2023 data security trends: Massive software-as-a-service outage predicted

Without access to critical data and systems, companies will stall at the roadside while their competitors race ahead. This is according to Byron Horn-Botha, business unit head at Arcserve Southern Africa.

Byron Horn-Botha, business unit head at Arcserve Southern Africa | image supplied

Horn-Botha says the following trends will influence how organisations secure and manage their data in 2023 and beyond.

A massive software-as-a-service (saas) outage may serve as a wake-up call

2023 could be the year we see the first significant saas outage.

The message will become quickly apparent that data backup and recovery must be front and centre of business strategies. Companies across the globe are increasingly consuming saas rather than running their IT infrastructure on-premises.

If a service such as Microsoft 365 has a major outage, the question is, what happens next? It's important to understand that top-tier saas providers like Microsoft guarantee their service but don't guarantee data safety.

That responsibility rests with the company using the service. Therefore, businesses must have third-party software to

survive an outage and ensure the long-term protection of their data.

Cost-cutting will cause more harm than good

With spiralling energy prices and runaway inflation, companies across the board will implement cost optimisation in 2023. But one thing that organisations cannot afford to do is to cut back on their data-protection efforts. Even as businesses rethink their operational expenditures to deal with inflation, they still need to invest in protecting, storing, and backing up their data.

Data protection may appear to be an easy place to trim and save money.

But any cuts to data defences will come with higher costs. The most recent IBM *Cost of a Data Breach Report* found that the average cost of a breach to a US business in 2022 was $9.44m– South Africa is not immune to such trends.

In 2023, it will be essential to recognise the importance of your data and make sure that any cuts to your budget have minimal impact on your business operations.

Companies will have to allocate their security budgets wisely

Despite the threat, many companies will do some belt-tightening in security.

Those that do should be aware that this is when the bad guys tend to pounce. Cyberthieves are always looking to exploit vulnerabilities.

Cost-cutting measures need to be taken with caution, and businesses must carefully scrutinise how and where they allocate budget on data security.

"Today, most companies invest in firewalls, antivirus, and intrusion-detection solutions. It's also crucial to embrace the 3-2-1-1 data-protection strategy.

This strategy directs that you have three backup copies of your data on two different media, such as disk and tape, with one of those copies located offsite for disaster recovery.

The final one in this equation is immutable object storage. Immutable object storage is a next-gen data-security tool that continuously safeguards information by taking snapshots every 90 seconds. It guarantees that even in the case of a significant saas outage, you can quickly recover your data.

Businesses need to plan for their first lines of defence failing and allocate their security budget accordingly, so they have a secure last line of defence to safeguard the lifeblood of their organisation and ensure continuity and data resilience.

Businesses need to understand the importance of critically reviewing the spending on data recovery solutions - after all, that's what counts," concludes Horn-Botha.