/weekly/aao3o2ooa.htm?once=true&)* and a ten-tape backup method *(http://www.ate.net/pages/tape_backup_strategy.htm)* useful.

In my experience, the only backup procedure that works reliably from a human perspective is one that is completely automatic. Unless their primary job is being responsible for data integrity, most people just expect to show up at work each day with things as they were left the night before. One of the biggest shortcomings of the backup solutions included with Windows is that they cannot run unattended. Veritas Software's Backup Exec is a worthwhile alternative.

I strongly encourage you to institute either a reliable, automatic backup Yes, it costs money to set up, but that cost is minor compared to what you'll pay to recover or regenerate your data, and the business you'll lose because your systems are down.
And don't forget to test that it works. Just in case.

Mike Duffy writes the monthly technology column, Tech Talk, for *Sonoma Business Magazine (http://www.sonomabusiness.com)*. His Web site URL is www.mikeduffy.com. ©2002 Mike E. Duffy & Associates. Reprinted with permission.