



DISASTER RECOVERY AND BUSINESS CONTINUITY

The terms are used interchangeably and bantered about as though they mean the same thing. But the reality is different. They are very much different things and individual plans need to be in place for both.

FOCUS

Disaster recovery is all about preparing. Preparing for something which may never happen but while adopting the processes, the organisation operates in a secure, resilient environment.

Although different, one shouldn't exist without the other. Every organisation has to think the unthinkable, that one day people may turn up to work and for some reason they can't work. What happens? The business continuity plan is put into action and as part of this, the disaster recovery plan is executed to allow the Information and Communications Technology (ICT) systems to perform as they should in a normal working environment.

WHAT'S BUSINESS CONTINUITY?

A business continuity plan covers all functions, departments and personnel in a business. Incorporating plans for practical things such as location of people if the office becomes unavailable for some reason, business continuity can be thought of as the top level plan which states how the business will physically continue if buildings and resources have fallen prey to a disaster of some sort.

WHAT'S DISASTER RECOVERY?

A disaster recovery plan forms part of the business continuity plan. It addresses the ICT side of the organisation outlining how systems will recover and operate in the event of a disaster. This disaster recovery plan must take into consideration the practicalities of the business continuity plan, supporting them completely.

CONSIDERATIONS FOR DISASTER RECOVERY

Drawing on the guidelines in the business continuity plan, the disaster recovery plan should cover a number of key areas. There will always be some considerations which are specific to each organisation, but in general the following main areas need to be addressed:

- **Backups** - preventing loss of data
- **Mirroring** - replication of systems
- **Virtualisation** - facilitating rapid recovery
- **Clustering** - distributed architecture with no single point of failure
- **Security** - protecting people, systems and data

When developing a disaster recovery strategy, our focus is on assessing the main risks to the organisation. While natural disasters occur, malicious actions and risks can be minimised and our aim is to design solutions which prevent the loss or corruption of data. We follow a series of steps to allow us to develop the best disaster recovery solution to address your specific risks:

- Step 1:** Analyse the existing infrastructure
- Step 2:** Assess data and identify access controls
- Step 3:** Evaluate IT and data processes
- Step 4:** Identify areas of risk and the impact of a natural disaster or malicious action
- Step 5:** Design a solution to address weaknesses
- Step 6:** Implement the solution and establish a continuous assessment cycle

THE PRACTICALITIES

The processes put in place to enable quick recovery from disaster, all work towards adopting best practice across the business. It doesn't always take a disaster to interrupt the day to day business in an organisation. In fact, in most organisations the threat from internal staff far outweighs the threat from anywhere else. And it's not always the case that internal threats are malicious, security breaches can be accidental if untrained users are allowed access to systems they don't need or understand. So, adopting some practical processes and procedures all help towards operating in a secure, protected and efficient environment:

- Take regular backups of critical information - either hourly, daily or whatever is deemed necessary. It may be the case that different types of information need different back-up schedules. For example, financial and transactional information probably require more regular back-ups than personnel information
- Always consider disaster recovery when reviewing new solutions and build resilience into these solutions at the beginning to simplify the disaster recovery plan
- Write and implement a security policy to identify and address specific threats. Train personnel on areas which are pertinent to them and put solutions in place to protect them, the data and the organisation

- Encourage the organisation to consider disaster recovery as a strategic issue and ensure that the plan supports this completely

Disaster recovery planning is a continuous process which needs regular reviewing. As things change, this needs to be reflected in the disaster recovery plan. As the saying goes, fail to prepare, prepare to fail... Disaster recovery is all about preparing. Preparing for something which may never happen but while adopting the processes, the organisation operates in a secure, resilient environment, and that only helps towards achieving cost and productivity efficiencies for everyone.

BENEFITS

Always consider disaster recovery when reviewing new solutions and build resilience into these solutions at the beginning to simplify the disaster recovery plan.

