

Will your business survive equipment theft?

 By [Marius Maritz](#)

13 Sep 2018

Today, data is the lifeblood of businesses, yet many individuals and businesses are clinging to outdated data security practices. Business owners therefore need to ask themselves the question 'Will my business survive equipment theft?'



Marius Maritz is department manager at CloudProtect

If the answer to this question is 'no', these businesses then need to look at other options like the cloud. It's an easy, inexpensive and infinitely more secure option for storing data.

In South Africa, physical computing devices are hard to secure. Theft is, sadly, a growing statistic. However, hardware devices such as servers, smartphones, laptops and desktops, USBs and hard drives are all vulnerable to other threats. Accidental damage, device malfunctions, data corruption, disaster and cyber threats all increase risk.

To address this, new ways of securing data are emerging. Cloud storage solutions address many of the new vulnerabilities that make yesterday's data storage best practices defunct.

What exactly do I mean? Well, let's look at some of those practices.

Data storage best practices

The first rule is that data should be backed up to an offsite and off-premise location. Companies should be backing up their data to a hosted facility, to their own off-premise disaster recovery site or may even backup to a hard drive and take that off-premise daily. In each of these scenarios, the data remains vulnerable to physical risk.

Moving to cloud? Take note of common security needs

Anton Jacobsz 4 Sep 2018





While more than one backup or copy of the backup is likely to be held to mitigate against such disasters, there is likely to be some losses if those backups are successive and there's a limit to how many times or how many instances of a backup one can have because making backups takes time and uses up disk space.

If ransomware hits in the morning, businesses would like to restore their data to a previous timeslot or perhaps the previous evening. Organisations, therefore, need a couple of recovery times to choose from that are not too far apart because that means a bigger data void.

Many have already moved their businesses and data into the cloud; it's more cost effective and it offers scalability. So, do you still need cloud storage if you are using Google, Azure or Amazon Web Services (AWS)? The short answer is yes. Google, Azure and AWS are just hosting the business' data.

If the database administrator or someone else in the organisation erroneously deletes the data, it is then lost. To restore it, the business will need a backup and a platform that enables them to easily restore the backed up data.

Cloud storage advantage

Businesses currently need a cloud offering that is designed for all sizes, from individuals backing up a cell phone and laptop or a home network, to small and medium-sized companies. As a front end, it should provide users with a lot of options and a good measure of control. In addition, offerings should also make the cloud easy to implement.

Applications have been making lives easier. For example, people can now order their food online from an app or they can use apps like Uber to get from 'A' to 'B'. So, imagine if an application can be used to initiate a cloud backup. Cloud storage providers need to start looking at things like applications in order to make backup easy and simple to do.

If the organisation could simply download the app and hit 'create client', the simplicity and ease of use would be of immense value. The app would be able to provide you with a portal to access all devices so that an individual can select each device, schedule backups and indicate where they want that backup to go (to a specific DR site, to a cloud provider, or to a hosted datacentre).

The decision-making power would then lie in the hands of the client and would help the client understand where their data is stored. Not only would you know where your data is, but it forces the client to understand the risk of data loss in specific systems, to their business.

Is my data safe?

Large data centres used by cloud storage solutions are safer than any single on-site data centre or server could ever be. From a physical security perspective to options like encryption that gives the business a key to decrypt the data as it is restored. It means the data is safe 'in-flight' and 'at rest'.



Data security in the cloud - whose responsibility is it really?

29 Aug 2018



Does it cost more?

Generally, a client would pay per GB of data size regardless of how many times data is backed up. Of course, clients will still have to pay for streaming the data backup into the cloud. However, as the backup is iterative, businesses will only pay to upload the data that has changed or is new in the backup period. Since the first instance of a backup is usually large and too costly to stream, the ideal cloud storage service provider would collect the first data iteration on physical media at a nominal cost.

Convinced about cloud yet?

Cloud storage is faster, easier, more cost-effective and hassle-free than businesses often imagine and it will save the business from the adverse impact of equipment theft. Businesses need to remember that devices can be replaced. Data, whether the photos of your kids or the week's business transactions, may be lost forever or may only be recovered with a huge loss in time and at a huge cost.

ABOUT MARIUS MARITZ

Operations Manager at DMP SA

- Your data should be living on the Edge - 17 Jul 2019
- Data backups need to be accessible 24/7 - 4 Dec 2018
- Will your business survive equipment theft? - 13 Sep 2018

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>