BIZCOMMUNITY

Why outdated data protection strategies put businesses at risk

By Chris de Bruyn

25 Jan 2021

The need to constantly back up critical data is not only now more crucial than ever but also requires that organisations understand the difference between remote and onsite backups.

Chris de Bruyn, operations director at Gabsten Technologies | image supplied

Traditionally, backups were done on-premise and companies simply relied on the '3-2-1' backup strategy, which requires organisations to have three copies of their data - production data and two backup copies - on two different media, with one copy offsite for Disaster Recovery (DR).

However, now that workforces are spread over a massive geographical area, organisations have had to adjust their backup strategies accordingly. Over the past few months, companies have been purchasing endpoint licences, so that their endpoint devices are protected.

At the same time, many organisations are also moving their critical data and systems to the public Cloud, but this has to be done in a financially sensible manner, as public Cloud computing through international vendors isn't always as affordable in South Africa as it is in other parts of the world.

Remote working has forced organisations to be a lot more agile and flexible and to consider things that weren't always part of their thought process at the start of 2020. Previously, most companies didn't even think about protecting laptops, desktops or endpoints. Instead, everything was kept on-premise, where shared drives were easily accessible and protected.

New dimension of risk

Now, organisations need to protect all these distributed endpoints, as remote working is adding new dimensions to the risks that they face. This means that companies have to put in place complete backup strategies to ensure that everything is protected, irrespective of where the devices and data are located.

When adopting a strategy, the key backup parameters that companies need to consider are organisational-based and aligned with what the organisation needs at the time. This is where agility is important, as a company's data management solution must be able to adapt to what it needs at any given point.

If an organisation's data management strategy does not provide for this, then it must be relooked at against the company's needs and against what is affordable.

The truth is that some enterprises simply cannot afford to throw money at the problem. In that case, organisations should rather team up with a data management partner that has the expertise to guide them through these problems and can also assist with a Business Continuity (BC) plan, which must include a DR strategy.

It is also very important to differentiate between remote and onsite backups. Onsite backup is a legacy strategy where hardware infrastructure that is run on-premise is replicated to a remote DR site or a secondary location. Depending on how thoroughly the strategy is applied, an organisation will either replicate their critical data or all of their data.

Not always feasible

Remote backups focus a lot more on protecting the endpoint or end-user. This may not be the most feasible strategy as an organisation could be burdened with having to protect thousands of laptops while bandwidth remains costly. A better solution would be to train staff to ensure that nothing is saved to the endpoint, but rather to shared drives or approved Cloud services.

While many organisations are likely to continue working from home, it is unlikely that there will be huge potential to save on office space. South Africa is intermittently plagued by load shedding and companies have, over the past five or six years, spent massive amounts on making sure that their business can function when the lights go out.

So, it is unlikely that these enterprises will throw that investment away and let people work entirely from home. Obviously, loadshedding also affects workers in remote locations, so these companies would have to incur massive expenditure to provide their employees with uninterrupted power supplies to keep them working during power outages.

Of course, having a distributed or rotational workforce does increase the risk of data loss, but these risks can be mitigated with the help of a data management partner. Organisations need to have a sound data management strategy, which should be used intelligently to ensure that all critical data is always protected.

ABOUT THE AUTHOR

Chris de Bruyn is operations director at Gabsten Technologies.