eBook

4 Reasons CEOs Should Care About BCDR

Introduction

You don't get to be a CEO without taking some chances, but there is a difference between taking on risk in search of an outsized reward and taking on unnecessary, avoidable risks. In an era when so much of business depends on data and computing, the proactive CEO values a solid business continuity and disaster recovery (BCDR) plan. After all, why would a leader risk the damage that could be done by failure to recover quickly from a systems outage, the destruction of a facility, a ransomware attack, or the loss of critical data?

Unfortunately, the necessity of BCDR is not apparent to everyone. To help you justify the investment, here are four critical reasons that you, the CEO, should care about business continuity and disaster recovery.

1. Because downtime is expensive

If your employees lose access to business-critical applications and data, there is a direct impact on productivity and revenue. While this sounds obvious, many organizations do not consider the total cost of downtime. To better understand how the damage adds up, consider the following example created with Datto's Recovery Time and Downtime Cost calculator.

Let's say your business has 100 employees, the average hourly revenue is $1,500 and the backup data set amounts to 2 TB. Given these parameters, a full restore from a local backup would take over 8 hours. The associated downtime cost would amount to $34,000 in lost revenue.

Modern BCDR products can quickly launch a virtual instance of an application and all its data on a virtual server hosted within the backup environment. This lets users continue operations while primary application servers are restored. Choosing a BCDR solution that minimizes downtime makes good business sense.

2. Because backup alone is not enough

Backup and business continuity are not the same.

You'd be hard-pressed to find a business today that doesn't conduct some form of data backup. But what happens if a flood wipes out your primary and backup servers? You need to know the systems your business relies on will continue to operate, no matter what.

Sending a copy of data offsite for disaster recovery is one way to ensure business continuity. Historically, this meant sending tapes to a secondary location or tape vault. Today, BCDR solutions can run applications from backup instances of virtual servers. The best of them extend this capability to the cloud—an approach known as disaster recovery as a service (DRaaS).

The ability to run applications in the cloud while onsite infrastructure is restored is a game-changer for disaster recovery. As CEO, you don't want yesterday's backup technology.

3. Because disasters take many forms

Not every disaster is broadcast on news and weather channels. Most IT downtime is a result of common, accidental (or malicious) data deletion, damage to computer hardware, or poor security habits. For example, a recent OWI Labs survey found that 81% of respondents occasionally or regularly use public WiFi, despite security risks. A ransomware attack or virus can halt operations just as easily as a tornado or a power surge. These "lowercased" disasters are typically a result of human error, which is unpreventable.

Having technology in place that allows your business to continue operations following these man-made disasters is equally, if not more important than protecting against a hurricane that may or may not strike your business.

4. Because resilience matters

Ensuring access to applications and data following a disaster is just one piece of the BCDR puzzle. Evaluating your business's ability to restore IT operations can be a good starting point for company-wide business continuity efforts, but good BCDR planning should look at the business as a whole, and the goal should be to develop business resilience, in addition to cyber resilience. In fact, many BCDR planning efforts start by conducting a business impact analysis or risk assessment — these studies can reveal weaknesses in your business's ability to continue operations that go far beyond IT.

You know a disaster (natural or otherwise) will be coming to your company at some point. When it does, you want to be as well-prepared as possible.

Conclusion

Business continuity and disaster recovery is a company-wide responsibility and failure to protect your business from human error, hardware failure, and/or natural disasters can be detrimental and impact every stakeholder. Once you've implemented a solid BCDR plan, you will sleep better knowing you're fully prepared for any disaster that might come your way.

We can help give you that assurance. Working with Datto, we ensure complete, ransomware-free backups and rapid data restoration. The Datto Cloud is immutable, so it's always possible to recover a clean copy of a file, email, or an entire server. Backups are protected against ransomware, data corruption, and files or emails being accidentally or maliciously deleted.

Care to learn more? Contact us today.