KnowBe4
Human error. Conquered.

REPORT

KnowBe4 Remote Working in Africa Survey 2021

Table of Contents

Key Findings 3
Remote Working: The Future 4
Remote Working: The Challenges 5
Cybersecurity Training 5
Security Controls 6
Remote Workforce Challenges 6
Security Incidents 6
Security Awareness Processes 7
Top Security Concerns 7
The Conclusion 8

KnowBe4, in partnership with Lynchpin and ITWeb, conducted online surveys across Nigeria, Kenya and South Africa respectively, to unpack the challenges, security concerns, risks and considerations influencing remote working across these three countries. The survey examines some of the key factors that influence remote working for organisations on the continent and how these can impact business decision-making around remote or hybrid working frameworks going forward.

The survey uncovers the reality of remote working by asking the difficult questions. Will remote working remain a reality for organisations within Kenya, South Africa and Nigeria? Have lockdown restrictions changed how people engage with the office? And what training have people had – do people need – to withstand social engineering attacks and ensure robust cybersecurity good practice?

The findings were taken from a total of 548 responses across Kenya (100), South Africa (348) and Nigeria (100). The roles of respondents are broken down into: middle management, IT staff, executive management/C-suite, and consultants across various industries.

Key Findings

The KnowBe4 Africa Remote Work Survey examined several key themes to determine how remote working has influenced business processes, security risks and controls across these three countries.

The following key findings underscore the importance of refining remote working best practices across security, training and management to ensure long-term success, security and stability.

The following are the key insights:

- 57% of organisations in South Africa, 29% in Kenya, and 32% in Nigeria, will continue with remote working on a flexible basis
- Only 31% of organisations in South Africa, 11% in Kenya and 36% in Nigeria, believe that their remote workers have been solidly trained and have the ability to withstand social engineering attacks
- The three key challenges facing Kenyan and Nigerian organisations with remote workforces are: implementations of remote working infrastructure; lack of infrastructure at the home and office; and lack of budget
- The three key challenges facing South African organisations with remote workforces are: building and keeping a team identity; motivation and productivity; and lack of infrastructure at home and the office
- The top four security risks for South Africans are: user behaviour; unsecure Wi-Fi networks; social engineering and personal devices
- Of the organisations that experienced a cyber-incident over the past year, 46% in Kenya, 61% in South Africa and 14% in Nigeria were hit by social engineering
- 66% of South African organisations have changed their security awareness since the start of the pandemic with 50% adding more security awareness talks and webinars compared with 52% of Kenyan organisations and 51% of Nigerian organisations
- The top three security concerns that keep management awake at night across all three countries are: preventing data breaches; compliance with regulations; reputational damage and extortion attacks (ransomware)

Remote Working: The Future

One of the key elements of the survey was to unpack how organisations within these countries felt about the future of remote working, especially now as the limitations around the pandemic are easing, globally. Most believed that remote working would very much remain a reality well into the future, but that this would be structured differently. In Kenya, 29% believed that remote working would remain a reality but with flexible policies and in Nigeria this was 32%. In South Africa the figure rose significantly to 57%.

Is remote working a future reality in your organisation?

	South Africa	Nigeria	Kenya
Yes, but flexible	**57%**	**32%**	**29%**
Yes, we will continue to work from home	**34%**	**39%**	**34%**
No, we have or will return to the office	**9%**	**29%**	**37%**

Across all countries, remote working was already part time or a permanent fixture but, there was a clear split between those companies that were back in the office full time and those that were not planning to return to work for the foreseeable future. In Nigeria, 21% of respondents said that they would not return to the office versus 28% that had already returned; while in Kenya 30% had fully returned to the office and only 11% would not be returning. South Africa saw these figures turned on their head with the majority (31%) not planning to return to the office for the foreseeable future while only 12% had already returned full time.

While there are some differences in statistic size between the different countries, it's clear that remote working is set to remain a consistent part of the average business framework for some time to come. This view is shared on the individual level as well, with 37% of Kenyan respondents stating that they were set to, or already had, returned to the office; Nigeria at 29%; and South Africa at 9%.

Remote Working: The Challenges

While remote working has introduced numerous benefits to the business landscape, it has brought its fair share of challenges. From limited access to infrastructure to increased cybersecurity risks and vulnerabilities, remote working has put many companies through their paces as they've rapidly tried to resolve these problems while minimising the risk to the business.

Cybersecurity Training

One thing that can provide the organisation with an immediate defence against cybercrime is the well-trained employee. The human firewall. People who can recognise social engineering attacks and who don't click on links and attachments and spot attempted fraud such as business email compromise scams.

When asked whether or not an organisation felt that its remote work users were adequately trained and capable of withstanding social engineering attacks, 31% of South Africans somewhat agreed and 28% completely agreed. That's just over 50% of organisations with a measure of confidence in their employee's ability to recognise, and prevent this threat. In Nigeria, 26% somewhat agreed and only 11% completely agreed; while in Kenya, 11% somewhat agreed and 16% completely agreed.

> *"Our remote work users are solidly trained and able to withstand social engineering attacks."*

	South Africa	Nigeria	Kenya
Completely Agree	**31%**	**26%**	**11%**
Somewhat Agree	**28%**	**11%**	**16%**
Neutral	**21%**	**25%**	**28%**
Somewhat Disagree	**12%**	**7%**	**16%**
Completely Disagree	**5%**	**16%**	**13%**
Do Not Know	**3%**	**15%**	**16%**

The figures point to an urgent need to invest more into security training that empowers employees and helps them to stand as the first line of defence against the ongoing onslaught of social engineering attacks. This is critical for those working within the office, but absolutely essential for those who continue with remote working.

Security Controls

For organisations in Kenya, only 34% agreed or somewhat agreed that their remote working infrastructure and security controls were solid, in Nigeria that figure was 21% and in South Africa it was 75%. There is a sharp disparity between the countries.

> *"Our remote working infrastructure and securitycontrols are solid"*

	South Africa	Nigeria	Kenya
Somewhat Agree	**52%**	**12%**	**18%**
Completely Agree	**23%**	**9%**	**16%**
Neutral	**12%**	**30%**	**22%**
Somewhat Disagree	**9%**	**10%**	**15%**
Completely Disagree	**3%**	**16%**	**10%**
Do Not Know	**1%**	**23%**	**19%**

This disparity serves to highlight a lack of confidence amongst Kenyan and Nigerian companies into their existing infrastructure and controls. This is underscored by the number of respondents who selected "do not know" when asked about their trust in their security controls – 19% in Kenya and 23% in Nigeria. If companies have the right tools and insights at their disposal, they are more likely to feel confident in their approaches and security hygiene.

Remote Workforce Challenges

There are several issues that have an impact on the management of the remote workforce, and these remain consistently the same across all three countries surveyed. For Nigeria, Kenya and South Africa, lack of infrastructure at home and in the office were a primary concern. In Kenya and Nigeria, the top challenge was the implementation of remote working infrastructure, while in South Africa, it was building a team identity.

In fact, in South Africa, the leading challenges around remote working were not connected to security but rather to team engagement and productivity. Organisations across all countries listed the wellbeing of their security teams, building a team identity and managing productivity and motivation as significant challenges.

Security Incidents

The biggest security risks associated with remote workers were listed as user behaviour and insecure home Wi-Fi networks, followed by social engineering, personal devices and sharing of corporate devices with family and friends.

Interestingly, only 16% of survey respondents in South Africa said they had experienced a security incident in the past 12 months related to remote working risks. Forty-six percent in Kenya and 56% in Nigeria.

Out of those who did, however, the most prevalent incidents were related to phishing and social engineering, ransomware and malware outbreaks.

South Africa had 61% social engineering and phishing; 26% ransomware; and 17% malware – unintentional data leaks actually sat in the third position for South Africa, along with credential theft and account compromise, at 22%. In Kenya, the statistics were 7% social engineering and phishing; 6% ransomware; and 11% malware. Nigeria had 14% social engineering and phishing; 3% ransomware; and 17% malware.

Security Awareness Processes

The pandemic threw everyone into the deep end. Organisations and individuals had to redefine and reshape how they approached working, living and technology. As work from home became work from anywhere and is now a hybrid methodology adapting to employee and organisation needs, security had to evolve. Respondents were asked whether their security awareness processes had changed since the start of the pandemic.

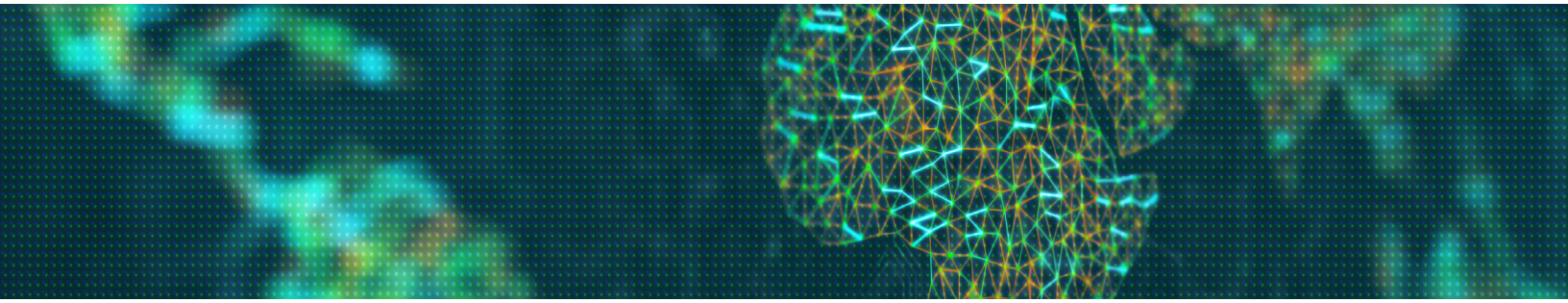
Most Kenyan respondents (52%) said their processes had changed, with 24% having introduced more eLearning training and phishing simulations. In South Africa, 66% of organisations have changed their processes, with 47% having introduced more eLearning training and phishing simulations, while 50% added more security awareness talks and webinars. This is not far off from Nigeria, which echoed both Kenya and South Africa with 51% reporting a change to their security processes, which comprised of 25% introducing more eLearning training and phishing simulations.

Top Security Concerns

Finally, when asked about their top security concerns and whether or not their budgets had changed to reflect their changing security priorities, the countries were mostly aligned. All three countries cited preventing data breaches, compliance with regulations and reputational damage as their most

pressing security concerns. These were closely followed by ransomware attacks and credential theft. These top five issues are the ones mostly likely to keep organisational leaders up at night as they look to ways of cementing better security and ensuring that they minimise vulnerabilities.

Unfortunately, security budgets have not comprehensively adjusted to meet these changing needs. Kenyan participants said that their budget had either stayed the same or increased with 21% stating it had increased but not significantly. Around 30% said it had stayed the same, while 19% said that they had severe budget cuts to security. In Nigeria, it was similar. 19% said it had increased but not significantly, and 28% said it had stayed the same. However, for Nigeria, 21% saw their budgets severely decreased. In South Africa, 45% stayed the same, 39% increased but not significantly, and only 5% had severe security budget cuts.



The Conclusion

With a median age of just 19.7 years, Africa has the youngest population in the world, consisting of potential future customers at a time when smartphone penetration, still under 50%, is rising sharply. And Africa's growing youth is demanding access to global connectivity while driving technology adoption and digitalization. The continent remains a point of investment interest as connectivity and mobility continue to grow. This situation has seen a subsequent surge in investor attention, particularly in the FinTech and telco spaces, and an equally high, but concerning surge in cybercriminal activity.

As incidents and financial impact are not officially disclosed, it's difficult to know how much cybercrime really impacts the African economy, but a recent study undertaken by Sophos found that 58% of South African organisations experienced an increase in cyberattacks since the pandemic. What is a fact is that the rapid growth in Africa's digital economy has outpaced developments in adequate cybersecurity.

While developed nations clamp down on ransomware actors, emerging economies and particularly African organisations with a high cyber dependency become more attractive to cybercriminals.

Most countries in the region do not have adequate cybercrime regulations in place and face significant skills shortages. A low level of general awareness means most consumers do not know how to ensure that their online behaviour is secure.

The findings of this report highlight the need for improving cybersecurity preparedness across all participants, in a world that will remain remote or at least in a hybrid set up.

Africa's organizations need to invest in security hygiene and prioritize cybersecurity best practices that will decrease their attack surface. This includes establishing a security culture and educating employees on how to spot and defend against social engineering attacks, upskilling their IT and security workforce, maturing patch and vulnerability management processes and investing in scalable cloud and remote working security architecture, technology and processes.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4 Africa | The Planet Art, 32 Jamieson St, Cape Town, 8001, South Africa
Tel: +27.21.813.9264 | Email: Popcorn@KnowBe4.com

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01B11K01