INSIDER SECRETS AND FACTS

Every Business Owner Should Know
About Choosing a Remote Backup Service

Dial a Nerd

Data is important to all businesses, and operations cannot be halted for days – or weeks, due to corruption, data loss, or unexpected power cuts during load shedding. This document will provide a summary of common and costly mistakes that small businesses tend to make when it comes to backing up data.

Highlights include:

- Explanations of what remote, offsite and managed backups are, and why ALL businesses should have a backup in place
- 7 important criteria you should ask for from any remote back up service; and remember, you cannot trust any company who does not meet these requirements
- Tape backups – where they fail and how they give you a false sense of security
- Terrifying scenarios, trends, and questions all business owners should know and consider when it comes to data security
- The most important factor to look out for in any remote backup service provider

FROM THE DESK OF: AARON THORNTON

MANAGING DIRECTOR

DIAL A NERD

Dear Colleague

Have you been in a situation where you lost an hour of work on your PC?

Now just imagine losing days or weeks' worth of work – or losing a clients database, financial documents and every single work file a company has ever produced or written.

Imagine if the network went down for days and what would happen if you could not access emails and information on your network. It would be devastating.

How about if there was a flood, major storm or fire that had destroyed your office and all the files inside it? Or if a virus attacked your server and wiped out everything? Do you have emergency recovery plans in place that you are confident will cover you in any of the above scenarios?

If you don't have the answers to these questions, or a strong disaster recovery plan in place, you are basically playing Russian roulette with your business. Due to the ever increasing number of threats, it's only a matter of time before serious problems materialize.

THAT WILL NEVER HAPPEN TO ME!

A recent case study based on 150 small and mid-sized businesses, found out that 6 out of 10 will suffer a major network or technology disaster that could cost them anything from R100,000 to R1,000,000 in repairs.

These costs don't even factor in loss of productivity, sales, and client goodwill that happen when a company is unable to operate or deliver on its promises due to technical problems.

It's not easy to put a price on the negative financial impact data loss has on a business, but it will most certainly be a large one.

"BUT I ALREADY BACK UP MY DATA."

Like most business owners, you've probably been smart enough to setup a tape backup. But, did you know: the average failure rate for hard drives is is 100%? All hard drives fail at some point or another.

Most businesses often underestimate this factor.

There are many instances of companies losing large amounts of Rands worth of data. Most of the time, these businesses already had a backup system in place but discovered too late that it did not function as it should have when it was most needed.

You should still maintain local data backups on hard drives but the following will render them useless:

- There is a malfunction with the actual drive thus rendering it useless and impossible to restore data. Important to note: it's common for a hard drive to malfunction without displaying any warning signs.
- Your office gets hit by a flood, destroyed in a fire, natural disaster, or if a power cut due to load shedding causes lasting damage to electrical equipment.
- The drives that you use for backups get physically damaged or corrupted by overheating or mishandling.
- A virus infects the drive. The more aggressive viruses, once corrupting the data, don't allow access at all.
- An employee accidentally formats the drive, thereby erasing everything saved on it.
- Theft by either a resentful employee or a break in.

The bottom line is that the last thing you want is to find out your backups are not working when you most need them.

TERRIFYING SCENARIOS, TRENDS AND QUESTIONS TO CONSIDER

- 93% of companies in the US that lost data for more than 10 days ended up filing for bankruptcy within a year of the disaster, 50% filed for bankruptcy immediately (Source: National Archives & Records Administration in Washington).
- On average, 20% of small to medium businesses will suffer major disasters every five year, which will cause loss of critical data (Source: Richmond House Group).
- Approximately 40% of small to medium businesses who manage their own network are prone to being hacked and more than 50% won't know if they've been attacked (Source: Gartner Group).
- The cause of data loss for 70% of business people will be due to accidental deletion, disk or system failure, viruses, fire or some disaster. (Source: Carbonite online backup service).
- The worst thing to do in an attempt to recover data is to restart or unplug the computer, this makes it near impossible to recover lost data later on (Source: 2005 global survey by Minneapolis-based Ontrack Data Recovery).

WHAT IS A REMOTE BACKUP AND WHY EVERY BUSINESS SHOULD HAVE ONE

The best way to completely protect your companies data and guarantee its potential for restoration after a major disaster is by maintaining regular backups at an offsite, highly-secure facility or in the cloud.

Remote backups are generally done automatically after hours via an internet connection. The solution must be simple and fast, so research for the right fit in your vendor is essential.

6 CRITICAL POINTS TO DEMAND FROM YOUR OFFSITE BACKUP SERVICE

When it comes to remote backup services, businesses face a huge risks due to lack of knowledge of what to look out for.

Hundreds of companies offer remote backup services because it is seen as a way to make a quick profit. Of course, not all service providers are created equal.

The next 6 points will help you choose a good, reliable vendor who won't charge you excessive fees or worse shrug off responsibility when it turns out your data wasn't backed up properly.

1. Security. An obvious point; you have to make sure the company safeguarding your data is secure. A lot is at stake here, such as financial information, client data, and sensitive information about your company. Never trust your data with anyone who doesn't have these security procedures in place:

   a) The physical location of where the data is stored is secure. Ask the provider if they have video surveillance, ID system, or a card key system that allows only authorised personnel into the building.

   b) Ensure that data transfers are encrypted with SSL protocols which prevent hackers from accessing data while it's being copied over.

2. Multiple data centres. Any expert in data security knows the way to avoid loss is to build redundancy into its operations. Put simply, the remote backup service should store multiple copies of your data in separate locations so that if one location is lost to some form of disaster, there is a backup elsewhere.

3. Physical copies of your data on demand. If you are in a situation where your network gets wiped out, you don't want an internet download to be the only option for recovery because that could take days or weeks. For this reason, you should pick a service provider who is able to provide overnight copies of your data physically.

4. Initial backup done physically. As mentioned, transferring this amount of data could take days or weeks. If you have a large amount of data to backup, it's faster and more convenient to do the first backup physically via hard drive.

5. Daily status reports. All service providers should send you a daily status update to verify the backup ran successfully or report if there was a failure or problem.

6. Good support. Even though most backup services are very easy to use, when a scenario arises that may have a huge impact on business continuity, it is essential to be able to get hold of support easily.

THE MOST IMPORTANT ASPECT TO LOOK FOR WHEN SELECTING A REMOTE BACKUP SERVICE PROVIDER

While the above mentioned points to look out for are important, the most important characteristic is often overlooked - Find a service provider that performs regular test restores to check your backup and make sure your data is recoverable.

You cannot afford to wait until your data has been lost to test your backup!

If your company has sensitive data you cannot afford to lose, you should perform test restores every month. If your data isn't as critical, every quarter is acceptable.

A number of things may cause a backup to become corrupt. Monthly tests mean bring peace of mind, knowing you have a good, solid copy of your data available to you in an emergency.

Dial a Nerd

Johannesburg, 260 Surrey Avenue, Randburg, 2194. Tel. 0100070012

Cape Town, Unit 11 Vine Park. Vine Road, Woodstock 7915. Tel. 0212001460

www.dialanerd.co.za email info@dialanerd.co.za National Phone 0861 4 NERDS (63737)