ContinuitySA takes a large multinational company on a BCM journey

With the help of ContinuitySA, a large multinational company has made significant progress on the road to a fully functional business continuity strategy. Luckily, it had already taken some of the crucial early steps when a real-life crisis intervened.

A large company, with headquarters in Europe, has a head office and several manufacturing/storage facilities around South Africa. It employs approximately 500 people just at head office alone.

ContinuitySA had been supplying the company business continuity management which included: work-area recovery and hosting services for over a decade. However, it took responsibility for the creation and management of its own business continuity and resilience strategy.

When a new risk manager was appointed, they were tasked to review and assess the business continuity plan, especially in light of the increasing emphasis placed on business continuity in the King III and now King IV Reports. ContinuitySA account manager, Wayde Anderson, recommended a Business Continuity Management Audit followed by an Executive Workshop to bring management up to date on the latest developments in business continuity management (BCM), and to evaluate the company’s total BCM programme in light of international standards and best practice. The workshop aimed to identify gaps, and create a roadmap for improving the plan in the context of the company’s business strategy.

“One of the key aims of the workshop was to gain real executive buy-in to the concept of BCM by educating them about its importance and showing how effective their existing plan was”
“One of the key aims of the workshop was to gain real executive buy-in to the concept of BCM by educating them about its importance and showing how effective their existing plan was,” says Mr Anderson.

Reality check
The workshop was held using interactive software that allowed the participants to respond to questions posed by the facilitators. The software then tallied up the responses to provide a view of what the executive team was thinking.
It became clear that the existing plan covered only the head office site for ICT-based disasters and work-area recovery. The plan failed to cover other key business continuity issues, including human resources, equipment, utilities and the external supply chain, as well as the company’s manufacturing/storage sites. The evaluation also showed that, as is commonly the case, each department head thought that his or her department was the most important and thus warranted priority when it came to the BCM plan.

Overall, the workshop fulfilled its purpose of alerting the executive team to the gaps in its BCM planning, and opened up a productive conversation.

ContinuitySA worked with the company’s risk manager on improving the BCM plan in line with the workshop’s findings, and integrating it better into the risk management plan. ContinuitySA proposed running a crisis simulation in order to test the existing IT disaster recovery plans. This was in line with ContinuitySA’s view that no plan could be considered credible unless it was regularly tested, and the results fed back into the plan.

Three potential crisis scenarios were presented to the company, and it chose one that involved staff being unable to access the head office site because of strike action. With only the executive team in the know, staff were informed one evening to report for duty at the disaster recovery facility at ContinuitySA Midrand the following morning.

Taking stock
After a day spent at the disaster recovery site, a post-mortem analysis was conducted. It became clear that the plan had certain weaknesses and incorrect assumptions. These included transport for the staff from the Gautrain station to the site, proper induction of staff at the site, and how to invoke a disaster with ContinuitySA. In addition, the company’s battle box was inadequate. (The battle box is the physical store of physical and non-physical items needed to be productive at a recovery site, and might include stationery, training and reference manuals as well as passwords and links to particular apps.)

A more serious challenge was the fact that the company’s global policy did not permit the desktop/personal computer image to be shared with ContinuitySA. Thus, instead of arriving to find each desktop already loaded with the appropriate software, the company’s own IT staff had to bring up the image on multiple computers, a process that wasted around two hours.

The crisis simulation was extremely fortuitous as, only a few months later, the partial collapse of the head office required a genuine disaster invocation. With the simulation fresh in their minds, the staff’s relocation to the recovery site went much more smoothly.
In addition, improvements to the BCM plan subsequent to the simulation meant that the company was in a position to action the necessary repairs rapidly because the eventuality had already been planned for.

“Since then, we have become our client’s partner in the journey towards comprehensive BCM,” Mr Anderson concludes. “We are currently working with them on emergency response plans for their other sites, and the rest of the African operations are keen to talk about getting their own BCM plans upgraded. The real lesson here is that BCM has to be treated holistically and aligned with the company’s own goals and circumstances. It may not be achievable immediately, but the journey brings many benefits in its wake.”