10 things you should do before disaster strikes

Takeaway: Organizations that isn't prepared when disaster hits may never get back on their feet. Take these steps to minimize losses and make a quicker recovery.

Disaster will strike. It's not a matter of IF; it's a matter of WHEN. People often say, "Yeah, I need to plan for that." But life gets in the way. And when life continues to get in the way, and you've failed to prepare for disaster, disaster will take you down. Instead of just sitting around and waiting for it, why not prepare for it? Here are some things you must do to be ready for a disaster.

1: Get a good battery backup

I know, I know… what is a battery backup going to do to help when disaster strikes? Here's the thing. A good battery backup could mean the difference between getting *some* data and getting zero data. Let me give you an example. We recently had a client that lost power to their building. Things started to escalate and it looked as if everything was going to get tragic fast. But I was able to remote into the machine and get a backup running immediately. Because of that battery backup, I was able to get in quickly and avert a total loss.

2: Start creating nightly data backups

This goes along with the previous step. Without backups, you are completely lost. No backups, no data. Making regular, reliable backups is the single most important thing you can do to prepare for a disaster and you need more than just a backup to an external drive. You need an offsite backup as well. As long as you have data, recovery is always a possibility. Make sure those backups are nightly and make sure they succeed. This is NOT a set it and forget it affair.

3: Start creating weekly full images

Full images are just as crucial as data backups. Why? Some backup products will allow you to take that backup image and load it on dissimilar hardware. (Acronis ABR with Universal Restore is one such product.) That is one of the fastest routes to recovery. Just make sure that you have a recent image (at least weekly) or else restoring that image is only going to land you with an out-of-date system.

4: Document server and client applications

One of the problems with recovery is knowing what software is on what system. Do yourself a huge favor and document all the software that is installed and used on your system. In fact, take this one step further and document the versions of each piece of software. Know as much about your system as possible, and don't rely on your memory for this.

5: Check the status of RAID arrays

I can't tell you how many times we've had clients come in with failing RAID arrays. Their array is on its last drive and that has failed. Simple solution. Had they monitored the status of their array and replaced it, they wouldn't be in a situation where the array couldn't be saved. RAID should not be looked at as a backup solution (though some seem to think that's its purpose). It is crucial that RAID drive status be monitored at all times to prevent disastrous levels of loss.

6: Rotate backups offsite

What good are those backups if they burn up in a building fire? Sure, you can place them in a fireproof safe, but why take any chances? Set up a system for rotating your backups weekly (at least) offsite. In fact, if you really want to be safe, have a set of three external drives. At all times, you'll have one working, one in a fireproof safe, and one offsite. Although this will require you to rotate them more frequently (to keep each backup from going stale), it will ensure that you always have a backup available.

7: Document the network

Your documentation shouldn't stop at software on servers and clients. You also need to document your network. Know what you used, how you used what you used, the address schemes, and security measures. With this documentation handy, your network will be much easier to recover. And make sure you do the documentation right. Use diagrams as well as descriptions. Make sure the documentation is clear and thorough enough to enable any network admin to re-create your network as quickly as possible.

8: Have an offsite failover for your Web site

It's great to have all these backup plans. But if you're faced with disaster and you depend upon your Web site for revenue, you need an offsite failover so that if your onsite server is out of commission, you can easily switch over to the offsite version. When you set this up, make sure that you have the sites set up to regularly update so you’re not switching over to an out-of-date server.

9: Relocate your software offsite

You have purchased all that software. And unless you’re like me and use only open source software, the cost of that investment is significant. Do yourself a favor and relocate all the installation media offsite. Better yet, burn copies of that data and store the originals offsite. That way, should disaster strike, you won’t have to spend days tracking down all the installation media to get yourself back up and running. While you’re at it, make sure that all install keys are stored with the media.

10: Develop a solid recovery plan

And finally, you must have a plan to go along with disaster. When the inevitable does finally strike, you need to know how to react. Every second you flounder piles onto the disaster. Make sure that you know exactly what to do immediately. And make sure that your plan is laid out, step by step, so that panic doesn’t get a chance to take over.

Other measures to take?

Disaster will happen. There’s hardly a way to avoid it. But you can at least be ready for it and take steps that will make recovery easier. What other emergency preparedness practices do you recommend? What preemptive measures have helped you bounce back from a disaster?