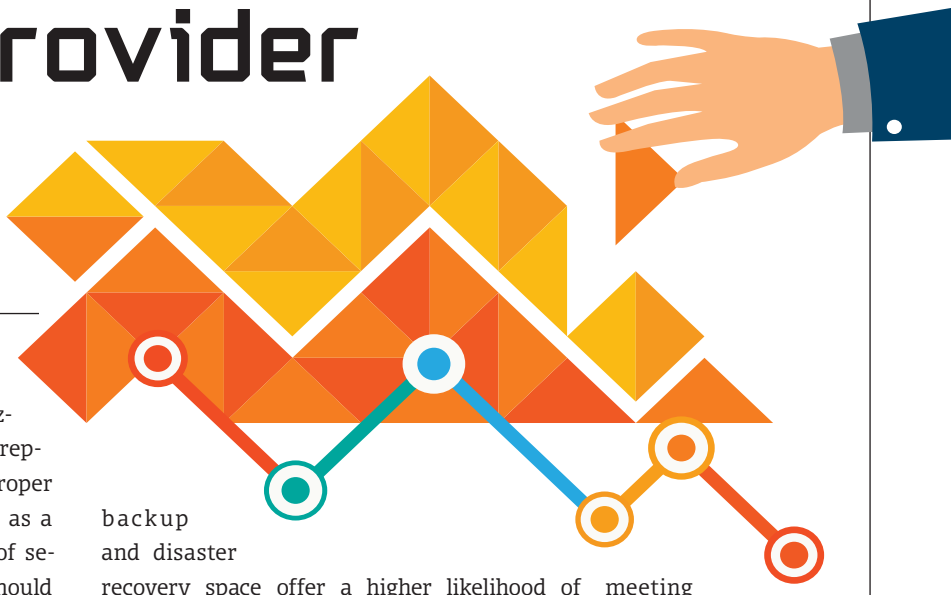
HOW TO FIND THE

Needle in the Service Provider Haystack

By Trevor Pott



Disaster recovery is demonstrably critical for businesses of all sizes. Offsite backups and standby replicas are an important part of proper disaster recovery. Once Disaster Recovery as a Service (DRaaS) is considered, the process of selecting a service provider begins, but what should systems administrators and solution owners be looking for from their DRaaS provider?

Choosing the right DRaaS provider could be the difference between surviving an unexpected IT event and not. The problem is that backup and recovery needs – and thus DRaaS needs – vary dramatically between businesses.

It's safe to say that the Saturn V rocket was the biggest, baddest and most powerful method of transportation for an individual (or small group thereof) that humans ever put into regular production. Despite this, it's still somewhat problematic for use as one's transportation for the daily commute.

So too is it with DRaaS. Trying to shoehorn all customers into a single model doesn't work. The service offered must be flexible enough to meet a variety of needs, at a variety of price points. It must also be able to cope with broad variations in customer technological requirements, capacity and – above all – bandwidth availability.

Solutions based on or offered by specialists in the backup and disaster recovery space offer a higher likelihood of meeting the unique demands of an organization. Backup vendors who have been in the business for a while have had exposure to edge cases and – hopefully – adapted their offerings to meet these needs.

Selecting the right service provider for the job

The first step in choosing a DRaaS provider is understanding your own needs. Against what kinds of disasters are you protecting, and what kind of personal touch do you really need?

Consider a simple small business manufacturing widgets. Orders from customers arrive at the business through the internet, are processed by computer systems on the manufacturing site and then widgets are made. Outside of computers associated directly with the manufacturing process there are some accounting systems, payroll systems and a small file server with files for sales, marketing and so forth.

The most common problems encountered are Oopsie McFumblefingers deleting a file they shouldn't have, ransomware encrypting everything and something corrupting the accounting database so they have to roll back to last night's backup. Any backup solution needs to provide accessibility to these file backups quick, easy and on a per-file basis.

If the power goes out for the business nobody is making widgets so none of the widget servers matter overmuch. It would be nice if orders sent in by clients didn't stop working, but this is easily solved with a

SHUTTERSTOCK

public cloud service acting as a buffer for incoming orders and relaying them back down to the shop when power is restored.

The worst case scenario is probably that the building burns down. If this happens, the widget servers still don't matter because there's nothing to make widgets with! Eventually, access to the accounting server will need to be restored so that insurance and tax issues can be dealt with, but if that takes a few days, it honestly isn't going to matter. Most likely the company will close and possibly reopen months later as a different legal entity.

So here is a sample company that needs to back up workloads to protect against Oopsie McFumblefingers, ransomware and disasters, but doesn't need the top-of-the-line ability to push a single button and light up their entire IT infrastructure on a service provider's cloud offering.

A separate example, say a small accounting firm, doesn't actually have any real physical assets to speak of. Everything they do involves accounting programs, and they could just as easily work from the café as they can from their office.

If the building burns down, this company absolutely needs the ability to push a button and be back online. The impact of the burned down building is an annoyance, but not one that should prevent the business from meeting customer needs, assuming they have the right disaster recovery plan in place.

Different businesses, different needs.

SHUTTERSTOCK

Questions to ask, answers to expect

The most important question to ask relates to what IT assets a given DRaaS offering can protect. Broad categories are file-based data, object and database storage, bare metal servers and virtualized servers. Virtualized servers come in flavors, so it's a good idea to make sure your DRaaS provider can back up the hypervisors you use or plan to use in the future.

If a DRaaS provider can't protect the assets you have deployed or plan to deploy then they aren't going to be of much help to you. Don't dismiss the DRaaS provider out of hand, however. The DRaaS market isn't particular diverse in what is supported; focus thus far has tended to be on those platforms, applications and services that meet arbitrary market share milestones. It may ultimately prove to be less expensive for organizations to abandon existing technological investments than to work with niche DRaaS providers.

If the building burns down, this company absolutely needs the ability to push a button and be back online.

The next question involves how IT assets are made available for recovery. In the early days of DRaaS, for example, individual file backup wasn't supported. Vendors required that file storage be provided by a virtual machine if it was to be supported at all, and restoring one file required downloading the entire file server VM.

Considering a file server VM can be terabytes in size, and single file restore operations are the most common recovery consideration. The old school file server VM without individual file recovery is an obvious no-go for most businesses. Some DRaaS vendors may still require file storage to be encapsulated in a VM, but hopefully can peer inside the VM to allow single file restore.

As discussed above, some businesses will also need to be able to make complete workload assets operational inside the service provider's public cloud. This is emphatically not a service offered by all, but it is also not a service required by all.

If you do need the ability to bring up workloads, you need to ask questions about

how networking can be configured to make this happen, and the technology and/or personnel expertise they have in this area. The most common failures of this service are related to networking issues.

Ask your service provider if they support WAN accelerators. The most expensive issue with offsite backups is frequently the cost of WAN bandwidth. If your DRaaS vendor can incorporate WAN acceleration, and other data reduction techniques like replica seeding, then you can save a lot of money in the long run.

Integration into existing backup solutions is also important. While DRaaS providers would naturally love to have every scrap of data a business makes protected by their offering, this isn't required by all organizations. Many organizations have data that, while it needs to be backed up to protect against issues such as ransomware, don't actually need to be backed up offsite. This is also important when businesses aim for a hybrid approach or D2D2C backup configuration.

Consider the previously discussed widget manufacturer. If their building burns down they're done. Having up-to-date copies of all their widget servers isn't going to help them. At best, they might want a one-time golden master of the known-good configuration for those servers in case they plan on restarting the business.

Our hypothetical widget manufacturer, however, is very likely to make regular backups of their widget servers that they store on site. The ability to integrate any DRaaS offering with this on-site solution is worth making a discussion point. Many popular backup vendors offer a fully multi-tenant offering for service providers, so this shouldn't be a big issue. If your DRaaS vendor says they can't integrate with your solution ask them which solutions they do integrate with, and push them to support ones that suit your organization best.

SHUTTERSTOCK

Test your DR plan

Above all, assume nothing; least of all that the DRaaS offering actually works. Test restores. Test disaster recovery. If you're using workload-to-the-cloud solutions, test every aspect of those, and test it all regularly.

Remember that any change you make to your local IT infrastructure can and most likely will affect your DRaaS solution. This is where the power of integration with local software can really shine.

Testing DRaaS can be expensive. Most businesses can't afford to pull down terabytes upon terabytes of data to test it, and lighting up an entire organization's worth of public cloud instances for workload-to-the-cloud testing can also run up the meter more than we'd ideally like.

Proper data protection, however, comes in layers. Done right, most organizations should have the running production copy of their data, a local copy of that data on separate media and an offsite copy of that data. This is known as the 3-2-1 rule: three copies of your data, on at least two types of media, one of which needs to be offsite.

Remember that any change you make to your local IT infrastructure can and most likely will affect your DRaaS solution.

If your DRaaS solution tightly integrates with your on-premises solution then the DRaaS component should simply appear as a remote data store. The testing you do locally can be reasonably assumed to be equivalent to testing on the remote DRaaS infrastructure, minimizing the need for more expensive external tests for minor changes. (Gross changes should be tested for all tiers of data protection regardless.)

In summary

Know your requirements. Ask lots of questions. Make frequent testing your plan, part of your plan. Look for DRaaS that works with what you already have, and don't let anyone talk you in to commuting to work on a Saturn V. Above all, remember this: if your data doesn't exist in two places then it simply does not exist. Good luck.