BIZCOMMUNITY

Focus on POPIA compliance, data mobility, integrity key in a world with a remote workforce

By Ian Engelbrecht

29 Jan 2021

Most South African businesses traditionally slow down or shut down completely over the festive period, except for retail and hospitality. 2020 was different. The second wave of the pandemic forced the closure of beaches and the reimposition of the alcohol ban and stricter curfew laws. Most non-essential workers only started reporting for work between 4 January and 11 January, many of them remotely.

Ian Engelbrecht, senior systems engineer at Veeam

Even if the front door of a business may have been locked, it doesn't mean the business was really closed. Critical IT systems needed to remain secure, stable and reliable during the three weeks that the country was on a go-slow. In other words, enterprises instituted an IT freeze, and many of these are still in this freeze and some only lifting it towards the end of January.

Yet, data has to be available all the time. If it isn't, or if there is an attack or breach, it can result in massive financial and reputational damage for an organisation. During the go-slow, organisations often run with skeleton staff and no further updates or changes to infrastructure can be made during this period. The reasoning is sound - with fewer people available to mitigate a crisis, anything that can cause a system to drop, or which can open doors to potential breaches, needs to be avoided at all costs.

There is a lot for the C-suite to consider at the best of times as it prepares to return an enterprise back to all-hand- on-deck. The fact that the freeze ends during the pandemic's second wave with heightened social distancing restrictions adds to the usual challenges.

Most IT managers would have spent the 2020-2021 festive break wondering what the new year will hold for the company and whether more lockdowns will force continued remote working or what percentage of the workforce will even return to the office post-pandemic. Many are consumed with the urgency to complete their transformation to the cloud so that they can continue to serve users remotely while simultaneously dealing with update backlogs.

Top IT security threats in 2021

Anna Collard 20 Jan 2021

How to plan for uncertainty

Enterprises must plan a fluid data mobility strategy to allow for a hybrid workforce with remote users as well as the possibility of an increased percentage of in-office users. Data needs to be in the location - that's in the cloud or on-premises - closest to the employee to ensure the best user experience.

We are finding that many companies are planning for a situation where they will never again have a full staff contingent working from the office. Not only will this reality change the way employees behave, but it will ensure that IT departments need to evolve in order to serve users in 2021 and beyond.

As we approach year-end for corporate South Africa, C-suites need to ask what needs to be budgeted for to ensure their companies continue to perform optimally regardless of the uncertainty or changing work conditions. In other words, this uncertainty needs to have minimal impact on efficiency and productivity. This requirement is likely to see a big shift towards platform-agnostic solutions and data mobility.

Every IT department in 2021 and beyond should have full control of their data and the ability to move this data across platforms with ease. Data should be able to go from on-premises to the cloud and back again, as well as migrate easily between different cloud providers. This will only be achieved by IT departments if they move away from any vendor platform lock-ins. They need to be able to decide where and when data should move to suit their real-time needs.

Why POPI compliance is not just an IT issue

Johan Scheepers 7 Dec 2020

Preparing for POPIA

The Protection of Personal Information Act (POPIA) will finally come into force in 2021. Companies will need to allow data subjects to object to their data being processed, as well as being able to withdraw previously given consent at any time. This means that as soon as the objection or withdrawal of consent has been received, a business must stop processing that subject's data immediately.

If we consider the annual IT freeze, it becomes apparent that if the cleansing of big customer data was put on hold, this would need to be addressed as soon as operations go live in order to ensure compliance with POPIA.

The complaint management of data requires that once a company no longer needs the information for processing purposes, it loses the right to keep that data unless required by law. Again, from an IT freeze perspective, this means that any data that reached the end of its life during the downtime, may no longer be processed once the systems are up and running.

Underpinning all of this, enterprises need to ensure integrity of their data when it moves across platforms. They need to ensure that the Veeam 3-2-1 rule is followed, meaning that there are three copies of data, two of which are on separate storage mediums, with one being offsite. At Veeam, we always recommend taking this one step further: we advocate for the 3-2-1-0 rule. This means zero errors on all three copies.

As companies ease out of their IT freezes and contemplate the uncertain year ahead, they would do very well to ensure that data management, mobility and integrity form a key part of their strategies. We have spoken for almost a year about the “new normal” or the “uncertain future”, but a carefully planned IT investment can mean that these phrases don’t have a material impact on the functioning of a business. It could mean business as normal in the new normal.

ABOUT THE AUTHOR

Ian Engelbrecht, senior systems engineer at Veeam