

Consider actual cloud security, not merely regulations

Cloud computing technologies and services in South Africa have gained popularity over the past few years. Local businesses are using cloud services because maintaining their own infrastructure is costly, and they hope to boost efficiency, lower costs and simplify their technology investments.



© knee0 – [za.fotolia.com](https://www.fotolia.com)

A substantial number of these local businesses, however, are storing sensitive information relating to clients, employees or the business itself, as well as using it for day-to-day operations. “This is particularly true of businesses involved in industries such as finance, healthcare and retail, as they house highly confidential customer data, and can face huge penalties should this data be compromised. Public disclosure in the event of a breach is now a legal requirement, which could result in lost revenues as well as customer confidence,” says spokesperson from MWR Infosecurity.

Incorporating security into business models

This creates an environment where you could seriously see companies losing business if they are repeatedly compromised. As a result, most businesses will (hopefully) be forced to consider and incorporate security into their business model. “However, lack of awareness of security issues is probably a major contributor to why businesses don’t take security as seriously as they should. From what I’ve seen, security is not necessarily a major concern in South Africa and the few companies that do try to take it into account just don’t have an adequate background to address security properly,” explains the spokesperson.

He says this could result in them focusing on the wrong things; the high-profile attacks that litter the headlines, and not the real threats themselves. “You may find that they simply assume that a cloud provider would take care of security without ever checking up on that, or assuming that there is no way a third party would be able to manage security better than they do.”

However, if a South African company ever wants to compete in the international market, they’ll be judged according to the same standards as foreign businesses and that means they need to give the same attention to security, he adds.

Almost like mobile security

Security of cloud infrastructure is also a concern because it is being shared with other users. “I read an article a while ago

about ransomware encrypting a company's entire system which resided mostly on the cloud. If you are sharing infrastructure with someone else, you need to secure your host because you don't want their problems to become yours. Alternatively, another client for the same cloud provider may be malicious, at which point an insecure cloud service could be something of a gold mine."

He believes cloud security is almost like mobile security, it's one of those things that get a lot of media attention in the form of "cloud security is important" but without a real exploration of what cloud security is.

"Much in the same way as mobile security, if you look at the Verizon Data Breach Report or similar, this is just how companies are now getting breached. Companies are still getting compromised through users and their workstations. Until the world at large starts focusing on how organisations are really getting compromised, we will keep throwing money at 'blindenboxes' that solve problems we don't have."

In terms of securing the cloud, he advises to consider actual security, not merely regulations, though they may help drive the minimum standard. He also believes that technical issues would probably be a major concern, including:

- Hosting system set up (OS, software, firewall, segregation of different user environments, services running, hard drive encryption, etc.)
- Communication security
- Security policies - updates, patch policies, information access control (This enables encrypted back-ups but companies should look at who in the business can access that and whether the host company has a key too.)
- Disposal of equipment (most specifically hard drives that may have sensitive info)
- Security of the actual services offered

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