

Security high on the agenda for 2016



By [Warren Olivier](#)

18 Jan 2016

The explosion of data has seen security taking on a new level of importance. I believe securing data and controlling access will join the likes of the Internet of Things and information management as one of the most influential trends for the Always-On business in 2016.



Warren Olivier

Being connected 24x7 using virtually any device means businesses will have to rethink their security strategy in the coming months. At the moment, it presents a massive pain point with companies and even countries at risk of being severely compromised by vulnerabilities and malicious users. At its most basic, companies should have multiple copies of their data, keep it encrypted, and store it off-site wherever possible. With Always-On meaning everything is connected, all devices and even appliances are targets. In the world of the Internet of Things, hackers can take over anything from televisions to fridges and even self-driving cars.

3-2-1

This connected environment does not necessarily mean that organisations need to reinvent the rules around backup. Instead, the 3-2-1 backup rule should be applied more religiously.

Simply put, it means that companies should have at least three copies of their data in at least two different formats with one of those copies being kept off-site.

We are already living in the future with the connectedness of things around us. The need to have an effective disaster recovery plan in place, is even more critical than before. But the amount of data that needs to be secured and included in such a plan means companies need to examine the cost of losing data versus the fees they need to pay for an Always-On and available environment.



©Sawitree Jaiw anglok via [123RF](#)

Be proactive

Being proactive around security becomes one of the most fundamental building blocks companies need to put in place.

Several IT companies have solutions built-in to their data environments looking for unusual behaviour. Think about it in real world terms. For example, malaria is best avoided by not getting bitten by an infected mosquito. But if you do get bitten, treatment is the next option. In security, prevention will always be better than the cure. However, it seems inevitable that the data of a company will get compromised, at some point in time. One of the most practical examples is the ability to verify recoverability of the workloads protected in the data centre; which can be a means to avoid being bitten.

Compliance drives what needs to happen in such an instance. Fortunately, with each security exploit making the news and breaking news cases of companies being attacked, there is an increasing awareness around the importance of security and data. But there are specific security opportunities today that organisations can leverage in the modern data centre. Specifically, virtualisation allows technologies like a virtual lab to be used to leverage the data of the data centre to avoid deployment risks and perform security tests in an isolated environment.

Is SA ready?

From a South African perspective, the question is whether companies are ready to deal with security issues? In all likelihood, not really. At this stage, there are no high profile cases of local organisations getting attacked and leaking data. But with data continuously expanding, it is a case of "when" rather than "if" such an attack takes place and what companies will do to get their systems back up and running."

Managing data is therefore becoming more of a focus than the actual production of it. With organisations able to leverage technologies such as virtualisation, modern storage, and the cloud, and being able to call on expert consultants who can provide them with the expertise, they need in this data-rich environment, the journey ahead is going to be an exciting one.

It is therefore imperative that decision-makers get their security in order before it is too late. After all, if there is a weak link in the modern data centre, availability could be compromised and the organisation could suffer financial and reputational damage.

ABOUT WARREN OLIVIER

- Warren Olivier is the regional manager for Southern Africa at VeeamSoftware
- [BizTrends 2016] Security high on the agenda for 2016 - 18 Jan 2016
 - When disaster strikes - 29 Sep 2015
 - The importance of data deduplication - 11 Sep 2015
 - Apps the pillars of the always-on business - 4 Sep 2015
 - The always-on business relevant to all industries - 26 Aug 2015

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

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