Why we should continue with digital resilience despite being 'back to normal'

By George Senzere

17 Nov 2022

While businesses in South Africa revert to a semblance of 'normality', many companies are moving their employees and operations back to the original workplace. Digital transformation and the mobilisation of a remote workforce have not been in vain, and organisations should continue leveraging these established systems and investments.

Source: Unsplash

Conversely, the same applies to business operations and resilience – both digitisation and digitalisation must continue in order to establish a transformed foundation for the future.

This sentiment is also echoed by analyst group, IDC, which estimates that by 2025 there will be 41.6 billion connected IoT devices, including machines, sensors, and cameras.

“In hospitals, data centres, critical manufacturing plants, and industrial sites, continuous uptime is non-negotiable, especially during catastrophic events,” says IDC.

To contextualise and re-emphasise the above, it's important we take one step back. The pandemic caught a lot of organisations off-guard, particularly when it came to allowing remote access. In a matter of weeks or even days, organisations had to transform their infrastructure to allow for remote working.

Unfortunately, as with most things in life that required a quick turnaround, the above came at a hefty price tag. In some instances, organisations had in days changed their IT corporate networks to allow for remote connectivity. This included making sure VPNs were up and running in no time, and organisations that were fortunate enough to have up-to-date architectures, implemented other alternatives such as SD-WANs and Sase (secure access service edge).

As mentioned, the above was undoubtedly a costly exercise. This brings us to the next important point, none of us can predict what the future holds which is why the adage "rather safe than sorry" couldn't be truer.

Building on what we have

Currently, most organisations have systems in place to allow for hybrid working, and whilst many employees have returned to company offices, they have the option and flexibility to work from home, depending on organisational policy.

If anything, we should encourage and foster agility amongst workers which is why digital resilience is key; it allows organisations to adapt to business disruptions by making use of digital technologies to continue with their daily operations.

Digital resilience was one of the key attributes that saw some organisations adapt to the pandemic quicker than others. Thus, to prepare for the future, organisations must take a strategic approach to deploying digital technologies.

For example, in the data centre industry, those companies which already had advanced data centre infrastructure management (DCIM) systems in place, had no problem running and securing their infrastructure even with data centre staff working offsite.

DCIM allowed organisations to conduct remote health checks of the power infrastructure which included overall performance and cooling. Also, data centre owners were not the only ones to benefit from the DCIM tools. Organisations moved quickly to install DCIM and reaped the benefits.

Establishing an agile workforce

Not all organisations have the luxury of running a remote workforce, however, those industries and resultant organisations that are in the position to do so should take the following steps to establish a secure, productive, and agile workforce:

- Conduct a thorough evaluation of the type of business and its workforce.
- Deploy the applicable digital tools and connectivity solutions that include remote software and devices.
- Cybersecurity must be prioritised.
- Provide continuous power to mitigate potential disruptions.
- Ensure that the remote and on-site working environments of the employees are ergonomic and professional.
- Adjust management styles to allow for a more 'flexible' working model with an emphasis on results and realistic performance matrixes.
- The workforce must be trained and prepared to work in remote environments.
- Regular review meetings to ensure teams are still productive.
- Consistent and continuous technical support.
- New employees must be given enough time to adjust to a hybrid and/or working model.

Lastly, cybersecurity remains a crucial element of organisations' infrastructure and working models. The attack surface is much bigger and organisations must ensure they are fully protected, and their employees trained to identify any potential threats.

ABOUT THE AUTHOR

George Senzere is a solutions architect: secure power at Schneider Electric.