pwc

Putting security at the epicenter of innovation

Global Digital Trust Insights Survey 2024: South Africa Report

Executive Summary

Chief Information Security Officers (CISOs) are taking the lead, empowered to step beyond their traditional roles as independent cybersecurity experts, and instead forge partnerships not only with a select few executives but with the entire C-suite and board. This collaborative approach ensures a comprehensive and unified front against emerging threats, safeguarding the integrity and trust of businesses in today's dynamic digital landscape.

As companies shift towards using mostly digital supply chains, there are new risks for cybersecurity. Each time they try something new, they face new challenges to keep information safe.

The latest insights from our 2024 Global Digital Trust Insights survey, representing the perspectives of over 3,876 business, security, and IT leaders spanning various industries and 71 territories, reveal that the field of cybersecurity is in a state of constant evolution, swiftly adapting to keep pace with business inventiveness. The survey indicates that Southern Africa and Africa have 3,428 responses with the same testaments. The fact that 30% of respondents have revenues of $10bn (R192,793,500 ,000) or more shows considerable room for improvement in cybersecurity.

Cybersecurity faces four major shifts, each of which could be disruptive on its own.

- C-suite insistence on modernising and improving technology infrastructure and investments in a year of cost-cutting and macroeconomic uncertainty.
- The rise of hybrid cyber threats and the blurring of the line between espionage and cybercrime, propelling cyber defence more fully into the national security arena.
- A ground-breaking new technology "generative AI", bringing new threats as well as unprecedented promise for defence.
- Regulations requiring openness about cyber incidents and risk management practices that could usher in a new era of transparency and collaboration.

Consider these findings. The costs of, and the number of high-dollar, breaches continue to increase. Although cloud attacks are the top cyber concern, about one-third of organisations have no risk management plan to address cloud servers. Generative AI is opening frontiers that are being explored, in the business and for cyber defence, by the more than 3,800 C-level business and tech executives who responded to our 2024 Global Digital Trust Insights (DTI) Survey are exploring in the business and for cyber defence.

Only half of the organisations are 'very satisfied' with their technology capabilities in key cybersecurity areas. More than 30% of companies don't consistently follow what should be standard practices of cyber defence.

About the survey

The 2024 Global Digital Trust Insights is a survey of 3,876 business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers) that was conducted in July and August 2023.

The respondents of this survey operate in a wide range of industries namely: Industrial Manufacturing (20%), Tech, Media, Telecom (19%), Financial Services (20%), Retail and Consumer Markets (17%), Energy, Utilities, and Resources (11%), Health (9%), and Government and Public Services (3%), and The respondents are based in the following regions: Western Europe (31%), North America (28%), Asia Pacific (18%), Latin America (10%), Eastern Europe (5%), Africa (4%), and Middle East (3%) .

Below are the key observations:

- Digital and technology risks are most interconnected with cyber risks, requiring CISOs and tech leaders to position themselves at the epicentre of innovation in their organisations.
- The proportion of costly cyber breaches ($1m+) has increased since last year.
- Cyber investments are a priority. Cyber budgets in 2024 are increasing, and at a higher rate compared to last year.
- In an environment where the majority of those surveyed expect revenue growth over the next 12 months, 79% of organisations plan to increase their cyber budget in 2024. ‘High growth’ companies are more likely to be increasing their cyber budget to a higher degree (15% or more).
- Those who experienced a cyber breach of $1m or greater are more likely to increase their cyber budget (88%).
- Business leaders prioritise the modernisation of technology and optimisation with their cyber investments. Integration, rationalisation, simplification and dealing with legacy debt will factor in investment discussions.
- Many companies report activities to transform cyber in their organisations, but only about a quarter are realising benefits.
- Movement to integrated tech solutions or suites is increasing, two-fifths already have an integrated suite and a further two-fifths intend to make this transition within the next two years.
- DefenseGPT, organisations are gearing up to deploy generative AI (genAI) tools for cyber defense. AI governance is needed to harness enthusiasm for genAI applications to grow the business and have more productive workers.
- Regulation, business and tech leaders see various regulations as helpful to securing future growth, but anticipate additional compliance costs and significant business transformation.
- The top performing organisations, who display greater maturity in their cybersecurity initiatives, report a greater number of benefits and a lower incidence of costly cyber breaches, of $1m+, or any breach at all.

The Global Digital Trust Insights Survey is formally known as the Global State of Information Security Survey (GSISS).

Overview of DTI 2024

The digital trust insights survey is conducted globally and locally on a yearly basis to get the views of senior executives on the challenges and the opportunities to improve and transform cybersecurity within their organisation in the next 12-18 months. The statistics of the respondents and their demographics are indicated below:

3,876 Respondents

Across **71** territories

Surveyed in **19** different languages

Between 9 May – 14 July 2023

30+ territories can report on survey findings

Survey Summary Analysis

Cyber Risk Management

Globally and locally, organisations seem to agree that they should prioritise digital and technology risks for mitigation. However South Africa and Africa seem to be a lot more concerned about prioritising inflation for mitigation than the rest of the world. (S1q1)

South Africa and Africa are less concerned about cloud related threats than their global counterparts. The former is more concerned about attacks on connected devices while the latter is concerned about hack-and-leak operations. This may be due to the fact that less organisations in Africa and South Africa have migrated to the cloud. (S1q2)

Globally and locally, organisations are concerned about loss of customer, employee or transaction data, damage to company brand and loss of revenue when it comes to cyber attacks. (S1q4)

Both global and local respondents estimated that the cost of data breaches is between US$1m – US$9m. And interestingly, 33% of South African and African organisations indicated that they had not been breached in the past three years compared to 15% globally. (S1q5)

Globally, organisations use the IS027001 industry framework to assess and report on their cybersecurity capabilities, whereas locally organisations make use of the NIST cybersecurity framework. NIST and ISO27001 have some differences in their focus and requirements. For example, NIST is considered to be more detailed, while ISO27001 offers a broader framework for information security management. (S1q6)

Working with Hyperscalers

Statistics indicate that the majority of organisations in South Africa that responded are using private clouds to host their infrastructure, indicating that there is a rapid move from on premise and hybrid to the cloud. (S2q1)

Globally and locally, the majority of the organisations that responded are not addressing their cybersecurity challenges with their cloud service providers. In some instances such as third party risks, only 16% of South African organisations have addressed this significant risk with their cloud service providers. (S2q2)

Africa is more concerned about fragmented regulations, whereas its global counterparts are more concerned about sharing resources with other organisations with the same cloud service provider. (S2q3)

Statistics indicate that both globally and locally, organisations are moving towards using one integrated solution suite of cybersecurity technologies or are planning to move towards using an integrated suite of solutions within the next two years. (S2q7)

Portfolio rationalisation, cyber fit for growth

The statistics below show that globally and locally there has been only an increase of between 6 to 10% or less in an organisation's cybersecurity budget. A small budget increase may not provide enough resources to address emerging threats, maintain and update security systems or hire skilled cybersecurity professionals. (*s3q1)

The statistics indicate that the majority of organisations in South Africa are prioritising their investments in application security, while most organisations in Africa are prioritising network security. Globally, organisations are prioritising cloud security. (*s3q2)

Globally and locally, statistics show that organisations invest into the modernisation of technology, including cyber infrastructure, because investing in modern technology allows organisations to adopt the latest security measures and tools to address new and emerging threats. Investing in modern solutions provides stronger defence against cybersecurity threats, which reduces the risk of breaches and data loss. (*s3q3)

The statistics indicate that the majority of organisations in South Africa and Africa responded that they do not have adequate security technology solutions, while globally most organisations responded that they have the right amount of cybersecurity technology solutions. (*s3q4)

Globally and in Africa organisations are satisfied with their networking/firewall and vpn technologies, whereas in South Africa organisations are satisfied with their cloud security because many cloud security providers offer managed security services or partner with third party security providers, which offloads some of the security management tasks. (*s3q5)

Globally and locally, organisations are prioritising upskilling the current workforce fast enough to keep up with the demands of the business. (*s3q6)

Cyber transformation, technical solutions

The statistics show that organisations that have implemented a cybersecurity framework are prioritising identifying critical business processes as a cyber resilience action, while the organisations that are in the process of implementing a cybersecurity framework are prioritising implementing cyber recovery technology solutions and integrating fully with the organisation's resilience strategy and activities. (S4q1)

Globally organisations are most concerned about identity and access management, whereas in Africa and locally organisations are more concerned about software defined access. (S4q2)

Regulations

South Africa is as concerned as its global counterparts to regulate artificial intelligence, whereas Africa is more concerned about reporting about cyber risk management. (S5Q1)

Defense GPT: genAI-powered cyber

South Africa is as concerned as its global counterparts about virtual environment tools and the risks associated with them. (S6q1)

Q 1: Which of the following risks is your organisation prioritising for mitigation over the next 12 months?

Globally and locally organisations seem to agree that they should prioritise digital and technology risks for mitigation, however South Africa and Africa seem to be a lot more concerned about prioritising inflation for mitigation than the rest of the world.

Organisation's risk mitigation priorities over the next 12 months (% Ranked top three)

	Global (3,876)	Africa (168)	South Africa (68)
Digital and technology risks	51%	44%	40%
Cyber risks	43%	44%	35%
Macroeconomic volatility	41%	33%	31%
Inflation	39%	43%	44%
Geopolitical risks	31%	20%	21%
Environmental risks	28%	32%	28%
Societal risks	24%	17%	21%
Health risks	20%	26%	31%
Unsure	1%	3%	3%

Key: 1st 2nd 3nd

Q 2: Over the next 12 months, which of the following cyber threats is your organisation most concerned about?

South Africa and Africa are less concerned about cloud related threats than their global counterparts, whereas South Africa is more concerned about attacks on connected devices and Africa is concerned about hack-and-leak operations. This may be due to the fact that less organisations in Africa and South Africa have migrated to the cloud.

Top cyber threats to organisations over the next 12 months (% Ranked top three)

	Global (3,876)	Africa (168)	South Africa (68)
Cloud-related threats	47%	25%	35%
Attacks on connected devices	42%	42%	47%
Hack-and-leak operations	37%	45%	46%
Business email compromise / account takeovers	29%	41%	38%
Ransomware	29%	29%	19%
Software supply-chain compromise	25%	24%	32%
Third-party breach	23%	23%	15%
Distributed denial-of-service attacks	17%	12%	4%
Exploits of zero-day vulnerabilities	17%	11%	10%
Disinformation	15%	14%	10%
Unsure	1%	1%	1%

Key: 1st 2nd 3nd

Q 3: Over the next 12 months, which of the following potential outcomes of cyber attacks is your organisation most concerned about?

Globally and locally, organisations are concerned about loss of customer, employee or transaction data, damage to company brand and loss of revenue when it comes to cyber attacks.

Organisation's top concerns for the outcomes of potential cyber attack in the next 12 months (% Ranked top three)

	Global (3,876)	Africa (168)	South Africa (68)
Loss of customer, employee or transaction data	52%	53%	44%
Damage to company brand (including loss of customer confidence)	50%	58%	53%
Loss of revenue (e.g., lost contracts, lost business opportunities)	48%	54%	47%
Operations downtime	34%	31%	24%
Damage to product / service quality	33%	23%	32%
Loss of intellectual property	26%	23%	24%
Criminal or civil liabilities	20%	17%	22%
Injury or death (to customers, employees)	16%	12%	15%
Unsure	1%	1%	1%

Key: 1st 2nd 3nd

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 4: Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation.

Both global and local respondents estimated that the cost of data breach is between US$1m – US$9m and, interestingly, 33% of South African and African organisations indicated that they had not been breached in the past three years compared to 15% globally.

Estimated costs to the organisation's most damaging data breach in the past three years

	Global (1,659)	Africa (49)*	South Africa (15)**
Less than US$10,000	5%	10%	7%
US$10,000 – US$49,000	6%	12%	13%
US$50,000 – US$99,000	8%	10%	13%
US$100,000 – US$499,000	15%	4%	7%
US$500,000 – US$999,000	11%	0%	0%
US$1 million – US$9 million	23%	14%	27%
US$10 million – US$19 million	9%	2%	0%
US$20 million or more	4%	0%	0%
No data breaches have occurred in the past 3 years	15%	33%	33%
Unsure	3%	14%	0%

**Base too low to report

Global = 1,659; Africa = 49; South Africa = 15

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 5: Which of the following does your organisation use to assess and report on your cybersecurity capabilities?

Top practices used to assess and report on cybersecurity risks

	Global (1,517)	Africa (40)*	South Africa (9)**
ISO 27001	43%	45%	22%
NIST cybersecurity framework	41%	55%	67%
Cloud Security Alliance Controls Matrix	39%	35%	33%
Cyber Resilience Review	32%	25%	22%
Financial Services Sector Coordinating Council (FSSCC) cybersecurity profile	31%	25%	44%
CIS CSC	28%	15%	11%
ISF standard of good practice	24%	20%	44%
SANS critical controls	21%	13%	33%
ISA/EAC 62443	19%	8%	0%
COBIT	18%	30%	22%
Sector or industry-specific framework	3%	3%	0%
Don't use any of these frameworks	2%	10%	11%
Other	2%	3%	0%

**Base too low to report

Global = 1,517; Africa = 40; South Africa = 9

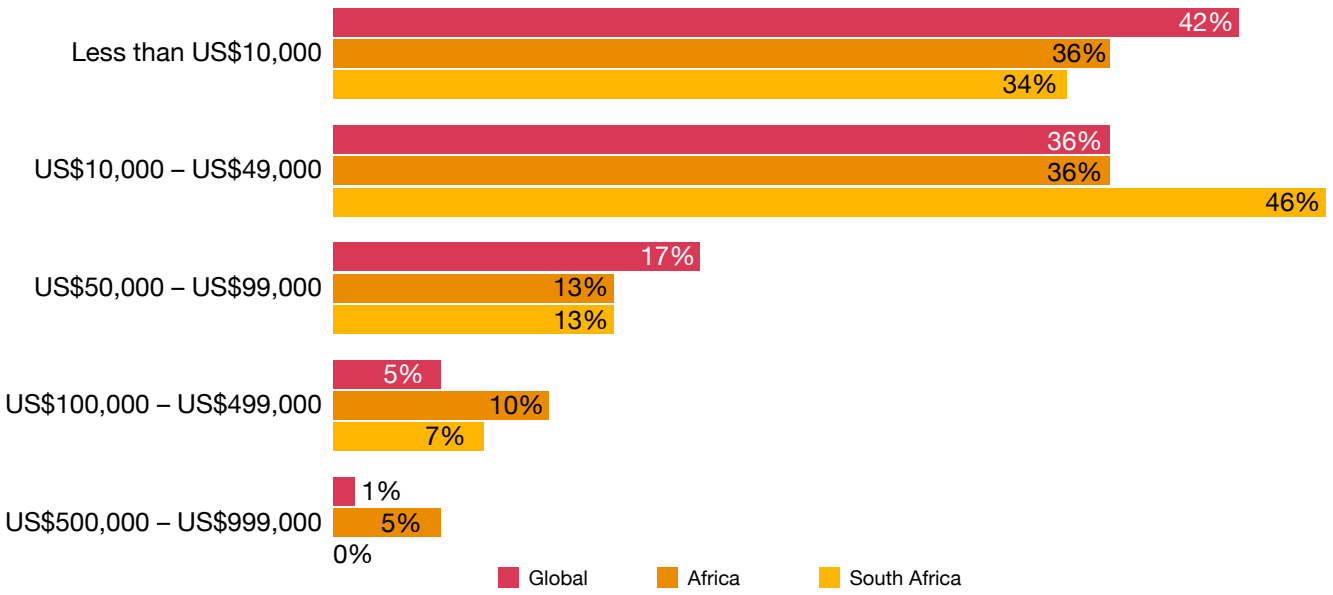
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 1: Which of the following best describes your organisation's use of cloud?

The statistics indicate that the majority of organisations in South Africa that responded are using private clouds to host their infrastructure, indicating that there is a rapid move from on premise and hybrid to the cloud.

Organisation's use of cloud computing

	Global (3,876)	Africa (168)	South Africa (68)
We use a hybrid of public and private cloud provider(s)	42%	36%	34%
We primarily use private cloud provider(s)	36%	36%	46%
We primarily use public cloud provider(s)	17%	13%	13%
We don't use cloud – we keep our data on-premise	5%	10%	7%
Unsure	1%	5%	0%



Q 2: To what extent has your organisation addressed the following challenges with your cloud service provider(s)?

Globally and locally, the majority of the organisations that responded are not addressing their cybersecurity challenges with their cloud service providers. In some instances such as third party risks, only 16% of South African organisations have addressed this significant risk with their cloud service providers.

Those who selected 'Implemented a plan and continually updated'

	Global (3,648)	Africa (143)	South Africa (63)
Disaster recovery and back-up	38%	48%	49%
Discovery / records management	34%	36%	43%
Third-party risk	33%	38%	48%
Data mapping / data use issues	33%	34%	44%
Shared responsibility with the cloud service provider	32%	26%	24%
Contract negotiation with cloud service provider	32%	38%	41%
Concentration risk	28%	21%	32%
Fragmented regulations	27%	18%	21%
Inability to grow in-house talent in cloud disciplines	26%	25%	30%

Global = 3,648; Africa = 143; South Africa = 63

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 3: To what extent has your organisation addressed the following challenges with your cloud service provider(s)?

Africa is more concerned about fragmented regulations, whereas its global counterparts are more concerned about sharing resources with other organisations with the same cloud service provider.

Those who selected 'Implemented a risk management plan'

	Global (3,648)	Africa (143)	South Africa (63)
Shared responsibility with the cloud service provider	33%	25%	30%
Contract negotiation with cloud service provider	32%	25%	32%
Fragmented regulations	31%	29%	35%
Concentration risk	31%	27%	29%
Third-party risk	31%	22%	25%
Inability to grow in-house talent in cloud disciplines	31%	20%	25%
Disaster recovery and back-up	30%	22%	22%
Discovery / records management	30%	22%	24%
Data mapping / data use issues	30%	22%	21%

Global = 3,648; Africa = 143; South Africa = 63

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 4: To what extent has your organisation addressed the following challenges with your cloud service provider(s)?

Africa is more concerned about fragmented regulations, whereas its global counterparts are more concerned about sharing resources with other organisations with the same cloud service provider.

Those who selected 'Creating a risk mitigation plan'

	Global (3,648)	Africa (143)	South Africa (63)
Inability to grow in-house talent in cloud disciplines	18%	20%	16%
Data mapping / data use issues	18%	13%	10%
Concentration risk	18%	15%	11%
Fragmented regulations	17%	15%	10%
Contract negotiation with cloud service provider	17%	9%	5%
Discovery / records management	17%	15%	13%
Shared responsibility with the cloud service provider	17%	19%	17%
Third-party risk	16%	10%	2%
Disaster recovery and back-up	16%	10%	13%

Global = 3,648; Africa = 143; South Africa = 63

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 5: To what extent has your organisation addressed the following challenges with your cloud service provider(s)?

Those who selected 'Monitoring and assessing risks'

	Global (3,648)	Africa (143)	South Africa (63)
Third-party risk	14%	17%	16%
Concentration risk	13%	22%	14%
Fragmented regulations	13%	18%	16%
Discovery / records management	13%	18%	16%
Inability to grow in-house talent in cloud disciplines	12%	15%	10%
Data mapping / data use issues	12%	22%	19%
Shared responsibility with the cloud service provider	12%	19%	17%
Contract negotiation with cloud service provider	11%	14%	8%
Disaster recovery and back-up	11%	11%	10%

Global = 3,648; Africa = 143; South Africa = 63

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 6: To what extent has your organisation addressed the following challenges with your cloud service provider(s)?

Those who selected 'Not at all'

	Global (3,648)	Africa (143)	South Africa (63)
Inability to grow in-house talent in cloud disciplines	7%	11%	11%
Fragmented regulations	6%	9%	10%
Concentration risk	5%	5%	8%
Data mapping / data use issues	4%	2%	3%
Contract negotiation with cloud service provider	3%	6%	8%
Shared responsibility with the cloud service provider	3%	5%	6%
Third-party risk	3%	4%	6%
Discovery / records management	3%	2%	3%
Disaster recovery and back-up	2%	2%	3%

Global = 3,648; Africa = 143; South Africa = 63

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 7: Which of the following best describes your organisation's current approach to cybersecurity technology?

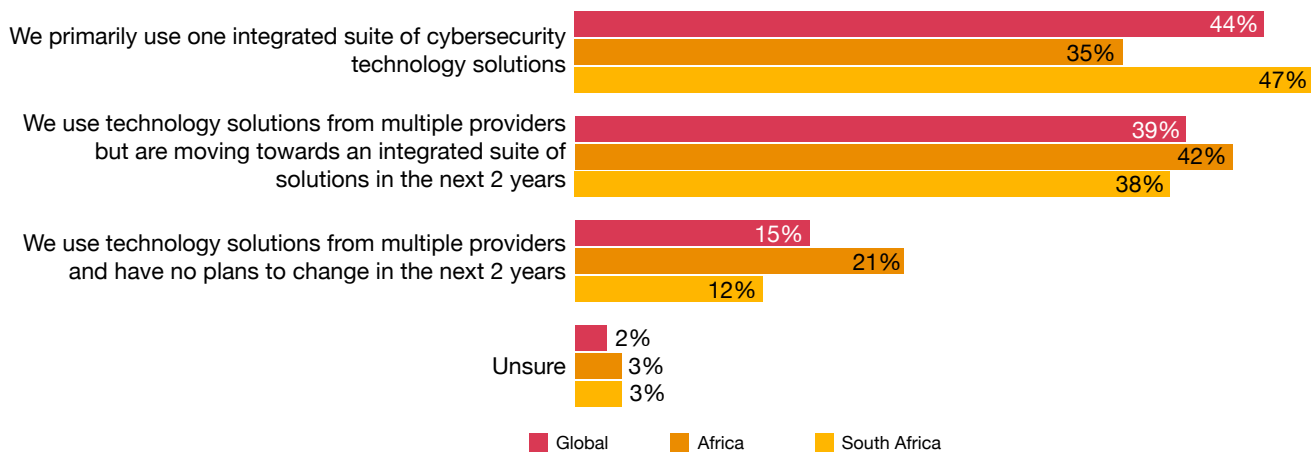
The statistics indicate that both globally and locally, organisations are moving towards using one integrated solution suite of cybersecurity technologies or are planning to move towards using an integrated suite of solutions within the next 2 years.

Approaches to cybersecurity technology

	Global (3,876)	Africa (168)	South Africa (68)
We primarily use one integrated suite of cybersecurity technology solutions	44%	35%	47%
We use technology solutions from multiple providers but are moving towards an integrated suite of solutions in the next 2 years	39%	42%	38%
We use technology solutions from multiple providers and have no plans to change in the next 2 years	15%	21%	12%
Unsure	2%	3%	3%

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.



Q 1: How is your organisation's cyber budget changing in 2024?

The statistics below show that globally and locally there has been only an increase of between 6 to 10% or less in an organisation's cybersecurity budget. A small budget increase may not provide enough resources to address emerging threats, maintain and update security systems or hire skilled cybersecurity professionals. (*Q13)

Changes to cybersecurity budgets in 2024

	Global (3,876)	Africa (168)	South Africa (68)
Increase by 15% or more	10%	13%	9%
Increase by 11–14%	15%	4%	4%
Increase by 6–10%	31%	27%	29%
Increase by 5% or less	24%	23%	28%
Unchanged	9%	10%	12%
Decrease by 5% or less	2%	1%	1%
Decrease by 6–10%	2%	2%	0%
Decrease by 11–14%	1%	2%	1%
Decrease by 15% or more	0%	1%	1%
Cannot determine at this time (e.g., due to economic and business uncertainty)	3%	11%	9%
I don't know any detail on the cyber budget	2%	6%	4%

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 2: Which of the following investments are you prioritising when allocating your organisation's cybersecurity budget in the next 12 months?

The statistics indicate that the majority of organisations in South Africa are prioritising their investments on application security, while most organisations in Africa are prioritising network security. Globally, organisations are prioritising cloud security.

Asked to Tech roles (% Ranked top three)

	Global (1,919)	Africa (55)	South Africa (14)**
Cloud security	33%	35%	36%
Application security	31%	33%	50%
IoT security	29%	9%	29%
Network security	28%	47%	36%
OT security	25%	7%	7%
Managed security services (e.g., managed security services, managed detection and response services)	25%	24%	21%
API security	25%	27%	21%
Security operations	22%	22%	29%
Identity and access management	21%	18%	21%
Security awareness training and cross training security operations	19%	29%	29%
Endpoint security	19%	27%	14%
Mobile security	12%	11%	7%
Unsure	1%	0%	0%

Key: 1st 2nd 3nd

**Base too low to report

Global = 1,919; Africa = 55; South Africa = 14

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 3: Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months?

Globally and locally the statistics show that organisations invest into the modernisation of technology, including cybersecurity infrastructure because by investing in modern technology it allows organisations to adopt the latest security measures and tools to address new and emerging threats. Investing in modern solutions can provide stronger defence against cybersecurity threats, reducing risk of breaches and data loss.

Asked to Business roles (% Ranked top three)

	Global (1,925)	Africa (111)	South Africa (54)
Modernisation of technology, including cyber infrastructure	49%	52%	48%
Optimisation of current technology and investments	45%	41%	44%
Ongoing improvements in risk posture based on cyber roadmap	42%	44%	43%
Ongoing security training	40%	33%	39%
Compliance with regulations or directives	31%	26%	24%
Remediation in the aftermath of recent cyber breaches or intrusions to organisation or industry	29%	20%	15%
New business initiatives	27%	37%	37%
Business priority shifts	19%	23%	22%
Unsure	1%	4%	4%

Key: 1st 2nd 3nd

Global = 1,925; Africa = 111; South Africa = 54

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 4: Which of the following statements do you agree with most?

The statistics indicate that the majority of organisations in South Africa and Africa responded that they do not have adequate security technology solutions, while globally most organisations responded that they have the right amount of cybersecurity technology solutions.

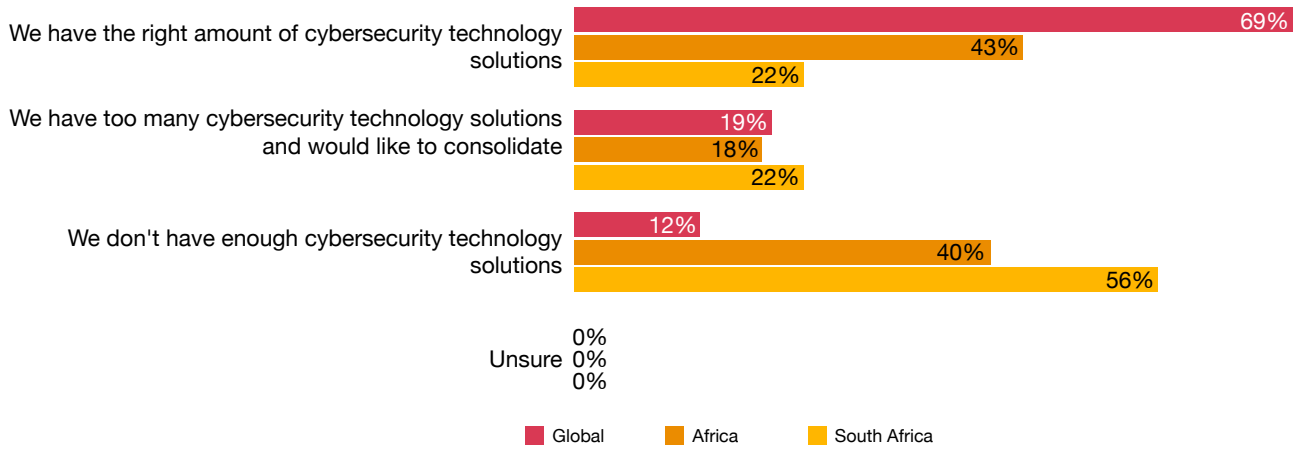
Cybersecurity technology solution sentiment

	Global (1,517)	Africa (40)*	South Africa (9)**
We have the right amount of cybersecurity technology solutions	69%	43%	22%
We have too many cybersecurity technology solutions and would like to consolidate	19%	18%	22%
We don't have enough cybersecurity technology solutions	12%	40%	56%
Unsure	0%	0%	0%

**Base too low to report

Global = 1,517; Africa = 40; South Africa = 9

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.



Q 5: How satisfied are you with your organisation's technology capabilities in the following areas?

Globally and in Africa organisations are satisfied with their networking/firewall and vpn technologies, whereas in South Africa organisations are satisfied with their cloud security because many cloud security providers offer managed security services or partner with third party security providers, which offloads some of the security management tasks.

Organisation's technology capabilities in key cybersecurity areas (% Very satisfied)

	Global (1,517)	Africa (40)*	South Africa (9)**
Networking / Firewall / VPN technologies	56%	65%	56%
Cloud security	53%	40%	67%
Security management and governance	52%	43%	44%
Endpoint detection and response	52%	63%	89%
Data security and privacy	52%	38%	44%
Identity and access management	50%	55%	56%
Supply chain security	43%	33%	44%
Security orchestration, automation, and response (SOAR)	42%	33%	56%
Industrial internet of things and control systems	41%	25%	67%

**Base too low to report

Global = 1,517; Africa = 40; South Africa = 9

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 6: Which of the following is your organisation prioritising in its cyber talent strategy over the next 12 months?

Globally and locally, organisations are prioritising upskilling current workforce fast enough to keep up with demands of our organisation.

Priorities in organisation's cyber talent strategy over the next 12 months (% Ranked top three)

	Global (3,876)	Africa (168)	South Africa (68)
Upskilling our current workforce fast enough to keep up with demands of our organisation	69%	79%	76%
Rebalancing between in-house and outsourced or managed services	55%	45%	53%
Identifying the right candidates for openings	52%	54%	51%
Retaining key talent	50%	49%	46%
Competing for the best talent in the market	46%	36%	38%
Other	0%	1%	0%
Unsure	1%	2%	0%

Key: 1st 2nd 3nd

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 1: To what extent is your organisation implementing or planning to implement the following cyber resilience actions?

The statistics show that organisations that have implemented a cybersecurity framework are prioritising identifying critical business processes as a cyber resilience action, while organisations that are in the process of implementing a cybersecurity framework are prioritising implementing cyber recovery technology solutions and integrating fully with the organisation's resilience strategy and activities.

Those who selected 'Optimised and continuous improvement'

	Global (3,876)	Africa (168)	South Africa (68)
Identifying critical business processes	29%	27%	25%
Implementing cyber recovery technology solutions (including immutable backups / isolated recovery environment)	28%	17%	22%
Developing cyber recovery playbook for IT-loss scenarios	27%	22%	25%
Establishing protocols with major technology providers (cloud, device m anufacturers, managed services) to coordinate incident responses	25%	17%	22%
Reporting to external stakeholders (regulators, investors)	25%	22%	25%
Establishing a resilience team with members from functions like Business Continuity, Cyber, Crisis Management and Risk Management	25%	20%	24%
Mapping technology dependencies	24%	17%	22%
Sharing information with industry peers, through formal processes, to prevent systemic risks	24%	22%	29%
Establishing relationships with local law enforcement to help with analysis and response	23%	17%	16%

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 2: What are your organisation's top priorities in the next 12 months as your organisation shifts to a zero-trust concept?

Globally organisations are most concerned about identity and access management, whereas in Africa and locally organisations are more concerned about software defined access.

Organisation's top concerns for the outcomes of potential cyber attack in the next 12 months (% Ranked top three)

	Global (1,434)	Africa (37)*	South Africa (8)**
Identity and Access Management	45%	49%	38%
Secure endpoints	44%	41%	50%
Software-defined perimeter and networking	42%	19%	38%
Secure cloud networking	42%		13%
Software-defined access	40%	51%	63%
Segmentation	38%	38%	25%
Establish governance and management	37%	59%	50%
None of the above	0%	3%	0%
Unsure	0%	0%	0%

Key: 1st 2nd 3nd

**Base too low to report

Global = 1,434; Africa = 37; South Africa = 8

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 1: Which of the following proposed regulatory goals and principles will have the greatest impact on your organisation's ability to secure future revenue growth?

South Africa is as concerned as its global counterparts to regulate artificial intelligence, whereas Africa is more concerned about reporting about cyber risk management.

Regulatory goals and principles greatest impact to organisation's future revenue growth (% Ranked top three)

	Global (3,876)	Africa (168)	South Africa (68)
Regulation of artificial intelligence	37%	33%	37%
Harmonised cyber and data protection laws in the region(s) where we operate	36%	39%	37%
Mandatory reporting of cyber risk management, strategy, and governance	35%	44%	31%
Harmonised privacy rights and / or protection in region(s) where we operate	32%	25%	18%
Regulatory requirements for operational resilience	32%	29%	29%
Mandatory reporting of incidents in financial reporting and disclosures	26%	30%	32%
Shifting the liability for cyber failures to specific companies (device makers, software companies)	25%	20%	21%
Regulation of cryptocurrency and other digital payments	19%	20%	25%
Making specific senior executives liable for negligence	18%	13%	19%
Mandatory reporting to law enforcement	18%	15%	15%
Other	0%	0%	0%
Unsure	2%	4%	3%

Key: 1st 2nd 3nd

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q 1: To what extent does your organisation understand the cyber risks related to the following technologies?

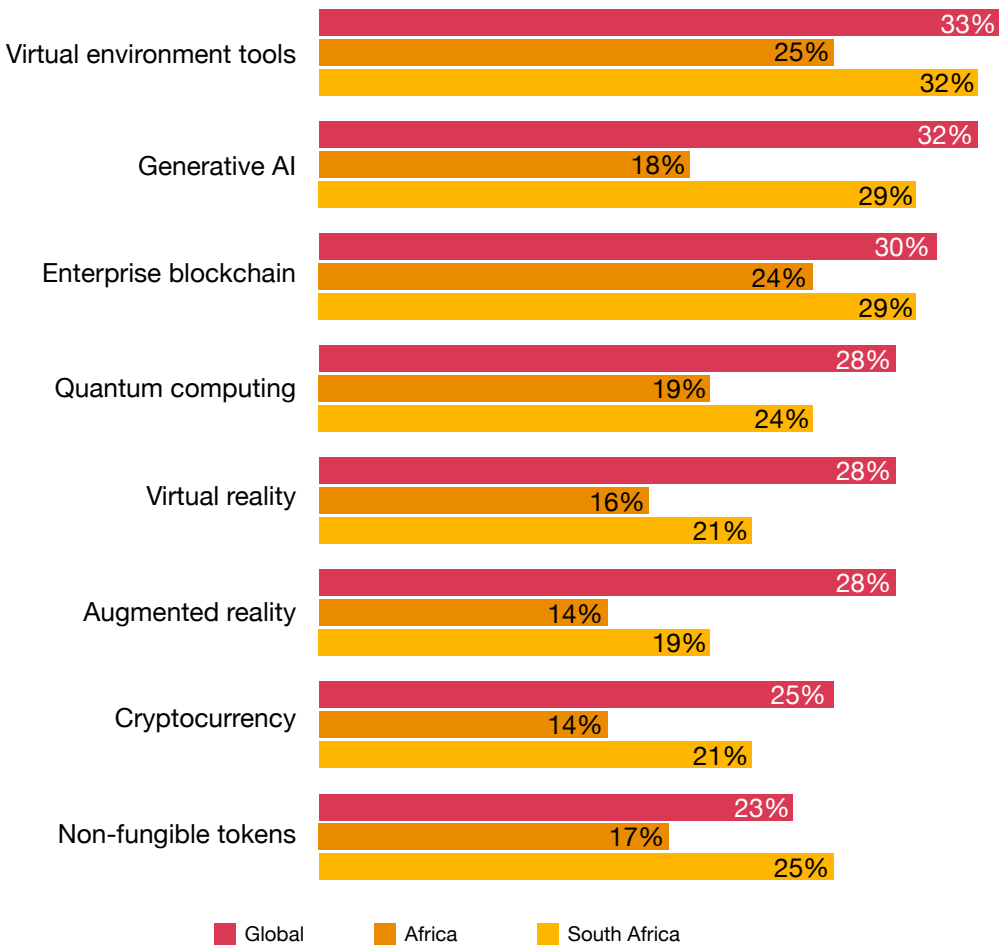
South Africa is as concerned as its global counterparts about virtual environment tools and the risks associated with them.

Those who selected 'Included in a plan and continually updated'

	Global (3,876)	Africa (168)	South Africa (68)
Virtual environment tools	33%	25%	32%
Generative AI	32%	18%	29%
Enterprise blockchain	30%	24%	29%
Quantum computing	28%	19%	24%
Virtual reality	28%	16%	21%
Augmented reality	28%	14%	19%
Cryptocurrency	25%	14%	21%
Non-fungible tokens	23%	17%	25%

Global = 3,876; Africa = 168; South Africa = 68

Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.



Contacts

Hamil Bhoora
Partner PwC Africa's Cybersecurity Competency Leader, PwC South Africa

Tel: +27 (0) 11 797 4102
hamil.bhoora@pwc.com

Wandile Mcanyana
Partner PwC South Africa

Tel: +27 (0) 11 797 4569
wandile.mcanyana@pwc.com