

# After the flood.

## How jacked up is your back up?

By Stephen De Campos, Clear Technologies

Remember the old Bible story about Noah's Ark? I've often wondered what really happened after the flood. That is, we all remember he was prepared, but do we know what he specifically did afterward?

This Bible tale reminds me of a conversation I recently had with a customer, who was telling me about his "great" backup and recovery plan. As I listened, I thought to myself, "okay...he religiously performs his back-up and recovery duties and has a disaster recovery plan in place, but what will this guy do the day after disaster strikes if his backup and recovery files are also lost?" Put differently, how jacked up is this guy's back up plan?

As I reflected on this, I came up with a couple of tips that he (or anyone else in his shoes) should do:



**Tip #1: Plan, Plan, and...plan!** Weathering a successful disaster always starts with planning. This planning usually needs to take place months or years before an actual disaster. Moreover, thorough plans increase the likelihood of a quick and complete recovery. Planning for an IT disaster should include the following components: a) Data Backup strategy, b) Backup Infrastructure, and c) a Recovery Procedure.

**Data Backup strategy.** Your data backup strategy should define what needs to be backed up and how frequently to perform the backups, and how long to retain the data. This is a critical part of your disaster recovery (DR) plan.

**Backup Infrastructure.** Since merely having a data backup strategy is meaningless unless you have the **ability** to restore your data to a "backup server", your plan should delineate the server or infrastructure that will be used to restore your data.

This backup server can be owned in-house, or, in many cases it can be leased on an 'as-needed' basis.

**Recovery Procedure.** Last, a recovery procedure is a documented guide which will be used in the event of a disaster. The recovery procedure should include details such as, where all media are located, how to access the backup infrastructure, how to perform the data recovery, and emergency contact information for critical persons.

**Tip #2: TEST!** Once the DR planning has been implemented, the next step is to test the plan with a DR Test.

Without testing your DR plan, you will have little chance of a successful recovery after a live disaster. It is advised that all elements of your DR Plan be tested annually (at a minimum,) and that all tests, and their results be thoroughly

documented, with special emphasis on any issues encountered, and, lessons learned.

**Takeaways.** A true IT disaster is never convenient or pleasant, but your recovery can be fully successful if you employ the aforementioned tips. Failing to do so, however, will almost certainly result in a failure, which could lead to significant business impact.

**Parting words.** While a company's backup, recovery and disaster preparedness plan is unique based on their own business needs, the above tips will help you assess, document, and execute your plans so your business can be up and running as soon as possible after a disaster. Though the plan I've outlined here can be done-yourself, it may make sense for you to bring on professionals for some elements, such as offsite data recovery services and testing. Clear Technologies' services team is always available to organizations of all sizes as a resource. With affordable, annual pricing, Clear Technologies is friendly to not only you, but also your budget.