

# Protecting Against Bad Back-Ups

By Doug Lucy, Allegro

Published in MFG/PRO Midwest User Group Fall 2006 Newsletter.

Are your backups good? Are they good enough to fully recover your system in the event of a crash? Don't let a bad backup ruin your business. Test your backups to make sure they are as good as they need to be.

As a Progress professional services company, we receive phone calls every day from users and far too many of them go like this:

*"Hello! Our system has crashed and the backups don't seem to work. Help!"*

*"When was the last good backup you got?" we ask.*

*"Well, they were good last year, sometime, but we've tried restoring all the tapes and it looks like the script failed or the tape filled up or something. What can we do?"*

Everyone should make backups of their business-critical systems. You have to be able to recover in the event of some kind of failure. The big questions to ask are, "Are the backups you're making each night really good?" and "Are they real backups, or was the tape just spinning?" All too often, these questions aren't asked and answered until some kind of failure or loss has occurred. At that point, the answers may be painful.

## **Best practices in I.T. regarding backups are as follows:**

- Make regular backups, as frequently as necessary to avoid transaction or data loss.
- Test each backup when it is made.
- Store the backups away from the equipment they protect, preferably offsite.
- Further test these backups by completely restoring selected tapes on different hardware at least twice a year.

Making frequent backups, the first point, is important to minimize business loss in the event in which you need to restore a backup. If you are only backing up once a week and there is a failure, you may lose that entire week's transactions or data, all the way back to the point at which the backup was created. For most businesses, it is important to reduce that potential loss to just one day and therefore they make nightly, full backups. With good, tested, nightly backups, the most a business would lose is one day's worth of data. You can further reduce that loss with a good After Imaging (AI) plan.

## Protecting Against Bad Backups (continued)

Testing each backup is equally important. With so many factors going into making a valid, usable backup, testing each tape is important. Changes to scripts, passwords, drivers, as well as increases in file sizes, among many other factors can contribute to a backup “going bad” or “failing” without giving anyone sufficient notice. By testing or verifying each backup and making sure those results are delivered to a human or a notification system, you are reducing the likelihood that a backup failure will go unnoticed for months (or even years).

When we visit client data centers, we often find backup tapes stored in close proximity to the systems they supposedly protect. That is accurate when the problem is limited to a simple system crash, but in the event of a fire, sprinklers, or even theft, the backup tapes may be subject to the same loss as the servers if they are in the same place. Storing backup tapes offsite is the simple way to guard against this kind of loss. You can use services that will pickup, store your tapes quickly, and professionally or just use a simpler method such as taking tapes home.

Either way, be sure you are carefully cataloging the tapes so you know the contents of each, you are rotating the tapes using a Tower of Hanoi scheme, and you are retiring the tapes before their end-of-read-life. Additionally, you want to make sure you are following a schedule that allows you to know where each tape is in the event you need to have it retrieved.

The last point is one so many companies ignore, but that if followed, could save so many companies. Reading a backup tape back using different hardware from that which it was created, exercises the tape itself, the tape drive, the recording format, the operating system drivers, the backup software and the system administrator’s procedures. This process does not need to be repeated more than once or twice a year, but it is the best way to guarantee the validity of all components of the backup process. If there is a problem or flaw in the procedure or any component, you will discover that flaw quickly.

This will give you an opportunity to correct it long before a system crash reveals the same problem. With the extremely low cost of slightly older equipment on eBay these days, it doesn’t cost much to assemble a backup testing machine, which provides this level of assurance without spending thousands of dollars.

Backing up your data isn’t enough to guarantee you can recover in the event of a system crash or failure. We’ve had so many of these emergency calls that we’ve actually created a fixed-price semi-annual service for those companies who want to be sure they are protected. Whether you look to a third party to test your backups or you do it yourself using the above best practices, regular testing and offsite storage are the keys to reliable, quick recovery and business continuity.

**If you have any questions, please email [Doug Lucy](#).**

*Any information or materials made available to download from our website or otherwise provided to you is the copyrighted work of Allegro. Any use, reproduction or redistribution of materials from our website without expressed permission is strictly prohibited.*