**What is Disaster Recovery?**

Disaster Recovery is an important process that organisations of all sizes implement to ensure the rapid recovery of applications, data and hardware that are critical to business operations in the event of a natural disaster, network or hardware failure or human error.

**The main role of a disaster recovery plan.**

A Disaster Recovery plan is used to quickly restore IT assets to ensure business continuity. However, successful Disaster Recovery requires vital planning and manpower to carry out the steps necessary to achieve recovery.

Disaster Recovery plans are typically part of a more extensive initiative which is commonly known as Business Continuity Planning.  After a thorough review of business procedures and planning, disaster recovery plans are well rehearsed so everyone is familiar with their role should a disaster suddenly occur.

**Practice makes perfect.**

Your business should also ensure that the DR plan is routinely updated to accommodate new staff members, hardware and software modifications or expansion to a branch office, to name a few examples.  The DR plan should also be routinely practiced to ensure everyone knows their role in recovery and remains on the same page, so to speak.

**Ensuring your data remains secure and compliant.**

Disaster recovery (DR) also plays a significant role in the level of security for your small business. Part of your strategy is to implement security planning into disaster recovery to ensure your data remains secure and in compliance with your specific industry. This part of the planning also provides you with the peace of mind that critical business functions can be recovered quickly after disaster strikes.

**In a nutshell.**

Disaster recovery is a solution that ensures your small business will continue to operate as close to normal daily operations as possible. In addition to planning, the disaster recovery process also involves testing and accessing a separate physical site at a distance to restore critical business function.

**Hardware or Network Failure.**

Hardware and network technologies are never 100 percent fool proof regardless of how modern or technologically advanced they are. What would happen if your business experiences a hardware or network outage?

**Human Error.**

Like technology and software, humans are not perfect when it comes to performing daily business functions.

Humans make mistakes, accidentally delete data, and forget to save data before a crash occurs or overlook an important step that leads to data loss.  It happens to all of us at one point or another.

If you have a disaster recovery plan in place, you can use incremental backup technologies that ensure you can restore the data to its original state. Deploying firewalls, anti-malware and antivirus solutions is only one part of the entire security scope.

Normally it would be costly to deal with the disruption and data loss. However, having a disaster recovery plan in place with an IT disaster recovery service provider, you can eliminate this risk at an affordable rate.

**Virtual Machine or Application Failure.**

Like hardware, virtual machines and software applications are not 100 percent fool proof. What would you do without access to software that performs critical business functions and staff access to virtual machines? How would you restore your organisation to normal business operations following a disaster?

Investing in manpower and technologies that address any failure in IT infrastructure can be costly in terms of IT capital expenses.

The only affordable way to avoid disruptions and application failure is to work with a disaster recovery service provider that can oversee data backup and ensure the proper data center technologies are deployed to help you to quickly restore operations. The service provider will also monitor the infrastructure as part of your contract to immediately detect any problems that may occur.