BIZCOMMUNITY

Having a backup plan for your backup when load shedding hits

By Raeford Liebenberg

11 Oct 2021

Load shedding is a reality of life in South Africa and having some sort of backup power plan in place is essential - especially now since work from home (WFH) and hybrid working have become increasingly mainstream. Aside from keeping equipment like computers and connectivity running, it is critical to consider the data. Backups that run to a local server or some form of network-attached storage, usually fail during load shedding if they are not part of the power redundancy plan. In addition, frequent power outages can damage storage and cause it to fail, and with it goes the data backups. A backup strategy for your backup is arguably even more important than making sure your internet runs during load shedding.

Source: Unsplash

Power failures = equipment failures

Power cuts obviously mean that any equipment that runs off electricity will not work. This includes desktops and fibre routers, as well servers and other IT equipment, so having power redundancy for these items is vital. Making sure that battery-powered equipment is charged is also a solid plan. However, this is not the only thing to consider.

When power is unstable, it causes something called a brownout, where equipment still runs, but the supply is inconsistent, which can damage electronics over time. In addition, when power suddenly cuts out, and when it suddenly switches back on, these surges can wreak havoc. Aside from backup power, having equipment like an uninterrupted power supply (UPS) in place is essential to minimise the risk of this kind of damage.

Don’t forget about the data

Protecting equipment is all well and good, and it is absolutely vital. The trouble is, when we know load shedding is scheduled, the first thing we think is ‘are my laptop and phone charged’ and not ‘is my data still protected’ and ‘have I

backed up my computer'. Redundancy is critical from a power point of view, but even more so from a data point of view, and all businesses need to have a proper strategy around their backups.

One of the unforeseen consequences of load shedding is system crashes. As mentioned, brownouts can damage and degrade equipment, and can cause hard drives to fail. Having no less than two data backups, preferably three, and at least one of those in the cloud is crucial. This is especially important when it comes to critical data because data access is essential in a remote working, digital world.

Best practices, best strategy

An even better practice is to have rotating backups on a daily, weekly and monthly basis, allowing you to recover at daily intervals for the past 14 days, weekly intervals for four weeks, and monthly intervals for the past 12 months. While many smaller businesses have not needed this level of backup in the past, the new environment we find ourselves in has changed requirements dramatically.

Load shedding is here to stay, but we need to remember that it is not only about making sure equipment has power. The impact on data is often not considered, and it can be catastrophic should something go wrong. Devices can be replaced, but once data is gone for good, it is gone. The right IT partner is essential in designing an appropriate backup strategy to ensure you do not fall foul of load shedding – either from a power or a data perspective.

ABOUT THE AUTHOR

Raeford Liebenberg is a manager at Silvermoon, a Galix company.