NetworkTitan

The 10 Disaster Planning Essentials For Any Small Business

If your data is important to your business and you cannot afford to have your operations halted for days – even weeks – due to ransomware or unexpected data loss or corruption, then you need to read this report and act on the information shared. A data erasing disaster can happen at any 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 no plan in place to handle the disaster. This report will outline 10 things you should have in place to make sure your firm could get back up and running quickly in the event of a disaster or ransomware attack.

1. **Have a written plan.** As simple as it may sound, just thinking through, *in advance* of what needs to happen if your data and communications networks have a "meltdown," will go a long way in getting things back up fast. At a minimum, the plan should contain details on what types of disaster could happen and a step-by-step process of what to do, who should do it and how. Also include contact information for your various providers and login credentials for those key web sites. 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. If you can afford to be down for a couple of days, there are cheaper solutions. Once written, store a hard copy in a fireproof safe, an offsite copy (at your home, for example) and a copy with your IT provider.

2. **Hire a trusted professional to help you.** 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.

3. **Have a communications plan.** If something should happen where employees can't get to the office, can't access e-mail and the internet or can't use land-line phones, how should they communicate with you? Make sure your plan includes this information including MULTIPLE communications methods.

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. 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. **Have remote access and management of your network.** Not only will this allow you and your staff to keep working, but you'll love the convenience it offers. Plus, your IT staff or an IT provider should be able to access your network remotely in the event of an emergency or for routine maintenance. Make sure they can.

7. **Image your server.** Having a copy of your data offsite is good, but keep in mind that all that information must be RESTORED someplace to be of any use. If you are using older or proprietary software and you don't have the original disks and licenses, it could take days to re-establish your applications (like your time management software, accounting software, etc.) even though your actual 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. Best of all, you don't have to worry about losing your configurations. To find out more about this type of backup, ask your IT professional.

8. **Network documentation.** Network documentation is simply a blueprint of your software, data, systems, hardware and devices in your firm's network. Your IT manager or IT provider should put this together for you. This will make the job of restoring your network faster, easier and certainly less expensive. It also speeds up the process of everyday repairs on your network since technicians don't have to spend time figuring out where things are located and how they are configured. And finally, when disaster strikes, 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.** The most important way to avoid disaster pitfalls is by maintaining the security of your network. While natural disasters are certainly a threat, you are much more likely to experience downtime and data loss due to a virus, worm, hacker or ransomware attack. That's why it's critical to keep your network patched and up-to-date. Additionally, monitor hardware for deterioration and software for corruption. This is another overlooked threat that can wipe you out. Make sure you replace or repair aging software and hardware to avoid this problem.

10. **TEST, TEST, TEST!** A study conducted by Forrester Research and the Disaster Recovery Journal found that 50 percent of companies only test their disaster recovery plan once a year, while 14 percent never test. If you are going to go through the task of setting up a plan, then at least hire an IT pro 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.

Want help implementing these 10 essentials? Call us to discuss what your firm needs to be well prepared if, or when, disaster strikes.

Network Titan 619-255-2621