10 Disaster Planning Essentials for Engineering Firms

Your data is important to your business and you can't afford to have your operations halted for days - even weeks - due to data loss or corruption. A disaster can happen at an time on any day and is likely to occur at the most inconvenient time. If you aren't already prepared, you run the risk of having the disaster hitting before you have a plan in place to handle it.

We've outlined 10 things you should have in place to make sure your business could be back up and running quickly after a disaster.

InhouseCIO

1. Have a written plan

As simple as it may sound, just thinking through *in advance* what needs to happen if your server has a meltdown or a natural disaster wipes out your office, will go a long way in getting it back fast. At a minimum, the plan should contain details on what disaster could happen and a step-by-step process of what to do, who should do it, and how. Also include contact information for various providers and username and password information for key websites.

Writing this plan will also allow you to think about what you need to budget for backup, maintenance, and disaster recovery. If you can't afford to have your network down for more than a few hours, then you need a plan that can get you back up and running within that time frame. You may want the ability to virtualize your server, allowing the office to run off of the virtualized server while the real server is repaired. If you can afford to be down for a couple of days, there are cheaper solutions.

Once written, print out a copy and store it in a fireproof safe, keep an offsite copy (at your home), and a copy with your IT consultant.

2. Hire a trusted professional to help

Trying to recover your data after a disaster without professional help is business suicide. One misstep during the recovery process can result in forever losing your data or result in weeks of downtime. Make sure you work with someone who has experience in both setting up business contingency plans (so you have a good framework from which you can restore your network), and experience in data recovery.

Writing this plan will also allow you to think about what you need to budget for backup, maintenance, and disaster recovery. If you can't afford to have your network down for more than a few hours, then you need a plan that can get you back up and running within that time frame. You may want the ability to virtualize your server, allowing the office to run off of the virtualized server while the real server is repaired. If you can afford to be down for a couple of days, there are cheaper solutions.

Once written, print out a copy and store it in a fireproof safe, keep an offsite copy (at your home),

3. Have a communications plan

If something should happen where employees couldn't access your office, email or use the phones, how should they communicate with you? Make sure your plan includes this information including multiple communications methods.

The #1 cause of data loss is human error.

4. Automate your backups

If backing up your data depends on a human being doing something, it's flawed. The #1 cause of data loss is human error (people not swapping out tapes properly, someone not setting up the backup to run properly etc). Always automate your backups so they run like clockwork.

5. Have an offsite backup of your data

Always, always, always maintain a recent copy of your data off site, on a different server, or on a storage device. Onsite backups are good, but they won't help you if they get stolen, flooded, burned, or hacked along with your server.

6. Image your server

Having a copy of your server offsite is good, but keep in mind that all that information has to be restored someplace to be of any use. If you don't have all the software disks and licenses, it could take days to reinstate your applications (like Microsoft Office, your database, accounting software etc) even though your data may be readily available. Imaging your server is similar to making an exact replica. That replica can then be directly copied to another server, saving an enormous amount of time and money in getting your network back up. Best of all, you don't have to worry about losing your preferences, configurations or favorites.

7. Have remote access and management of your network

Not only will this allow you and your staff to keep working if you can't go into your office, but you'll love the convenience it offers. Plus, your IT staff or an IT consultant should be able to access your network in the event of an emergency or for routine maintenance. Make sure they can.

8. Network documentation

Network documentation is simply a blueprint of the software, data, systems, and hardware you have in your company's network. Your IT manager or IT consultant should put this together for you. This will make the job of restoring your network faster, easier, and cheaper. It also speeds up the process of everyday repairs on your network since the technicians don't have to spend time figuring out where things are located and how they are configured. And finally, should disaster strike, you have documentation for insurance claims of exactly what you lost. Again, have your IT professional document this and keep a printed copy with your disaster recovery plan.

9. Maintain your system

One of the most important ways to avoid disaster is by maintaining the security of your network. While fires, floods, theft, and natural disasters are certainly a threat, you are much more likely to experience downtime and data loss due to a virus, worm or hacker attack. That's why its critical to keep your network patched, secure, and up-to-date. Additionally, monitor hardware for deterioration and software corruption. This is another overlooked threat that can wipe you out. Make sure you replace or repair aging software or hardware to avoid this problem.

One of the most important ways to avoid disaster is by maintaining your network.

10. Test, test, test

If you are going to go through the trouble of setting up a plan, then at least hire an IT professional to run a test once a month to make sure your backups are working and your system is secure. After all, the worst time to test your parachute is after you've jumped out of the plane.