High-Performance IT

Disaster Recovery

russell
futcher
.com

The Best practice IT Standard is:

A detailed Business Continuity Plan (BCP) with a matching Disaster Recovery Plan (DRP) and a back-up site agreement. The BCP and DRP should at minimum have been paper tested several times.

Most of us think of a disaster as being a data centre that has been gutted by fire or hit by an aircraft, in other words, it's off the air and we think or rather hope – is unlikely. While these disaster types rarely happen, flooding however is a common cause of Data Centre DR, as is power outages, that's when the generators don't kick in (murphy's law), sabotage is another and not to be forgotten - data corruption is a big contender. Each of these can have catastrophic consequences for a business. Back-up data centres with data mirroring are the best protection you can get; however, they are only as good as the WAN links that connects them, and they can fail when needed (murphy's law again). It's all an insurance game where by and large you get what you pay for.

I know quite a bit about Data Centre DR and actual recovery. However, when the crunch comes, only people can recover systems and restore businesses. The trouble is there is very little sensible information prepared in advance, and what there must be kept current. Being prepared (defeating murphy's law) usually means that you won't suffer a disaster; but you must have a plan.

Consider this table below. Prepared by an enterprising guy for a SharePoint application, this small example is a good reminder that disasters can start from little things and have significant effects.

Dependency	Assumptions
User Interface / Rendering Presentation components	• Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g., client or server side, web interface or downloaded application). • Infrastructure and back-end services are still assumed to be active/running.
Business Intelligence / Reporting Processing components	• The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). • Standard backup processes (e.g., mirrored disk and tape backups) are not impacted, but the active / passive or mirrored processes are not functioning.

	• Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.
Network Layers Infrastructure components	• Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. • Assumption is that terminal connections, serially attached devices and inputs are still functional.
Storage Layer Infrastructure components	• Loss of SAN, local area storage, or other storage component.
Database Layer Database storage components	• Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable
Hardware/Host Layer Hardware components	• Physical components are unavailable or affected by a given event
Virtualizations (VM's) Virtual Layer	• Virtual components are unavailable • Hardware and hosting services are accessible
Administration Infrastructure Layer	• Support functions are disabled such as management services, backup services, and log transfer functions. • Other services are presumed functional
Internal/External Dependencies	• Interfaces and intersystem communications corrupt or compromised

Table. Alexander Windel, Senior Microsoft Premier Field Engineer.

To be prepared, at a minimum you need:

1. A disaster recovery plan (DRP) and a business continuity plan. (BCP).
2. Determine the Maximum Tolerable Downtime (MTD) for each application.

3. Determine a reasonable Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application.
4. Sort applications into MTD or RTO order.
5. Develop priorities and RTO's.
6. Develop recovery strategies for each application.
7. Prepare a hardware inventory (e.g., servers, desktops), applications and data inventories. Make sure that all the back-ups are working. Develop a list of critical applications and data and the hardware to run them. Make sure that application copies are available for re-installation on replacement equipment. Develop a priority list of hardware and application restorations.
8. Create an emergency response team.
9. Create procedures for declaring a disaster.
10. Develop an emergency communications plan.
11. Investigate alternative back-up data centres and or processing alternatives.
12. Document the DR plan.
13. Practise paper based dry runs of the DR plan and emergency response teams' procedures.

Some business applications cannot tolerate any downtime

They make use of a back-up data centre that can handle all their data processing needs, they run paralleled data mirroring between the two centres, this is a costly solution that usually only larger companies can afford. However, there are other solutions available for small to medium-sized businesses with critical business applications and data to protect. Many companies have access to more than one facility. Hardware at an alternate facility can be configured to run similar hardware and software applications when needed. Assuming data is backed up off-site or data is mirrored between the two sites, data can be restored at the alternate site, and processing can continue.

Cloud-based disaster recovery as a service (DRaaS), WAN optimized replication, for highly efficient use of backup storage is growing in popularity, especially among SMBs and mid-sized organizations. The service is based on the protected capacity of your cloud platform and stores a configurable number of daily, weekly, and monthly backups for one base price.

Some vendors provide "hot sites" for IT disaster recovery. These sites are fully configured data centres with commonly used hardware and software products. Subscribers may provide unique equipment or software either at the time of a disaster or store it at the hot site ready for use.

Performance Questions

1. Is there a BCP in place?
2. Is there a DR Plan in place?
3. Have the plans been paper tested by the disaster recovery response team?
4. What kind of back-up, alternate site arrangement is in place?
5. What is the current level of risk?
6. How do you rate your back-up provider?
7. What fundamental rights do you have under the back-up agreement?
8. If the back-up site is a shared outsourcers site, what rights and privileges do you have?

Sample Task list

1. Conduct a risk analysis.
2. Investigate what level of DR you need.
3. Work with the business to build a BCP.
4. Form a DR response team.
5. Paper test DR plans with response team.
6. Determine further works required and scope out.
7. Breakdown the scope of works to task level, ready for loading into the change management project schedule.