

A Pragmatic Approach to Disaster Recovery

By John Dusek, President, Convergent Storage Solutions

When we're talking about disaster recovery, a typical disaster doesn't involve a fire. In my life the typical disaster is when a CEO can't get his email because a server is down. To me, the definition of a disaster is loss of important data, loss of productivity and the loss of security. Of course a fire, flood or malicious attack is certainly disaster in my book too. It's just that often, we plan for the latter, which rarely happen. Instead, something else goes wrong that can be just as damaging to your company business.

Disasters tend to happen in groups. Many of my clients think about disaster recovery as a type of 'risk management.' Until it happens to them. What are the most common types of system disasters? Here are some we deal with all the time.

Corrupt Servers

Most corporate environments are using Microsoft Exchange server for their company email and file sharing. One of the worst things that can happen is for an Exchanger server to become 'corrupt' or damaged. This can happen because of a strange file, losing communication with a drive, or any number of things. In the computer world, we can't always explain why perfectly good servers go wrong. It just happens. When an Exchange server goes down, so does the company email system. If the company is engaged in ecommerce or is handling major transactions online, this can definitely be a real disaster.

In a typical network, there are little 'islands' of systems. These might include payroll applications, accounting and financial software, human resource systems, or sales and marketing systems. Each of these islands sometimes fail independently. Or they fail in pairs or groups. Obviously, it causes tremendous problems if a payroll system goes down on payday. Or the billing system fails the day before invoices need to be run. Again, another disaster.

Real Attacks

Almost everyone is afraid of malicious attacks. The disgruntled ex-employee who takes down the system from a small computer in his bedroom is often the scenario played out in the movies. In my experience over the past eleven years, I've really only encountered two or three of these cases. And I've literally worked with hundreds of companies. It's still something to be conscious of. If it does happen, make sure you have staff that knows how to find the security hole and fix it quickly.

Ten Steps to Safety

So what are the ways to mitigate disaster damage, whether it's the movie kind or my more mundane scenario? I give my clients ten simple steps to follow. Remember, it might not be likely that your office will burn down. But servers fail every day. Sometimes taking the most critical data with them. You can be a hero in your organization by implementing these tips. If disaster strikes, you'll be ready.

1. Design your plan around individual systems rather than one big plan. Remember the 'islands' we talked about? Try to build a series of plans that include action items for each system. It makes more sense to do disaster recovery on an individual system level. And it's easier to test each plan.
2. Plan for the 'what ifs' and work your way up to a full disaster. Remember, a system failure is much more likely than an earthquake. Figure out where the dependencies lie between your systems, and build those dependencies into your plan.
3. Document EVERYTHING. Don't make planning for a disaster a yearly event or your plan will soon be out of date and worthless. Several small plans will be easier to develop and maintain than one big one.
4. Consider working with a service provider. Sometimes, holding an outside party accountable for your disaster recovery planning and implementation will get a better result. Internal employees are often focused on day to day tasks running the business. Disaster recovery may be one of those 'nice to dos' that somehow gets put on the back burner. Until it's too late of course.
5. Schedule tests. A plan is great, but without testing it's just a piece of paper. Try to test one individual disaster recovery plan each month. Stagger tests so you're covering everything a couple times a year.
6. Document what you find in test, and update your plan. Enough said on that one.
7. Make disaster recovery planning another step in your system implementation methodology. Consider no system fully loaded until its plan has been created and tested once.
8. Offsite locations for high speed recovery are becoming increasingly popular, and less and less expensive. If downtime is not an option, the ability to retrieve data real time from another location might be a good thing to look into.
9. Take advantage of new technology. Every day, new software and hardware is made available to help disaster recovery happen faster and more efficiently. Stay on top of these solutions. They could save you money in the long run.

And finally, "Time to Recovery" is the new buzz word in our world. Everything drives that today. You must know how long it will take to recover your systems. We had a situation recently in a large bank, where it took over three days to recover a critical file. A good plan, an offsite location, and/or the right technology could have reduced that time to minutes. And saved the bank an enormous amount of problem and lost business.

Don't wait until a disaster to find out your plan is too high level, out of date or simply doesn't work. In our current business environment, system availability is key to having a competitive edge. Don't wait for the fire or flood. Remember that my kind of disaster happens all the time. You can be ready for it. It just takes a few simple steps.