

## The 5 Ingredients of a Great Backup and Recovery Plan

Backup and recovery for your company's data is a little bit like insurance: Most business owners suddenly reach a point where they realize that what they have is way too valuable to leave unprotected. Sometimes, it's the news of a hurricane like Irene or Ike, or seeing a friend or colleagues lose their business to a disaster or theft that spurs this awareness; other times, it's just a glance at your client records. No matter what the reason, all that really matters is that they see the need for a good backup and recovery system before they actually need it.

However, even if you have decided to invest in a good backup and recovery plan there's the question of what you actually need. A good technology partner can give you a lot of guidance in this area, but here are five things you should definitely make sure to include:

- 1. Verification that the backup system is saving everything you need.** Ironically, we frequently come across backup systems that are only saving part of the company's critical data. Why? Often it's because whatever they were using for storage ran out of space, or the company acquired new technology (a second server, for example), and no one remembered to change the backup procedures. It goes without saying that these kinds of issues can lead to serious problems.
- 2. A regular and thorough testing system.** How confident are you that the data and applications you're backing up could be restored quickly? We like to perform test recoveries for our clients just to ensure that the backup systems are working the way they're supposed to. You should consider doing the same. It's a lot easier to find out you have to make adjustments *before* the future of your company is riding on the result.
- 3. Offsite data storage.** Here's another irony of backup and data recovery: A lot of businesses store their backup files in the same office or facility as their everyday technology. When something happens to the physical location, they lose everything all at once. That's why it's crucial to have at the very least, a set of your data stored elsewhere, either physically or through a cloud-based system.
- 4. Data Archiving.** If you had corruption or loss of data –someone accidentally deleted a key file, etc. and you did not notice the data was missing for a week –would you still have a copy of the data? Remember any loss is copied on to the data backup and if you are just rotating hard drives or tapes weekly, then after a week that deleted data is gone! Do you need to retain crucial project data, accounting data etc. for months or years? If so, you need to archive older data and keep it safe – on a weekly/monthly basis as needed for as long as you need to reliably retain that data.
- 5. Disaster Recovery.** Backup and disaster recovery are two different things – sometimes critically different. In the event of a disaster you can have a good copy of your data and archived copies

of your data and still be days away from recovery! To recover systems you usually need to have hardware, which is certainly a key element and needs to be planned for, but you also need all the software on your systems – operating system, applications, drivers, active directory data, all installed and configured to run just the way you need it on the new hardware, so it can run, print and fully do its job. Note that we often hear the line –“Well if something happens we’ll just pick up a server quick. ” The problem is that while that sounds plausible it is not possible in most cases, certainly it will not be feasible in a widespread disaster like a hurricane. Even in Houston there are very, very few servers available on the shelf and those that are available are unlikely to meet your needs. You can get a generic server overnight, but again it will only approximate your needs. You need a workable plan for hardware replacement.

Backup and data recovery is something a lot of people don't spend too much time thinking about, often until after something has happened to data or a server and then it is often too late.

Check with EBS to see how we can add these five elements – and a lot more – into your backup and recovery plan.