eBook

How Your Business Can Recover Quickly from Any Disaster

To ensure you are protected, get beyond these myths and misconceptions about Business Continuity and Disaster Recovery

Making Sure Your Business Is Ready for Anything

You've seen disasters in the news that could be fatal to your business. They range from unforeseen natural disasters — like severe weather, flooding, wildfires, or an earthquake — to man-made disasters like ransomware and simple human error. You hope it doesn't happen to you, but hope is not enough.

You need a strong business continuity and disaster recovery (BCDR) plan to keep your organisation up and running, no matter what. A complete BCDR plan addresses business issues, such as work-at-home contingencies for employees who can't go into the office, as well as IT issues, such as how to restore inoperable computer systems and prevent business interruption. Otherwise, you risk the loss of sales, loss of customers, and ultimately the loss of your business.

When a server suffers a fatal crash, is compromised in a cyberattack, or burns to a crisp in a fire, you need more than just backup. You need a solution that lets you get back in business quickly.

Many businesses can't hire experienced, dedicated disaster recovery personnel or invest in elaborate off-site recovery facilities. But they can have an effective BCDR process by working with a managed service provider that provides access to a modern, cloud-based BCDR solution — also known as disaster recovery as a service (DRaaS). Modern BCDR solutions enable very fast restores when compared with traditional backup solutions, partly by taking advantage of DRaaS.

Business Continuity and Disaster Recovery Myths and Misconceptions

Whether you are new to BCDR or looking for an upgrade, it's important to get beyond common myths and see the bigger picture.

Myth #1: BCDR seems unnecessary for a business my size

This is perhaps the most dangerous misconception you could have, particularly given the growing threat from ransomware. This breed of malicious software, used by cybercriminals to prevent businesses from accessing their own data, is often aimed at small to medium-sized organisations simply because they are regarded as
easy targets.

In 2020, healthcare organisations large and small were among the biggest targets for ransomware, both in the U.S. and Europe, because the sensitivity of private patient information made them particularly vulnerable. Globally, no organisation or industry is immune. This is especially true for organisations in the Asia Pacific (APAC) region, who are 80 per cent more likely to be the target of a cyberattack.

By encrypting the contents of critical operational systems such as sales and payroll records and holding that data hostage, bad actors can threaten to put small and medium-sized business (SMBs) out of business. Even if your business pays the ransom (against the recommendation of law enforcement), you might not get your data back.

Ransomware is a big deal but far from the only threat. Consider what would happen if flood or fire wiped out your systems. What if a cloud service you depend

on suffers an extended outage? Think through the worst-case scenarios, and you will find plenty of reasons to invest in BCDR.

Myth #2: Backup is good enough

Backup is a critical part of BCDR.

However, on its own, backup leaves businesses susceptible to costly downtime. Why? Because recovering large data sets (such as the contents of an entire server) can be time-consuming. Not to mention the time it takes to procure new hardware if primary systems become inoperable.

Meanwhile, productivity grinds to a halt, and revenue stops flowing.

That's why businesses need a solution that enables fast restores in addition to a backup. For many organisations today, that means BCDR. BCDR solutions use backup, snapshot, virtualisation, and the cloud to protect data and enable fast restores that will keep your business running without a hiccup.

A 2020 survey found that, on average, 70% of SMBs had servers protected by a backup solution of some sort but only 55% of servers were protected by a full BCDR solution. You don't want to be the one leaving critical services exposed.

Myth #3: I don't have to worry about BCDR because most of my data is in the cloud

While having data in the cloud can be useful in some BCDR scenarios (for example, allowing employees to log in to applications from home after the office burns down), don't overestimate how much protection you are getting "for free" by using software as a service (SaaS) applications or cloud storage.

Both Microsoft and Google, the two major providers of cloud office productivity suites, explicitly specify that their services are offered under a "shared responsibility" model in which you bear much of the responsibility for data protection and data integrity. The same is true for Amazon Web Services. That means cloud providers won't necessarily help you recover a file that was accidentally deleted. Nor are you necessarily protected against ransomware or other hacks if your cloud credentials are compromised and are used to delete, encrypt, or corrupt data.

File sync and share tools aren't a substitute for BCDR, either. Why? Because, when a cloud file sync and sharing service detects that a file has been deleted, it typically deletes all copies, local and remote, including older versions. If you ever need to get one of those files back, for example, for an audit, lawsuit, insider fraud, or security breach investigation, you could be out of luck.

Myth #4: All clouds are the same

Yes, all cloud providers deliver highly available server and storage infrastructure. But, that does not mean they are ideal for BCDR. Public cloud costs on Amazon Web Services, Microsoft Azure, and similar infrastructure are unpredictable at best.

Yes, you only pay for what you use, but that means costs spike at the worst possible time—when you mount and run a recovery virtual machine (VM). Additionally, cloud providers charge egress fees for moving data out of the cloud. Downloading a large data set from the cloud, as you must do to restore a server, can be costly. Some vendors will also surcharge you for testing the integrity of your disaster recovery configuration — even though such testing is an essential best practice for BCDR.

General purpose public clouds have different tiers for computing, storage, and security, which can add complexity. In other words, you might not be able to understand the final cost until you get the bill.

When you use a purpose-built BCDR solution, with all costs for backup and restoration bundled into a single monthly fee, you know exactly what you will pay.

Cloud services also vary in their performance characteristics and how well they meet your security, data privacy, and compliance requirements. If a service provider promises you "cloud backup," make sure you understand what cloud service is behind that promise and how far you can trust it.

Myth #5: All BCDR solutions offer equal protection against business risk

This simply isn't true. All BCDR solutions are not created equal. Proper BCDR software enables:

- Local and cloud backup
- Local and cloud failover
- Restore capabilities that meet a variety of recovery scenarios

Recovery scenarios can range from restoring a few lost files to a complete server failure. So, look for solutions that address all those needs. In addition to VM failover, a BCDR solution should offer capabilities like file and folder restore, ransomware detection and rollback, server image export, and bare metal recovery.

Data immutability is another important consideration. Data immutability means that data is stored in a manner that it cannot be modified by external operations. It ensures that backups cannot be corrupted by ransomware or deleted in some

other form of attack. Your solution should take advantage of the bandwidth and storage efficiencies gained from incremental backup but also ensure the integrity of the entire chain of backups for reliable data restoration.

Additionally, many BCDR products require multiple vendors to build a full solution. This can result in multiple points of failure and potential finger-pointing among vendors, so it takes longer to resolve issues. Choose a solution unified around a consistent architecture to avoid these issues.

Beyond the Myths: A Complete Cloud BCDR Solution

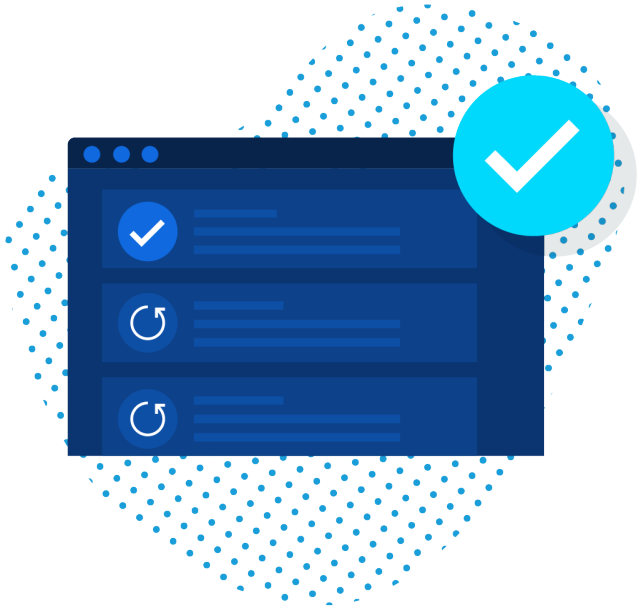
We offer BCDR services in partnership with Datto, a specialist in cloud BCDR for businesses of any size. We provide deep knowledge of your business and ongoing, attentive service. They provide the scalable cloud infrastructure specifically designed for BCDR, as well as the software to be installed locally.

Together, we construct and maintain a reliable and cost-effective safety net for your business.

Here is how Datto Continuity stacks up against the myths we have discussed.

Myth #1: BCDR is only for large enterprises. It is just as critical for SMBs to have a BCDR plan. The 2019 Verizon Data Breach Investigations Report showed that 43 % of security breaches involved small businesses. Datto's technical architecture, pricing, and partnerships make BCDR accessible to any sized business.

Myth #2: Backup is good enough. Datto goes beyond basic backup -- or even backup to the cloud -- to provide a service optimised for rapid data restoration and screened against malware.



Myth #3: I don't have to worry because my business uses cloud services. Datto Continuity backs up cloud servers, as well as local ones. By adding Datto SaaS Protection, you can also protect Microsoft Office 365 and Google Workspace accounts.

Myth #4: All clouds are the same. Unlike generic public cloud services, both the performance characteristics and pricing of the Datto Cloud are optimised for BCDR. Because Datto provides predictable pricing (no "data egress" surcharges for retrieving data from the cloud), we protect you against being hit with excessive fees when you can least afford them.

Myth #5: All BCDR solutions offer equal protection. Datto provides an all-in-one BCDR solution that prevents data loss and corruption. Where some other incremental backup technologies are vulnerable to errors anywhere in the "backup chain," Datto's patented Inverse Chain Technology ensures every point-in-time snapshot is complete and bootable.

Datto Continuity is a complete BCDR solution that offers comprehensive backup and recovery for physical and virtual servers. Deployed as a physical appliance, as software installed on a virtual machine, or an image on your own hardware, Datto Continuity provides local and cloud backup, recovery, and failover. That means you can quickly restore a deleted file from local backup, or restore a whole cluster of servers to an alternate location or a virtual machine in the cloud.

Here is what the Datto Continuity offers to protect your business

- Immutable backups, protected against tampering
- Cloud Deletion Defence against accidental or malicious file deletion
- Backups screened against ransomware

- Instant recovery
- World-class cloud infrastructure
- End-to-end security
- Infinite scalability
- Infinite retention
- 24/7/365 dedicated, in-house support
- Unlimited Cloud Storage
- Flexible deployment
- Secure, multi-tenant cloud management

If you want your business to be resilient, you need a BCDR plan grounded in reality. You can't afford to be misled by myths and misconceptions, or a false sense of security. You need a strategic and technical partner who is committed to giving you the insight and direction you want to implement the BCDR plan you need. Our dedicated team is committed to helping you plan and execute growth, and not break along the way.

Get in touch today to learn more. We'd love to answer your questions.

LabyrinthTechnology

Paul Ravey | Business Development Manager | Phone: 02037907500 | Email: paul.ravey@labyrinthit.com | Labyrinth Technology