eBook

8 Disaster Recovery Best Practices for Business Continuity

Introduction

Disaster can strike at any moment, and it's impossible to plan for every eventuality.

When Hurricane Katrina hit New Orleans, no one was prepared for the devastation. Flooding destroyed countless businesses while others went weeks without power and still others were reduced to rubble. In fact, many companies were down for weeks or, even, months. And downtime is devastating.

But it's not just natural disasters that you have to be worried about. Accidental and malicious data loss happens regularly. In fact, according to Richmond House Group, 20% of small to medium businesses will suer a major disaster causing loss of critical data every five years. Whether natural or otherwise, data loss hurts your bottom line and can, potentially, cause a catastrophic end of all business events.

For example, in July of 2016, Southwest Airlines experienced a system outage that lasted for more than 12 hours and resulted in canceling more than 1,850 flights, delaying hundreds more, and worse. Southwest had no warning before their network router shorted and that's why it's vital to have a plan of action in place far in advance.

[Source : http://www.usatoday.com/story/travel/flights/todayinthesky/2016/07/22/southwest-airlines-flightwoes-cascade-into-friday/87430038/"]

Your company needs to be ready to not only deal with the aer-eects of any disaster-level event but to make it through successfully. And that's where a cloud-to-cloud backup plan comes into play

Cloud-to-Cloud Backup Plan

Don't be like 32% of companies that lost data from the cloud (Aberdeen Group). Instead, follow our top eight disaster recovery and data backup best practices that we recommend for every organization that believes business continuity is a high priority.

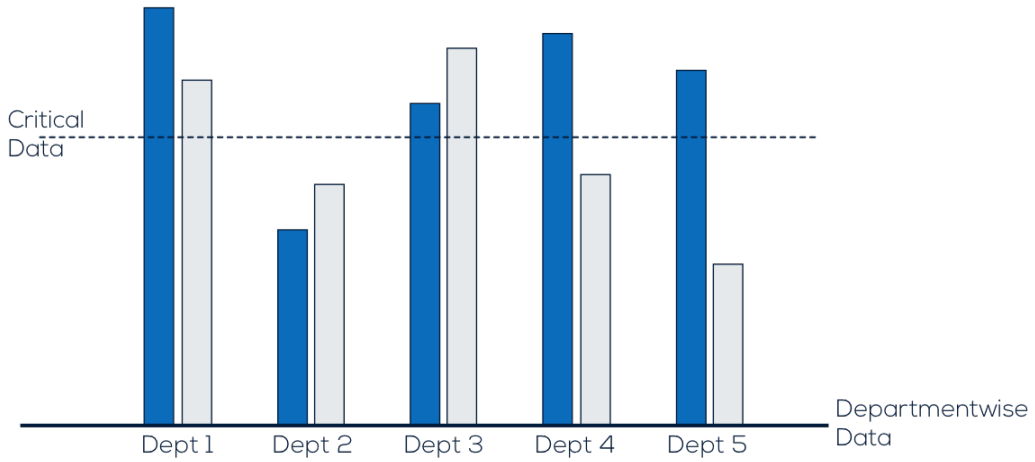
[Source: http://www.aberdeen.com/research/8323/ai-cloud-data-loss/content.aspx]

1 Understand the Total Risk and Opportunity

You can't protect your company from disaster if you don't first understand the total risk and total opportunity presented by the disaster. The risk and opportunity might be slightly dierent for every situation but, in general, you can prepare by looking at all sides of the equation.

To understand total risk, each department within your organization from IT to operations, sales, marketing, and finance should ask themselves a few simple questions. "What disasters could strike (natural or otherwise)? What operations are most critical for us and where are they located (on the cloud or on hardware)? How would a disaster eect us?" For example, if you were a shipping company, do you have so even if the unexpected happens, you're able to access your data from anywhere in the world and you know that it's been automatically archived daily (even the recycle bin)?

[Source: http://www.cloudally.com/oice-365-backup/]

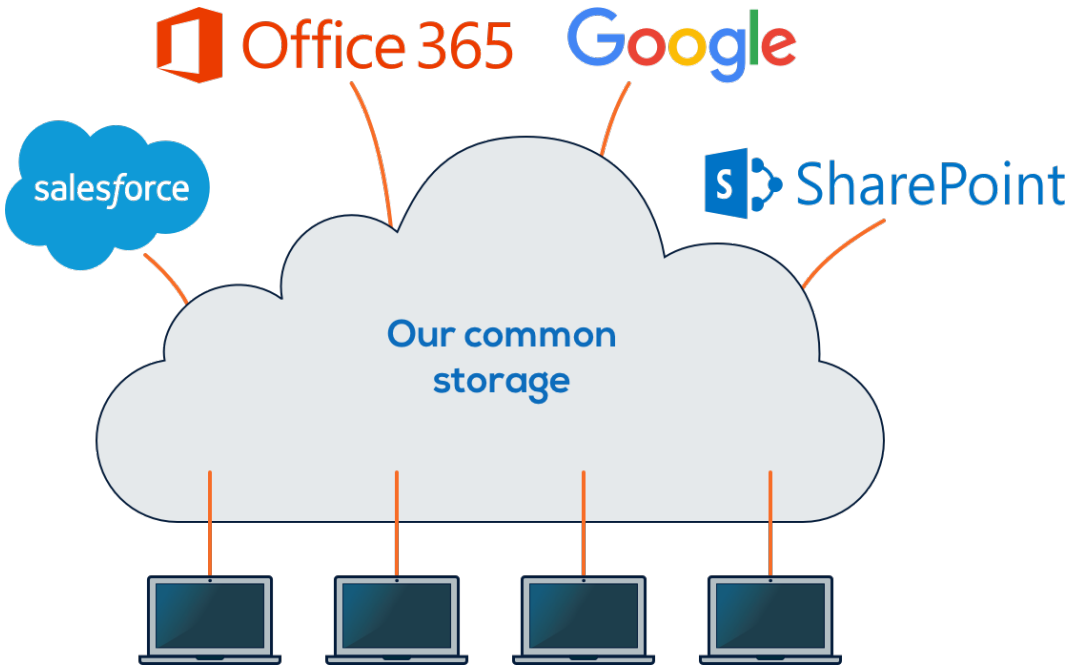


The opposite side of risk is opportunity. Disasters don't just aect your company but also your competitors. You should be prepared to take advantage of various situations in any way you can. For example, you should consider how your business can help from a monetary, humanitarian, or social good standpoint when a natural disaster strikes. You should also be prepared to demonstrate to your clients how you have in place, unlike your competitors, so your critical data is never at risk.

[Source:http://www.cloudally.com/backup-salesforce/]

2 A Well-Trained Leadership Team

Your company is only as successful as its leadership. An empowered and dedicated staff can turn any disaster into a success story. This is especially true for small- to mid-sized businesses that aren't required by industry regulations to have a specific disaster recovery or backup plan in place. A well-trained leadership team should ensure that data loss is never a point of no return.



Daily backup training through reports

The first key is to empower your leadership team to take control of the data and operations in their department with an all-in-one-tool. For example, when you sign up for our cloud-to-cloud backup solution, all of your data from Salesforce to Office 365 and Google Apps is stored in one location. From there, all you need to do is to train your leadership team to manage the daily backups through reports, to control user access for security, and to recover lost or corrupted data when the worst happens. Without our cloud-to-cloud backup, the training required for your leadership team is much more complicated. With us, all you have to do is trust your leadership team to support your efforts and to manage business continuity within their realm.

3 Use the Right Tools

In today's highly digital and complex business world, old-school backup systems and disaster recovery plans developed in Excel and Word won't suffice. Your data is a living system that constantly changes during day-to-day operations. That's why daily, automated backups for all of your software platforms from Google Drive to Salesforce and Box are necessary. A backup tool that requires manual saving or only covers certain operational functions can leave you wanting.

That's why we offer a simple three-step process for managing your data

1. Set It: We allows you to select your archive location, backup time, and frequency for every platform and user.

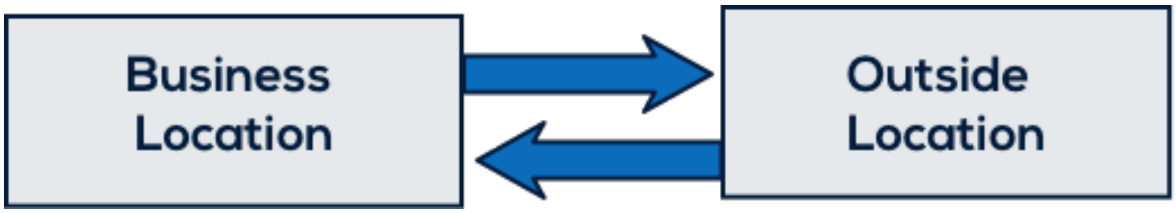
2. Manage It: With our cloud-to-cloud backup, you receive daily backup reports containing all your activity, so you can double check it's accuracy. You can also manage your users and export backups and archives.

3. Access It: Finally, we make it quick and easy to search for and locate data in your archives. From there you can also perform non-destructive restores.

Before you choose your DR and backup tool, make sure it does what you want and need.

4 Maintain a Full Copy of Critical Data Outside of Your Business Location

This is vital particularly in cases of natural disasters or malicious data deletion. If your only backup data center is on site or just a few miles away from your current location, a single event could easily disable both your headquarters and your backup. In general, it's best if you keep a full copy of your critical data at least 150+ miles away from your business or completely online. That distance is typically sufficient to ensure that both backup centers are not affected by a single disaster.



Ideally, your data backup should be stored safely in the cloud. Unfortunately, the cloud isn't always safe. In fact, 47% of enterprises have lost data in the cloud according to Symantec. That's why at our solution is **ISO 27001 and HIPPA certified** and uses advanced **AES-256 bit encryption. This level of security ensure that your data remains private and is retained online as long as you need it.**

[Source:http://www.symantec.com/content/en/us/about/media/pdfs/ b-state-of-cloud-global-results-2013.en-us.pdf] [Source:http://www.cloudally.com/secure-online-backup]

5 Focus on Consistency

Nowadays, rarely does a business use a single software, application, or piece of technology to handle all operations. That's why the biggest challenge of any backup and DR plan is to ensure consistency across all applications. We offer data backup for multiple applications and software all within one interface because if you're replicating a complex business ecosystem, it's critical that all backups are in sync.

6 Test Your Plan Regularly and Realistically

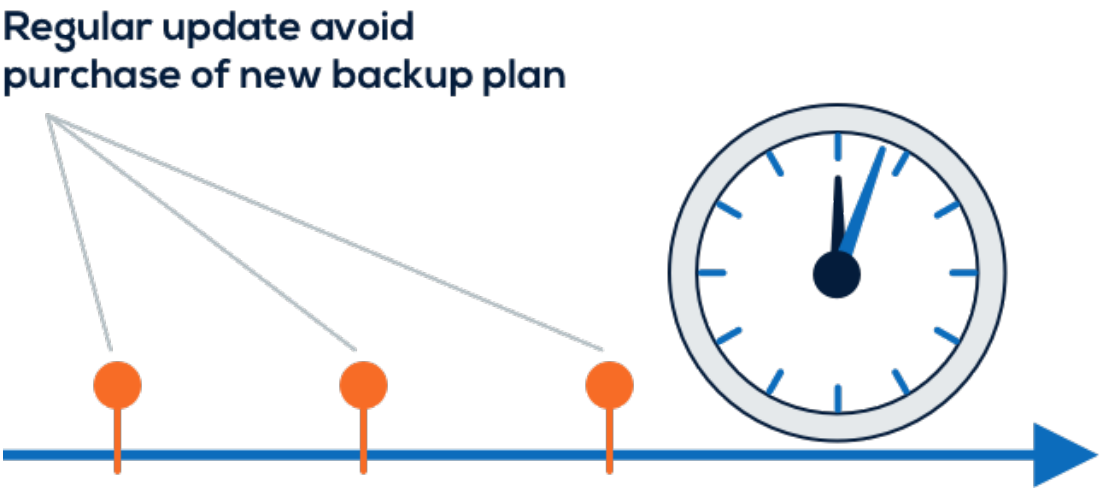
There's nothing worse than trusting in your backup and disaster recovery plan only to discover that it wasn't up to the task when it was needed most. The truth is that untested plans are failed plans. If you've never tested your BC/DR plan realistically, your company won't be ready to handle the situation when disaster strikes.

When it comes to testing, there are many kinds of tests and you should use them all. We recommend testing one particular process at a time before implementing a test that assumes your business has become nothing but a smoking ruin. The reason why testing is so important is that it helps to verify that your recovery procedures are correct while also helping your employees become familiar with crisis procedures. The most well- prepared companies implement testing at least twice a year.

With our service, testing is easy. All you need to do is login and look at your daily report containing all the details of your backup activity. You can even export data for local use or search and locate within your archives to ensure everything has been saved appropriately.

7 Update Your Disaster Recovery and Backup Plan Regularly

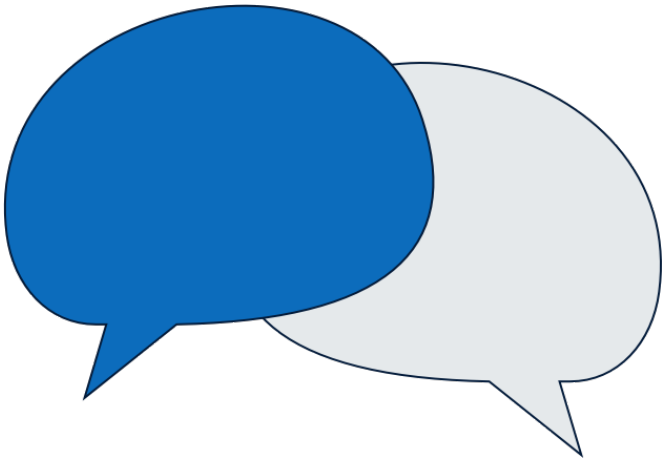
No company remains stagnant. Business practices constantly evolve and update based on new information, updated applications, and new infrastructure. Now, imagine you spent six months designing the perfect BC/DR plan but since then you've implemented new software that works off a physical server and not the cloud. Suddenly, your plan and tests are outdated and don't protect you fully. In that situation, a disaster would make all your hard work for naught unless you consistently update your plan.



To stay protected, your company should practice rigorous change management that keeps your backup and disaster recovery plan in line with your current business practices. And when you use our service, changes in your business don't have to mean a major change in your backup. Our backup solution works with all of your software, even Amazon Cloud, and it can even detect new users automatically. So, not matter how much your business advances, you don't have to purchase a new backup solution, you just have to update our cloud-to-cloud backup solution.

8 Make Communication a Priority

Too often, a DR/BC plan is the work of a single IT person or small department. Unfortunately, this means that if a critical individual becomes sick, leaves the company, or is unavailable during an emergency, the entire plan falls apart. That's why communication before, during, and after a disaster or incident is vital.



The disaster recovery planning process should involve several people and departments, and the plan should be well-written enough that it can stand on its own. That way, if a widespread problem or incident renders several people unavailable, the recovery program can still take place. The key is to outline work expectations, application procedures, and information dissemination for every department and individual.

Unfortunately, no matter how carefully and diligently you plan for every eventuality, you can't prepare for everything. Anything and everything can and potentially will go wrong. That's why having a data recovery and business continuity expert is key to your success. Contact us today to discover how we can help.