RESTECH SOLUTIONS

DATA BACKUP SURVIVAL GUIDE:
PROTECTING YOUR MOST VALUABLE ASSET

Your Data Is Highly Vulnerable to Loss

As extraordinary and as reliable as technology has become over the years, it is by no means foolproof. Perhaps even scarier is the high probability that you could encounter any number of these various threats to your data at least once.

PHYSICAL SYSTEM FAILURES:
Hard drive failure, software crashes or corruption.

EXTERNAL THREATS
Cyberattacks and hackers, malware, viruses and ransomware.

NATURAL & LOCAL DISASTERS
Fires, floods, power surges and rodent or construction damage.

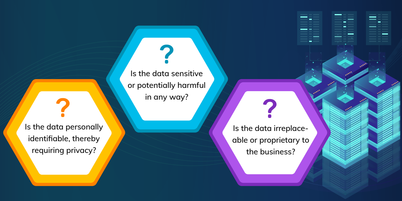
HUMAN ERROR
User mistakes and errors continue to be a major cause of data loss.

LOST/DAMAGED DEVICES
1 in 5 laptops are lost during their lifecycle.

INSIDER THREATS
Disgruntled employees with malicious intent can put your data at risk.

What Data Needs Backup?

The simple answer is ALL DATA. Including all data and information assets in your backup process is a data protection best practice. Some data, if lost, may have a larger impact on your business, so it is important to identify all business-critical data by performing a risk and business impact assessment that includes the following questions:



How Often Do I Need To Back Up?

You will want to configure your backups to fit your specific business needs and normal rates of change. A good way to start is by automating a daily backup of all the activities or transactions that take place each day. In addition, you should configure a minimum of one full image backup of all systems once every week.

What Backup Types Should I Include?

There are 3 main types of backup approaches you should include as part of your backup and disaster recovery plans.

FULL BACKUPS
Entire data set, regardless of any previous backups or circumstances.

DIFFERENTIAL BACKUPS
Any additions or alterations to the data set since the most recent full backup was performed.

INCREMENTAL BACKUPS
Only additions or changes that have taken place since the last/most recent incremental backup.

Where Should My Backups Be Stored?

It is strongly encouraged that you implement the 3-2-1 backup method or strategy as a minimum best practice for protecting your data.

Generate 3 independent copies of your data at all times.

Store copies using at least 2 separate media storage types.

Keep 1 or more copies in an off-site location, such as in the cloud.

Test Your Backups Regularly

It is crucial that you check and test all your backups at least once per quarter as a minimum. However, this frequency would likely increase if your business has very high data entry change rates or large quantities of data assets.

Regular testing is the only way to monitor the success rates of the backups and to verify the integrity of your data.

It is helpful to routinely check your backups for proper configuration and automation rules, especially if you are growing rapidly or have a high turnover.

Testing ensures that your business has the proper tools and correct infrastructure needed to store and recover its critical data during and after any situation.

Regular Testing Is Insurance For Your Backups

Data is the lifeblood of every business and is one of the most valuable assets you can acquire and possess. Proactive prevention is always better and less costly than a cure.

Make routine testing a standard process as part of your backup and disaster recovery strategy because it protects your data, your reputation and your long-term business success.

If you need support implementing a comprehensive data backup and protection solution or want to make sure your current solution is up to the job, contact us to schedule a consultation today.

RESTECH SOLUTIONS

713-936-6855
info@restech.solutions
https://restech.solutions/contact