DISASTER **RECOVERY**

Published January 23, 2017

Too many companies aren't prepared to handle a disaster or business continuity event. Rather than putting it off indefinitely, companies need to make an effort to get a disaster recovery plan in place. The list below offers a series of steps that can be taken to reinforce the ability to bounce back from anything that may become a disaster – whether it's a broken water pipe or a full-blown natural disaster.

1 **Protect your data.** If you don't have your data, it's all over. Even if you don't have a formal recovery plan, backing up your data is one of the quickest and easiest ways to protect your coop. There are now backup appliances available from over a hundred vendors that allow you to save your data every 15 minutes or so, with one appliance on-site and another in a remote location, for a relatively reasonable price. Companies can also save their data in the cloud, either through dedicated backup providers, or through individual cloud-based software applications. Companies might consider a mutual aid arrangement, where two companies in different locations host backup facilities for each other.

Whatever your method, you'll want to make sure that you're backing up everything at your company, from individual PCs and portable devices up to multi-location networks. And picking a method is only the beginning. You need to test it on a regular basis. This can range from spot checks to see that individual documents have been saved, up to full "bare metal restores" of all of your data and applications.

Without double-checking the backups, firms may find themselves in the same shoes as the accountant who provided a favorite quote about a failed system: "Our backup was working perfectly – we just can't restore from it." Until the backups are restored, you won't know if you have data or not.

2 **Write the plan.** Get something in writing – if it's not in writing, it doesn't exist. A number of companies were able to weather the 9/11 attacks because they were able to dust off and execute disaster recovery plans that they had set up for Y2k.

There are variety of sample Disaster Recovery plans available online, but as part of the process you should review the critical elements of your business and diagram your workflows (most firms have around 40). Once you know what your company looks like pre-disaster, you can start deciding which operations you need to have back in service first -- not all emergency restorations will support 100 percent of company operations right away. Have a categorized list of what you'll restore first, second and so on. It's better to decide this when you're not in the heat of battle.

As part of your plan, you'll want to know where licenses, product key information and user policies are stored, and have an inventory of all systems, workstations and storage devices. This will be valuable for a variety of purposes, not least for insurance claims: Unless you can document what you had, the insurance policies won't come across.

You'll also want lists of employees, customers, vendors, as well as critical contracts, certificates and policies – and you'll want them printed out, because in many cases you may not have power.

3 **Have a risk management officer.** This person will be responsible not just for taking the lead in the event of a disaster, but also for keeping the plan up to date and making sure everyone's trained and ready to execute. It is recommended that it not be your controller or chief technologist.

4 **Create an emergency response team (ERT) and assign specific responsibilities.** If your company has multiple locations, you'll want to have people at each location who can handle those responsibilities. It is important to emphasize the importance of training and education: You need to train your ERT. The top fault in companies is the lack of training. You can never have too much extra training on the Emergency Response Team, so they know what to do.

Among other things, a group of people need to know how to handle a data restore.

5 **Test and revise the plan on a regular basis.** Besides frequent tests of your data backup, there needs to be a quarterly read-through of the overall disaster recovery plan, an annual physical test, with a debriefing afterward so you can fix what didn't work and be ready for the next time.

In the end, the important thing is to get started. Many people have had this on their calendar for a long time, but it keeps getting pushed aside. You can do a really simple plan or a really complex plan – the one that doesn't work is the one that doesn't get done.

(Source: AccountingToday - Accounting Technology - October 30)