How Can I Create a DR Strategy without a Second Data Center?

For a Disaster Recovery (DR) strategy to be effective, there must be a second data environment. The premise is that your production environment, or primary data center, must be perpetually replicated to a safe and secure second data center. In the case of a critical disruption that threatens the continuity of your business, the primary data center quickly fails over to the second data center, ideally without users experiencing any delay. What your second data center is, and how it is set up and configured, depends on your requirements and the availability of technology and resources to meet those requirements.

Let's take a look at the two most common scenarios companies find themselves in when implementing a second data center in the quest for the perfect DR solution.

Scenario A
The company has a second data center offsite that it built and manages on its own. However, the corporate 2018 cost-reduction plan eliminates the funding for the existing, outdated data center and calls to replace it with a third-party vendor who will provide data center services with newer technology, but most likely proprietary.

Scenario B
The company is developing a DR plan but does not have an existing second data center. The plan is to build a company-owned data center by repurposing old equipment that was to be decommissioned, as a more cost-effective approach. Beware, this strategy is flawed in two significant ways. In trying to minimize purchase costs by leveraging older equipment, the approach doesn't take into consideration the costs that will be incurred for updating the hardware and software, and adding and training IT staff. The second flaw is that older equipment is decommissioned for a reason, most likely because it can no longer perform as needed. If your DR solution is supposed to be the guardian of your business, you want state-of-the-art technology behind it.

Both strategies are myopic, focusing on cost savings while sacrificing quality technology and expertise needed to address today's threats. Let's take a look at the options for setting up a second data center and their advantages, along with their disadvantages.

- **Build your own** - This option is expensive because it requires the company to have the budget to purchase the hardware and software, and invest in IT staff dedicated to the DR responsibilities. This option is usually only feasible for large enterprises. However, the benefit is that your security strategy remains under your direct control.
- **Data center provider** – The provider supplies the space, equipment and software. Often, the provider is associated with a specific vendor and its products and rarely are the best solutions comprised of technologies from the same manufacturer. Whether operations personnel are on your staff or the provider's staff, they must be experienced in all deployed technologies no matter the manufacturer.
- **Traditional vendor** – Much like the data center provider, the vendor provides the facility and most definitely offers only its own software and hardware. For the company who values working with a one-stop-shop, this could seem like an attractive option. However, no single vendor provides the best available technology to handle all facets of DR.
- **Hybrid approach** – With this strategy, the company secures the space and then works with a DR provider who provides the equipment. This approach offers cost savings by going direct to acquire the necessary real estate, and also gives access to the technology best suited to your

unique solution. The subtle disadvantage is that you might not have full access to a best-of-breed solution.

- **Public cloud** – The company deploys DR technology that replicates to the cloud. The lower operating expenses are compelling, but this strategy requires that your staff has the right experience to monitor, test and manage the solution.
- **Managed DR service** – A managed service provider architects the solution with the technologies best suited to your business objectives. Because the provider is often bound by SLA agreements, the equipment and processes are linked to performance rather than to a specific vendor which elevates the quality of your DR solution.

Is One Better than the Other?
With many of the options, there are tradeoffs. For example, the most attractive option might be to build your own second data center and maintain control of operations and security. In turn, you would be spending a significant amount of your budget and allocating valuable resources to the company-owned solution. For many, that trade-off is not an option.

Maybe leveraging public clouds for a DR strategy is the answer. After all, the approach has been gaining popularity over the past 24 months. The concept is particularly compelling because of the perception to reduce costs. However, the trade-off is that you are relinquishing much of the control to the cloud provider so you are limited in managing your recovery time objectives (RTO), making it inappropriate for certain needs. For example, you may discover that the storage is not sufficient for the I/O demands of your machines as you spin them up. If this is the case, you will be faced with having to pay for a higher storage tier. Now the myth of potential cost savings is dispelled, aside from the fact that the solution does not easily fit your needs.

As far as the other options we mentioned? They have similar trade-offs, and settling for something less than ideal is not something you want to do with a DR solution. However, there is one option that requires no compromise. A managed service provider can tailor the solution, because your ideal DR strategy depends on your requirements, your budget, and the value you place on your business continuity. This type of partner knows right technologies for the job and has expertise with best practices including comprehensive testing and continuous monitoring to ensure compliance with RTO and RPO objectives, as well as industry regulations.

“Cybercrime caused 22 percent of data center outages in 2015, reported in a recent survey conducted by the Ponemon Institute and sponsored by Emerson Network Power.”[i] Now is the time to up your game. Whether you want to build your own data center, leverage public or private cloud options, or want to work through a third-party vendor, a managed DR partner can work with you to devise the solution that best meets your requirements – with no trade-offs.

For further information, refer to Data Recovery as a Services (DRaaS).

[i] “Cybercrime Fastest-Growing Cause of Data Center Outages”, Data Center Knowledge