

Improving Your IT Resilience

As organisations have become increasingly dependent upon the uninterrupted operation of the machine to support mission-critical business processes, they have also become more vulnerable to various disaster potentials that can interfere with the normal operations of their IT infrastructure.

Disaster Recovery (DR) planning is about business survival. It is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organisation following a natural or human induced disaster.

It is a subset of the much larger process, business continuity planning and should incorporate planning for resumption of hardware, communications (such as networks), applications, data and other IT infrastructure.

The creation and maintenance of a sound disaster recovery plan, is a complex undertaking that involves the following series of steps:

- ✓ Risk Evaluation
- ✓ Business Impact Analysis
- ✓ Strategy Development
- ✓ Disaster Recovery Plan (DRP) development
- ✓ Plan Maintenance and Testing

Advantages of Disaster Recovery Planning

The key objective of DR planning is to minimise the impact that an event will have on the business. The advantages can be numerous, touching on many aspects of the business including:

- ✓ Provides capability to maintain or resume operational trading
- ✓ Minimises downtime
- ✓ Increases confidence of business associates, shareholders, stakeholders, clients and suppliers

- ✓ Prevents loss of customers to competitors due to inability to trade
- ✓ Safeguards against business reputation, brand and image
- ✓ Lessens the cost of recovery and risk of business survival than if your organisation doesn't have a plan.

The DRP is what an organisation needs to turn to if there is a disaster or other serious incident.

Hopefully, you will never have to use it, but if you do, it can mean the difference between the loss of your organization and its survival. It is therefore absolutely critical that the DRP is workable and that it is of sufficient quality to guide your organisation through the crisis.



"A company denied access to mission critical data for more than 48 hours will be out of business within one year."

Source: www.drplanning.org

Want to know more?

Please contact us.