

4 ways businesses can embrace digital transformation securely

By [Stergios Saltas](#)

2 Jun 2021

Most organisations in business today understand the importance of digital transformation. But just as companies have woken up to the importance of adopting new technologies, so have cybercriminals.



Stergios Saltas, operations director, Striata Africa | image supplied

This has resulted in a technological arms race, where organisations not only have to keep up with the pace of technological change but also with a rapidly evolving threat landscape. Every new piece of technology, including apps and push notifications, offers cybercriminals a new way of targeting an organisation's customers.

With people working remotely on home networks that are often less secure than enterprise networks, incidents of cybercrime have risen dramatically. In the months following the start of the pandemic, for example, the FBI reported a 300% increase in cybercrime.

Brands continue losing customer loyalty to cybercriminals, report reveals



With that in mind, there are four things your organisation can do to ensure that your customer communication is as secure as possible

1. Balance innovation with security

Organisations must be cautious of introducing innovation into customer communication without adequate testing and assessment of any risk factors.

There is nothing wrong with organisations trying out new technologies that they think might benefit their operations in the short and long term. In fact, if they want to stay relevant, they should. When introducing those new technologies, however, they should make sure to adhere to security best practices.

2. Don't prioritise access over data protection

Data and data analytics should play a vital role in any organisation's digital strategy. The introduction of artificial intelligence (AI), as well as Internet of Things (IoT) enabled devices, means organisations now have access to vast amounts of data to fuel their digital initiatives. As much potential as there is in these technologies, however, they also bring with them an increased risk of data breaches and devastating consequences for an organisation.

The accelerated adoption of digital processes during COVID lockdowns, means it's also possible that many organisations prioritised the setting up of digital access, without the requisite focus on security. Those processes need to be revisited for security risks and to ensure the protection of personal data.

3. Encrypt and protect personal data

Most countries, including South Africa, have data protection laws that require companies handling personal information to protect it. That means not sending personal information over insecure channels, both internally and to customers. Personal customer correspondence should be attached as an encrypted document, that only the intended recipient is able to access. This ensures the privacy of that information while it is in transit, and when it resides on the personal device.

4. The human issue

People remain the greatest point of security vulnerability. There's a reason why 95% of cybersecurity breaches are as a result of human error. Organisations must therefore audit customer communication processes to identify where employees or customers could inadvertently expose the company or themselves to a security risk. The most powerful way to combat risk is to an ongoing education programme, internally and externally.

Organisations also need to ensure that customers and employees are able to recognise phishing attempts and know not to click on links or open any document that they are not expecting. This is especially important now, as it's likely you have a number of new digital users who are not experienced when it comes to spotting online scams.

Ongoing efforts

Ultimately, it's vital that organisations do not see security as a "once and done" initiative when it comes to their digital transformation initiatives. Instead, they should approach it as an ongoing project. Moreover, they need to stay on top of the latest threats and ensure that employees and customers alike understand those threats and how they can keep themselves safe.

ABOUT THE AUTHOR

Stergios Saltas is the operations director at Striata Africa.

For more, visit: <https://www.bizcommunity.com>