HotLink®

6 Key Elements of Successful DRaaS

Business resiliency is no longer an option – it's mandatory

In today's world of around-the-clock operations, few companies can afford IT downtime, yet most can't afford to prevent it. Traditional models for disaster recovery (DR) and business continuity (BC) are proving much too costly, unrealistically time-consuming and completely unable to meet the aggressive recovery objectives companies need to maintain business-as-normal operations.

If a disaster takes place and recovery is invoked, getting the organization's services and applications back is the most important task an IT team will ever face. However, recent research from the Disaster Recovery Preparedness Council shows that 73 percent of companies are failing in terms of disaster readiness, and 58 percent rarely or never test their DR plans because the process is overly difficult, manual and expensive. Not having a solution to recover services isn't a viable option anymore; the question is how to accomplish it with the resources available.

The public cloud now brings business resiliency within reach of organizations of every size, and **HotLink® Managed DRaaS™** (Disaster Recovery as a Service) could be the ideal option for you. Following are six critical elements to help you pick the best DRaaS solution for your business, so you can achieve affordable disaster recovery and business continuity for all of your IT services and applications.

> 73% of companies are FAILING in terms of disaster readiness, and 58% rarely or never even test their DR plans

1
INFRASTRUCTURE IS THE FOUNDATION

Instead of having to maintain your own recovery site or worse, locking yourself into a colocation provider, DRaaS lets your organization leverage the scalability of public cloud computing to store a mirror image of all servers and data. When a disaster strikes, you can quickly and fully restore your data center in the cloud-based protection site. According to industry research firm Gartner, AWS is the public cloud 800-pound gorilla, with more than 10 times more storage and compute capacity in use than the aggregate total of the next 14 providers combined.

Keep in mind, the DR/BC target site is only part of the infrastructure equation. In a failure scenario, you will also need integration with your on-premise management environment to ensure a seamless recovery. This allows you to handle your cloud-based DR/BC site just like you manage day-to-day operations today. As an example, HotLink DR Express™ is

a VMware-certified technology that is deeply integrated with VMware management and provides intuitive and automated VMware data protection in Amazon Web Services (AWS) – including backup, replication, disaster recovery AND business continuity. Don't make the mistake of considering your data protection infrastructure and management as an isolated environment – integrate it instead for an efficient failover following a disruption to on-premise services.

2

SKILLS CAN'T BE IGNORED

The public cloud allows flexibility and affordability, however it also introduces a hybrid IT environment, and with it, new complexities. Inherently, DR/BC requires a secondary site, and maintaining this remote site to achieve reliable business continuity requires a range of IT skills and an ongoing time investment. Many IT teams simply aren't able to provide this on their own. The good news is that DRaaS opens the door to use expert managed services and support to complement your internal IT skills. Rely on a skilled provider to deliver the expertise AND systematic management of your DR/BC environment, from initial setup to reliable

replication and continuous testing of the environment. This ensures that if a disaster happens, you will be prepared and ready to go. Using a provider's managed service lets your IT team focus on daily IT tasks, while ensuring your business operations are protected and resilient. Most managed service providers provide tiered service offerings to help you match the optimal service level with your business needs and budgetary requirements. HotLink Managed DRaaS was specifically designed to give you advanced technology, expertise, services and management – all with the lowest cost managed DRaaS offerings available.

DR/BC involves specialized skills – if you don't have them internally, seek out managed DRaaS providers to help

3   TEST EARLY AND OFTEN

The problem with disasters is that they, by definition, are unexpected. If you aren't testing your disaster recovery plan frequently for different situations, you might find yourself hung out to dry when the failure occurs. Because effective DRaaS doesn't have the physical infrastructure and synchronization complexities associated with traditional disaster recovery, there is no reason why tests can't be conducted on a systematic basis. A sandbox copy is created on demand in the public cloud, paid for while being used and deleted once the test is complete. Testing can and should include a variety of approaches, from routine application tests to all-hands, full-environment DR/BC tests. With DRaaS, testing should be automated and non-disruptive, which enables you to test specific applications without interfering with production environments. When considering DRaaS providers, be sure to focus on how the environment will be integrated with on-premise systems. Otherwise, you will likely end up with considerable manual effort in the testing process. With HotLink Managed DRaaS, not only does the service include systematic testing, but it also includes tight integration into your on-premise VMware management environment, so testing is easy and fully automated.
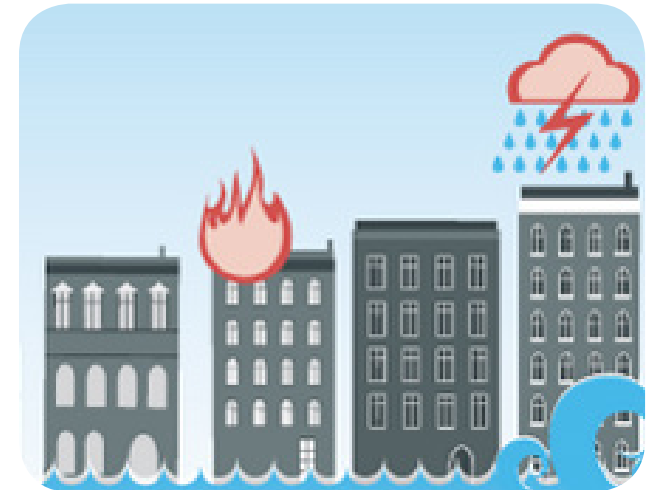
4

AUTOMATED RECOVERY IS A MUST

There are generally two types of disasters. A major disaster is often top of mind and frequently caused by a natural event like a hurricane, flood, fire or earthquake. However, this is not the typical failure situation. The most common disruptions to IT operations include security breaches, networking failures, software issues and human error. While not as dramatic as a hurricane or fire, these disasters are far more frequent, impacting companies multiple times a year. As you consider DRaaS, be sure you have a business resiliency solution for both natural and common disasters, and frequently test for both conditions to ensure you can mimic these disasters within your DR/BC environment. At HotLink, we understand the importance of automation in an effective recovery. This is why we have the advanced technology needed to easily automate your recovery in AWS and restore back on-premise at any time.

> The most common IT disruptions are security breaches, networking failures, software issues and human error

5

PERFORMANCE AFTER A FAILURE IS CRITICAL

Performance is clearly a critical aspect of business resiliency. An important question to ask a potential DRaaS vendor is, "What will the performance of my systems look like after recovery?" Many DRaaS service-level agreements (SLAs) do not specify what this performance will be. Worse yet, if you find that more capacity is needed than originally planned, this may be a big obstacle since many service providers pre-define your hardware allocation. Once you are up and running following a disaster, whether big or small, you need the flexibility

to readily monitor performance and change the configurations to increase computing capacity on-demand, not months in advance. Finally, you should be allowed to run indefinitely in the cloud just as you do on-premise, including the ability to grow and expand as needed. HotLink Managed DRaaS leverages AWS as the back-end infrastructure for your data protection site. This means you have unlimited capacity to restore and expand any or all of your applications; best of all, you only pay for what you need – when you need it.

Following a failure, you should be allowed to run indefinitely in the cloud just as you do on-premise

6

AFFORDABILITY OBVIOUSLY MATTERS

We all have budgets, and the financial reality of any IT initiative can't be ignored. In the past, business resiliency service options were so far out of reach for most organizations, they really couldn't be considered. The public cloud has completely changed the landscape and enables cost-effective DR/BC that is accessible by organizations of all sizes. So how do you get started with your TCO model? Consider the following:

a. Evaluate DRaaS solutions that take advantage of a public cloud, such as AWS. This allows you to benefit from low pricing, broad reach and unlimited scalability. With AWS, you can readily evaluate ongoing costs, including storage and compute costs, and scale up or down at any time, giving you the flexibility you need as IT budget grows or shrinks. Have the potential DRaaS providers help with this assessment to reduce your burden.

b. Estimate the post-recovery costs of running in the cloud. In case of a disaster, ensure that you have the ability to run in the cloud without any limitations.

Make sure you can scale your infrastructure up or down to meet SLAs and that you know the costs associated with changes. Importantly, understand any costs associated with moving your data and servers back on-premise when you want, not based on predetermined contract timelines. Again, don't be shy about asking vendors to support this analysis to potentially win your business..

c. Realistically assess your existing IT skills and time available for an ongoing DR/BC project. Most IT organizations don't have spare personnel sitting around waiting for a project, and existing staff may lack specialized skills in hybrid IT and public cloud deployments. Initially, you might think you cannot afford a managed service offering that provides the expertise and systematic DR/BC monitoring and testing needed. Don't be too quick to judge. For example, HotLink Managed DRaaS leveraging AWS has a service level that's suitable for virtually any IT budget.

IT leaders in businesses of every size now accept the public cloud as a cost-effective option for data protection

All companies need a way to economically deploy and manage a DR/BC environment, and public cloud-based DRaaS offers a new model to make this possible. DRaaS is the ideal solution for organizations that wish to protect their growing IT environments but cannot practically deploy and maintain DR/BC sites themselves.

HotLink Managed DRaaS provides affordable business resiliency options for IT shops of all sizes with a compelling value proposition – public cloud scale and economics, advanced DR/BC technology and highly skilled expertise. Your contingency site will be built using AWS, the most robust and scalable public cloud in the world. Most importantly, HotLink will extend the capabilities of your IT staff to ensure the DR/BC site is always ready for any potential business disruption. Customers can select the optimal service level to meet individual business needs and budgetary requirements

with Silver, Gold and Platinum options available – spanning weekly, daily and 24/7 service-level delivery.

Whether the disruption is a security breach, networking failure, software issue, human error or significant natural disaster, HotLink can provide you with a comprehensive, fully-managed DRaaS offering at unprecedented prices.

For more details or to learn more about the HotLink Managed DRaaS offerings, please contact us today at **sales@hotlink.com**

HotLink

HotLink Corporation

3130 De La Cruz Blvd., Ste. 211

Santa Clara, CA 95054

408.463.6130

www.hotlink.com

Sales: sales@hotlink.com