KnowBe4

KnowBe4 Africa Human Risk Management Report 2025: The Human Element in African Cybersecurity

Insights From Decision-Makers

KnowBe4 Africa & Red Ribbon Insights

WWW.KNOWBE4.COM

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

052025

Table of Contents

Executive Summary

KnowBe4's Africa Human Risk Management Survey Report 2025 reveals a striking paradox: while organisations across the continent believe they are aware and prepared, critical blind spots remain in how they manage their most dynamic risk vector and potentially strongest defence – their people.

This survey report captures responses from senior cybersecurity decision-makers across 30 African countries. While there's growing recognition of human risk as a priority, the numbers paint a more complex picture:

- Over 41% of responding organisations say their biggest challenge is measuring whether security awareness training (SAT) actually works. In other words, leaders are investing in awareness, but find it difficult to tell if it's translating into action.
- Only 10% of respondents are fully confident their teams would report a suspicious email or threat.
- And while 68% claim to tailor SAT by role, the second most-cited challenge is a lack of role-based alignment – suggesting this tailoring may be more ambition than reality.
- The human element in cybersecurity isn't just misunderstood – it's under-managed.

5 key fault lines in Africa's cyber readiness

1. **Overconfidence vs Reality**
High scores in awareness (typically 4/5) mask the fact that only a small fraction of employees are seen as truly ready to act when threats appear. This "confidence gap" is consistent across regions and industries.

2. **BYOD and Shadow AI Risks**
Up to 80% of employees use personal devices for work, and 46% of organisations admit their AI policies are still "in development". This leaves doors wide open for unmanaged risk.

3. **Training Without Impact**
Many organisations run annual or biannual security awareness programmes – but with little role relevance, no behavioural tracking, and even less accountability. One-size-fits-all training isn't moving the needle.

4. **The Bigger the Business, the Bigger the Blind Spots**
Larger companies (501+ employees) report lower training frequency, lower confidence in reporting of security issues, and greater difficulty measuring outcomes. In scaling up, many seem to be scaling out of human-centred governance.

5. **Stark Regional Contrasts**
East Africa leads with proactive AI governance. Southern Africa trains most frequently. North Africa has the highest BYOD exposure. West and Central Africa report the most human-related incidents. Resilience isn't one-size-fits-all – and strategies shouldn't be either.

INTRODUCTION

Across Africa, organisations are making strides in cybersecurity awareness – the results, however, are as dynamic as the countries they are achieved in. To better understand the evolving landscape across the continent, KnowBe4 Africa commissioned Red Ribbon Insights to conduct the Africa Human Risk Management Survey 2025. The dataset captures insights from 124 cybersecurity decision-makers with respondents sourced across 30 African countries. These respondents include CISOs, CIOs, risk managers, and awareness leads – professionals responsible for policy compliance and that are shaping digital defences on the continent. The responses to this survey provide a range of interesting signals that can help describe emerging trends in Africa.

The picture that emerges is both promising and concerning. While awareness of cybersecurity policies is rated highly across most organisations, there are alarming gaps in implementation – particularly around incident reporting, tailored training, and governance over emerging risks like artificial intelligence (AI).

In other words, the continent's cybersecurity posture may be more confident than it is resilient.

KEY TAKE-AWAYS

High Perceived Awareness, Low Structure

Despite rating policy awareness at four to five out of five, many organisations lack formalised processes for reporting and responding to incidents.

Training Misalignment

One-size-fits-all training is common – but largely ineffective. Decision-makers cite the need for more tailored, role-specific and measurable learning.

Overconfidence in Readiness

Leaders are concerned that perceived awareness does not translate into real-world vigilance or accountability.

The Human Element: A Consistent Focal Point

Africa's workforce is more connected than ever – and that connectivity extends beyond office walls. A significant portion of employees (between 41% and 80%, depending on the organisation) use the same devices for both personal and work-related tasks. This widespread Bring Your Own Device (BYOD) culture is no longer novel – it's the norm. But its security implications remain deeply under-addressed.

Decision-makers across the continent acknowledge that the blurring of work and personal boundaries creates vulnerabilities, particularly when device management and security controls are inconsistent. Nowhere is this more evident than in North Africa, which reported the highest BYOD exposure (with half of regional respondents indicating BYOD-rates of 61% - 80%), yet also ranks among the lowest in training frequency (67% training annually) and confidence in incident reporting (average score of 3 on a scale of 1-5).

Compounding this risk is the creeping presence of "shadow AI" – unregulated use of AI tools by employees. As many organisations (46%) still report that their AI governance policies are "in development", the risk of unsanctioned, potentially unsafe use of AI is rising. East Africa is the exception, with more respondents indicating they already have AI policies in place (50% of respondents) – a positive signal in an otherwise cautious landscape.

Add to this a widespread lack of formal incident reporting procedures (a persistent issue across the continent due to a lack of disclosure culture), and the picture becomes clearer: while awareness of risks may be high, the structural safeguards to act on that awareness often lag behind.

KEY INSIGHTS

BYOD risks persist: Up to 80% of employees use personal devices for work – with broader studies finding 70% of these devices are unmanaged.

Managing Human Risk: The Confidence Gap

Confidence ratings in employees' ability to spot and report incidents, identified in the 2025 Annual African Cybersecurity & Awareness Report, cluster around 3 and 4 out of 5, with only 10% expressing full confidence (5/5). Nearly 39% of leaders responding to the 2025 survey rate confidence at 3/5 or below – suggesting a widespread uncertainty in workforce readiness, despite high awareness scores.

If awareness is the foundation of cybersecurity, then action is its real-world expression. But this survey shows that confidence in the workforce's ability to respond appropriately – to recognise, report, and mitigate threats – is often overestimated.

Across the board, decision-makers rated employee awareness of policies as high (typically 4 out of 5 or more). Yet when asked whether their teams would reliably report an incident, that confidence began to waver.

KEY INSIGHTS

→ Larger organisations appear paradoxically less prepared, reporting lower training frequency and confidence – suggesting that scale can dilute structure if not managed deliberately.

→ Measuring impact is the top challenge: Over 40% of respondents cite difficulty in measuring security awareness training effectiveness – making it the single biggest obstacle to meaningful change. Research recently published in the Oxford Academic Cybersecurity Journal echoes the urgency of finding ways to address this challenge.

In Central and North Africa, for instance, confidence scores dipped below average despite strong awareness ratings – highlighting a clear gap between knowing and doing.

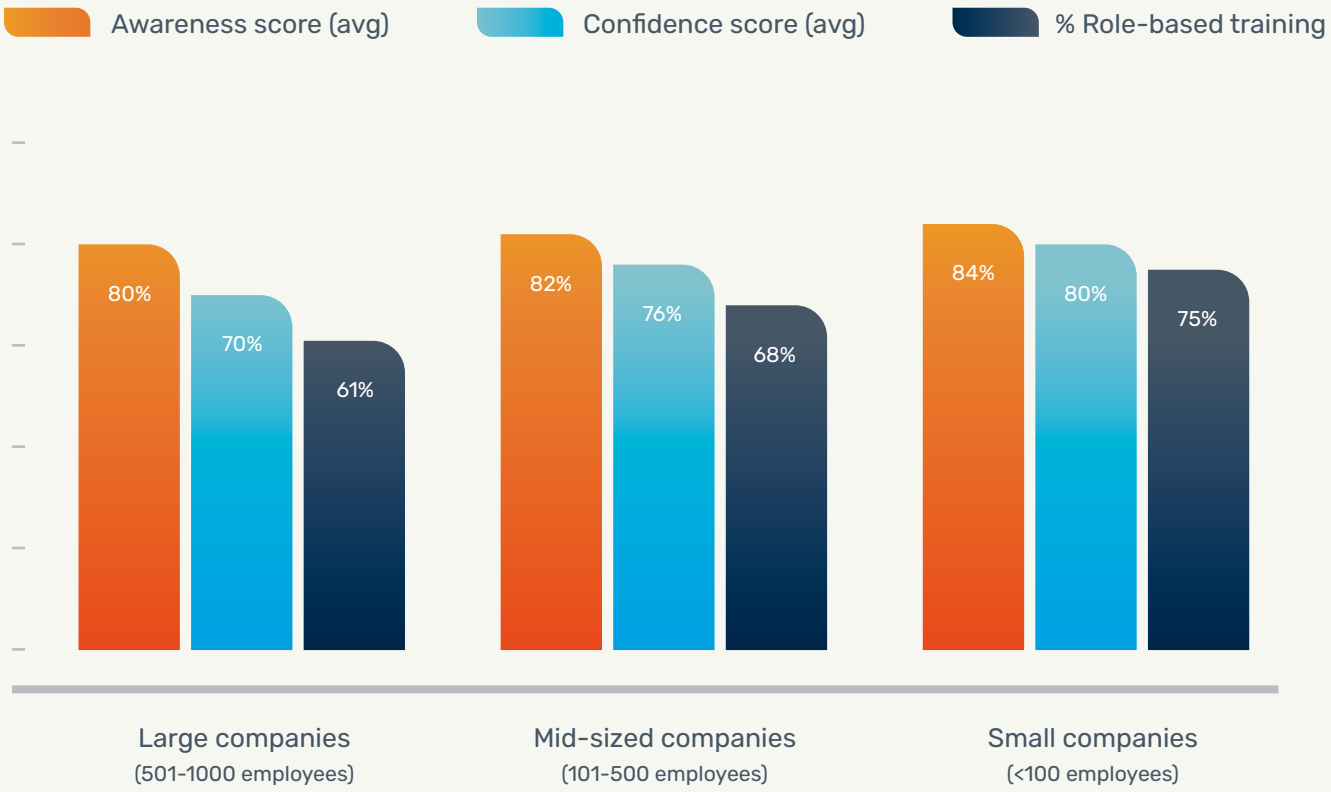
Training is often cited as the main tool for bridging that divide, yet it, too, faces challenges. Most organisations conduct training either annually (29%) or biannually (39%), but frequency alone is not the issue. Rather, decision-makers report that much of the training remains too generic to shift behaviour meaningfully (more than a third reporting training is not tailored to roles or risk exposure). Manufacturing and healthcare sectors are especially prone to this "one-size-fits-all" approach (50% and 40% reporting no tailoring at all, respectively), and even technology firms – which boast some of the most confident awareness scores – often neglect role-specific customisation (25% not tailoring SAT at all, and 17% only somewhat).

This disparity seems to grow even more in relation to how many employees a company has. Larger organisations (501-1,000 employees) consistently show lower training frequency and lower confidence in employee reporting. Growth without governance = increased human risk.

Moreover, as organisations grow, the impact of all types of SAT becomes harder to measure. Larger companies (501+ employees) not only train less frequently (with an average of 65% reporting biannual or annual frequencies) but also report lower confidence in employees' incident response capabilities (averaging 3 on a scale of 1 -5, whereas companies with less than 500 employees averaging 4 out of 5). Without metrics to assess training effectiveness, organisations are left in the dark about whether their investments in human risk mitigation are paying off.

The Confidence Gap

The disparity between perceived awareness, confidence in employees to act, and the actual customisation of training.



Phishing Simulations and the Prevalence Effect: Frequency Matters

It's encouraging to see that the majority of respondents have adopted phishing simulations as part of their cybersecurity strategy, with 90% indicating some level of testing. However, the **frequency of these simulations remains too low to be truly effective**. Only 7% conduct them monthly and 27% quarterly, while the largest group (40%) runs simulations just twice a year. A further 16% do so annually, and 4% not at all.

This low frequency poses a critical challenge in light of the "**prevalence effect**," a psychological phenomenon where rare or infrequent events are more likely to be overlooked or misjudged. Simply put, when phishing attempts are simulated too infrequently, employees are less likely to build the consistent, instinctive responses needed to detect and report real threats. With more than half of the organisations running phishing **simulations just once or twice a year**, most workforces across the continent are being underexposed to this crucial form of security training. To truly reduce human cyber risk, organisations must shift to more frequent, ongoing simulations—helping staff internalise threat patterns and develop the kind of reflexive awareness necessary to stop attacks before damage is done. This is supported by KnowBe4's research from over 60,000 individual organisations worldwide, comprising 32,604,108 separate individual users, which confirms that increased phishing simulation frequency directly correlates with measurable improvements in security behaviour over time.

Policies, Procedures and the AI Blind Spot

The shift to digital-first operations across Africa has not always been matched by formalised governance. In 2025, this is especially evident in the growing gap between rapid adoption of new technologies and the policies required to use them safely.

AI is the standout case. Across regions and industries, 46% of respondents report that their AI policies are still "in development". This is particularly alarming given AI's potential to both aid and undermine cybersecurity – from generating convincing phishing content to automating insider threat detection. Without clear guidelines, these tools risk being misused or poorly understood by employees.

Incident reporting protocols – another cornerstone of cybersecurity resilience – are similarly underdeveloped. Many decision-makers admit that while employees are aware of the importance of reporting, the absence of clear, enforced processes leaves room for inconsistency and inaction. In fact, only a handful of industries – notably finance – report frequent, structured training and reporting frameworks. Most others still rely on ad hoc or under-resourced approaches.

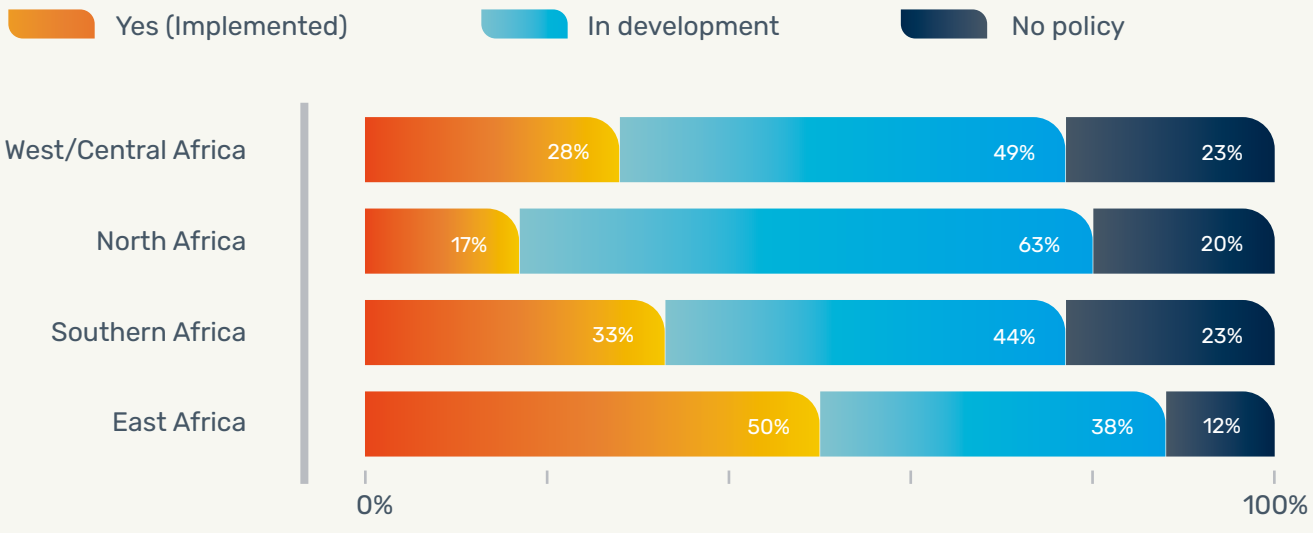
These gaps are not just theoretical. They represent real exposure – and a missed opportunity to convert awareness into resilient practice.

KEY INSIGHTS

→ The manufacturing sector stands out for its **lack of tailored training and formalised reporting structures** – suggesting heightened exposure that demands immediate attention.

→ **Shadow AI risks:** AI policy remains a governance blind spot in many organisations, with similar research published in the Data and Policy journal indicating most African nations lag in global AI governance readiness.

Distribution of AI policy status across regions



Risk is Not Uniform: Regional and Role-based Contrasts

The African cybersecurity landscape is anything but homogenous. This survey underscores the contrasts in readiness and perception depending on where an organisation is based – and who within that organisation is responding.

By Region

- **North African** respondents report the highest BYOD usage (average rate of 61% - 80%) and the lowest training frequency (67% reporting annual frequency), suggesting elevated risk in operational exposure.
- **Central and West African** participants report the highest proportion of security incidents linked to the human factor (rate of 51% - 75%, with other regions averaging 26% - 50%), underscoring the need for stronger mitigation strategies.
- **East African** respondents stand out for their early adoption of AI governance. These organisations are more likely to have formal AI policies in place (50% already have policies in place), positioning them ahead of the curve.
- **Southern African** respondents lead in training frequency, with 44% conducting quarterly sessions. Yet paradoxically, they lag in AI policy development (with 56% reporting no AI policies in place, compared to the overall average of 46% reporting policies in development), highlighting a divide between procedural rigour and forward-looking governance.

KEY INSIGHTS

→ Regional contrasts in our data set: From high BYOD exposure in North African respondent groups to advanced AI governance in East Africa, cybersecurity readiness seems far from uniform across the continent.

→ Seniority shapes risk perception: Executives focus on strategic gaps (like AI and incident reporting), while managers highlight day-to-day training and implementation challenges.

By Role

- **CISOs and CIOs**, express strategic concerns: weak incident reporting, poor AI oversight, and gaps in structural governance.
- **Risk managers and security awareness leads** are more focused on training quality and relevance. They highlight the misalignment between training content and job-specific responsibilities.
- **Security staff members**, despite being close to the action, often feel under-supported – especially when reporting structures are vague or unenforced.

Comparing Insights From Employees to That of Employers: A Gap Between Perception and Reality

While this report focuses on decision-makers, the 2025 Annual African Cybersecurity & Awareness Report surveyed general employees across Africa. Comparing the two reveals a troubling divergence between what leaders believe and what employees experience.

Confidence disconnect

In 2025, half of leaders rate employee reporting confidence at 4/5 – but only 10% rate it at 5/5. Meanwhile, in 2024, just 43% of employees felt fully confident recognising a threat, and 36% rated themselves 3/5 or lower.

50%

of leaders report employee confidence at 4/5

Training perception gap

68% of 2025's decision-making respondents say training is tailored to roles, yet in 2024, only a third of employees felt they had received adequate training – with 16% actively disagreeing.

68%

of leaders say training is tailored to roles

Awareness ≠ readiness

Despite 57.5% of employees in 2024 expressing deep concern about cyber threats, many also felt overwhelmed, unprepared, and unsure how to respond.

57.5%

of employees expressed deep concern about cyber threats

Conclusion: Aligning Perception with Practice

The Africa Human Risk Management Survey Report 2025 points to a critical truth: Cybersecurity cannot rest on perceived awareness alone. African organisations need to embed resilience into every layer of their operations – especially the human layer.

To do this, we recommend the following actions:

1. Customise training by role and risk exposure

Generic training is no longer fit for purpose. Organisations must develop learning interventions aligned to employees' day-to-day responsibilities – particularly in sectors where risk profiles vary widely.

2. Measure what matters

Implement clear metrics for tracking training effectiveness. Metrics that go beyond training participation can be derived from culture and security proficiency surveys, phishing simulation and reporting trends. This will not only justify budget allocation but also identify blind spots in workforce readiness.

3. Formalise incident reporting structures

Employees must know exactly how and when to report potential incidents – and must trust the process. Clear and easy to follow reporting paths, immediate feedback, regular phishing simulations tests, and executive support are critical.

4. Close the AI governance gap

Develop and enforce policies that regulate the use of AI, including generative tools. AI is a growing asset – but without oversight, it can easily become a threat vector.

5. Contextualise strategy by region and sector

What works in East Africa may not work in Central Africa. Build cybersecurity strategies that respect the regulatory, cultural, and operational nuances of each region.

The findings in this report call on African cybersecurity leaders to build deeper resilience – not just by investing in technology, but by elevating the human element of security through structure, governance, and tailored behavioural interventions.

The human layer is not a flaw to fix, but a frontier to strengthen. Awareness is only the beginning. The future of Africa's cybersecurity depends on the actions that follow.

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organisations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organisations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

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

KnowBe4

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