CIO Guide:

Best Practices For Disaster Recovery Success

OnX CANADA

Technology, covered.

Disaster Recovery as a Service (DRaaS) cuts operating costs and frees companies to focus on top-line business initiatives

Disaster recovery must be planned, documented, executed, and tested. All these processes take time and money away from business-critical IT priorities for a "what-if?" scenario that may never happen. Still, planning for the unknown is necessary to reduce a company's risk and, in many cases, to meet regulatory compliances. Consuming Disaster Recovery protection from a service provider in a consumption model is an attractive option to many organizations because it:

Frees up scarce IT resources.

In today's lean IT departments, managers dread the prospect of devoting time and budget to something that seems like a mundane, commodity-based chore (until, of course, they desperately need it). Handing off Disaster Recovery (DR) to a cloud or managed service provider makes the vendor accountable for DR, freeing IT leaders to focus on other areas like business continuity planning.

Addresses DR staffing skill sets and gaps.

Many companies operate on a thin margin of IT staff to handle management of day-to-day IT support functions—much less something catastrophic. With tight staffing, unplanned issues can kill other critical IT projects. This makes it advantageous to partner with a DRaaS provider who will always have staff and equipment dedicated to mission-critical recovery tasks and employ subject matter experts with years of experience.

Eliminates costly idle on-premises infrastructure and avoids large capital deployments.

DRaaS eliminates the need to pay for licensing and infrastructure that sits idle at their Disaster Recovery sites. Instead, the cloud and managed service provider hosts, manages, and maintains the servers, networks, replication capabilities, and other data center infrastructure for your DR site.

4 Best Practices for DRaaS success

The advantages of cloud computing make deploying Disaster Recovery as a Service an increasingly attractive option. DRaaS frees IT teams from data backup and disaster recovery duties and assigns them to experts who can get systems and applications back online quickly and efficiently during a critical incident.

Delivered as a success-based outcome service, DRaaS has a straightforward appeal for companies developing Business Continuity and Disaster Recovery (BCDR) programs. The implementation of DRaaS, however, can be quite complex.

A recent meeting of IT executives untangled some of these complexities. Sponsored by OnX Canada, the Technology Executives Club BCDR Special Interests Group convened a collection of seasoned BCDR professionals who have substantial experience with DRaaS programs.

Their roundtable discussion focused on data backups in a remote cloud environment—specifically whether they helped or hindered the ability to recover from a disaster. This e-book boils their insights down to four best practices companies can follow when choosing a DRaaS provider.

Best practice 1:

Know what to ask potential DRaaS providers.

Companies must scrutinize DRaaS providers carefully. You don't want to wait until a catastrophe strikes to find out you've made a poor choice. It's crucial to have a checklist of questions for potential cloud and managed services providers, such as:

- **Where does the data reside?** Your cloud provider must be far enough away that it won't suffer regional outages that happen with hurricanes and earthquakes.
- **How compliant are their policies?** It's mandatory that your DRaaS vendor upholds all of your regulatory compliance obligations.
- **Who is managing your data?** This goes back to compliance: How can you stay compliant if you don't know who is personally accountable for managing your data?
- **How secure are their networks?** Cloud providers have a vested interest in keeping their networks as secure as possible, but you still need to make sure you understand their security protocols—and to ensure they are compliant.

These questions are just a starting point, of course. Take time to research the full range of concerns that DRaaS providers must address. Build your own checklist of questions to ensure that each potential vendor adheres to standard operating procedures, security policies, and industry standards that are tested by external third-party audit firms.

Best practice 2:

Make sure DRaaS goes beyond compute and Infrastructure as a Service (IaaS).

DRaaS is a pay-as-you-go model, meaning you only pay for the resources that you use. This creates a temptation to think of it primarily as a means to access your compute and backup resources remotely, but DRaaS should be much more than that.

For DRaaS to be truly effective, it must provide access to people, skills, and equipment that, when combined, ensure a successful recovery of your data. DRaaS should also always include a testing component to confirm successful recovery of critical systems and applications in the event of a disaster. Anything less could make you vulnerable to critical gaps in your backup and DR process.

This is where it becomes crucial to partner with a DRaaS provider who truly understands your business challenges, IT environment, and unique needs when a significant incident occurs.

Best practice 3:

Fully test your DR program—but don't disrupt your business.

Too many companies neglect Disaster Recovery testing and discover the flaws in their BCDR programs when it's too late to fix them. Testing needs to be comprehensive and executed regularly. The challenge is that testing has the potential to disrupt the production environment.

Below are some suggestions for minimizing downtime during a DR test:

- **Isolate.** Create an isolated VPN to test recovery of critical servers without touching production.
- **Prepare for a full outage.** To test an entire production environment, you may need to have a full outage—preferably over a weekend. It may be wiser to test portions of your production environment individually rather than all of it at once.
- **Pull data.** Document the test results, especially Recovery Time Actual (RTA), which quantifies the test's success and provides a good estimate of your recovery time.
- **Create controlled data sets and scripts.** These ensure everything is accounted for and that you can resume operations after an incident. Tests will show where to refine these scripts to cover anything missed in previous testing phases.
- **Use virtual desktops.** These can be a huge asset for Business Continuity because they let users keep working from home in a natural disaster.
- **Turn off monitoring.** Running a production-to-DR role-swap or switch test can trigger alerts that disrupt production systems. Make sure your IT staff knows about the tests—otherwise they will try to "fix" the test-related problems that trigger the alerts.

Working with a DRaaS provider makes it easier for companies to test their Disaster Recovery plans—which in turn encourages more testing. Every test reveals small problems that can be fixed in advance, making companies all that much more prepared.

Best practice 4:

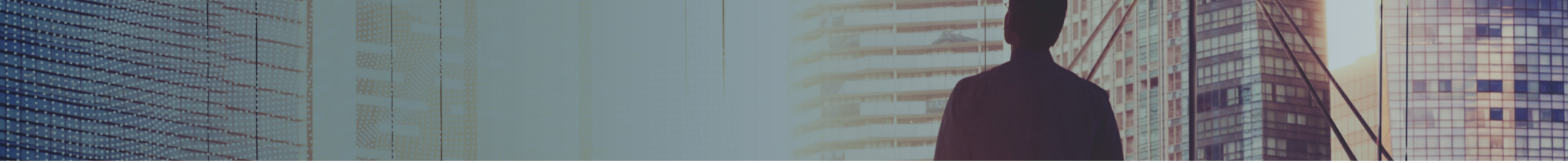
Acknowledge the pitfalls of traditional DR.

The disadvantages of traditional Disaster Recovery underscore the allure of DRaaS:

- **Duplicate costs.** Colocation and dedicated equipment require you to maintain twice the infrastructure and costs to manage replication and sync points. Paying for licensing, rack space, power, and hardware—and managing it all just in case something happens—is expensive and draining on your staff.
- **Location issues.** When you grow, you can't always install the next cabinet of IT equipment next to the existing gear. This adds extra complications for your DR program. You also have to build a DR environment far enough away to survive a regional outage, which imposes time and travel costs for you and your staff.
- **Longer time to deploy.** Traditional DR equipment must be planned out as a capital expenditure, which drags out the time it takes to get it up and running. There's also less flexibility in traditional DR compared to a DRaaS solution, which also delays deployment.

Surging data demands are forcing companies to add more and more IT capacity. Every new rack of servers and networking gear represents equipment and operations that must be duplicated in a dedicated Disaster Recovery environment. Those costs and complications add up quickly.

In sum, DRaaS makes sense for many companies, especially those who face growing demands on their IT systems and staff. The key is to carefully choose a DRaaS provider that takes the time to understand your business and clients and is capable of developing a DR plan that will keep you up and running no matter what.



About OnX Canada

OnX Canada is a leading technology solution provider that serves businesses, healthcare organizations, and government agencies across Canada. From unified communications to cloud services and beyond, OnX combines deep technical expertise with a full suite of flexible technology solutions that drive business outcomes, improve operational efficiency, mitigate risk, and reduce costs for its clients. OnX simplifies IT and Communications strategies with local knowledge and support for Canadian organizations. For more information, please visit **www.onx.ca**.

Contact us today at 1.866.906.4669 | onx.ca