

6 Common Data Backup Mistakes That Established Businesses Make – and the Costly Consequences That Follow

Opinions expressed by Entrepreneur contributors are their own.

Key Takeaways

- While most established and larger companies with big IT budgets employ professional backup solutions, they still often make costly mistakes.
- These include long intervals between backups, not testing backup recovery systems regularly, not being able to restore a backup to a different device quickly, keeping backups in a single location or only in a remote cloud and failing to do a cold backup.
- Keeping data backed up, protected and tested is a big investment, but it is well worth it in the long run.

In my previous article, I examined five data backup mistakes that could bankrupt a startup. Now, nearly all established and larger companies with huge IT budgets will employ professional backup solutions and prevent these errors. But even these companies can still make some other mistakes in backup, which may cost them millions of dollars.

So, here are five of the most common backup mistakes that established companies make and some tips on how to avoid them.

Related: 5 Data Backup Mistakes that Could Bankrupt Your

Mistake 1: Long intervals between backups

One of the most important steps that anyone can take to protect data is to make a backup. In case the data is stolen or lost, you can always recover it. However, even larger organizations make the mistake of not backing up their data storage in a short interval regularly. According to a recent report, 91% of all organizations back up their data, but only 26% actually do it daily.

A majority of organizations either do it once every week or once every month. A large organization can have thousands of customers, inventories and products, and accumulate terabytes of new data every week. Once a data disaster occurs, even with the backups, you will still lose data for about one week.

For example, Walmart, the world's largest retailer, handles 240 million customer transactions a week. That's 2.5 petabytes (*1 petabyte equals 1 million gigabytes*) of data every hour. Even losing a single hour's worth of data can be costly for a company of this scale. Therefore, for larger companies, a minimum of daily backups and even automated live backups are the only solution.

Mistake 2: Failing to test backup recovery regularly

Keeping a backup of all your data does not automatically make it secure. According to a report, more than 50% of all backups actually fail when data is being restored. This can be due to incomplete backups, corrupt files or just the recovery software not performing.

Whatever the case, even large organizations fail to understand the importance of testing backup recovery systems. It is important to “test drive” data recovery systems, modules and their efficiency regularly.

What use are data backups when they fail to work when needed the most? Most leaders view this as an expensive chore that takes up resources. Nothing can be further from the truth. A large organization should test its data recovery systems every quarter as a minimum and every week for the most important data.

Mistake 3: Cannot restore to a different device quickly

Another common mistake is using backup software that cannot restore the backup to a different device quickly.

If a computer is damaged, lost or stolen, the company might have to buy a new one with a completely different hardware configuration. If the backup software cannot restore the backup to the new computer and make it a bootable system directly, the company needs to manually install the operating system on the new computer and restore the other data separately, which costs a lot of time and human resources.

This problem is more critical if your data recovery plan has a lower recovery time objective (RTO).

Related: One of the Most Overlooked Risks in Business – and How to Protect Yourself Before It’s Too Late

Mistake 4: All backups in a single location

Many large companies, instead of storing their data on the cloud, build their own in-house data storage. The idea is to

keep data “within the company” and safe from potential theft. However, having all physical storage and backups in a single location is a disaster waiting to happen.

Therefore, in times of a disaster, such as a fire, burglary or even earthquakes, your data might not really be safe since they are all stored in one location.

Mistake 5: All backups in a remote cloud

On the other hand, there are large companies that only rely on remote cloud networks for data storage and backup. This might make it difficult and time-consuming when there is a need to restore data.

However, a more serious problem can be that of cloud servers failing. One of the most famous examples is that of OVHcloud, a French data center that caught fire and brought millions of websites down. This included websites of government agencies, banks and businesses.

Any organization that did not have a physical storage probably lost all of its data. Therefore, storing on the cloud alone comes with its own risks.

Mistake 6: No cold backup

Many large companies fail to make a cold backup of their data. A cold backup is an offline backup on an air-gapped external hard drive. When ransomware attacks, it not only attacks your data but also your online backups connecting to your system. Keeping an external air-gapped backup of all your data is one of the best ways to keep your data protected.

Related: [**5 Reasons to Make Regular Data Backups a Part of Your Business Plan**](#)

Even large and established companies make common backup mistakes that can jeopardize their data management. Properly backing up data is one of the easiest ways to protect yourself against ransomware attacks, human errors and even hardware failure.

Keeping data backed up, protected and tested is a major investment for large companies. By some estimates, an organization of 1,000 employees can typically look to spend \$267,000-\$675,000 or 7% of their IT budget on backing up data.

Such an investment, if done right and if these common mistakes are avoided, is well worth it in the long run.

Key Takeaways

- While most established and larger companies with big IT budgets employ professional backup solutions, they still often make costly mistakes.
- These include long intervals between backups, not testing backup recovery systems regularly, not being able to restore a backup to a different device quickly, keeping backups in a single location or only in a remote cloud and failing to do a cold backup.
- Keeping data backed up, protected and tested is a big investment, but it is well worth it in the long run.

In my previous article, I examined five data backup mistakes that could bankrupt a startup. Now, nearly all established and larger companies with huge IT budgets will employ professional backup solutions and prevent these errors. But even these companies can still make some other mistakes in backup, which may cost them millions of dollars.

So, here are five of the most common backup mistakes that established companies make and some tips on how to avoid them.

The rest of this article is locked.

Join Entrepreneur+ today for access.

<https://www.entrepreneur.com/science-technology/6-common-data-backup-mistakes-established-businesses-make/498620>