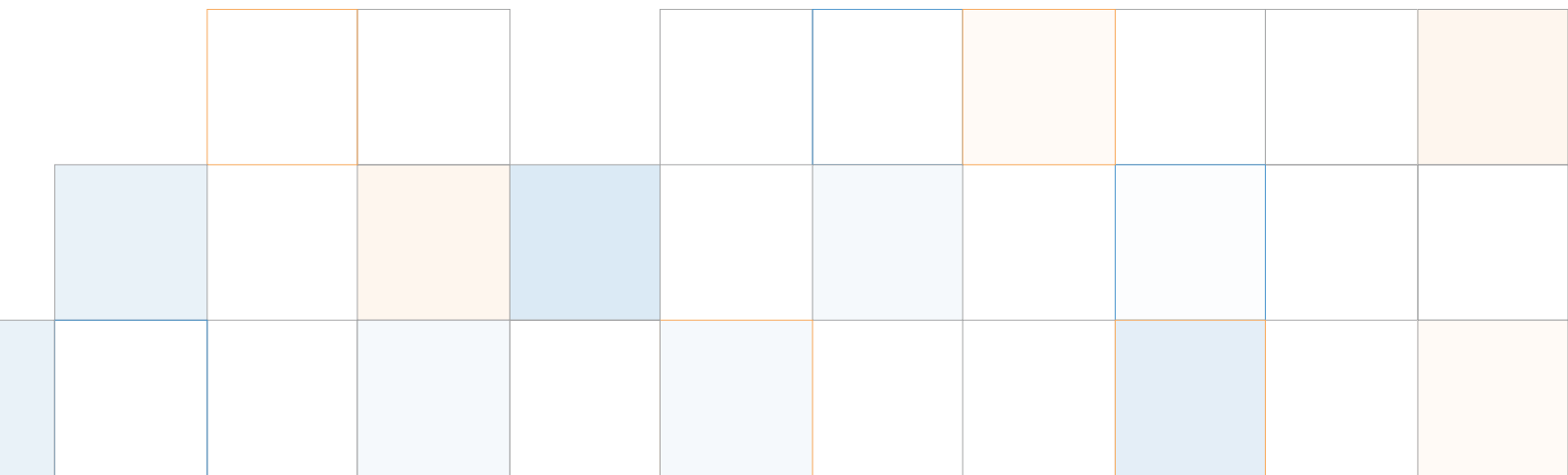




articles



Types of Disaster Recovery

Types of Disaster Recovery

Business continuity and disaster recovery are the processes and procedures that return your business systems – hardware, software and data – to full operations following a natural or man-made disaster.

As businesses increasingly rely on IT for their mission-critical operations, it is essential to have plans in place to ensure your business viability is not at risk from a critical incident. Here, we look at a few different levels of data recovery:

- *No disaster plan at all*
- *No disaster plan, but good backup procedures*
- *A disaster plan, with no resources in place*
- *A 'cold site' disaster recovery solution*
- *A 'split site' disaster recovery solution*
- *A 'warm site' disaster recovery solution*
- *A 'hot site' disaster recovery solution*
- *What level of protection is right for you?*

No disaster plan at all

Despite the risks, millions of businesses globally have no formal business continuity or disaster recovery plan in place. Should a disaster occur, panic and confusion tend to be the result and timely recovery of data, software and hardware is not possible. The chances are very high that these businesses will never recover.

A simple server crash, equipment failure, power surge or human error is all it takes for a critical database to be wiped. Fires, floods, viruses, unauthorised users or hackers can play havoc with your entire business systems. Unlike hardware or software, data is an even more valuable asset that cannot be replaced.

If you work in a company which has an IT department that does not plan for disasters, then it is absolutely essential that an effective plan is developed before it is too late. Fortunately there are many reliable and cost-effective solutions available to safeguard your business.

No disaster plan, but good backup procedures

The absolute minimum companies must do – even the smallest business – to prevent a disaster from wiping out business information is to back up the data on your computers daily and store the backups offsite at a secure archival company. Never store it at employee's homes.

That way even if your hardware and software is ruined, you can still replace it and load it up with all your irreplaceable data. If your IT department is not making good backups of at least the critical systems at least every single day, then it is simply not doing its job.

Another important thing to remember about backups is that they must be tested regularly to make sure they are working. Nothing is more frustrating than to need a backup and find that the data is corrupt or non-existent.

Another smart and reasonably simple step is to build fault tolerance into all of your critical systems. This means installing RAID drives – disk drives which are redundant copies of each other – clustered systems and other types of local recovery procedures that at least provide an extra layer of protection.

A disaster plan, with no resources in place

Once you have a good backup and archival procedure and your critical systems are fault tolerant, the next step is to put together procedures for remote disaster recovery. This simply means you ask and answer the question, “What do we do if the computer center is utterly destroyed?” You might, for example, make arrangements with another division or company to share equipment and space if either is struck by disaster. Agreements need to be made with critical computer vendors to quickly ship new systems in the event of an emergency. This kind of planning is a good first step, although recovery would be slow in the event of disaster so you need to be sure your business can afford a few days of downtime if required.

A ‘cold site’ disaster recovery solution

A simple yet effective business backup solution, a cold site is simply a reserved area on a data centre where your business can set up new equipment in the event of a disaster. This is a popular disaster recovery method because it tends to be less expensive than other options, yet still gives a company the ability to survive a true disaster.

If you outsource your disaster recovery to a third party, then odds are they will establish this form of disaster recovery solution. This will work as long as your planning is good, your backups are sound and your documentation is excellent. Of course, extended downtime in the event of a disaster must be acceptable for a cold site to be a valid option. Plan on 24 hours for critical systems and as long as a week for less important functions.

A ‘split site’ disaster recovery solution

If your organisation is large enough, it may be feasible to house the IT department across more than one location. In the event of a disaster to one site, operations can then reasonably simply shift to the other site and any new equipment needed could be purchased as necessary as long as the backups were properly maintained. The advantage to this method is it eliminates the need for the major up-front costs of building a dedicated disaster center.

As your organisation will need to purchase or lease the equipment in the warm site, this option does involve more set-up costs than a cold site, but has the advantage of being able to get your business systems up and running much faster. Even sites with multiple applications can generally be back to full operation within 24 hours.

A 'hot site' disaster recovery solution

A hot site is a premium level of disaster recovery where the business IT systems and up-to-date data are duplicated and maintained at a separate data centre. In this scenario, a duplicate computer center is set up in a remote location with communication lines set up and actively copying data at all times. The site has a duplicate of every critical server, with data that is up-to-date to within hours, minutes or even seconds. At the highest level it even has desks, phones and whatever else is necessary for operations to continue if the worst happens.

Following a disaster, your business can very quickly 'switch' to the hot site with minimal disruption. This is the ultimate in disaster preparation, reserved for companies with excellent management and highly skilled IT staff. Hot sites are expensive, difficult to set up and require constant maintenance, but in the event of a disaster operations can continue with a minimum of downtime. [This is a popular option for institutions such as finance companies and stock exchanges where downtime is not an option.](#)

What level of protection is right for you?

Before determining exactly what business continuity and disaster recovery plans you need in place for your business it is essential to analyse your systems, data and requirements and develop a solution that cost effectively meets your needs today and into the future. TRT's specialised data protection strategies and solutions are all about finding the most efficient and cost effective way for your IT department to achieve the appropriate recovery objectives.