



CITO Research

Advancing the craft of technology leadership

Balancing the Scales: How the Cloud Brings Equilibrium to Disaster Recovery and Backup Planning

SPONSORED BY



EQUINIX



CONTENTS

<u>Introduction</u>	1
<u>The Cost of Imbalance</u>	1
<u>BDR Matters More than Ever</u>	4
<u>Business Before Technology</u>	4
<u>Is Balance Attainable?</u>	5
<u>Weighing the Cloud</u>	5
<u>What to Look for in Hybrid BDR</u>	6
<u>Balancing the Scale: Equinix and Datapipe</u>	7
<u>Conclusion</u>	8



Introduction

The discussion of proper disaster recovery and backup procedures is nearly as old as the notion of an IT department. Ensuring the continuity of data, applications, and service assets is widely acknowledged by enterprise executives as an important function, but there have always been significant catches that stand in the way of smooth implementation.

The simple fact is that, on a typical day when the sun is shining, the cost of keeping the necessary systems and support for comprehensive backup and disaster recovery (BDR) running far outweighs the perceived immediate value. It's the conundrum common in nearly every insurance scenario: pay something now or potentially pay a lot in the future.

60% of surveyed organizations do not have a fully documented BDR plan in place

The Cost of Imbalance

There are many reasons why organizations fail to protect themselves. Just a few of the barriers to effective backup and disaster recovery include:

- **Cost:** Implementing BDR has typically required significant expense including additional storage, administration, power, off-site real estate, and more.
- **Complexity:** The distributed nature of modern IT infrastructure complicates BDR practices. Instead of being neatly contained in a single data center on site, today's information systems are spread across a complex array of cloud and local services and must also support many mobile devices and applications. While this distribution affords some disaster protection, it is often fragmented and unwieldy.
- **Support:** Building and maintaining a BDR solution requires not just technology but expertise, which is rarely something companies have staffed for or can afford to keep on an ongoing basis.

The result of these obstacles is, if not inaction, ineffectiveness. According to the Disaster Recovery Preparedness Council, 60% of surveyed organizations do not have a fully documented BDR plan in place, despite the fact that an EMC study found that 66% of organizations acknowledge having experienced unplanned system downtime in the past year.



Do Not Have a B/DR Plan

60%

do not have a fully documented B/DR plan in place

Have a B/DR Plan

23%

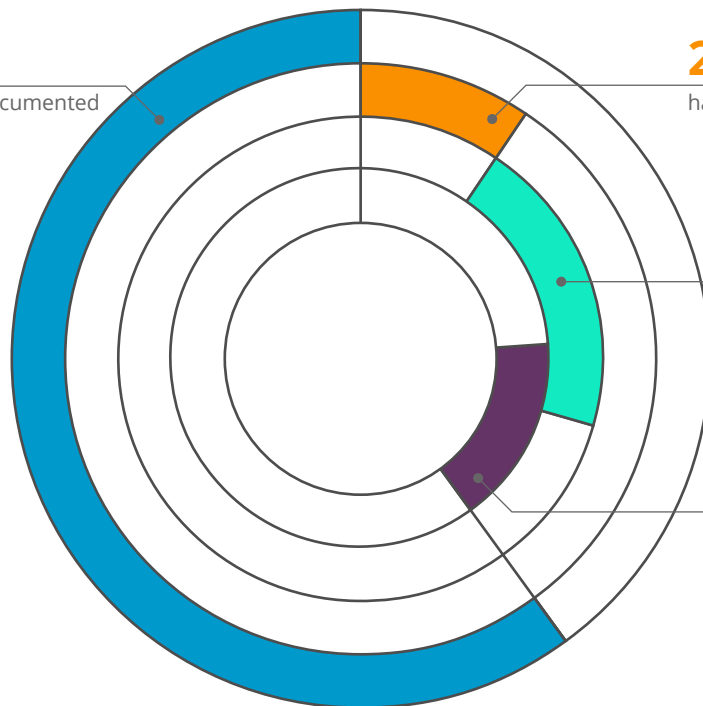
have never tested it

65%

tested it but failed

40%

implemented it but not useful



It is not that enterprises do nothing, but rather that their choices have been limited by cost and complexity. What is most typically in place is a profusion of backup and recovery tools applied at specific points of concern. The sheer diversity and isolation of those tools stand in direct opposition to creating something that can be considered a coherent BDR strategy. No wonder organizations are frustrated. Thanks to that legacy BDR landscape, more than 65% of organizations could not pass their own tests of their BDR systems and 40% stated that their current plan did not prove useful when called upon (BDR Council).



Clearing the Air

Before one can talk about solutions, one must understand what is meant by backup and disaster recovery. This can be surprisingly challenging. The two have become such commonplace terms that few outside those responsible for implementing them stop to consider specific definitions. The proper meanings are helpful not only for clarity, but because the definitions contain useful hints as to how to best address the business challenge presented by each.

Backups are reliable copies of all important information. The most common location for backups is a local disk or tape repository, although today the cloud is a commonly used third option. Backups are typically handled as periodic full copies of all files, supplemented by incremental backups of what has changed since the last full backup was performed. Inherent in the term backup is the element of time. How often an entity executes a backup reflects how the business values data as well as its capacity to absorb data loss. Data loss is simply determined by time between backups.

Associated with backup is the term **Recovery Point Objectives (RPO)**, which refers to how much data loss an enterprise will accept should data loss occur. In simple terms, RPO is dictated by when the last backup was made. For a credit card processor, it would be the last transaction, reflecting a low tolerance for data loss. Another company might be content with a backup made the previous day.

Disaster recovery refers to the ability to get systems and applications back in working order within a certain timeframe. Effective disaster recovery is a solution that enables an organization to recreate the production environment within a certain amount of time, given that the original systems are no longer available. The standard approach has been to invest in the replication of some portion of an enterprise's data and IT systems at a different location with its own distinct physical infrastructure, security, connectivity, and maintenance protocols.

Disaster recovery is ultimately guided by **Recovery Time Objectives (RTO)**, which refers to how long an enterprise can go without a specific IT service, also known as the maximum tolerable outage. RTO might be measured in seconds, hours or days depending on the particular requirement and its impact on revenue, brand awareness, legal obligations and other business-level factors. That means RTO dictates a variety of considerations, from the type of technology deployed to the frequency of backups.



BDR Matters More than Ever

Enterprise users and customers rely on applications and data being available and reliable. Organizations deploy more web, cloud, and mobile applications daily, and these applications are ever more the interface through which all business is done, from transactions to operations. In today's business environment, those data and systems require BDR because those technologies define the business. IT organizations must maintain the uptime and availability for mission-critical applications such as Exchange, SharePoint, Oracle and SAP, as well as critical line-of-business apps and data, not to mention the physical servers, storage, and networks through which everything flows.

In 2014, data loss and downtime directly cost organizations around the world \$1.7 trillion

Data Loss and Downtime

In 2014, data loss and downtime directly cost organizations around the world \$1.7 trillion (EMC). Depending on their industry, organizations face a variety of regulatory and compliance requirements such as PCI-DSS, SOX, FedRAMP and HIPAA, each with their own requirements that do not necessarily overlap.

All information systems are susceptible to downtime. How well a business prepares dictates where on the continuum of possible outcomes it will re-emerge from an incident, from little to no impact or minor inconvenience, to massive loss or even collapse.

Business Before Technology

While backup and disaster recovery require technical solutions, the overriding issues are matters of business resiliency and risk assessment. RTO and RPO dictate BDR by reflecting a business's unique requirements based on careful consideration of what systems are critical to the organization. These are questions of how much pain—to finances, reputation, and the like—a company believes it can absorb when its data and systems become unavailable. These considerations must be weighed against the cost of the physical requirements described in those definitions. How much can a company afford to spend on the infrastructure needed to protect itself?



Until recently, organizations had essentially two choices:

- Make significant investments in redundant infrastructure that will seldom be used, must be constantly maintained, and requires re-investment to reflect changing requirements
- Restore data from old, slow, and unreliable backup media

The first of these choices is expensive and the second is too slow to meet the RTOs of most organizations. So while organizations want to be prepared to handle downtime or potential disaster, the available options for addressing BDR have not been in equilibrium with the need.

Is Balance Attainable?

BDR is not a deployment with a finish line. The company that deploys, tests and finds that it meets its RPO and RTO objectives today may still fail to meet them when disaster strikes. In order to fully protect the interests of the organization, a BDR solution must be flexible.

The Achilles Heel of BDR

Every time the organization implements a new application, updates an existing application, moves a service to the cloud, virtualizes a server or acquires new infrastructure, the BDR plan must be tested and be capable of accommodating the new requirements. Lack of flexibility has been the Achilles heel of BDR. In the past it has been easier to divide and conquer, spending money and making changes to individual pieces of the system. As business systems become more intertwined, it is best to have a system that can be centrally managed.

Weighing the Cloud

It is important to be wary of the kneejerk reaction that defaults to “the cloud” as a solution for everything. Moving to the cloud offers many benefits, but simply putting data and IT services in the cloud does not necessarily constitute having a disaster recovery solution.

The emergence of cloud-based backup and disaster recovery does nevertheless offer compelling options for realigning costs and value to reflect the needs of today’s IT-driven business. Some of the benefits are common to most cloud services: lower costs, less infrastructure to maintain, geographic separation, and on demand scalability are some of the obvious ones.

For most organizations however, a hybrid cloud BDR solution will provide a compelling option. Hybrid cloud BDR leverages a combination of private and public cloud capabilities, as well as traditional techniques in some cases. When properly implemented, hybrid cloud BDR can be easy to use, low cost, flexible, and secure.



Pay as You Go Cloud Resources

A hybrid cloud BDR solution takes advantage of the elasticity of public cloud providers. A hybrid cloud BDR solution offers the flexibility to test BDR scenarios in the public cloud on demand, reducing investments in redundant infrastructure. IT sets BDR policies and ITIL that dictate how the enterprise will execute their BDR strategy in the event of a disaster (as defined in the policy).

The hybrid cloud supports monitoring and instrumentation so IT knows how and when to kick over to a failover or disaster recovery scenario. If and when these applications and servers are needed in the event of a disaster, they can be started up again in similar fashion. Since you pay only for the cloud resources you use, it is much less expensive than maintaining always-available redundant infrastructure. It also enables IT to follow best practices regarding testing disaster recovery practices.

By enabling IT to leverage the public cloud, a hybrid cloud BDR solution allows a measured approach and augments existing infrastructure and private cloud environments, supplementing them with on-demand capacity in multiple geographies.



What to Look for in Hybrid BDR

With the growing number of cloud options available, how does one identify the best choice? While cost and flexibility have already been mentioned, there are many other considerations:

Support for multiple clouds, which ensures future flexibility and prevents vendor lock-in. Multi-cloud support allows the IT organization to choose one or more cloud service platforms to best meet the needs of its business, such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM SoftLayer. Furthermore, with broad multi-cloud support, the IT organization doesn't risk creating pockets of unprotected data and applications as new cloud services are consumed.

High availability, which supports the sub-second response times that are required when organizations are working to carry on their business in the wake of a disaster or unplanned outage.



Proximity is the distance between production and backup systems. It is a key factor to help prevent network bottlenecks. Cloud computing is bandwidth intensive. IT organizations should be able to move critical infrastructure and applications to a data center that is in close proximity to the services that they are dependent upon. In addition to enhancing performance, proximity helps reduce costs and risk.

Expertise, which is essential to all facets of effective BDR. A vendor with deep expertise can help vet your organization's BDR plan and ensure that it meets the needs of the organization to serve business continuity goals as well as cost efficiency. IT organizations should choose an experienced partner to assist with all aspects of the BDR solution — from conducting a business impact analysis, to developing an IT DR strategy design and operating model, to implementing, managing and regularly testing the hybrid cloud BDR solution.

Balancing the Scale: Equinix and Datapipe

Equinix and Datapipe have teamed to offer a hybrid cloud BDR solution that provides businesses with BDR that stands firmly on the following three priorities Recovery Point Objectives, Recovery Time Objectives and the budget to achieve those ends.

The Equinix and Datapipe solution brings together a unique combination of best-in-class capabilities. With its focus on data center operations and availability, Equinix is able to ensure uptime during optimal and less-than-optimal conditions including manmade and/or natural disasters. Datapipe complements those features with deep experience in the design, implementation and maintenance of clients' information systems. This includes the integration of legacy infrastructure with public cloud environments to create elastic hybrid environments.

The Equinix and Datapipe BDR solution has a unique profile in the category with features that include:

- **Proximity.** Equinix is a global provider with the world-class coverage needed to minimize the distance between production and backup systems. Datapipe's BDR services are optimized to meet application requirements.
- **High availability.** Equinix offers very high availability globally (>99.9999%), combined with low latency (<10 ms). Enterprise users experience sub 5-millisecond response times regardless of their location, even when a disaster strikes. This is further enhanced by Datapipe's proven reliability; the company consistently ranks high in Netcraft's Hosting Provider Performance Monitoring.



- **No vendor lock-in.** Equinix offers seamless accessibility to major cloud providers (AWS, Microsoft Azure, Google, SoftLayer, Cisco). Enterprises can select cloud providers based on business needs.
- **Integration between public and private clouds.** Equinix and Datapipe hybrid cloud BDR implementations protect sensitive company data on a private cloud while offering fast, direct links to public cloud computing resources via Equinix. Seamless integration between the public cloud and an enterprise's IT environment means highly available, data-intensive applications are supported in a secure, compliant environment.
- **Tailored to business needs.** Equinix and Datapipe consultants are experts in architecting the best BDR solution for each enterprise, based on its unique needs, regulatory requirements and business priorities.
- **Assurance.** The solution includes the assets, processes, people and infrastructure at the scale required to meet any organization's BDR requirements.

Conclusion

While the cloud is transforming BDR by lowering barriers such as cost and complexity, that does not, however, make BDR simple. It is imperative that IT management educate themselves in order to differentiate between offerings. Given the constantly changing IT landscape, it is important to choose a solution backed by the best infrastructure, connectivity, and expertise.

CITO Research advises enterprises to deploy an Equinix-Datapipe disaster recovery solution, particularly in a hybrid cloud implementation, to attain fault tolerance and resiliency at all layers of the stack (facilities, infrastructure and applications). Together, Equinix and Datapipe employ a cost-effective, highly available and globally extensible solution that will ensure up-time in the event of manmade and natural disasters.

This paper was created by CITO Research and sponsored by Equinix

Learn more

[Tune in to the Equinix/Datapipe webinars produced by TechTarget ►](#)

[Read more about the Equinix/Datapipe advantages ►](#)



About Equinix

Purposed to protect, connect and power the digital economy Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most interconnected data centers. In 33 markets across five continents, Equinix is where companies come together to realize new opportunities and accelerate their business, IT and cloud strategies. A foundational commitment to interconnection began when they first opened their doors to offer the networks that powered the early Internet a neutral place to exchange traffic. The interconnection that Equinix enables through a variety of services and solutions has set them apart ever since. Today Equinix connects 4,750+ companies directly to the customers and partners that matter most to their businesses. Equinix enables 145,000+ connections between their customers, which makes Equinix the global interconnection platform for the world's leading businesses.

About Datapipe

Datapipe is the managed hosting and cloud services provider with the most complete set of services, global locations, and industry leading partners. Datapipe delivers choice, control, and confidence in architecting, deploying, and managing multi-platform hybrid IT solutions tailored to individual customer needs. Optimizing mission-critical and day-to-day enterprise IT operations, Datapipe enables businesses to transform, innovate and scale. Backed by a global team of experienced professionals and next-generation data centers Datapipe provides comprehensive security, governance, orchestration, and analytics solutions. Analyst firm Gartner has named Datapipe a leader in the 2014 and 2015 Magic Quadrant for Cloud-Enabled Managed Hosting.

CITO Research

CITO Research is a source of news, analysis, research and knowledge for CIOs, CTOs and other IT and business professionals. CITO Research engages in a dialogue with its audience to capture technology trends that are harvested, analyzed and communicated in a sophisticated way to help practitioners solve difficult business problems.

Visit us at <http://www.citoresearch.com>