vodacom business

CNBC AFRICA

Opinion Article

Securing the future in a rapidly evolving world of work

-- Kabelo Makwane, Managing Executive; Cloud, Hosting & Security at Vodacom Business Africa

When you really take a moment to look back, it's crazy to think just how much the world of work has changed in recent years. So many of the business processes that we used to do manually are now done at the touch of a button thanks to new and emerging digital technologies. And our working day is no longer defined by a set number of hours that we have to spend in front of our desks in an office.

In addition to this, changing employee and customer expectations demand that businesses deliver technologically-enabled ways of working so that they don't fall behind the competition. This is particularly true in Africa, where the simplest solutions can bring about quite massive leaps forward. But when implementing new technologies and embracing the transformation of work, a lot of business leaders battle with maintaining control, while also trusting that the technology can do what it promises. This is where conversations around cybersecurity are so important.

In our hyperconnected world, businesses always have to keep an eye on security to guarantee that they meet changing customer needs without upping risks. In recent years, we have seen cybersecurity rise on the business agenda, as more and more organisations realise that cyber attacks are no longer something that "only ever happens to others".

For modern businesses the challenge is to bring in emerging technologies to improve the level of service they offer to their customers without creating new pathways for cyber attacks.

Today, if you want to safely accelerate your business operations, it is critical that you have robust cybersecurity measures in place. But unfortunately, the same technologies that can help businesses improve agility, predict customer demands and improve efficiency, can also be leveraged by threat actors to create more advanced methods of attack.

For example, in recent months, we have all been caught up in the hype around artificial intelligence (AI) and have witnessed how incredibly powerful AI is; able to transform every aspect of our lives. Yes, the AI genie is well and truly out of the bottle but if we are to benefit from it, we must be aware of what it can do when it falls into the wrong hands. When used by sinister actors, AI can create malicious software, draft more convincing phishing emails and spread disinformation in less time and with less effort, making it easier for hackers to launch multiple attacks at the same time.

According to Vodacom research, few are finding a happy balance between product, process and service innovation, keeping an eye on emerging trends and prioritising security. While more than 65% of businesses claim to have never been affected by a cybersecurity incident, recent research from independent analyst and consultancy firm, Omdia, found that a staggering 91% of security decision makers have had to deal with a security-related incident in the last year. Unfortunately, in many instances, legislation trails technological innovation. And when it comes to cybersecurity this can be a major stumbling block because there are no guidelines around how to innovate, safely. With all of this in mind, it's essential that organisations build resilience so that they can disrupt but also prevent themselves from being disrupted in the future.

The successful transformation of work and the creation of fit for future businesses cannot happen without the five Cs – collaboration, communication, connectivity, consumers and cybersecurity. In order to deliver on the final C on this list, businesses need to start with a plan. Not only must your cyber strategy be built into the foundation of everything you do, it must also be understood and adopted by all key stakeholders and employees. A simple way to improve your security resilience is by changing the behaviour of your people. We know that people are often the weakest link in an organisation's cyber defences, which is why fit for future businesses work to cultivate a culture of cyber awareness by constantly reinforcing security priorities.

In line with this, it's important to remember that having strong cybersecurity measures in place is not only about safeguarding your business against malicious activities; it's also about building trust – among your customers, partners and stakeholders. When you take cybersecurity seriously this showcases that you care about data and privacy and are actively working to keep sensitive information secure.

Cybersecurity is not a one-time implementation. It requires ongoing maintenance and improvement process; especially with the playing field shifting as quickly as it is. This makes it essential for businesses to regularly assess the strength of their cybersecurity defences and quickly fill in any gaps that might exist. What does this look like? Running regular workshops to educate employees about the latest threats, keeping up-to-date with software updates, conducting vulnerability assessments (internally and across your supply chain) and always staying informed about emerging threats. As a simple example, in the same way that AI can be used by cybercriminals to improve their attacks, cybersecurity professionals can also leverage AI to boost their defences. When using AI, cyber teams are able to process large amounts of data quite quickly, which empowers them to make more timely decisions, enhances threat intelligence and detection as well as speed up incident response.

At Vodacom, we have witnessed the level of innovation that can happen when you connect people and when you place something as simple as a mobile device in someone's hand. We have also seen society regularly downplay how much potential there is for seemingly 'low tech' solutions to deliver big results. But innovations also carry risks. Truly impactful innovation can only be achieved if cybersecurity is at its core. When this is the case, businesses are able to tap into future ways of working that will unlock new levels of competitiveness for the country and the continent

vodacom
business