DR 101

WHAT IS DISASTER RECOVERY?

BUSINESS CONTINUITY (BC)

All of the processes and planning required for keeping every aspect of your business functioning in the midst of disruptive events. Business Continuity planning includes making critical contingencies for people and business processes.

DISASTER RECOVERY (DR)

A subset of business continuity that details a plan for bringing key IT resources (the technology that supports the business) — both data and systems — back online after a natural or human-induced disaster.

SOLUTIONS

Backup

One of the many options for accomplishing disaster recovery (typically for less critical systems) by archiving data/files from a single server to mitigate against user failure and potentially replicating the data out of region.

Continuous Availability

Another one of the many options for accomplishing disaster recovery (for very critical systems) through maintaining multiple

PARTNERS IN SUCCESS:

EMC² AVAMAR

3PAR *Microsoft*

vmware f5

MISSION CRITICAL

Your business cannot operate without this system. You will incur serious financial impact if it is not available.

BUSINESS CRITICAL

Your business cannot operate effectively without this system. You may incur additional expenses or delayed business processes if it is not available.

NON CRITICAL

Your business can operate without this system for an extended time period without substantial additional expenses, delays or other impact so long as the data is retained.

This analysis should allow for those developing the recovery plan to take into account the true criticality of each system and determine recovery time and recovery point objectives that are realistic and meet the needs of the business.

HOW MUCH DR DO YOU REALLY NEED?

The first and most important aspect of any DR plan is a Business Impact Analysis. The purpose is to identify all of the IT systems that support the business processes and to quantify the impact of unavailability of the systems whether it be delayed or lost income, regulatory fines, breached contractual obligations or other intangible effects.
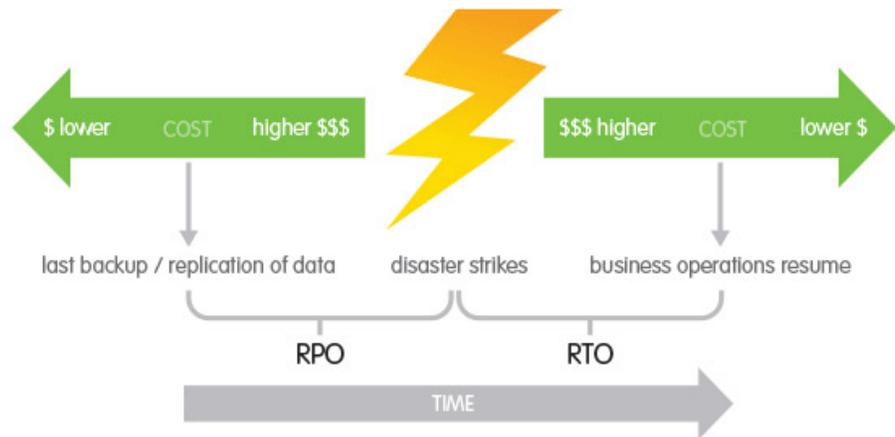
NOT SURE WHERE TO START?

In order to make the case for disaster recovery, you will need to get familiar with these three key concepts:

Recovery Point Objective (RPO):

How much data can you afford to lose? With inexpensive daily backups, you might lose up to 24 hours of data. With more expensive solutions, you can cut your losses to virtually zero.

Recovery Time Objective (RTO):

How soon do you need to have your systems up and running? Again, the less expensive solutions may involve post-disaster reconfigurations, which take more time.

Cost of downtime:

How much does an hour of downtime cost your company? This figure puts your RTO in perspective: if downtime is costing you only $100 an hour, you can realistically afford an RTO of multiple hours or days much more easily than if it costs you $25,000 per hour.