**How to Choose the Right Disaster Recovery Partner**

A few years ago, a managed services provider[[1]](#footnote-1) went bankrupt and announced to clients they had two weeks to remove all data and resources from its cloud. Needless to say, customers were stressed. Most companies cannot move that quickly. Why didn’t somebody anticipate what to do if the DR plan or provider failed?

History is littered with technology providers who have come and later disappeared from the industry landscape, failing to ensure the security and safety of their customers. With little or no recourse, those companies found themselves in precarious situations with business continuity and even their existence, threatened. As a stakeholder in your company’s longevity and success, how do you guard against selecting the wrong DR provider?

Let’s start first by identifying the most common issues contributing to the failure of DR transactions. These not only threaten the reputation of the DR provider but more importantly the business continuity of their customers. Most DR failures can be linked to one or more of the following behaviors:

* Falling short of Service Level Agreements (SLAs) – If providers cannot meet basic SLA requirements, you cannot trust their ability to protect your assets
* Unprepared to protect all the critical data – When the DR solution does not identify and include all critical data areas, failure is inevitable; backups are not the solution
* Unable to meet Recovery Point objectives – Without collaborating on which data needs which level of protection and understanding how your systems work, there is no way of achieving RPOs consistently
* Neglecting to perform sufficient testing - You will never know how the DR solution will perform unless your provider tests it regularly and when changes occur to the environment or business performance requirements

**Evaluating Potential DR Providers**

As a stakeholder in your company’s success and longevity, you need to ensure these DR blunders do not occur in your environment. To aid in evaluating and selecting an experienced and respected DR provider to join your team, you should sit down with your prospects and ask very specific questions. The investment up front is critical to limiting your risk and finding a partner you can work with and trust to achieve your objectives. Questions to include in your discussion with prospective DR providers follow:

Q: How do you measure your SLA performance and how is it tied to our mutual success?

A: The key to defining and measuring and success is how the provider performs testing (see next question). DR providers depends on your If the provider cannot meet agreed upon SLAs, it’s time to discontinue the relationship.

Q: How will you ensure that all our critical data is protected?

A: Your environment and requirements are unique. DR providers should work with you to clearly understand your business and the systems that comprise your infrastructure so they can identify which data areas are critical for protection.

Q: How will you meet our Recovery Point Objectives (RPO)?

A: To meet your RPOs, the DR provider must know specific details about your system and use that knowledge to select the right technology solution. Once the provider has selected the technology for the job, it must then be aligned with right approach. So it is the responsibility of your provider to manage the technology so that it serves your RPO needs.

Q: How do you plan and coordinate your fail-over testing?

A: Testing is conducted anywhere from once a year to more frequently, depending on business performance objectives. An experienced provider will act as an extension of the customer’s IT team and take proactive measures such as hooking into change management so they can stay ahead of updates to critical data DR settings. Providers should also leverage testing to predict potential outcomes and check them against SLAs.

Q: How do you allocate DR resources?

A: If a disaster occurs, you will need to operate business safely out of the DR data center for a potentially extended period. Unfortunately, many providers do not have the backend infrastructure and resources to cover customer workloads. This could be a problem when a failover event occurs, and you discover too late the data center environment does not perform as advertised. The ultimate proof point to resource allocation is testing the company resources that matter. It’s important to pay close attention to the user experience during the test because it is likely a prelude to what will occur in a real disaster scenario. An expert DR provider can modify resource allocation as a customer’s requirements change, as well as be able to integrate new technologies into the DR environment as needed.

Q: Can you provide us with information about your company finances, history and experience? Do you have references we can contact?

A: By gathering recent financial information you can gauge provider’s business solvency. You also want a provider who has extensive experience in disaster recovery and years of successful engagements. Ask for referrals, testimonials and case studies. You may also want to ask your colleagues what they may know to determine if the provider is respected in the industry.

Choosing a disaster recovery partner is important to your business continuity. As “the devil is in the details,” you need to ask potential providers the questions that will uncover the details that will inform you about their skillset, resources, ability and determination to ensure your success. The right DR partner will be a part of your team and get your back during any disaster.

For further information, refer to [Data Recovery as a Services (DRaaS)](https://veristor.com/services/managed-services/data-recovery/).

1. N[irvanix failure – a blow to the cloud storage model?](http://www.computerweekly.com/opinion/Nirvanix-failure-a-blow-to-the-cloud-storage-model) ComputerWeekly.com [↑](#footnote-ref-1)