A
Lynchpin
Media
BRAND

CXO priorities

REMOTE WORK

TRENDS, RISKS AND PRIORITIES

A CXO priorities REPORT, IN PARTNERSHIP WITH KnowBe4

Human error. Conquered.

CONTENTS

The world today is not the same as it was just two years ago. In early 2019, the COVID-19 pandemic arrived and caused widespread disruption, not only resulting in a devastating global death toll but leaving economies in disarray as various nations imposed lockdowns and restrictions.

Businesses and organisations held crisis talks to consider the way forward as uncertainty became the daily agenda. Budgets were impacted, resources reduced and, in a bid to keep employees safe and to comply with government guidelines, many organisations adopted a ‘work from home’ approach.

Overnight, the relative controls provided to IT teams in their corporate environments were gone, and the challenge of securing a new remote workforce became a top priority for many CISOs.

Since then, organisations have pivoted from an entirely remote workforce in many cases to new hybrid models. But flexibility remains key and so security remains top of mind.

To gain insight into the status quo of remote working and to find out about the risks, priorities and the role of the ‘human factor’ for organisations, we surveyed 100 IT security leaders and executives in both Kenya and Nigeria.

Through this survey we set out to discover:

- the biggest challenges and security risks for remote workers
- how the pandemic has impacted approaches to security awareness
- the role of technology in assisting remote team management

> “Overnight, the relative controls provided to IT teams in their corporate environments were gone, and the challenge of securing a new remote workforce became a top priority for many CISOs.

KnowBe4
Human error. Conquered.

priorities

A Lynchpin Media BRAND

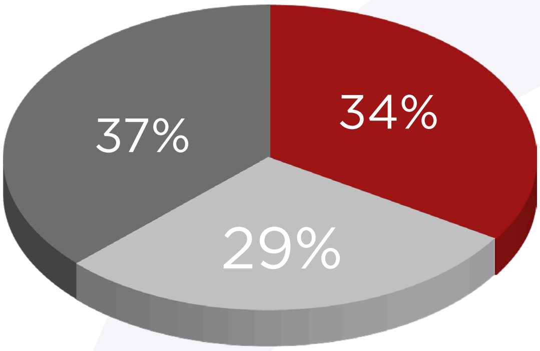
1. A NEW WORLD OF WORK – AND THE SECURITY IMPLICATIONS

One of the biggest impacts of the pandemic was the rapid mobilisation of a remote workforce. Many organisations may have already operated a partial work from home model but there is no doubt that this is where the future lies.

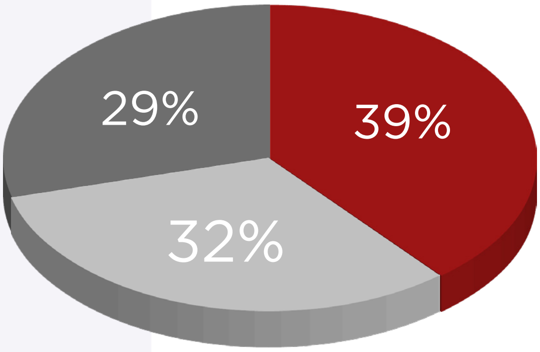
REMOTE WORKING – FUTURE REALITY

We asked respondents whether remote working was a future reality in their organisation.

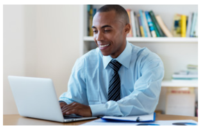
Of the **100** respondents that took part in the survey from **KENYA**, a total of **34%** said that it was a reality, and employees would continue to work from home. A further **29%** said it was a reality but they had flexible policies, while the remaining **37%** stated that they had either already returned to offices or were set to.



In **NIGERIA**, respondents provided similar feedback, with **39%** stating that they would continue to work from home. A further **32%** said 'yes, but flexible' while the remaining **29%** said they had already, or were set to, return to offices.



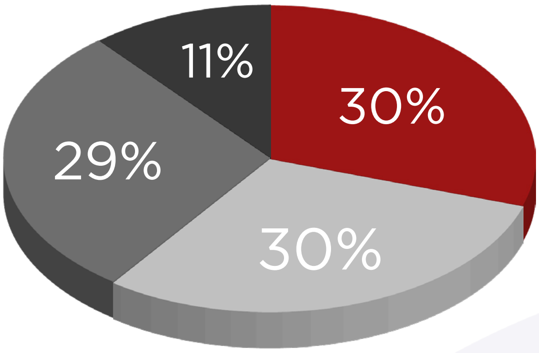
> In Nigeria, respondents provided similar feedback, with 39% stating that they would continue to work from home.



1. A NEW WORLD OF WORK – AND THE SECURITY IMPLICATIONS

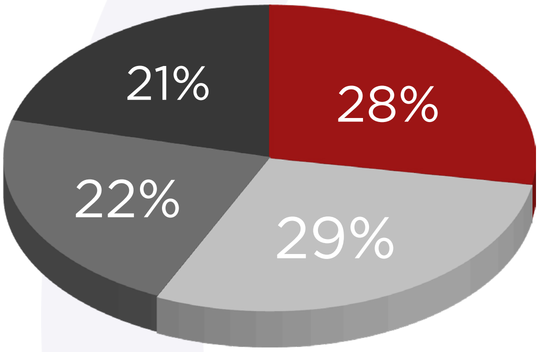
RETURN TO OFFICE

In **KENYA**, **30%** of respondents said remote workers had fully returned to the office. A further **30%** said workers had returned part time, while **29%** said they had not – but planned to. The remaining **11%** said they would not be returning for the foreseeable future.



> In Kenya, 30% of respondents said remote workers had fully returned to the office.

In **NIGERIA**, **28%** said remote workers had fully returned to the office while **29%** had returned part time. A further **22%** had not but planned to while the remaining **21%** said this would not be the case for the foreseeable future.



1. A NEW WORLD OF WORK – AND THE SECURITY IMPLICATIONS

SOCIAL ENGINEERING ATTACK READINESS

To identify organisations' readiness for social engineering attacks, we asked participants to what extent they agreed that remote work users were solidly trained and able to withstand social engineering attacks.

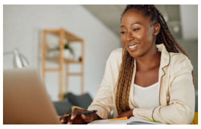
		KENYA	NIGERIA
😀	Completely agree	16%	11%
🙂	Agree	11%	26%
😐	Neutral	28%	25%
☹	Disagree	16%	7%
😠	Completely disagree	13%	16%
😵	Don't know	16%	15%

1. A NEW WORLD OF WORK – AND THE SECURITY IMPLICATIONS

SECURITY CONTROLS

We also asked to what extent respondents agreed that remote working infrastructure and security controls were solid.

	KENYA	NIGERIA
Completely agree	18%	12%
Agree	16%	9%
Neutral	22%	30%
Disagree	15%	10%
Completely disagree	10%	16%
Don’t know	19%	23%

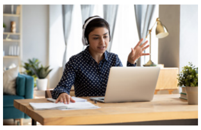


2. REMOTE WORKFORCE CHALLENGES

The challenges of managing cybersecurity for modern enterprises is challenging, with sophisticated new attack methods being developed constantly.

Survey participants were asked to rate the challenges of managing a remote workforce. The below table highlights the percentage of respondents that rated each of the listed concerns as the biggest problem which keeps them up at night, with the results demonstrating the somewhat even split between each individual issue.

	KENYA	NIGERIA
Speed of roll out/implementations of remote working infrastructure	15%	13%
Lack of infrastructure at home and the office	7%	11%
Lack of budget	10%	8%
Lack of relevant security policies	15%	4%
Lack of cybersecurity awareness	10%	6%
Well-being of my security team (added pressure)	16%	18%
Building and keeping a team identity	9%	21%
Motivation and productivity	18%	19%



2. REMOTE WORKFORCE CHALLENGES

SECURITY INCIDENTS

Respondents were asked whether they had experienced a security incident in the last 12 months due to remote working risks.

In **KENYA**, a majority of **54%** said they had not.

Of the **46%** that had, these incidents included:

Phishing/social engineering	Ransomware	Malware outbreak	Unintentional data leak such as a laptop sent to the wrong person etc	Credential theft/account compromise
(**7%**)	(**6%**)	(**11%**)	(**9%**)	(**12%**)

For **NIGERIAN** respondents, however, **44%** had not experienced a security incident.

Of the **56%** that had, these incidents included:

Phishing/social engineering	Ransomware	Malware outbreak	Unintentional data leak such as a laptop sent to the wrong person etc	Credential theft/account compromise
(**14%**)	(**3%**)	(**17%**)	(**9%**)	(**13%**)

2. REMOTE WORKFORCE CHALLENGES

SECURITY AWARENESS PROCESSES

Participants were asked whether their security awareness process had changed since the beginning of the pandemic.

Most **KENYAN** respondents (**52%**) said their processes ***had*** changed . . .

. . . with **24%** having introduced more e-learning training and more phishing simulations . . .

. . . and **28%** having added more security awareness talks and webinars.

The results were similar among **NIGERIAN** respondents, with **51%** reporting a change to their security processes.

These comprised of more e-learning, training and phishing simulations (**25%**)

and more security awareness talks and webinars (**26%**)

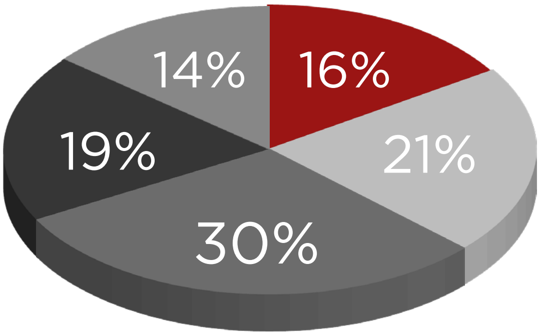
3. TOP SECURITY CONCERNS

We asked participants to rate their top security concerns. The below table highlights the percentage of respondents that rated each of the listed concerns as the biggest problem which keeps them up at night.

	KENYA	NIGERIA
Preventing data breaches	12%	15%
Compliance with regulations	19%	10%
Reputational damage	11%	12%
Ransomware attacks	16%	18%
Credential theft	15%	11%
Theft of intellectual property or personal information	16%	16%
Loss of availability and Business Continuity	11%	18%

3. TOP SECURITY CONCERNS

SECURITY BUDGETS



Survey respondents were asked whether their security budget had been adjusted due to the pandemic or the economic situation in their country.

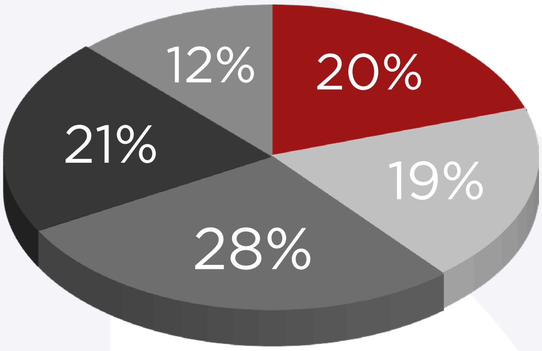
Responses were mixed among **KENYAN** participants, but a majority said their budget had either stayed the same or increased.

A total of **16%** stated their budget had increased by 'quite a lot', while **21%** said it had increased, but not significantly, and **30%** reported their budget had remained the same.

A total of **19%** stated that severe budget cuts to security and IT budgets had led to a decrease in budget, while the remaining **14%** reported a budget decrease – though 'not significant'.

For **NIGERIAN** respondents, it was a similar picture.

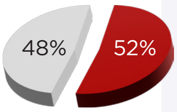
A total of **20%** stated their budget had increased by quite a lot, while **19%** said it had increased, but not significantly, and **28%** said their budget had stayed the same. For **21%** of respondents, the budget for security and IT had severely decreased and the remaining **12%** reported a decrease, which was not significant.



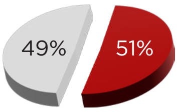
NEW TECHNOLOGIES

Participants were also asked whether they had adopted any new technologies or processes to assist in their remote team management.

A total of **52%** of Kenyan respondents said they had, while **48%** had not.



A total of **51%** of Nigerian respondents said yes, while **49%** said they had not.



4. CONCLUSION

The survey findings shine a light on the key challenges that security and IT leaders have been navigating during the shift to remote working.

Many respondents from both **KENYA** and **NIGERIA** highlighted that remote working was now the norm for them, although some stated they had flexible policies and others had returned to the office.

This demonstrates the complex situation that many CISOs are grappling with today, as they need to find ways to secure their employees from multiple locations.

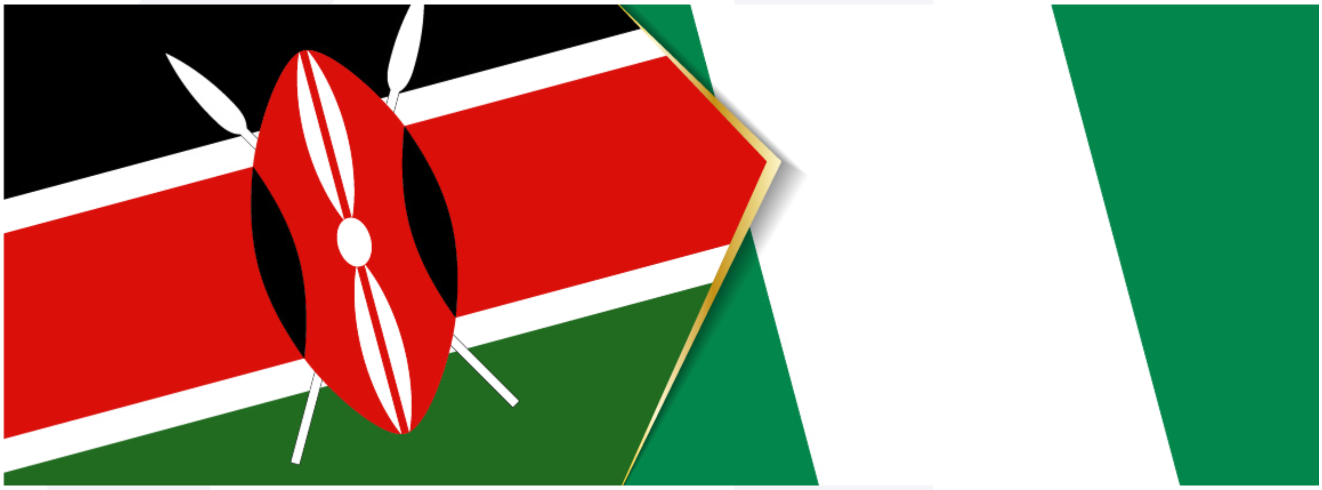
The hybrid workforce is likely to be a dominant feature of organisations' future strategies, so finding effective security awareness training programmes will be crucial.

Given the somewhat even split between the biggest security concerns for organisations, there are clearly multiple areas of concern for security leaders.

In both countries, respondents said they had introduced new security awareness processes since the beginning of the pandemic.

This demonstrates the emphasis placed on the 'human factor', as organisations recognise the importance of ensuring their newly remote or hybrid workforces are able to clearly identify threats, report them and, as a result, improve cyber-resilience.

> “ The hybrid workforce is likely to be a dominant feature of organisations' future strategies so finding effective security awareness training programmes will be crucial.



KnowBe4
Human error. Conquered.

32 Jamieson St, Gardens
Cape Town, 8001
South Africa

Find out more: **www.knowbe4.com**

CxO priorities

A Lynchpin Media BRAND

CxO Priorities, a Lynchpin Media Brand
63/66 Hatton Garden
London, EC1N 8LE

Find out more: **www.cxopriorities.com**