BIZCOMMUNITY

CIOs embrace opportunities in post-lockdown market

By Tim Wood

26 May 2020

As South Africa enters another week of the nationwide lockdown, the business focus has shifted from enabling employees to work remotely to now planning for what the new normal is likely to look like.

Tim Wood, executive head of Information Systems and Technology at Vox

This requires CIOs to balance existing organisational priorities with ways of becoming more adaptive to the changing environment. Critical to this is decisive decision-making that positions the business for growth.

For small to medium-sized businesses that do not have all the skills in-house to transform their IT environments, decision-makers should consider going the outsourcing route. By partnering with a managed service provider (MSP) that can deliver everything from a cloud-readiness audit through to helping identify the technology gaps that exist between the business strategy and what is already in place, the company can manage its spend and can more easily scale up (or down) as market demands require.

A further advantage of going the outsourcing route is getting access to the depth of knowledge a partner that is an expert in its field can provide. This will help inform the cloud-readiness audit by providing a better understanding of where new technology investments will make the biggest impact as the organisation transitions to a cloud environment.

An important element driving this agility centres on engaging with the right partners to enable efficiencies. By leveraging the respective strengths of these partners, an organisation can enhance its own. For example, during the rush to equip people with the tools required to work from home, a company might have relied on a hardware partner to supply and support laptops on a month-to-month basis instead of having to make a long-term commitment. The supplier gets the benefit of new business while the company can remain focused on meeting customer demand.

Prepare for the cloud

CIOs should also consider implementing systems that help the company re-integrate operations for a post-lockdown world. This entails identifying how best to balance the 'new' culture of remote working with a traditional one that was more geared towards an office environment.

Throughout this, a CIO should remain cognisant of what is required for the business to be considered cloud-ready. But more than simply having connectivity and laptops for remote workers in place, this requires a foundation built around effective cyber security. Security systems must always be adapted to reflect the changing business landscape with companies adhering to best practices.

These best practices are informed by globally recognised standards such as the ISO 27001 that specifies a management system intended to bring information security under management control and gives specific requirements around aspects of data security. Users need to be continually educated on what constitutes good cybersecurity practice as it pertains to working from an office environment and what they need to be aware of when working remotely.

Nowhere is this more important than when it comes to meeting the demand for collaboration tools. In a post-lockdown environment, employees will continue accessing data and working on documents from anywhere they have a reliable internet connection. However, this will lead to increased cybersecurity threats due to the increasing number of entry points now into the business back-end. It is therefore critical for cybersecurity solutions to reflect this and encompass more than just anti-virus and firewalls.

If remote working is going to be part of business operations moving forward, then the CIO should work with the HR department to update policies and incorporate measurable deliverables as part of this. For their part, employees need to understand what is required of them and how to deliver the productivity required in this rapidly-evolving environment.

New business models

It is inevitable that technology-enabled business models will become more critical to organisational success in the future. Having said that, every company should find its own way forward – there is no off-the-shelf strategy that can fully anticipate all the unique requirements of each business.

However, the success of the remote working environment will likely lead to companies reducing the size of its office space. This will bring about cost-savings on leases that could be passed on to employees. Think of the competitive advantage an organisation can derive from offering remote working perks such as connectivity and power solutions as part of its staff packages.

Of course, remote working is not without its risks. The uncertainty around electricity supply in the country means CIOs should consider how best to equip remote workers with power supply solutions that are more effective (and environmentally-friendly) than traditional generators. With load shedding expected to return in the winter months due to an increase in demand, companies need to start examining the options available to them.

Given how the new world of work will likely see employees spread across a number of locations, CIOs need to have oversight of the effectiveness of the IT systems in place. Being able to use a centrally managed IT system that provides an integrated view of all devices, applications, infrastructure, security, and other components behind a single pane of glass is essential.

Refocusing IT spend

Despite the uncertainties of what the post-lockdown business world will entail, CIOs should keep the following things in mind to help focus their spend:

- Cyber security must be a priority
- Managing the connectivity requirements of remote users. Fibre provides an ideal environment as it also enables employees to make calls using VoIP technology, significantly reducing mobile call expenses
- Have cloud-enabled systems that allow for remote work including collaboration tools, hosted PBX systems, and virtual private networks
- Consider embracing hardware-as-a-service where the company can rent hardware based on their requirements and upgrading it as needed
- Centrally managed IT system that manages all devices and users from a singular console that also ensures asset management is done with the right policy management in place
- Supporting home users with access to reliable power supply solutions for when load shedding resumes

CIOs can create opportunities for their organisations by following a focused approach towards what the new normal could look like. Underpinning this is a basis built on cybersecurity and cloud-centric tactics. Throughout this, the CIO should keep the requirements of the business stakeholders firmly in mind to help navigate the complexities of this new environment.

ABOUT THE AUTHOR

Tim Wood, executive head of Information Systems and Technology at Vox