certus technology group

DR solutions

www.certustg.com/connect

DR solutions

What is disaster recovery and why is it important for your business?

It's easy to dismiss disaster recovery as something that only large businesses like banks and multinationals need to worry about. But, it's **something all businesses should think about, whatever their size**.

Of course for smaller companies the 'hot site' options employed by bigger businesses, allowing them to quickly switch to alternative systems in the event of a problem, are unattainable. But that's not to say that there aren't more affordable options that can help your business survive anything from a significant cyberattack to a natural disaster.

Putting a disaster recovery plan in place

The first step on the route to developing a disaster recovery strategy is to have a plan. In its simplest form, this will simply be a case of documenting where your backups are and who is responsible for retrieving and restoring them.

The bigger the business, the more complex the plan will become, as you need to have provision for finding alternative accommodation, sourcing new equipment, getting communications up and running, and more.

You need to understand where your systems are. For example, what is run and stored internally and what is in the cloud?

Just because something is in the cloud doesn't mean you can ignore it from a business continuity point of view. You need to consider how you would access it in the event of a disaster, but you must also plan for what would happen if the cloud provider itself were to have a problem. Do you have online backups of your data elsewhere?

Making a disaster plan also involves deciding the relative importance of different systems. Which are essential to your operation and need to be retrieved quickly and which are less vital and can be left for later?

The amount of data you have comes into play here too. The more files you have, the longer they will take to restore. You will want to think about how you structure the retrieval.

You need to think about the type of disaster you might encounter. Immediately we think of fire or perhaps cyberattacks, but what about other things?

Flooding, for example, can be devastating and if your company is in a vulnerable area, you might want to think about moving to reduce the risk. Think about other problems beyond your control: Power outages, theft, vandalism, or even one of your major suppliers experiencing a disaster that prevents them from fulfilling their commitments to you.

As your plan grows, it needs to take account of who is responsible for various aspects of the recovery process too. You may want to think about making specific individuals responsible for different parts of the process. In doing so, however, you must make sure they know what their responsibilities are and have the appropriate training and resources to carry them out.

However, having a plan is only part of the picture, it's vitally important to keep it up to date. A plan that's out of date is just as useless as having no plan at all.

Online and offline backups matter

At the heart of all disaster recovery solutions is an online cloud backup. Software and data are the lifeblood of your company's systems, so you need to have up to date copies should you need to restore your systems.

It's **essential to have a structure to your backups too**. If you backup to the same external disk each week and only discover a virus infection after you've done your latest save, then your backup will be infected too. It's important to have structured backups so that you can go back to an earlier version if required. The **'grandfather, father, son'** approach where you have three generations of saves is one of the most common ways of doing this.

You may take daily backups of your most crucial production data, but other information can be saved less often, perhaps once a month or once a week.

This helps to reduce the amount of storage space needed for each save. You still need multiple generations of backup at each level, however.

Where you keep your backup is important too. It's going to be of little use if it's next to the computer and the equipment gets stolen, or the building burns down. Even if they're in a fireproof safe, you may be unable to access the building to retrieve them in the event of a disaster. It's therefore **essential to have a backup stored off-site**. If your business has multiple locations, you can take the data to another office, or often IT staff take backup drives home for safe keeping.

The cloud for their day-to-day backups. This automatically solves the off-site problem. However, you need to choose the supplier carefully. Make sure you trust them with the security and safety of your data and ensure that how and where the information is stored meets your compliance requirements. Even if your primary backup is in the cloud, it's still a good idea to take a belt and braces approach and have a local backup too. This doesn't have to be done on the same frequency, but a backup to an external hard drive – taken weekly or monthly – is a useful fallback.

Business continuity communication solutions

So far we've concentrated on looking at computer systems, but there are other things that your disaster planning needs to take into account. Primary among these is communication. If your business can't operate normally for a time, it's essential that you can let your customers and suppliers know what's happening.

If your building is out of commission, you can arrange for a service to divert incoming calls to another number so that your business contacts can still reach you. If you have a **hosted telephone system**, it's relatively easy to redirect calls to other numbers or mobiles.

Of course, you need to be able to contact your staff too – whether it's to bring critical employees in or tell others to stay at home. Make sure you have an up to date list of contact details with landline and mobile numbers plus email addresses.