



The Importance of Testing Your Backups

Most businesses are aware of the need for data backup. Without it they risk losing important files in the event of a hard drive failure or cyberattack. Yet having a backup in place isn't enough: it's important to also regularly test that backup. You need to be able to restore that essential data when you need it.

The many reasons to establish data backups include:

- protecting against natural or man-made disasters (including hacker or insider attack)
- ensuring compliance with tax, financial, and other industry standards
- reducing downtime
- improving productivity

It's recommended that backups are stored in the cloud. The cloud option gives you the most flexibility. It can be accessed from anywhere, regardless of conditions in your particular environment.

Yet while many people know they need backups, too few do recovery tests. The worst time to find out there's a problem with your backup solution is when you need it the most.

Testing Data Backups

Regular data backups can offer peace of mind, but you'll really know you are ready to go if you regularly test your ability to recover your system from a backup.

Testing your backup lets you verify the necessary data is available for recovery. Plus, testing helps you learn how to actually implement recovery following a data loss. If a backup test fails, you can take the steps needed to ensure you don't actually lose valuable information. Otherwise, you're throwing money at storage space and backup services that are no help, and you'll find out too late.

Regular monitoring helps you keep track of any software or hardware changes that may have an impact on data backups. Via testing, you might also learn some staff members are storing data somewhere that isn't being backed up, and you can now intervene with those employees or extend your backup protocols to prevent that data getting lost.

Scheduling data backup tests can also help you to identify a misconfiguration in the backup software or ways in which you're not adequately addressing your backup needs. For instance, you might not have set up a complete backup in the first place. This might mean you're backing up the data but not the settings.

Most backup software will send error messages if there was an issue backing up. Still, they're easy for an overworked IT team to miss.



Actively testing backups allows the business to confirm fallback data accuracy and effectiveness. Additionally, you'll be able to gauge:

- how long it takes to perform the backup
- any issues that arise during recovery
- what steps need to be taken to address those problems

All of this is something you want to consider proactively. Some people say they work best under pressure, but most of us think more clearly and perform better if not in the midst of a data catastrophe.

A managed service provider can help your business with data backup and recovery testing. They can monitor for failures and make any changes needed to get the backup running properly again. You'll be glad you did recovery testing in advance when things run smoother and quicker amid your disaster recovery.