How Can I Manage a Full-Time Disaster Recovery Effort on My Part-Time Budget?

Companies know they must plan to ensure business continuity in the event that a disaster occurs. But most companies are unaware that a disaster recovery (DR) plan requires more than simply managing backups. DR is a different from backup. It requires different planning, preparedness and expertise.

The common approach is to simply assign current IT staff to manage DR tasks, when they are already busy with higher priority production environment tasks. This increases the risk of failure.

Another approach companies often take is to implement and manage their own DR solution. But this requires investing in a secondary data center with duplicate hardware, software and personnel. Often, this endeavor is fraught with difficulty in maintaining both production and DR environments and the patches, updates and testing that come with each.

This article describes the common misunderstandings about disasters, backups and data recovery. It also describes how DR managed services through a trusted advisor can replace the necessity for a full-time DR staff and offer a solution that is synchronized with your business continuity requirements.

Definition of a disaster

When people think of disasters affecting businesses, they typically envision natural disasters, such as fire, flood or hurricane. While these are all possible, there are many other disasters that can impact your business if you are unprepared, such as the following:

- An extended power outage occurs, the UPS system fails, and you don't have enough runtime to ensure all recent transactions have been replicated to the data center
- A construction crew down the street from your data center accidentally cuts the fiber, leaving your company without connectivity to the DR site, and your data redundancy capability
- A malware outbreak occurs on the network, and although this typically would be remedied using your backups, a failure occurs causing further unexpected havoc
- A storage array fails during expansion, or a rack loses power, or any other hardware failure occurs

Common mistakes in managing DR

Most companies believe their only choices for implementing a DR solution is to manage DR themselves by setting up their own data center or assigning DR tasks to existing in-house IT staff as time permits.

But setting up and running your own secondary data center is no small feat. It creates an enormous expense and effort. Essentially you need to duplicate all hardware and software resources and add personnel to manage them. Delays in installing patches and upgrades to both the production environment and secondary data center can contribute to the DR system failing. Typically, companies underestimate the personnel resources they will need to run and maintain the facility to be ready for disaster response.

Having your current IT staff maintain your DR solution and environment may mean you are operating a part-time solution unless full-time resources are dedicated to this purpose. This does not bode favorably for expertise and readiness which should be in place 24x7x365 as you don't get to choose when a disaster occurs. Here are some of the common mistakes companies make:

- Relying on backups for recovery - DR is not backup. Backup captures a point in time and is purposed for specific data recovery issues or application issues. DR must replicate multiple points with the sole intent of managing business disruption and continuity. Most companies believe that if they are backing up data every night the data is safe. That particular data may be, but can you open your doors for business and carry on as usual if you lose a day's worth of data?
- Approaching DR from a technology viewpoint – Basing your DR plan on a specific technology is more than likely the wrong approach. The reason is that DR typically involves more than just protecting data. It must ensure the business can continue to survive and operate as usual. Often this requires multiple technologies and expert integration.
- Using existing IT staff – Current IT staff are typically busy with pressing priorities in the production environment. DR tasks are often delegated to staff piecemeal, and do not get completed in a timely fashion in compliance with SLAs agreed by stakeholders.

What is the right approach to effective DR?

A DR solution should start with business and IT getting together and identifying what successful DR is, and identifying the critical applications and business services that must be protected. Smart companies realize that the best-case scenario would be to restore everything, but that path is very expensive.

The compromise is to refine the approach and look at systems that involve movement of money, execution of transactions, and maintenance of business-to-customer relationships. Your DR priorities and your business priorities should be aligned to focus on the areas where your risk of loss is the highest.

Although a robust backup solution is important, too, it should be used for routine data recovery efforts and as a last line of defense against isolated data loss events such as malware/ransomware data destruction. In contrast, your DR solution should be on a completely different level. You should be considering replication technologies that can take DR to numerous points of recovery and get there fast. Technologies are available today that make it possible to recover from an event in minutes.

Think of your DR system as a high-speed DVR – you can go back 5 minutes or 15 minutes. This is in sharp contrast to a backup where your nearest data point might be from 24 hours ago—if your last backup was successful. In the spectrum of time and data, the backup restore might be able to find an application data point, but it most certainly cannot accommodate business continuity where everything from recent financial transactions and real-time access to customer are critical. This is especially important in complex environments where a business does not depend on a single isolated system, but on numerous interdependent systems that work together to deliver a particular service.

Because DR requires monitoring, adapting, and testing your environment for potential gaps which may change as technology upgrades are applied to your environment, an effective DR solution requires full-time expertise. These demands can be eased by working with a DR managed services expert to strategize, plan and implement data recovery services with a primary focus on minimizing business disruption.

Because readiness is essential, whichever DR managed service provider you choose should be concerned daily with:

- Complying with SLAs

- Protecting data
- Meeting recovery point objectives
- Fulfilling data protection requests, such as protecting new systems and decommissioning older systems no longer requiring protection
- Allocating DR resources as needed on a monthly basis
- Coordinating failover tests (hygiene) at least 1x per year or more frequently based on business requirements
- Collaborating with you to update and maintain your runbook as a part of routine testing

By utilizing DR managed services, you can optimize use of your current IT personnel for priority production tasks and at the same time be assured that your team is ready to respond and ensure continuous service to minimize the business impact when a disaster (natural or otherwise) occurs.

For further information about Veristor's disaster recovery managed services, please visit Data Recovery as a Service (DRaaS).