DATA BACKUP SURVIVAL GUIDE

PROTECTING YOUR MOST VALUABLE ASSET.

YOUR DATA IS HIGHLY VULNERABLE TO LOSS

As extraordinary and reliable 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.

We've highlighted some of the key threats to your business and the questions you need to ask yourself.

SHACKLETON
your information technology team

THREATS TO LOSS OF DATA

PHYSICAL SYSTEM FAILURES

Hard drive failure, software crashes or corruption.

EXTERNAL THREATS

Cyberattacks and hackers, malware, viruses and ransomware.

LOST/DAMAGED DEVICES

Device damage or loss due to intentional or unintentional causes, as well as natural disasters.

NATURAL & LOCAL DISASTERS

Fires, floods, power surges or construction damage.

INSIDER THREATS

Employees who are disgruntled or have malicious intent.

HUMAN ERROR

User mistakes or unintentional errors.

WHAT DATA DO I NEED TO 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 significant impact on your business, so it's crucial to identify all business-critical data by performing a risk and business impact assessment that includes the following questions:

1. **IS THE DATA PERSONALLY IDENTIFIABLE, THEREBY REQUIRING PRIVACY?**
2. **IS THE DATA SENSITIVE OR POTENTIALLY HARMFUL IN ANY WAY?**
3. **IS THE DATA IRREPLACEABLE OR PROPRIETARY TO THE BUSINESS?**

HOW OFTEN DO I NEED TO BACK UP ?

A **minimum** of **one daily backup of all the activities or transactions**.

However more backups, spread throughout the day, will cut down on the amount of data you could lose in the event of an issue.

We **recommend** **three backups, a day** as a good starting point, but it will depend on your business needs.

WHAT TYPE OF BACKUP SHOULD I USE ?

Modern backup systems are based around an initial **full backup image** and then subsequent backups are differential, and any additions or alterations to the data set are backed up.

All modern backup systems should be **fully automated** and include copying your data offsite to a cloud-based storage system. This removes the need for rotating disks or taking media offsite where it could be lost. It also removes the human approach, where errors can easily occur, and offsite backups do not take place.

Some backup systems allow **local virtualisation**, this means even in the event of your server catching fire you can be back up and running again in minutes/hours, by starting your last backup as a virtual machine. This can be business critical if the server needs repairing or replaced.

WHERE SHOULD MY BACKUPS BE STORED ?

Your data should be stored in three places:

1

Live on the server/ storage device you are working from.

2

A local copy of the data to allow for quick restores if required.

3

Offsite in a secure data centre.

It is critical that your data is stored offsite so in the event of a major event like fire/flood at your premises your data can be recovered and the business restored once you have recovered.

TEST YOUR BACKUPS REGULARLY

Check and test all your backups at least once per quarter. This frequency will 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 backups and verify your data's integrity.
- Check your backups routinely for proper configuration and automation rules, especially if you are growing rapidly or have a high turnover.
- Testing ensures your business has the proper tools and right 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 your business and 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 of your backup and disaster recovery strategy.

If you need support implementing a comprehensive data backup and protection strategy, or want to ensure your current solution is up to the task, we can help.

SHACKLETON
your information technology team

enquiries@shacktech.co.uk