BIZCOMMUNITY

When does disaster recovery matter?

The recent disaster at the Kenyan International Airport is yet another example of why businesses are being urged to take a closer look at their disaster recovery plans.

Getting your business up and running after a disaster is what the nightmares of CIOs are made of. A natural or man-made disaster can cripple your business in the blink of an eye - are you ready for the potential fallout this will have on your business, asks Kerry Evans of Quintica.

If you take a closer look at the recent fire at Nairobi's Jomo Kenyatta International Airport in Kenya, the impact of which destroyed large parts of the international terminal and brought East Africa's largest aviation hub to a standstill, we will see a real business case for a focus on disaster recovery (DR) measures across the continent.

The airport, built in 1978, has a capacity for 2.5 million passengers a year; however it currently handles 6 million - or about 16 000 a day - itself a risk to the business. As a result of the fire, several passengers were not only stranded, but were suddenly without luggage and, in some instances, in the country illegally as a result of expired visas.

The entire airport system also came crashing down, causing valuable information to be lost. The reality is that worldwide disaster recovery and business continuity arrangements are not what they should be, and a report released by The Chartered Management Institute in the UK, showed that business continuity management (BCM) uptake has increased by a meagre 3% in the UK over the past few years.

So what happens when disaster strikes?

Do you pitch tents, like they have in Kenya? Revert to collating data manually? While the Kenyan disaster is a shocking one, the business of the airport is to facilitate the entry and exit of people and goods to and from the country via flights. What would have happened if its entire business was information or data based?

A recent report published by a large storage vendor, highlighted that close to 74% of IT decision makers in South Africa are not confident that they could fully recover after a disaster. The report also highlighted that DR plans are usually only reviewed after a disaster and not before, and that IT budgets often don't really take DR plans or the need for them, into cognisance.

It is also important to remember that when certain aspects of your business go down, the impact to the rest of your supply chain can be devastating. A young up-and-coming florist in, say, Amsterdam, who has a large wedding for which to deliver the flower arrangements, of which the bulk of the arrangements are made up of Kenyan roses, could well now be out of business. It is important always to have alternatives in place in order to spread the risk as much as possible.

The fact that disasters occur is not something new, and businesses that are at the ill-fated end of these disasters should not be surprised if they are required to have their systems "back to normal" as quickly as possible. In short, with an effective and well-planned DR and BCM strategy in place, a major disaster, such as the one at the Kenyan airport, should only set business back by a few hours - or as long as it takes to replace the onsite hardware that was damaged, or for a relocation to occur.

Minimise the time of the disruption

It is your obligation to assess all the risks facing or potentially impacting on your business. Therefore, it is paramount that you try to minimise the time of the disruption; remember that revenue, productivity and declines in loyalty are most often a result of prolonged disruptions. In Kenya, as an example, flights resumed within hours, albeit that there was a backlog.

In Africa our circumstances are unique and the main reasons you should adopt a DR and BCM strategy, include erratic power supply and power spikes, hardware failure, which is often a by-product of this erratic power supply and, lastly, software failures, which are sometimes related to illegal or counterfeit software.

While the Kenyan disaster is not an everyday occurrence, it is a stark reminder that disaster does strike, and when it does it can be devastating.

At the end of the day, we should not be asking the question as to whether or not a system is backed up, or if there is a DR or a BCM solution or policies in place. The question should rather be based on how long we will be back up and running should there be a disaster, because we have taken the necessary steps to ensure that our information is backed up and available.