GREEN HOUSE DATA

Disaster Recovery as a Service
3 Questions to Ask

Disaster Recovery as a Service, or DRaaS, is a cloud computing technology that helps organizations of any size plan for the unexpected. Unlike traditional disaster recovery methods, DRaaS does not carry the same requirement of having to own two of everything and, because it is cloud-based, can offer a higher degree of geographic separation, since data can be stored virtually anywhere around the globe. However, like when planning any move to the cloud or as-a-Service model where processes are taken off-premise, businesses must ask key questions so they can appropriately assess if the service level meets their business continuity needs.

Here are 3 questions to ask a DRaaS provider to ensure critical systems and information are protected in the event of a disaster

How is the data replicated and backed up?

Though data alone will not be enough to restore a business to working order, without data, many systems are meaningless.

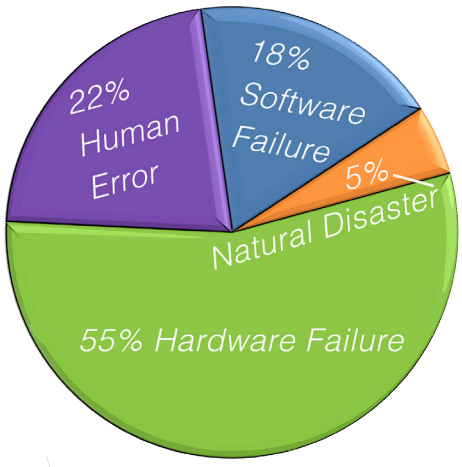
First, understand how a provider performs backups, and how often. Typically, a provider should work to balance the client's unique needs against what is practical in terms of cost. For some regulations, older backups must continue to be stored to meet compliance regulations. Though these backups will not be immediately needed in a disaster scenario, in the event that a primary site is lost, having this check in place can prevents headaches—and fines—down the road. Second, gather information about data encryption. Make sure your data is encrypted during transit, and also ask if it will be encrypted at rest (or when it is being stored). Third, make sure the backup method matches your current environment. If your organization is highly virtualized, for example, your provider should leverage backup applications that are tailored to your hypervisor.

What is the recovery timeline and process?

Much like backups, recovery timelines should be tailored to individual organization. For example, a business that is open 24/7 – like an online retailer – will require a faster recovery time than businesses with open and close times. Yet, in either case, speed is still key. Your disaster recovery plan will be pointless if employees do not understand what they should do in a disaster event.

If your business can afford to be down for an hour, this may help you mitigate disaster recovery costs, though this must also be

What Causes Disaster Recovery Scenarios?



Source: http://www.continuitycentral.com/news06645.html

What is N+?

N+ is used to designate redundancy in data centers. N = need, and + designates the level of redundacy for certain systems. For example, an N+2 for power facility will have two backup methods of power should a the grid go down.

weighted against lost productivity and revenue. If your business, as increasingly many are, is an always-on organization, ask your provider how they will help you mitigate the risk of an outage. Make sure you understand which systems are your priority to get online first, and ensure this is clearly communicated to your provider. For example, it may be enough for productively applications, like email, to be up and working, even if they are not immediately populated with much historical data. You must be specific about your required timeline. If you require a particular system to be back online within half an hour, for instance, communicate this, and communicate how much data much come along with it, and how long you could potentially wait the rest. Finally, different events necessitate different recovery actions. The loss of an entire site because of a natural disaster will dictate a more comprehensive course than a single server failure. Walking through these scenarios is important to your own business continuity planning and will offer guidance to employees who are tasked with execution. Your provider should also have clear expectations, from initial notification to full system restore.

Where are my data and systems going?

Even in the era of the cloud, disaster events are frequently a failure, however caused, of physical infrastructure and on-premise applications, and this is where DRaaS offers the most advantages.

Ask your provider about the location of their facilities in relation to natural disasters. If there is an event in your area, is there enough geographic separation to ensure continuity? Also, understand what the actual facilities are like. Even if your provider is regionally separated, they may be effected by other events, and should be able to guarantee redundancy. It's also important to ask what your provider's DR plan is. While meant to be a failsafe for you, there is always the possibility they could experience their own issues and should have a failover plan in place that is consistent with your needs. Make sure you get documentation of this plan, including how often it is tested. For example, data centers who are confident with their infrastructure redundancy will regularly perform "slam" tests, where they literally turn off their own power to ensure backup power, cooling, network, and other infrastructure can function if the grid is lost. You should and can ask for documentation and results of these tests. Finally, trade up. For DRaaS providers, continuity, uptime, and integrity are their entire business, and their service level agreements and compliance levels should reflect this. More than just the right number of 9's, your provider should act as a partner—your data is your business, but protecting your data is theirs.