Global Digital Trust Insights Survey 2025:

South Africa and Africa Report

pwc

About the survey

The Global Digital Trust Insights Survey, now in its 27th year, is the longest-running annual survey on cybersecurity trends. It's also the largest global survey in the cybersecurity industry and the only one that draws participation from senior business executives, not just security and technology executives.

This survey assesses 4,042 business and technology leaders across 77 territories and was conducted in May through July 2024. Of the 4,042 businesses surveyed, a total of 312 (8%) organisations were surveyed on the African continent, with 94 (2%) of these businesses based in South Africa. The regional breakdown includes Western Europe (30%), North America (25%), Asia Pacific (18%), Latin America (12%), Central and Eastern Europe (6%), Africa (5%) and Middle East (3%).

Our study is a comprehensive analysis that explores the state of cybersecurity and digital trust across organisations worldwide. A quarter of leaders are from large companies with $5bn (R87,667,500,000) or more in revenues. Respondents operate in a range of industries, including industrials and services (21%), tech, media, telecom (20%), financial services (19%), retail and consumer markets (17%), energy, utilities, and resources (11%), health (7%) and government and public services (4%).

Introduction

The Global Digital Trust Insights Survey 2025 highlights several pressing concerns for organisations in South Africa and across Africa. One of the primary concerns is the mitigation of cyber risks. Organisations are increasingly aware of the potential threats to their digital infrastructure and are prioritising efforts to safeguard their systems and data. This heightened focus on cybersecurity reflects the growing recognition of the importance of protecting against cyberattacks and ensuring the resilience of their operations

Another significant concern is the threat posed by hack-and-leak operations. These incidents, where sensitive information is stolen and publicly disclosed, pose a severe risk to the reputation and operational integrity of organisations. The survey indicates that African organisations are particularly vigilant about these threats, emphasising the need for robust data protection measures and incident response strategies.

Data breaches remain a critical issue, with many organisations reporting significant impacts from such incidents. The financial and reputational damage caused by data breaches underscores the necessity for comprehensive security protocols and continuous monitoring to detect and respond to breaches promptly. The survey reveals that while some organisations have managed to avoid breaches, the threat remains ever-present, necessitating ongoing vigilance and investment in cybersecurity.

Key insights from South Africa:

Cyber risk mitigation:

66%

of South African organisations prioritise mitigating cyber risks, surpassing the global average of 57%. This reflects heightened vigilance and a proactive approach to addressing the increasing threat landscape, ensuring robust cybersecurity measures, and protecting against potential cyber threats.

Cloud-related threats:

47%

of South African organisations are most concerned about cloud-related threats over the next 12 months. This highlights the critical need for enhanced cloud security measures to protect sensitive data and ensure business continuity in an increasingly digital landscape.

Data breach costs: The most damaging data breaches in the past three years have cost South African organisations between $100,000 (R1,759,000) and $499,999 (R8,794,982.41). These significant financial impacts underscore the importance of robust cybersecurity measures to prevent data breaches.

Cyber budget increase:

29%

of South African organisations expect a six to ten percent increase in their cyber budget for 2025. This planned increase reflects a commitment to strengthening cybersecurity defences and addressing the evolving threat landscape.

Generative AI (genAI) challenges:

47%

of South African organisations face significant challenges with internal stakeholder trust in genAI. This indicates a need for better communication, education and trust-building measures to effectively integrate genAI technologies.

Regulatory compliance confidence:

34%

of South African organisations are extremely confident in their compliance with data protection regulations. This high level of confidence reflects strong regulatory adherence and robust data protection practices within these organisations.

Cybersecurity as a competitive advantage:

68%

of South African organisations view cybersecurity as a significant competitive advantage for business growth opportunities and staying ahead of business disruption. This perspective highlights the strategic importance of cybersecurity in achieving business objectives.

Cyber risk quantification:

45%

of South African organisations measure the potential financial impact of cyber risks to a large extent. This practice helps organisations prioritise cyber investments, allocate resources effectively and communicate the value of their cybersecurity programmes.

Key insights from Africa:

Cyber risk mitigation:

61%

of African organisations are prioritising the mitigation of cyber risks over the next 12 months, highlighting the growing awareness and proactive stance towards cybersecurity threats in the region.

Hack-and-leak concerns:

African organisations are more concerned about hack-and-leak operations than cloud-related threats, indicating a focus on protecting sensitive information from being exposed through malicious breaches.

Data breach costs:

21%

of African organisations report that they have not experienced any data breaches in the past three years, suggesting effective cybersecurity measures or possibly underreporting of incidents.

Cyber budget increase:

31%

of African organisations expect their cyber budget to increase by six to ten percent in 2025, reflecting a commitment to enhancing their cybersecurity infrastructure and capabilities.

GenAI challenges:

African organisations face significant challenges with genAI, particularly due to a lack of training resources for employees, which hampers effective implementation and utilisation of this technology.

Regulatory compliance confidence:

23%

of African organisations are extremely confident in their ability to comply with data protection regulations, indicating a strong focus on regulatory adherence and data security.

Cybersecurity as a competitive advantage:

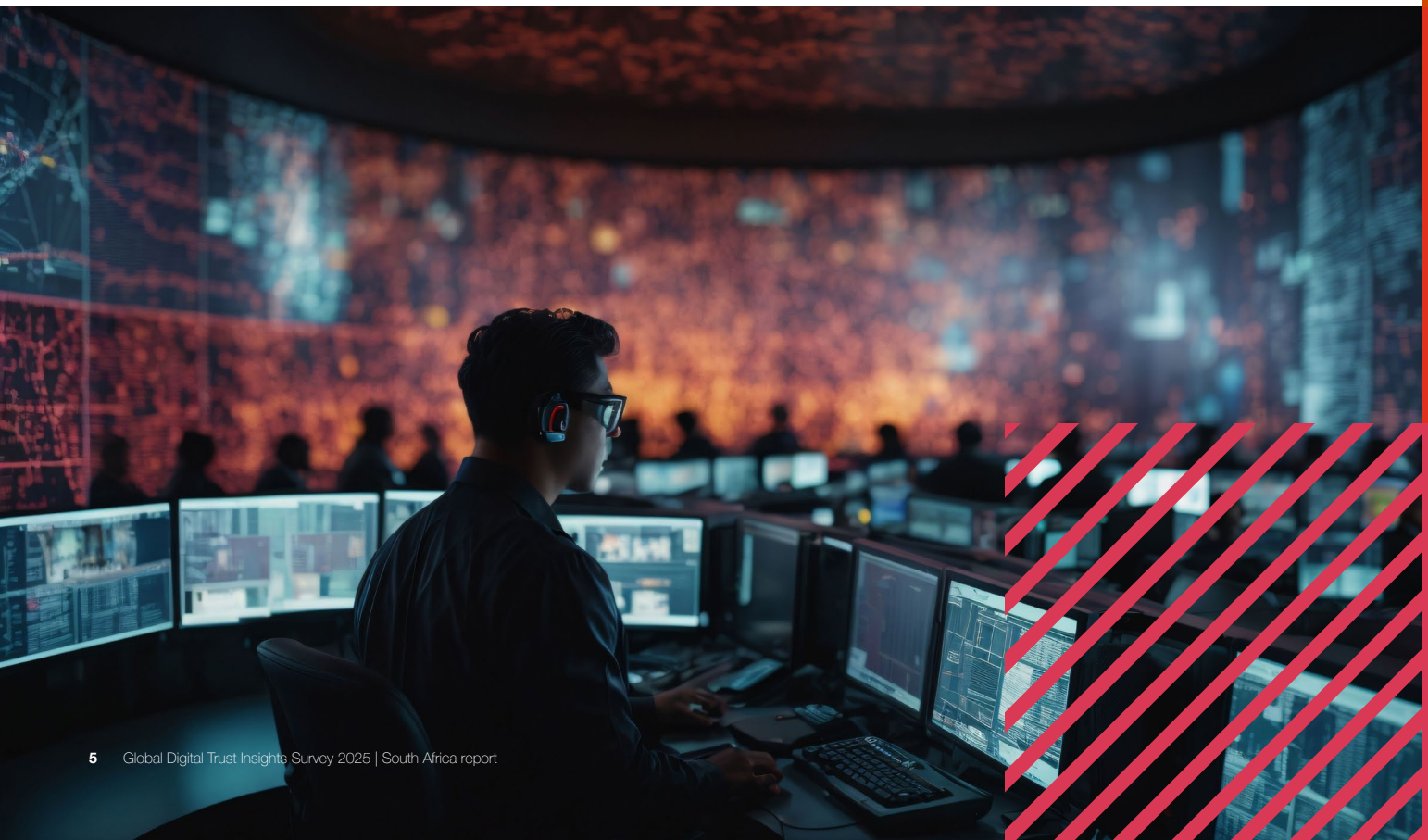
68%

of African organisations view cybersecurity as a critical factor in building customer trust and maintaining brand integrity, underscoring its importance in competitive positioning.

Cyber risk quantification:

38%

of African organisations measure the potential financial impact of cyber risks to a large extent, demonstrating a sophisticated approach to understanding and managing cyber threats.



Research overview

The 2025 Digital Trust Insights Survey has been designed to capture the views of business and tech leaders around the world on the challenges and opportunities to improve and transform cybersecurity in their organisation over the next 12 months—covering topics such as threat outlook, investments, emerging tech, regulation and more.

Final results are based on 4,042 survey responses across 77 territories across a range of industries, sub-industries and organisation sizes.

Eighty-nine percent of responses (3,585) are via an external panel provider and 11% (457) are from PwC's territory network outreach, with responses gathered from 7 May to 12 July 2024.

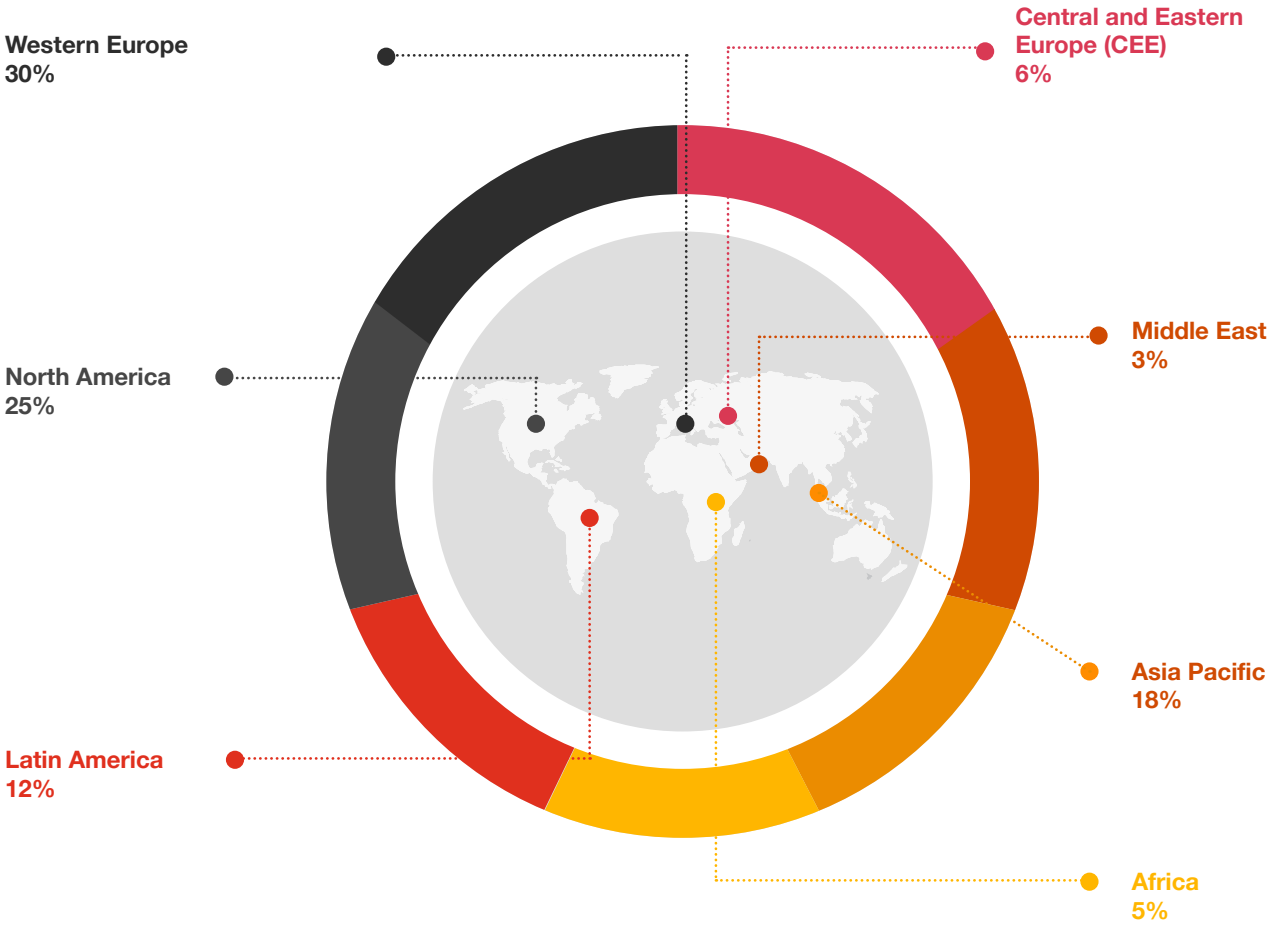
4,042
Respondents

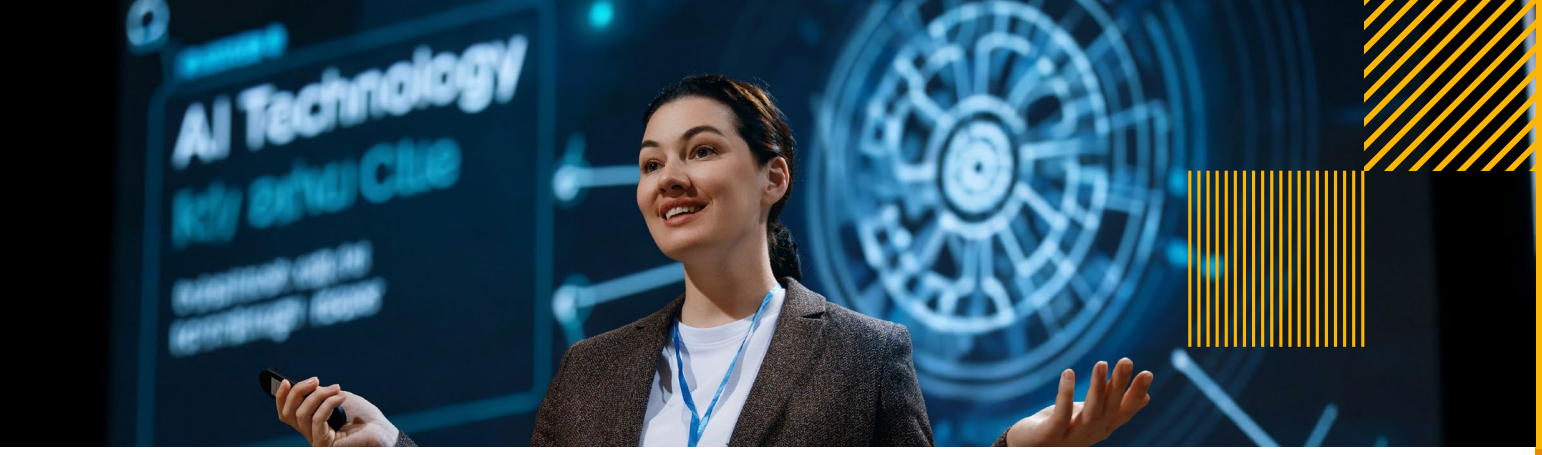
19
Surveyed in different languages

Between 7th May – 12th July 2024

77
Across territories

30+
Territories can report on survey findings





Survey summary analysis

Threat outlook and emerging risks

- Global, African (4% more so than global) and South African (5% more so than Africa) organisations appear to have prioritised the mitigation of cyber risks.
- Global and South African (5% more so than global) organisations appear to be more concerned about cloud-related threats over the next 12 months, while Africa appears to be more concerned about hack-and-leak operations.
- Global (1% more so than Africa), African and South African (1% more so than global) organisations appear to be least prepared for cloud-related threats, with Africa appearing to place quantum computing at the same percentage.
- Global and South African (4% more so than global) organisations appear to estimate that their most damaging data breach cost in the past three years is between $100,000 – $499,999 (around R1,740,000 – R8,700,000), while Africa appears to estimate that no data breaches have occurred in the past three years.

Cyber investment and priorities

- Global (1% more so than South Africa), African (1% more so than global) and South African organisations appear to estimate an increase of six to ten percent to the cyber budget for 2025.
- Global, African (13% more so than global) and South African (12% more so than Africa) organisations appear to prioritise data protection/data trust when allocating their cyber budget in the next 12 months for business leaders.
- Global (2% more so than South Africa) and South African organisations appear to prioritise cloud security when allocating their cyber budget in the next 12 months for tech leaders, while Africa appears to prioritise data protection/data trust.
- Global organisations' premiums appear to have increased significantly due to the changes in the cyber liability insurance market in the last 12 months, while there are no percentages for Africa and South Africa.

Emerging technologies and genAI

- African and South African (3% more so than Africa) organisations appear to have significantly increased their cyber attack surface in their IT environments due to Software as a Service (SaaS) with South Africa appearing to place blockchain at the same percentage, while global appears to be significantly affected by genAI.
- African (6% more so than South Africa) and South African organisations appear to have slightly increased their cyber attack surface in their IT environments due to genAI, while global appears to be slightly affected by cloud technology.
- Global, African and South African (4% more so than global and Africa) organisations appear to have not affected their cyber attack surface in their IT environments in regards to quantum computing.
- African and South African (8% more so than Africa) organisations appear to have significantly increased their cyber investment for machine learning, while global appears to have increased their cyber investment for genAI.
- African and South African (6% more so than Africa) organisations appear to have slightly increased their cyber investment for genAI, while global appears to have increased their cyber investment for machine learning.
- African and South African (2% more so than Africa) organisations appear to have not changed their cyber investment for virtual reality (VR) with Africa placing blockchain at the same percentage, while global appears to have not changed their cyber investment for non-fungible tokens (NFTs).
- Global organisations appear to have prioritised the use of genAI to threat detection and response over the next 12 months, while Africa prioritises threat intelligence and South Africa prioritises Security Operations Centres (SOCs) modernisation.
- Global and South African (8% more so than global) organisations appear to be facing a challenge with the lack of trust in genAI by internal stakeholders over the next 12 months, with global appearing to place difficulty incorporating with existing systems/processes at the same percentages, while Africa appears to be facing a challenge of a lack of training resources for employees.
- Global, African (1% more so than global) and South African (4% more so than Africa) organisations' risk management investments appear to have significantly increased in regards to talent hiring and training due to genAI.
- Global and African (3% more so than global) organisations' risk management investments appear to have increased slightly in regards to artificial intelligence (AI) governance due to genAI, while global and Africa (12% more so than global) appears to have increased slightly in regards to model development, training and tuning.
- Global and South African (same percentage as global) organisations' risk management investments appear to have no change in regards to third-party services due to genAI with South Africa placing the same percentage on compliance and legal, while Africa has no change in regards to talent hiring and training.

Regulatory developments

- African and South African (11% more so than Africa) organisations appear to be extremely confident that they are in compliance with the data protection regulation, while global appears to be extremely confident in regards to the consumer privacy regulation.
- Global, African (2% more so than global) and South African (2% more so than Africa) organisations appear to be very confident that they are in compliance with the network and information security regulation.
- Global and South African (1% more so than global) organisations appear to be moderately confident that they are in compliance with the AI regulation, with global appearing to place resilience on the same percentage, while Africa appears to be moderately confident in regards to the cyber disclosure regulation.
- African (4% more so than South Africa) and South African organisations appear to be slightly confident that they are in compliance with the resilience regulation, while global appears to be slightly confident in regards to the AI regulation.
- Global, African (2% more so than global and South Africa) and South African organisations appear to not be confident that they are in compliance with the AI regulation, with global placing data protection on the same percentage and South Africa placing network and information security on the same percentage.
- Global (2% more so than Africa) and African organisations appear to view that cybersecurity regulations have moderately increased their cybersecurity investments over the last 12 months, while South Africa appears to view that regulations have increased their cybersecurity investment to a large extent.
- Global, African (10% more so than South Africa) and South African (8% more so than South Africa) organisations appear to agree that cybersecurity regulations challenged their organisation to strengthen current cyber risk management programmes, processes and governance approaches over the last 12 months.

Cyber strategy

- Global and African (7% more so than global) organisations appear to have prioritised the identification of critical business processes; however, South Africa appears to have prioritised the establishment of a resilience team over the identification of critical business processes.
- Global organisations appear to have prioritised the establishment of a resilience team and protocols with major providers for incident response coordination as well as technology dependency mapping in a portion of their organisation; however, African and South African (7% more so than African) organisations appear to have prioritised the implementation of cyber recovery solutions.
- Global and African (2% more so than global) organisations appear to agree that they should prioritise the deployment of quantum computing in the next two years when it comes to cyber defence and resilience; however, South Africa appears more concerned about technology dependency mapping.
- Global (6% more so than Africa), African (3% more so than South Africa) and South African organisations appear to agree that they are not planning on deploying quantum computing for cyber defence and resilience.
- Global organisations appear to use ISO 27001 to assess their cybersecurity capabilities, while African organisations appear to use the National Institute of Standards and Technology (NIST) cybersecurity framework and South African organisations appear to use the Cyber Risk Institute (CRI) profile.
- Global and African (11% more so than global) organisations appear to agree that cybersecurity plays a large role in customer trust; however, South Africa appears to view cybersecurity as a competitive advantage to business growth opportunities.
- Global organisations appear to agree that cybersecurity plays a moderate role in public relations, while African (2% more so than South Africa) and South African organisations appear to view cybersecurity playing a moderate role to brand integrity and loyalty with South Africa placing staying ahead of business disruption at the same percentage.
- Global, African and South African (1% less than global and Africa) organisations appear to agree that cybersecurity plays a limited role in market leadership.
- Global and African (1% more so than global) organisations appear to agree that cybersecurity plays no role in public relations with global organisations placing business growth opportunities and market leadership at the same percentage; however, South Africa appears to view cybersecurity playing no role in business growth opportunities.
- Global and African (7% more so than global) organisations appear to agree that they should prioritise for faster response times to incidents and disruptions; however, South Africa appears more concerned about the improvement of leader confidence in managing threats.

Cyber leadership

- Global organisations' CEO involvement in following cyber and privacy matters appears to be prioritised around the discussion on their implications of future corporate strategies, while African organisations appear to prioritise the discussion of key cyber metrics and South African organisations appear to prioritise the discussion of the implications of a major operating model change.
- Global and African (9% more so than global) organisations' involvement in following cyber and privacy matters appears to be prioritised around when regulators can contact them for cybersecurity-related actions, with global organisations placing discussions on their implications of future corporate strategies at the same percentage. There are no percentages for South African organisations.
- Global and South African (13% more so than global) organisations appear to have CISOs who take an active role, to a large extent, in strategic planning about cyber investment with South Africa placing the product development as well as sales and marketing at the same percentage, while African organisations appear to prioritise reporting and regular meetings with the board.
- Global (3% more so than global), African (1% more so than South Africa) and South African organisations appear to have CISOs who take an active role, to a moderate extent, in drafting and reviewing regulatory disclosures.
- Global (2% more than South Africa), African (3% more so than global) and South African organisations appear to have CISOs who take an active role, to a limited extent, in sales and marketing.
- Global (2% more so than South Africa), African (1% more so than global) and South African organisations appear to have CISOs who do not take an active role in sales and marketing.
- Global and African (9% more so than global) organisations appear to think that their board is very effective in regulatory responsibilities, while South Africa appears to think their board is very effective in cyber risk oversight.
- Global (4% more so than Africa), African (1% more so than South Africa) and South African organisations appear to think that their board is moderately effective in cyber expertise with global organisations placing the same percentage on fostering cyber innovation and growth.
- Global and African (2% more so than global) organisations appear to think that their board is slightly effective in cyber expertise with global organisations placing cyber training and expense at the same percentage, while South Africa appears to think their board is slightly effective in cyber strategy engagement.
- Global and African (2% more so than global) organisations appear to think that their board is not effective in cyber expertise with global organisations placing cyber training and education as well as fostering cyber innovation and growth at the same percentage, while South Africa appears to think their board is not effective in cyber training and education.

Cyber risk quantification

- Global, African (9% more so than global) and South African (7% more so than Africa) organisations appear to, at a large extent, measure the potential financial impact of cyber risks to their organisation with global organisations also appearing to, at a moderate extent, measure the potential financial impact at the same percentage.
- Global, African (4% more so than South Africa) and South African (9% more so than global) organisations appear to use security posture assessments for cyber risk quantification.
- Global and African (6% more so than global) organisations appear to be uncertain about the intended scope of risk quantification outputs when it comes to quantifying the potential financial impact of cyber risk, while South African (4% more so than Africa) and African organisations appear to face challenges with data issues when it comes to quantifying the potential financial impact.
- Global, African (7% more so than global) and South African (10% more so than Africa) organisations appear to place extreme importance on prioritising cyber investments in regards to quantifying cyber risk with global placing the same percentage on allocating resources to higher risk areas.
- Global, African (9% more so than South Africa) and South African (2% more so than global) organisations appear to place the evaluation and communication of cyber risk as very important with global placing the same percentage on supporting financial reporting or insurance negotiations and South Africa placing the same percentage on measuring and comparing threats and incidents.
- Global (2% more so than South Africa), African (2% more so than global) and South African organisations appear to place moderate importance on measuring the impact deals can have on the risk profile.
- Global (1% more so than both Africa and South Africa), African and South African organisations appear to place no importance on measuring the impact deals can have on the risk profile, with both Africa and South Africa placing the same percentage on the demonstration of the cyber risk management programme's value. Additionally, Africa places the same percentage on financial reporting or insurance negotiations support and South Africa places the same percentage on the evaluation and communication of cyber risks.

Behaviours

- Global (18% less than Africa and South Africa), African and South African organisations cybersecurity teams appear to focus most of their efforts on putting controls in place and responding to threats.
- Global, African (4% more so than global) and South African (6% more so than Africa) organisations cybersecurity teams appear to often focus their efforts on expediting digital and other major transformation initiatives, with Africa placing the same percentage on anticipation of future cyber risks and global placing the same percentage on anticipation of future cyber risks, collaborating with other parts of business, putting controls in place and responding quickly to threats.
- Global (5% more so than Africa) and African organisation cybersecurity teams appear to sometimes focus their efforts on expediting digital and other major transformation initiatives, while South Africa appears to sometimes focus their efforts on delivering insights on changing cyber risk exposure, regulatory developments and mitigation measures to the relevant parties.
- Global (1% more so than Africa) and African organisation cybersecurity teams appear to occasionally focus their efforts on allocating cyber budgets to the top risks with global placing the same percentage on expediting digital and other major transformation initiatives, delivering insights on changing cyber risk exposure, regulatory developments and mitigation measures to the relevant parties and collaborating with other parts of business. South Africa appears to occasionally focus their efforts on collaborating with other parts of business.
- Global (1% more so than Africa and South Africa), African and South African organisation cybersecurity teams appear to rarely focus their efforts on anticipating future cyber risks with global placing the same percentage on allocating cyber budgets to the top risks, collaborating with other parts of business, expediting digital and other major transformation initiatives, and delivering insights on changing cyber risk exposure, regulatory developments and mitigation measures to the relevant parties.

Threat outlook and emerging risks

Q1 Which of the following risks is your organisation prioritising for mitigation over the next 12 months?

Global, African (4% more so than global) and South African (5% more so than Africa) organisations appear to have prioritised the mitigation of cyber risks.

Risks that are being prioritised for mitigation in organisations over the next 12 months (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Cyber risks	57%	61%	66%
Digital and technology risks	53%	55%	53%
Inflation	48%	41%	47%
Environmental risks	30%	35%	33%
Macroeconomic volatility	30%	28%	18%
Geopolitical risks	25%	14%	16%
Societal risks	21%	15%	16%
Health risks	17%	21%	22%

Key: 1st 2nd 3rd

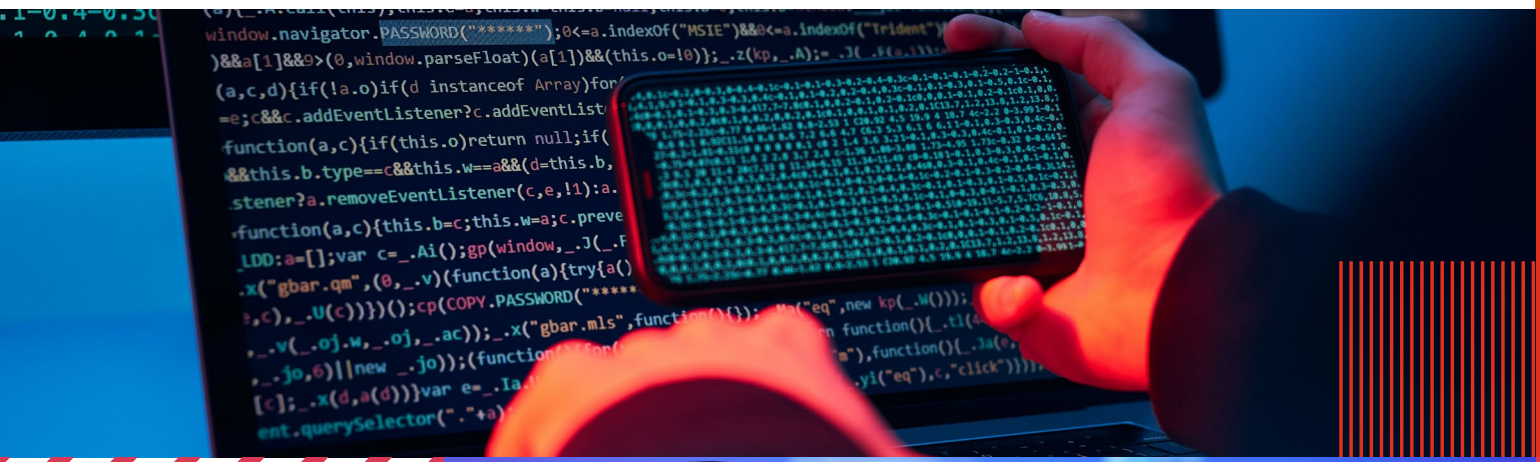
Q2 Over the next 12 months, which of the following cyber threats is your organisation most concerned about (e.g., risk to your brand, loss of business or business disruption or compliance)?

Global and South African (5% more so than global) organisations appear to be more concerned about cloud-related threats over the next 12 months, while Africa appears to be more concerned about hack-and-leak operations.

Cyber threats that organisations are most concerned about over the next 12 months (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Cloud-related threats	42%	36%	47%
Hack-and-leak operations	38%	38%	40%
Third-party breach (i.e., data breaches)	35%	37%	28%
Attacks on connected products	33%	36%	46%
Ransomware	27%	18%	16%
Business email compromise / account takeovers	24%	29%	26%
Social engineering (i.e., deep fakes, disinformation)	24%	29%	26%
Software supply-chain compromise	22%	22%	28%
Distributed denial-of-service attacks (DOS)	17%	15%	13%
Exploits of zero-day vulnerabilities	13%	11%	6%
Quantum computing	9%	4%	6%

Key: 1st 2nd 3rd



Q3 Over the next 12 months, which cyber threats do you think your organisation is least prepared to address?

Global (1% more so than Africa), African and South African (1% more so than global) organisations appear to be least prepared for cloud-related threats, with Africa appearing to place quantum computing at the same percentage.

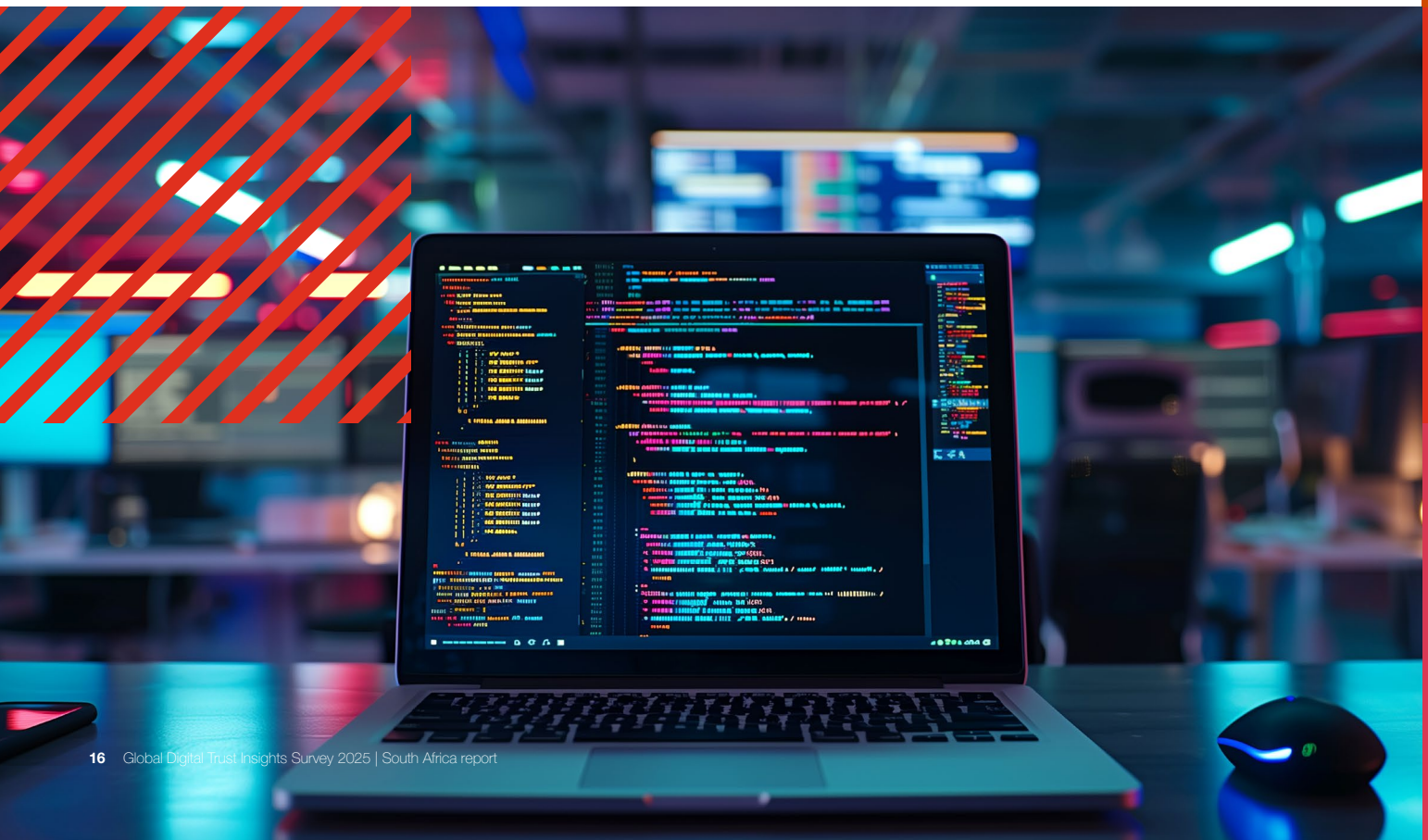
Cyber threats that organisations are least prepared to address over the next 12 months (% Ranked top three)

	Global (1,951)	Africa (84)	South Africa (37)*
Cloud-related threats	34%	33%	35%
Attacks on connected products	31%	26%	27%
Third-party breach (i.e., data breaches)	28%	25%	27%
Hack-and-leak operations	25%	31%	30%
Social engineering (i.e., deep fakes, disinformation)	25%	27%	30%
Ransomware	25%	21%	24%
Quantum computing	24%	33%	32%
Software supply-chain compromise	23%	17%	14%
Exploits of zero-day vulnerabilities	20%	20%	19%
Distributed denial-of-service attacks (DOS)	20%	14%	16%
Business email compromise / account takeovers	18%	18%	24%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Key: 1st 2nd 3rd

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q4 Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation.

Global and South African (4% more so than global) organisations appear to estimate that their most damaging data breach cost in the past three years is between $100,000 – $499,999 (around R1,740,000 – R8,700,000), while Africa appears to estimate that no data breaches have occurred in the past three years.

Estimation of the cost to the organisation due to a data breach in the last three (3) years (% Ranked top three)

	Global (1,951)	Africa (84)	South Africa (37)*
Less than US$10,000	6%	10%	3%
US$10,000 – US$49,999	9%	17%	19%
US$50,000 – US$99,999	12%	12%	14%
US$100,000 – US$499,999	18%	19%	22%
US$500,000 – US$999,999	11%	4%	5%
US$1 million – US$9.9 million	17%	6%	11%
US$10 million – US$19.9 million	7%	5%	8%
US$20 million or more	3%	1%	3%
No data breaches have occurred in the past three years	14%	21%	14%
Unsure	3%	6%	3%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Cyber investment and priorities

Q1 How will your organisation's cyber budget change in 2025?

Global (1% more so than South Africa), African (1% more so than global) and South African organisations appear to estimate an increase of six to ten percent to the cyber budget for 2025.

Estimation of how organisations will change their cyber budget for 2025 (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Increase by 15% or more	8%	11%	12%
Increase by 11%–14%	12%	10%	14%
Increase by 6–10%	30%	31%	29%
Increase by 5% or less	27%	23%	26%
Will not change	11%	5%	4%
Decrease by 5% or less	3%	2%	2%
Decrease by 6–10%	2%	3%	3%
Decrease by 11–14%	1%	0%	1%
Decrease by 15% or more	1%	1%	1%
Cannot determine at this time (e.g., due to economic and business uncertainty)	4%	10%	9%
I don't know any detail on the cyber budget	2%	3%	0%

Q2a Which of the following investments, if any, are you prioritising when allocating your organisation's cyber budget in the next 12 months?

Global, African (13% more so than global) and South African (12% more so than Africa) organisations appear to prioritise data protection/data trust when allocating their cyber budget in the next 12 months for business leaders.

Investments that are being prioritised when allocating the organisation's budget in the next 12 months for business leaders (% Ranked top three)

	Global (1,867)	Africa (117)	South Africa (41)*
Data protection / data trust	48%	61%	73%
Modernisation of technology, including cyber infrastructure	43%	50%	59%
Ongoing security training	34%	38%	27%
Optimisation of current technology and investments	34%	28%	20%
Ongoing improvements in risk posture based on cyber roadmap	30%	28%	34%
Compliance with regulations or directives	26%	25%	12%
New business initiatives	20%	20%	20%
Remediation in the aftermath of recent cyber breaches or intrusions to organisation or industry	20%	10%	10%
Business priority shifts	17%	16%	20%
Connected products	14%	9%	10%

Total = 3648; Africa = 143; South Africa = 63
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Key: 1st 2nd 3rd

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q2b Which of the following investments, if any, are you prioritising when allocating your organisation's cyber budget in the next 12 months?

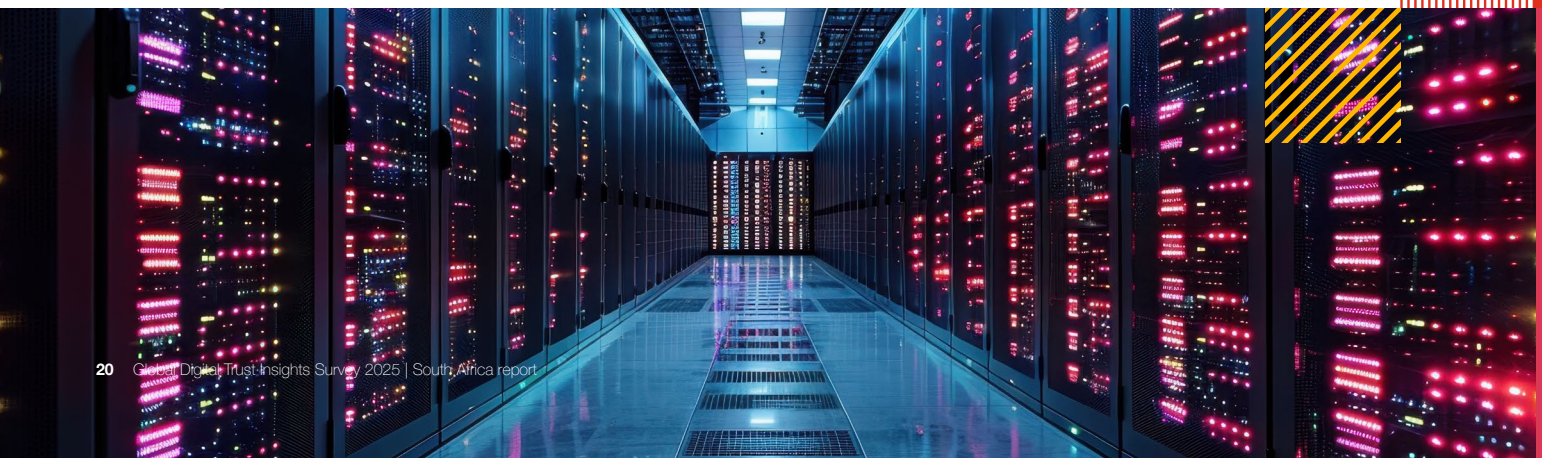
Global (2% more so than South Africa) and South African organisations appear to prioritise cloud security when allocating their cyber budget in the next 12 months for tech leaders, while Africa appears to prioritise data protection/data trust.

Investments that are being prioritised when allocating the organisation's budget in the next 12 months for tech leaders (% Ranked top three)

	Global (2,092)	Africa (95)	South Africa (53)
Cloud security	34%	27%	32%
Data protection / data trust	28%	36%	32%
Network security and continuity	27%	33%	28%
Generative AI / machine learning	26%	22%	26%
Operational technology (OT) security	23%	19%	26%
Cyber managed services	22%	24%	25%
Security awareness training	19%	18%	15%
Endpoint security	17%	16%	4%
Identity and access management	16%	19%	13%
Application security	16%	16%	9%
Cyber liability insurance	15%	19%	23%
Mobile security	14%	9%	11%
Connected products	13%	12%	15%
API security	12%	13%	13%
Quantum computing	9%	2%	4%

Total = 3648; Africa = 143; South Africa = 63
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Key: 1st 2nd 3rd



Q3 In the last 12 months, how have changes in the cyber liability insurance market affected your organisation, if at all?

Global organisations' premiums appear to have increased significantly due to the changes in the cyber liability insurance market in the last 12 months, while there are no percentages for Africa and South Africa.

Changes organisations are experiencing due to the changes in the cyber liability insurance market in the last 12 months (% Ranked top three)

	Global (355)	Africa (20)**	South Africa (12)**
Premiums have increased significantly	56%		
Terms and exclusions have become stricter (e.g., resulting in more limits on eligibility, claims, payout)	48%		
Cyber liability insurance is less available (i.e., more difficult to obtain coverage or renew existing coverage)	40%		
No significant changes/not applicable (e.g., in availability, premiums, terms and exclusions)	10%		
Unsure	3%		

Total = 3648; Africa = 143; South Africa = 63
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Emerging technologies and generative genAI

Q1 To what extent have the following technologies affected the cyber attack surface in your IT environment over the last 12 months?

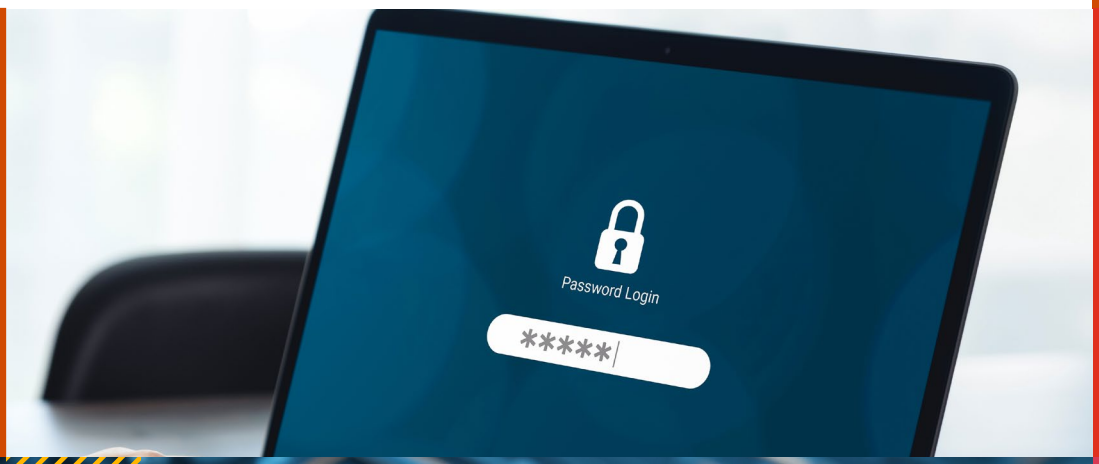
African and South African (3% more so than Africa) organisations appear to have significantly increased their cyber attack surface in their IT environments due to Software as a Service (SaaS) with South Africa appearing to place blockchain at the same percentage, while global appears to be significantly affected by genAI.

Technology that has affected organisations' cyber attack surface significantly in the last 12 months (% Ranked top three)

	Global (1,762)	Africa (75)	South Africa (37)*
Generative AI	31%	21%	22%
Cloud technology (either multi-cloud or single)	26%	23%	27%
Software as a Service (Saas)	22%	27%	30%
Connected products (e.g., internet of things (IoT), medical devices)	19%	20%	22%
Operational technology (OT)	19%	25%	24%
Blockchain (e.g., cryptocurrency)	17%	20%	30%
DevOps	16%	17%	22%
Quantum computing	15%	15%	22%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q2 To what extent have the following technologies affected the cyber attack surface in your IT environment over the last 12 months?

African (6% more so than South Africa) and South African organisations appear to have slightly increased their cyber attack surface in their IT environments due to genAI, while global appears to be slightly affected by cloud technology.

Technology that has slightly affected organisations' cyber attack surface in the last 12 months (% Ranked top three)

	Global (1,762)	Africa (75)	South Africa (37)*
Cloud technology (either multi-cloud or single)	40%	39%	32%
Connected products (e.g., internet of things (IoT), medical devices)	39%	29%	27%
Generative AI	37%	44%	38%
Software as a Service (Saas)	37%	32%	27%
Operational technology (OT)	36%	33%	30%
DevOps	32%	31%	27%
Quantum computing	27%	21%	19%
Blockchain (e.g., cryptocurrency)	26%	24%	24%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q3

To what extent have the following technologies affected the cyber attack surface in your IT environment over the last 12 months?

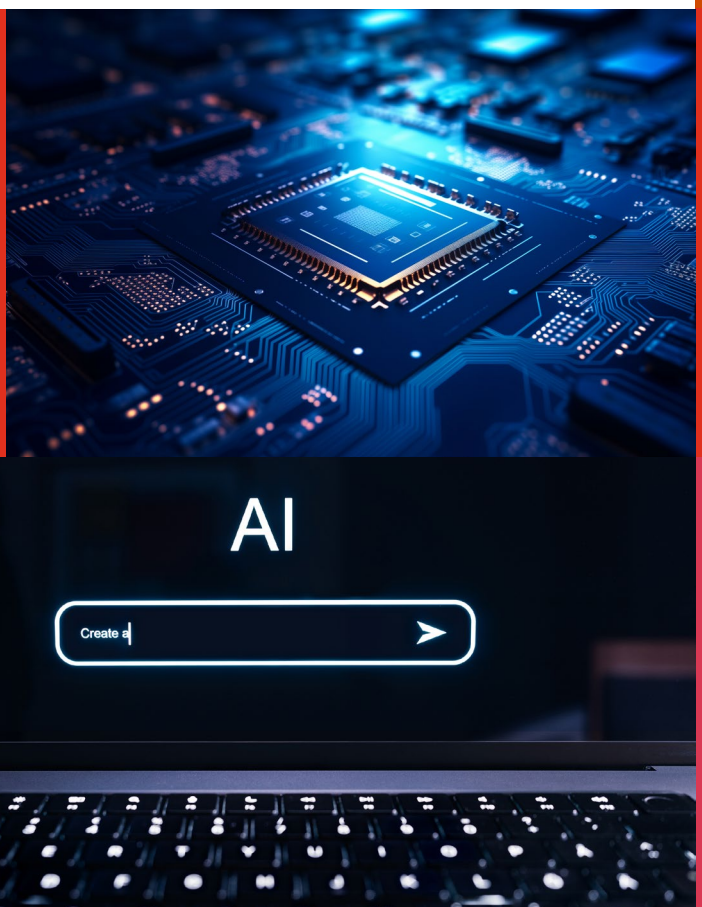
Global, African and South African (4% more so than global and Africa) organisations appear to have not affected their cyber attack surface in their IT environments in regards to quantum computing.

Technology that has not affected organisations' cyber attack surface in the last 12 months (% Ranked top three)

	Global (1,762)	Africa (75)	South Africa (37)*
Quantum computing	39%	39%	43%
Blockchain (e.g., cryptocurrency)	36%	33%	30%
DevOps	35%	33%	32%
Operational technology (OT)	32%	24%	27%
Software as a Service (Saas)	31%	24%	24%
Connected products (e.g., internet of things (IoT), medical devices)	29%	32%	35%
Cloud technology (either multi-cloud or single)	21%	16%	16%
Generative AI	21%	24%	32%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q4

To what extent has your cyber investment changed, if at all, for these emerging technologies in the past 12 months?

African and South African (8% more so than Africa) organisations appear to have significantly increased their cyber investment for machine learning, while global appears to have increased their Cyber Investment for genAI.

Technologies for which organisations' cyber investment has increased significantly in the last 12 months (% Ranked top three)

	Global (1,929)	Africa (84)	South Africa (37)*
Generative AI	40%	29%	32%
Machine learning	29%	33%	41%
Robotics	23%	17%	24%
Virtual reality	21%	19%	24%
Quantum computing	20%	12%	19%
Blockchain (cryptocurrency)	20%	20%	22%
Non-fungible token (NFTs)	15%	12%	16%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q5

To what extent has your cyber investment changed, if at all, for these emerging technologies in the past 12 months?

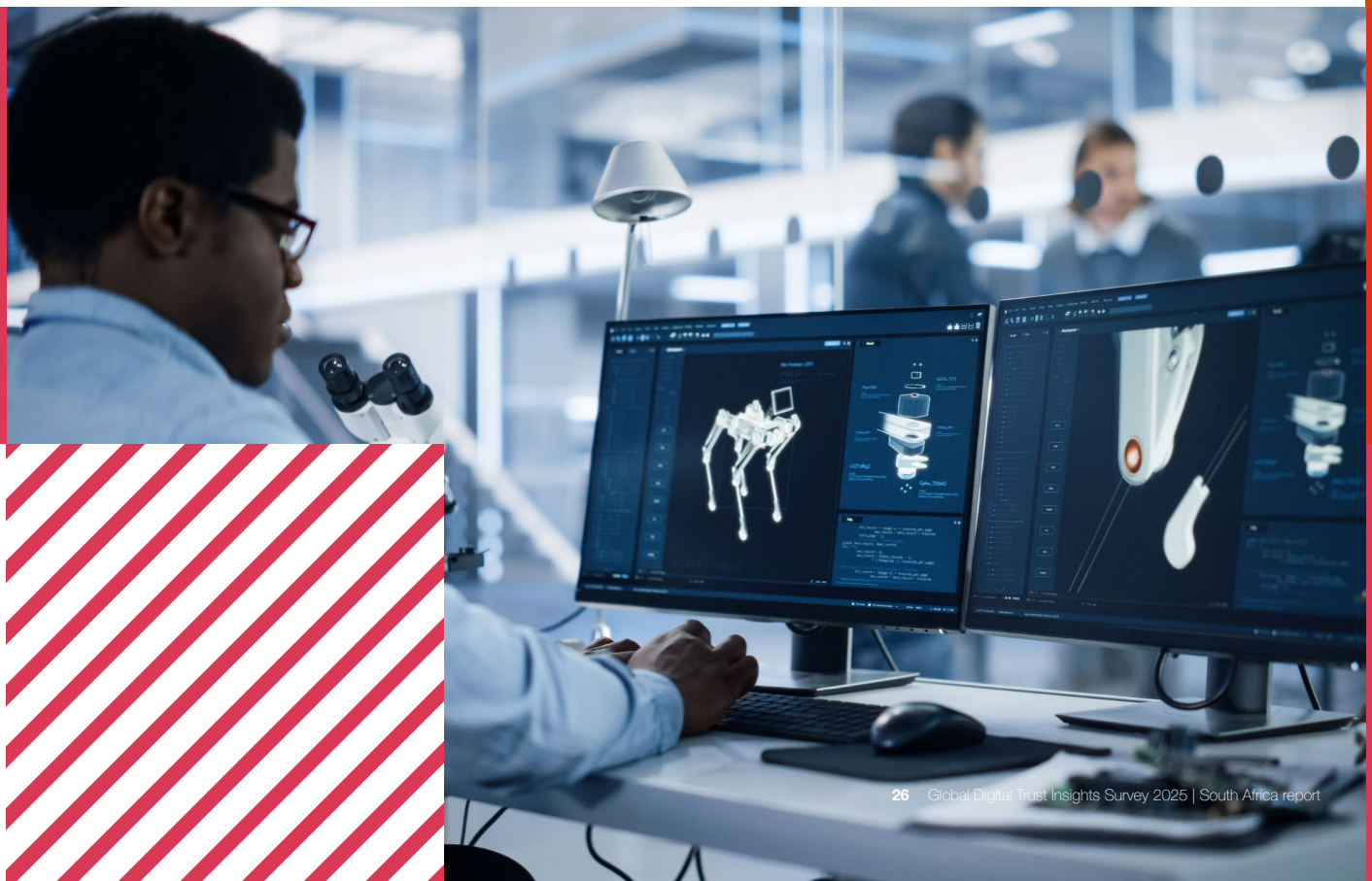
African and South African (6% more so than Africa) organisations appear to have slightly increased their cyber investment for genAI, while global appears to have increased their cyber investment for machine learning.

Technologies for which organisations' cyber investment has increased slightly in the last 12 months (% Ranked top three)

	Global (1,929)	Africa (84)	South Africa (37)*
Machine learning	41%	33%	32%
Generative AI	38%	43%	49%
Quantum computing	33%	33%	38%
Robotics	32%	35%	41%
Blockchain (cryptocurrency)	31%	23%	32%
Virtual reality	31%	26%	27%
Non-fungible token (NFTs)	25%	25%	27%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q6 To what extent has your cyber investment changed, if at all, for these emerging technologies in the past 12 months?

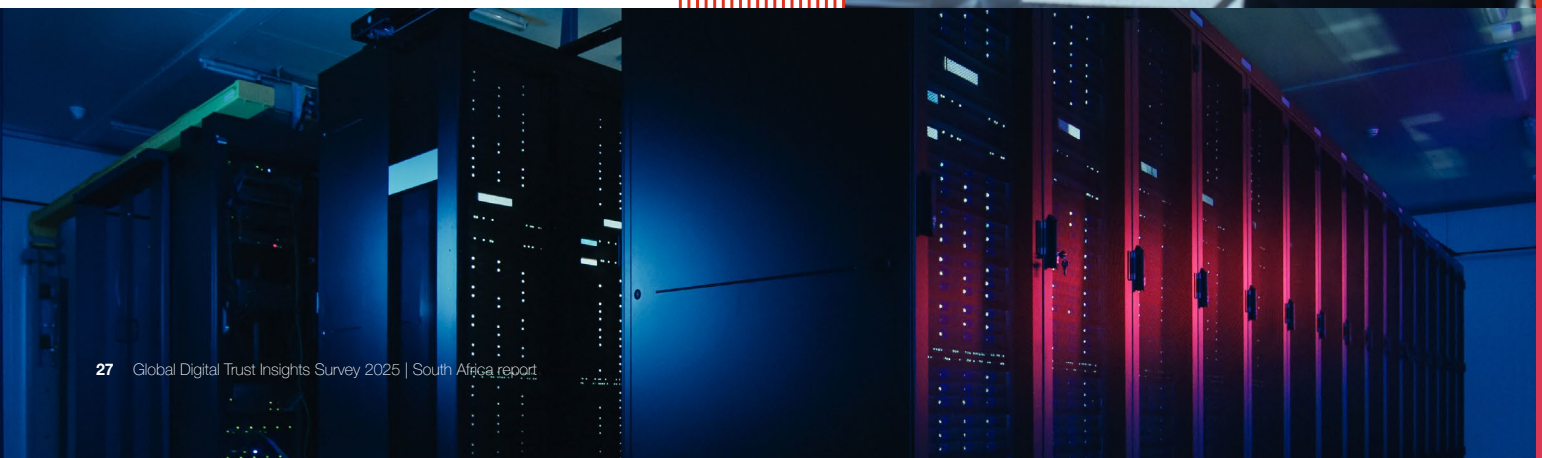
African and South African (2% more so than Africa) organisations appear to have not changed their cyber investment for virtual reality (VR) with Africa placing blockchain at the same percentage, while global appears to have not changed their cyber investment for non-fungible tokens (NFTs).

Technologies for which organisations' cyber investment has not changed in the last 12 months (% Ranked top three)

	Global (1,929)	Africa (84)	South Africa (37)*
Non-fungible token (NFTs)	37%	33%	35%
Quantum computing	32%	33%	24%
Virtual reality	32%	36%	38%
Blockchain (cryptocurrency)	31%	36%	30%
Robotics	30%	29%	22%
Machine learning	21%	19%	16%
Generative AI	14%	20%	11%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q7 In what aspects of cyber defence, if any, is your organisation prioritising the use of genAI over the next 12 months?

Global organisations appear to have prioritised the use of genAI to threat detection and response over the next 12 months, while Africa prioritises threat intelligence and South Africa prioritises Security Operations Centres (SOCs) modernisation.

Technologies for which organisations' cyber investment has not changed in the last 12 months (% Ranked top three)

	Global (1,762)	Africa (75)	South Africa (37)*
Threat detection and response	44%	37%	30%
Threat intelligence	39%	47%	46%
Malware and phishing detection	38%	31%	41%
Security Operations Centres (SOCs) modernisation	35%	45%	54%
Security log analysis	32%	37%	32%
Vulnerability management	31%	28%	22%
Identity and access management	30%	25%	16%
Endpoint security	29%	19%	24%
Other	0%	1%	0%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Key: 1st 2nd 3rd

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q8 What are the most significant challenges your organisation is facing internally on genAI relating to cybersecurity and privacy over the next 12 months?

Global and South African (8% more so than global) organisations appear to be facing a challenge with the lack of trust in genAI by internal stakeholders over the next 12 months, with global appearing to place difficulty incorporating with existing systems/ processes at the same percentages, while Africa appears to be facing a challenge of a lack of training resources for employees.

Challenges that organisations are facing internally on genAI relating to cybersecurity and privacy over the next 12 months (% Ranked top three)

	Global (1,694)	Africa (73)	South Africa (36)*
Difficulty incorporating with existing systems/ processes	39%	34%	22%
Lack of trust in genAI by internal stakeholders (e.g., leadership, employees)	39%	36%	47%
Inadequate internal controls and risk management	38%	40%	42%
Lack of standardised internal policies governing its use	37%	42%	39%
Lack of training resources for employees	37%	45%	42%
Implementing data governance	35%	29%	33%
Deliberate misuse of genAII technology by an employee	33%	32%	31%
Inability to comply with new regulations	22%	22%	28%
Other	0%	0%	0%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Key: 1st 2nd 3rd

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q9 What impact, if any, have genAI had on your organisation's risk management investments in the following areas?

Global, African (1% more so than global) and South African (4% more so than Africa) organisations' risk management investments appear to have significantly increased in regards to talent hiring and training due to genAI.

Areas where GenAI had a significant increase on organisations' risk management investments (% Ranked top three)

	Global (1,694)	Africa (73)	South Africa (36)*
Talent hiring and training	26%	27%	31%
AI governance	25%	16%	22%
Infrastructure upgrades	23%	23%	25%
Model development, training and tuning	22%	21%	17%
Compliance and legal	21%	16%	19%
Third-party services	19%	14%	17%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q10 What impact, if any, have genAI had on your organisation's risk management investments in the following areas?

Global and African (3% more so than global) organisations' risk management investments appear to have increased slightly in regards to AI governance due to genAI, while global and Africa (12% more so than global) appears to have increased slightly in regards to model development, training and tuning.

Areas where GenAI had a slight increase on organisations' risk management investments (% Ranked top three)

	Global (1,694)	Africa (73)	South Africa (36)*
AI governance	46%	49%	44%
Model development, training and tuning	46%	47%	58%
Infrastructure upgrades	45%	44%	50%
Compliance and legal	43%	38%	42%
Third-party services	40%	37%	33%
Talent hiring and training	40%	27%	39%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q11 What impact, if any, have genAI had on your organisation's risk management investments in the following areas?

Global and South African (same percentage as global) organisations' risk management investments appear to have no change in regards to third-party services due to genAI with South Africa placing the same percentage on compliance and legal, while Africa has no change in regards to talent hiring and training.

Areas where GenAI had a no change on organisations' risk management investments (% Ranked top three)

	Global (1,694)	Africa (73)	South Africa (36)*
Third-party services	31%	32%	31%
Compliance and legal	28%	33%	31%
Talent hiring and training	26%	37%	19%
Infrastructure upgrades	25%	21%	11%
Model development, training and tuning	24%	26%	19%
AI governance	21%	23%	19%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

(*) number of responses is low (between 30–49 responses). The results are indicative only

Regulatory developments

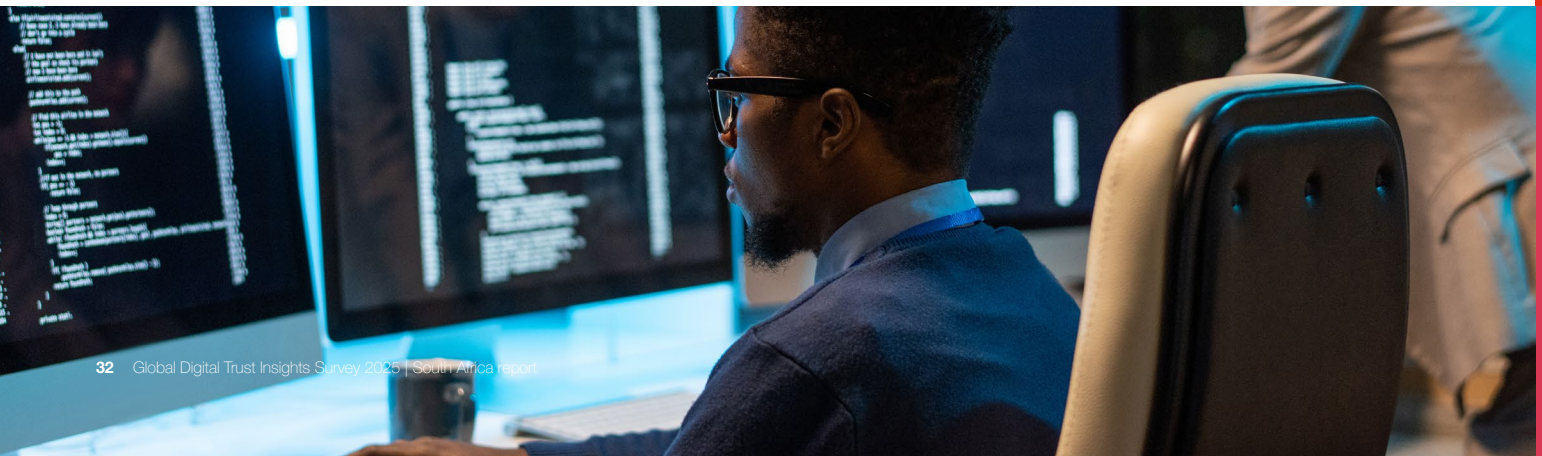
Q1 How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates?

African and South African (11% more so than Africa) organisations appear to be extremely confident that they are in compliance with the data protection regulation, while global appears to be extremely confident in regards to the consumer privacy regulation.

Types of regulations where organisations are extremely confident they are in compliance for their geographical area (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Consumer privacy (e.g., EU GDPR, California Privacy Rights Act)	26%	20%	27%
Network and information security (e.g., EU Network and Information Security Directive)	24%	20%	29%
Data protection (e.g., China Data Security Law, Singapore Personal Data Protection Act)	24%	23%	34%
Cyber disclosure (e.g., US SEC cyber disclosure rule)	23%	18%	29%
Artificial intelligence (e.g., EU AI Act)	22%	22%	33%
Critical infrastructure (e.g., US CIRCIA)	21%	14%	25%
Resilience (e.g., EU DORA, UK SS1/21)	20%	14%	19%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.



Q2 How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates?

Global, African (2% more so than global) and South African (2% more so than Africa) organisations appear to be very confident that they are in compliance with the network and information security regulation.

Types of regulations where organisations are very confident they are in compliance for their geographical area (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Network and information security (e.g., EU Network and Information Security Directive)	40%	42%	44%
Consumer privacy (e.g., EU GDPR, California Privacy Rights Act)	39%	37%	37%
Critical infrastructure (e.g., US CIRCIA)	37%	34%	36%
Cyber disclosure (e.g., US SEC cyber disclosure rule)	36%	36%	38%
Data protection (e.g., China Data Security Law, Singapore Personal Data Protection Act)	36%	35%	35%
Resilience (e.g., EU DORA, UK SS1/21)	35%	31%	34%
Artificial intelligence (e.g., EU AI Act)	34%	27%	30%

Total = 1434; Africa = 37; South Africa = 8
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q3 How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates?

Global and South African (1% more so than global) organisations appear to be moderately confident that they are in compliance with the AI regulation with global appearing to place resilience on the same percentage, while Africa appears to be moderately confident in regards to the cyber disclosure regulation.

Types of regulations where organisations are moderately confident they are in compliance for their geographical area (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Artificial intelligence (e.g., EU AI Act)	26%	27%	27%
Resilience (e.g., EU DORA, UK SS1/21)	26%	23%	25%
Critical infrastructure (e.g., US CIRCIA)	25%	26%	22%
Cyber disclosure (e.g., US SEC cyber disclosure rule)	24%	30%	23%
Data protection (e.g., China Data Security Law, Singapore Personal Data Protection Act)	23%	25%	16%
Network and information security (e.g., EU Network and Information Security Directive)	23%	22%	13%
Consumer privacy (e.g., EU GDPR, California Privacy Rights Act)	23%	24%	19%

Q4 How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates?

African (4% more so than South Africa) and South African organisations appear to be slightly confident that they are in compliance with the resilience regulation, while global appears to be slightly confident in regards to the AI regulation.

Types of regulations where organisations are slightly confident they are in compliance for their geographical area (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Artificial intelligence (e.g., EU AI Act)	10%	12%	4%
Resilience (e.g., EU DORA, UK SS1/21)	9%	20%	16%
Data protection (e.g., China Data Security Law, Singapore Personal Data Protection Act)	9%	11%	9%
Critical infrastructure (e.g., US CIRCIA)	8%	17%	13%
Cyber disclosure (e.g., US SEC cyber disclosure rule)	8%	8%	6%
Network and information security (e.g., EU Network and Information Security Directive)	8%	8%	10%
Consumer privacy (e.g., EU GDPR, California Privacy Rights Act)	7%	13%	13%

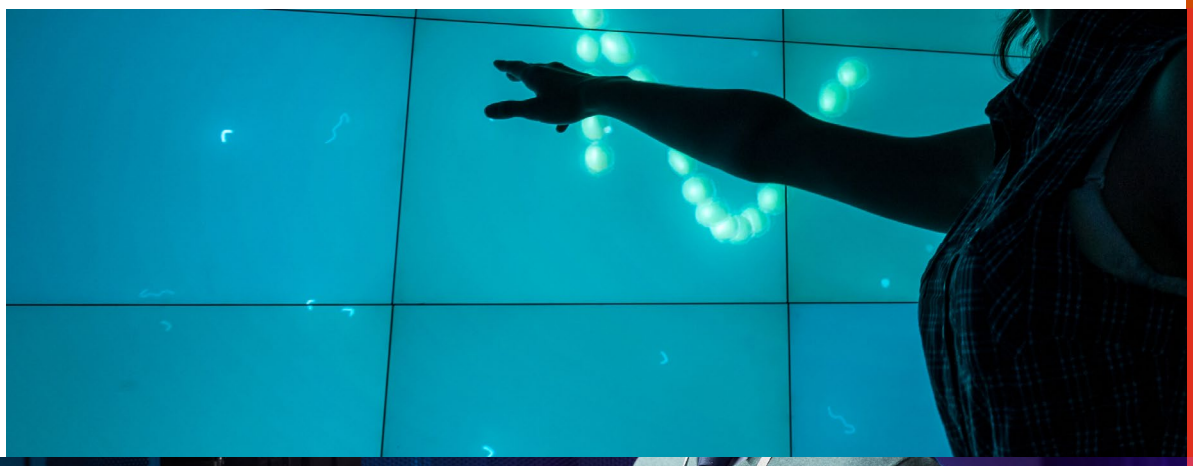
Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

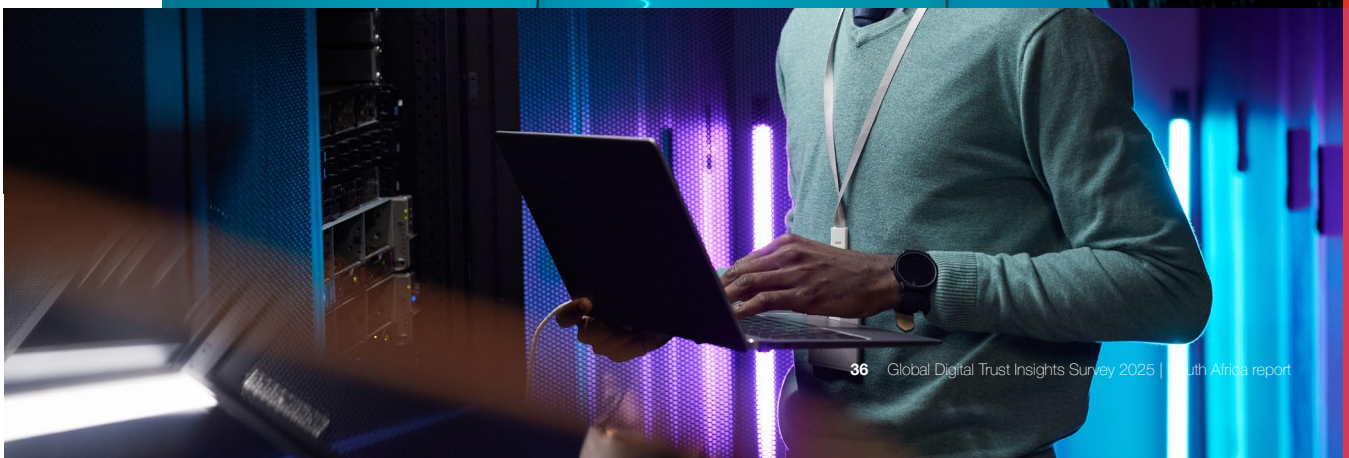
Q5 How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates?

Global, African (2% more so than global and South Africa) and South African organisations appear to not be confident that they are in compliance with the AI regulation, with global placing data protection on the same percentage and South Africa placing network and information security on the same percentage.

Types of regulations where organisations are not at all confident they are in compliance for their geographical area (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Artificial intelligence (e.g., EU AI Act)	3%	5%	3%
Data protection (e.g., China Data Security Law, Singapore Personal Data Protection Act)	3%	1%	2%
Cyber disclosure (e.g., US SEC cyber disclosure rule)	2%	2%	1%
Resilience (e.g., EU DORA, UK SS1/21)	2%	3%	2%
Critical infrastructure (e.g., US CIRCIA)	2%	2%	1%
Consumer privacy (e.g., EU GDPR, California Privacy Rights Act)	1%	1%	1%
Network and information security (e.g., EU Network and Information Security Directive)	1%	3%	3%





Q6

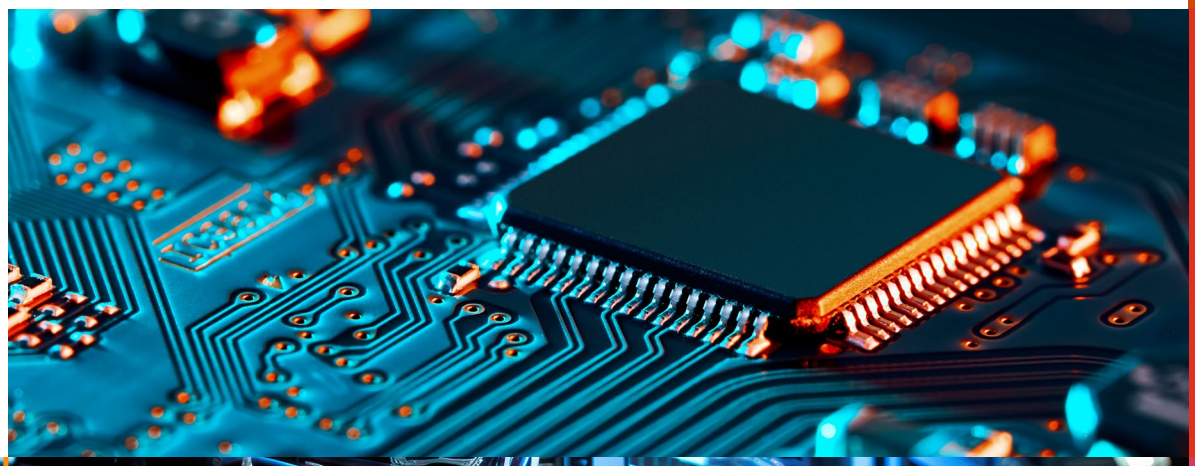
To what extent, if at all, have cybersecurity regulations increased your organisation's cybersecurity investment over the last 12 months?

Global (2% more so than Africa) and African organisations appear to view that cybersecurity regulations have moderately increased their cybersecurity investments over the last 12 months, while South Africa appears to view that regulations have increased their cybersecurity investment to a large extent.

Extents to which cybersecurity regulations have increased organisations' cybersecurity investments over the last 12 months (% Ranked top three)

	Global (1,951)	Africa (84)	South Africa (37)*
To a significant extent	14%	17%	22%
To a large extent	32%	31%	35%
To a moderate extent	37%	35%	30%
To a limited extent	13%	13%	8%
Not at all	3%	4%	3%
Unsure/Not applicable	1%	1%	3%
To a significant extent	14%	17%	22%

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q7 Which one statement, if any, best reflects the impact of new cybersecurity regulations on your organisation over the last 12 months?

Global, African (10% more so than South Africa) and South African (8% more so than South Africa) organisations appear to agree that cybersecurity regulations challenged their organisation to strengthen current cyber risk management programmes, processes and governance approaches over the last 12 months.

Impacts of new cybersecurity regulations on organisations over the last 12 months (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Cybersecurity regulations challenged our organisation to strengthen current cyber risk management programme, processes and governance approaches	24%	42%	32%
Cybersecurity regulations helped our organisation establish guardrails for technology innovation and transformation efforts	20%	18%	16%
Cybersecurity regulations helped our organisation become more resilient by mandating an industry-wide framework	19%	17%	17%
Cybersecurity regulations led us to consider cyber managed services to address regulatory requirements	15%	10%	14%
Cybersecurity regulations hindered our organisation's ability to manage regulatory change and maintain compliance (including other conflicting cyber requirements), resulting in unexpected cost and disruption	9%	7%	14%
Cybersecurity regulations caused delays in our strategic, product, and/or operational plans, delivery outcomes	7%	3%	4%
Cybersecurity regulations had no material impact	5%	1%	2%
Unsure/Not applicable	2%	2%	1%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Cyber strategy

Q1 To what extent is your organisation implementing or planning to implement the following cyber resilience actions?

Global and African (7% more so than global) organisations appear to have prioritised the identification of critical business processes, however South Africa appears to have prioritised the establishment of a resilience team over the identification of critical business processes.

Cyber resilience actions that organisations have already implemented (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Identifying critical business processes	42%	49%	43%
Implementing cyber recovery technology solutions (including immutable backups / isolated recovery environment)	39%	36%	32%
Reporting to external stakeholders (regulators, investors)	35%	45%	36%
Developing cyber recovery playbook for IT-loss scenarios	35%	35%	39%
Establishing protocols with major technology providers to coordinate incident responses	35%	35%	35%
Establishing a resilience team with members from functions like business continuity, cyber, crisis management and risk management	34%	44%	44%
Running tabletop exercises and simulations	33%	34%	36%
Sharing information with industry peers, through formal processes, to prevent systemic risks	32%	39%	36%
Mapping technology dependencies	31%	37%	33%
Establishing relationships with local law enforcement to help with analysis and response	31%	36%	35%
Implementing tools for greater visibility of operational technology (OT) assets	31%	35%	34%
Deploying quantum computing for cyber defence and resilience	23%	22%	27%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q2 To what extent is your organisation implementing or planning to implement the following cyber resilience actions?

Global organisations appear to have prioritised the establishment of a resilience team and protocols with major providers for incident response coordination as well as technology dependency mapping in a portion of their organisation, however, African and South African (7% more so than African) organisations appear to have prioritised the implementation of cyber recovery solutions.

Cyber resilience actions that have been implemented in parts of the organisation (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Establishing a resilience team with members from functions like business continuity, cyber, crisis management and risk management	39%	37%	37%
Mapping technology dependencies	39%	35%	37%
Establishing protocols with major technology providers to coordinate incident responses	39%	39%	40%
Developing cyber recovery playbook for IT-loss scenarios	38%	33%	31%
Identifying critical business processes	38%	38%	43%
Implementing tools for greater visibility of operational technology (OT) assets	38%	38%	40%
Implementing cyber recovery technology solutions (including immutable backups / isolated recovery environment)	38%	43%	50%
Sharing information with industry peers, through formal processes, to prevent systemic risks	37%	33%	38%
Running tabletop exercises and simulations	37%	34%	33%
Reporting to external stakeholders (regulators, investors)	36%	37%	45%
Establishing relationships with local law enforcement to help with analysis and response	34%	36%	39%
Deploying quantum computing for cyber defence and resilience	30%	32%	42%

Total = 3876; Africa = 168; South Africa = 68
Source: PwC's Digital Trust Insights Surveys, Final Results, August 2023.

Q3 To what extent is your organisation implementing or planning to implement the following cyber resilience actions?

Global and African (2% more so than global) organisations appear to agree that they should prioritise the deployment of quantum computing in the next two years when it comes to cyber defence and resilience, however, South Africa appears more concerned about technology dependency mapping.

Cyber resilience actions that organisations plan to implement in the next two (2) years (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Deploying quantum computing for cyber defence and resilience	23%	25%	20%
Implementing tools for greater visibility of operational technology (OT) assets	21%	19%	15%
Mapping technology dependencies	20%	22%	26%
Developing cyber recovery playbook for IT-loss scenarios	19%	23%	21%
Establishing protocols with major technology providers to coordinate incident responses	19%	19%	19%
Running tabletop exercises and simulations	19%	20%	22%
Establishing a resilience team with members from functions like business continuity, cyber, crisis management and risk management	18%	11%	12%
Establishing relationships with local law enforcement to help with analysis and response	18%	14%	15%
Implementing cyber recovery technology solutions (including immutable backups / isolated recovery environment)	18%	16%	14%
Sharing information with industry peers, through formal processes, to prevent systemic risks	18%	17%	16%
Reporting to external stakeholders (regulators, investors)	16%	8%	11%
Identifying critical business processes	15%	11%	14%

Q4 To what extent is your organisation implementing or planning to implement the following cyber resilience actions?

Global (6% more so than Africa), African (3% more so than South Africa) and South African organisations appear to agree that they are not planning on deploying quantum computing for cyber defence and resilience.

Cyber resilience actions that organisations are not planning on implementing (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Deploying quantum computing for cyber defence and resilience	15%	9%	6%
Establishing relationships with local law enforcement to help with analysis and response	11%	6%	4%
Sharing information with industry peers, through formal processes, to prevent systemic risks	9%	5%	5%
Reporting to external stakeholders (regulators, investors)	8%	2%	2%
Running tabletop exercises and simulations	8%	3%	1%
Mapping technology dependencies	6%	2%	1%
Implementing tools for greater visibility of operational technology (OT) assets	6%	3%	4%
Establishing a resilience team with members from functions like business continuity, cyber, crisis management and risk management	5%	4%	3%
Establishing protocols with major technology providers to coordinate incident responses	5%	4%	2%
Developing cyber recovery playbook for IT-loss scenarios	5%	2%	2%
Identifying critical business processes	3%	0%	0%
Implementing cyber recovery technology solutions (including immutable backups / isolated recovery environment)	3%	1%	1%

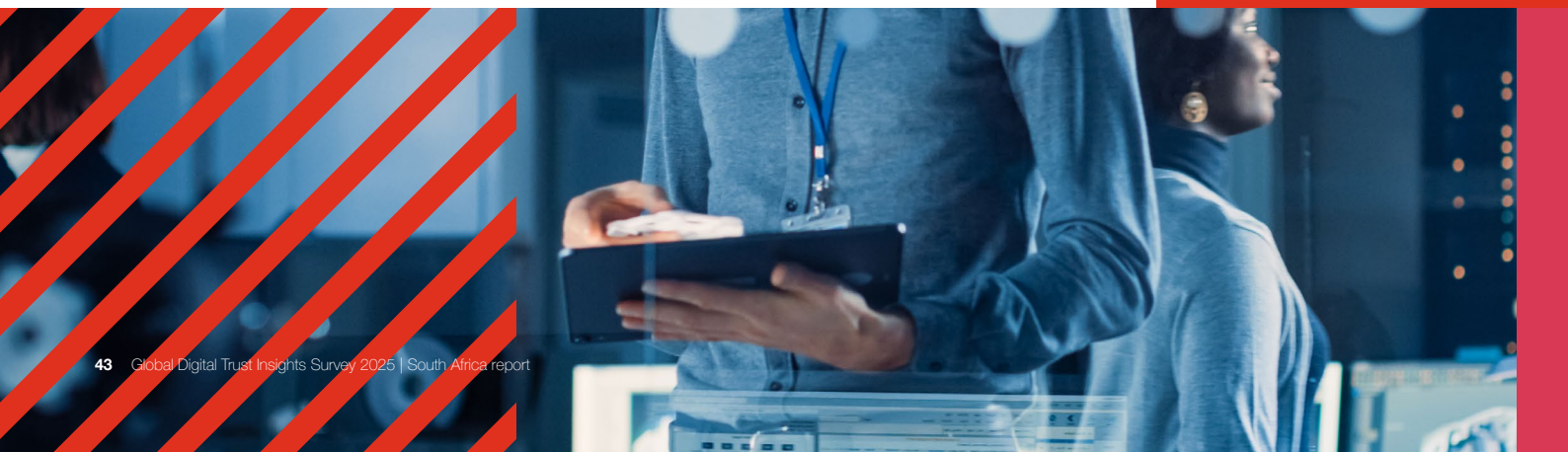
Q5 Which of the following does your organisation use to assess and report on your cybersecurity capabilities?

Global organisations appear to use ISO 27001 to assess their cybersecurity capabilities, while African organisations appear to use the NIST cybersecurity framework and South African organisations appear to use the CRIProfile.

Organisations use the following to assess and report on cybersecurity capabilities (% Ranked top three)

	Global (1,762)	Africa (75)	South Africa (37)*
ISO 27001	39%	36%	16%
NIST cybersecurity framework	36%	43%	40%
Cloud Security Alliance Controls Matrix	33%	35%	42%
Cyber Resilience Review	27%	32%	37%
Cyber Risk Institute Profile	26%	31%	45%
CIS CSC	24%	17%	24%
Sector or industry-specific framework	23%	16%	21%
ISF standard of good practice	21%	20%	21%
SANS critical controls	19%	24%	29%
NIST 800-53	19%	15%	13%
COBIT	17%	23%	18%
ISA/EAC 62443	16%	7%	11%
Other	2%	4%	5%
We don't use any of these frameworks	2%	1%	0%
Unsure	2%	1%	0%

(*) number of responses is low (between 30–49 responses). The results are indicative only



Q6 To what extent does your organisation position cybersecurity as a competitive advantage in these areas?

Global and African (11% more so than global) organisations appear to agree that cybersecurity plays a large role in customer trust, however, South Africa appears to view cybersecurity as a competitive advantage to business growth opportunities.

Areas that organisations selected 'To a large extent' in regards to the position of cybersecurity as a competitive advantage (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Customer trust	57%	68%	67%
Brand integrity and loyalty	49%	58%	59%
Business growth opportunities	46%	57%	68%
Staying ahead of business disruption	46%	54%	63%
Leadership in the market	43%	58%	61%
Public relations	41%	53%	57%

Q7 To what extent does your organisation position cybersecurity as a competitive advantage in these areas?

Global organisations appear to agree that cybersecurity plays a moderate role in public relations, while African (2% more so than South Africa) and South African organisations appear to view cybersecurity playing a moderate role to brand integrity and loyalty with South Africa placing staying ahead of business disruption at the same percentage.

Areas that organisations selected 'To a moderate extent' in regards to the position of cybersecurity as a competitive advantage (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Public relations	41%	31%	29%
Staying ahead of business disruption	39%	31%	31%
Leadership in the market	38%	25%	23%
Brand integrity and loyalty	37%	33%	31%
Business growth opportunities	37%	28%	19%
Customer trust	32%	20%	20%

Q8 To what extent does your organisation position cybersecurity as a competitive advantage in these areas?

Global, African and South African (1% less than global and Africa) organisations appear to agree that cybersecurity plays a limited role in market leadership.

Areas that organisations selected 'To a limited extent' in regards to the position of cybersecurity as a competitive advantage (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Leadership in the market	13%	13%	12%
Business growth opportunities	12%	10%	7%
Public relations	12%	11%	10%
Staying ahead of business disruption	10%	11%	5%
Brand integrity and loyalty	10%	6%	7%
Customer trust	8%	8%	10%

Q9 To what extent does your organisation position cybersecurity as a competitive advantage in these areas?

Global and African (1% more so than global) organisations appear to agree that cybersecurity plays no role in public relations with global organisations placing business growth opportunities and market leadership at the same percentage, however, South Africa appears to view cybersecurity playing no role in business growth opportunities.

Areas that organisations selected 'Not at all' in regards to the position of cybersecurity as a competitive advantage (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Public relations	4%	5%	3%
Business growth opportunities	4%	4%	5%
Leadership in the market	4%	4%	4%
Brand integrity and loyalty	3%	2%	3%
Staying ahead of business disruption	3%	2%	1%
Customer trust	2%	3%	3%

Q10 What, if any, are your organisation's strategy, people and investment goals relating to cyber and privacy over the next 12 months?

Global and African (7% more so than global) organisations appear to agree that they should prioritise for faster response times to incidents and disruptions, however, South Africa appears more concerned about the improvement of leader confidence in managing threats.

The strategy, people and investment goals that relate to cyber and privacy that organisations are planning for over the next 12 months (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Faster response times to incidents and disruptions	36%	43%	35%
Improved confidence of leaders in ability to manage present and future threats	31%	37%	38%
Improved customer and employee experience	30%	37%	37%
Improved compliance with regulations	30%	36%	30%
Greater use of cyber managed services	29%	33%	27%
Lower costs of compliance and managing risks	25%	16%	19%
Support in the way of resources and collaboration with the CISO	23%	27%	34%
Lower downtime and associated costs	21%	16%	17%
Less burdensome employee experience in managing risk and compliance	21%	12%	15%
Accelerated entry of our organisation into new markets	21%	19%	25%
Expedited launch of new products	18%	11%	12%

Key: 1st 2nd 3rd

Cyber leadership

Q1 How involved is your CEO in the following cyber and privacy matters?

Global organisations' CEO involvement in the following cyber and privacy matters appears to be prioritised around the discussion on their implications of future corporate strategies, while African organisations appear to prioritise the discussion of key cyber metrics and South African organisations appear to prioritise the discussion of their implications of a major operating model change.

Where the CEO is involved in cyber and privacy matters (% Ranked top three)

	Global (3,595)	Africa (184)	South Africa (74)
Discussion of cyber and privacy implications of future corporate strategy	40%	42%	35%
When regulators contact our organisation for cyber incident reporting, matters requiring attention, or enforcement action	36%	41%	37%
Discussion of key cyber metrics at the board level	35%	47%	41%
Discussion of cyber and privacy implications of a major operating model change	34%	35%	46%
Discussion of cyber and privacy implications in a new business initiative	33%	32%	38%
After our organisation experiences a major cyber breach or attack	32%	23%	18%
After a major cyber breach or attack in our industry	30%	26%	20%
Discussion of cyber and privacy implications in deals (e.g., M&A, IPO, spin-off)	29%	22%	28%

Key: 1st 2nd 3rd

Q2 How involved are you in the following cyber and privacy matters?

Global and African (9% more so than global) organisations' involvement in the following cyber and privacy matters appears to be prioritised around when regulators can contact them for cybersecurity-related actions with global organisations placing discussions on their implications of future corporate strategies at the same percentage. There are no percentages for South African organisations.

Where organisations are involved in following cyber and privacy matters (% Ranked top three)

	Global (447)	Africa (34)*	South Africa (20)**
Discussion of cyber and privacy implications of future corporate strategy	38%	38%	
When regulators contact our organisation for cyber incident reporting, matters requiring attention, or enforcement action	38%	47%	
Discussion of key cyber metrics at the board level	37%	41%	
Discussion of cyber and privacy implications in deals (e.g., M&A, IPO, spin-off)	36%	41%	
Discussion of cyber and privacy implications of a major operating model change	35%	32%	
Discussion of cyber and privacy implications in a new business initiative	34%	41%	
After our organisation experiences a major cyber breach or attack	33%	26%	
After a major cyber breach or attack in our industry	31%	15%	

Key: 1st 2nd 3rd

(*) number of responses is low (between 30–49 responses). The results are indicative only

Q3 How involved is your organisation's CISO in taking an active role in the following areas?

Global and South African (13% more so than global) organisations appear to have CISOs who take an active role, to a large extent, in strategic planning about cyber investment with South Africa placing the product development as well as sales and marketing at the same percentage, while African organisations appear to prioritise reporting and regular meetings with the board.

Areas where CISOs take an active role 'To a large extent' (% Ranked top three)

	Global (3,640)	Africa (199)	South Africa (80)
Strategic planning with CFO about cyber investment	47%	54%	60%
Reporting and regular meetings with the board	46%	57%	55%
Oversight on tech and infrastructure deployments	45%	51%	55%
Product development	41%	54%	60%
Drafting and reviewing regulatory disclosures	41%	48%	54%
Sales and marketing	37%	46%	60%

Q4 How involved is your organisation's CISO in taking an active role in the following areas?

Global (3% more so than global), African (1% more so than South Africa) and South African organisations appear to have CISOs who take an active role, to a moderate extent, in drafting and reviewing regulatory disclosures.

Areas where CISOs take an active role 'To a moderate extent' (% Ranked top three)

	Global (3,640)	Africa (199)	South Africa (80)
Drafting and reviewing regulatory disclosures	40%	37%	36%
Oversight on tech and infrastructure deployments	39%	34%	33%
Reporting and regular meetings with the board	37%	27%	30%
Strategic planning with CFO about cyber investment	36%	30%	30%
Product development	36%	31%	29%
Sales and marketing	36%	23%	21%

Q5 How involved is your organisation's CISO in taking an active role in the following areas?

Global (2% more than South Africa), African (3% more so than global) and South African organisations appear to have CISOs who take an active role, to a limited extent, in sales and marketing.

Areas where CISOs take an active role 'To a limited extent' (% Ranked top three)

	Global (3,640)	Africa (199)	South Africa (80)
Sales and marketing	17%	20%	15%
Product development	15%	9%	8%
Drafting and reviewing regulatory disclosures	13%	9%	5%
Oversight on tech and infrastructure deployments	11%	11%	11%
Strategic planning with CFO about cyber investment	11%	11%	9%
Reporting and regular meetings with the board	11%	11%	13%

Q6 How involved is your organisation's CISO in taking an active role in the following areas? (i.e., risk quantification)?

Global (2% more so than South Africa), African (1% more so than global) and South African organisations appear to have CISOs who do not take an active role in sales and marketing.

Areas where CISOs take an active role 'To a large extent' (% Ranked top three)

	Global (3,640)	Africa (199)	South Africa (80)
Sales and marketing	6%	7%	4%
Product development	4%	3%	3%
Reporting and regular meetings with the board	3%	2%	3%
Strategic planning with CFO about cyber investment	3%	2%	1%
Drafting and reviewing regulatory disclosures	3%	2%	3%
Oversight on tech and infrastructure deployments	2%	1%	0%

Q7 How effective do you think your organisation's board is across the following areas?

Global and African (9% more so than global) organisations appear to think that their board is very effective in regulatory responsibilities, while South Africa appears to think their board is very effective in cyber risk oversight.

Areas where organisations are 'Very effective' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Regulatory responsibilities	50%	59%	55%
Cyber strategy engagement	47%	50%	54%
Cyber risk oversight	46%	51%	61%
Cyber training and education	45%	50%	59%
Fostering cyber innovation and growth	43%	45%	51%
Cyber expertise	43%	42%	50%

Q8 How effective do you think your organisation's board is across the following areas?

Global (4% more so than Africa), African (1% more so than South Africa) and South African organisations appear to think that their board is moderately effective in cyber expertise with global organisations placing the same percentage on fostering cyber innovation and growth.

Areas where organisations are 'Moderately effective' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Fostering cyber innovation and growth	40%	35%	34%
Cyber expertise	40%	36%	35%
Cyber risk oversight	39%	32%	28%
Cyber training and education	38%	33%	26%
Cyber strategy engagement	38%	34%	31%
Regulatory responsibilities	37%	27%	34%

Q9 How effective do you think your organisation's board is across the following areas?

Global and African (2% more so than global) organisations appear to think that their board is slightly effective in cyber expertise with global organisations placing cyber training and expense at the same percentage, while South Africa appears to think their board is slightly effective in cyber strategy engagement.

Areas where organisations are 'Slightly effective' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Cyber training and education	13%	12%	11%
Cyber expertise	13%	15%	10%
Fostering cyber innovation and growth	12%	14%	11%
Cyber strategy engagement	12%	12%	13%
Cyber risk oversight	11%	13%	9%
Regulatory responsibilities	10%	10%	7%

Q10 How effective do you think your organisation's board is across the following areas?

Global and African (2% more so than global) organisations appear to think that their board is not effective in cyber expertise with global organisations placing cyber training and education as well as fostering cyber innovation and growth at the same percentage, while South Africa appears to think their board is not effective in cyber training and education.

Areas where organisations are 'Not effective' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Cyber expertise	3%	5%	4%
Fostering cyber innovation and growth	3%	4%	2%
Cyber training and education	3%	3%	5%
Cyber risk oversight	2%	2%	2%
Cyber strategy engagement	2%	2%	2%
Regulatory responsibilities	2%	1%	1%

Cyber risk quantification

Q1 To what extent is your organisation currently measuring the potential financial impact of cyber risks (i.e., risk quantification)?

Global, African (9% more so than global) and South African (7% more so than Africa) organisations appear to, at a large extent, measure the potential financial impact of cyber risks to their organisation with global organisations also appearing to, at a moderate extent, measure the potential financial impact at the same percentage.

The extent to which organisations measure the potential financial impact of cyber risks (% Ranked top three)

	Global (2,570)	Africa (143)	South Africa (67)
To a significant extent (e.g., extensive cyber risk quantification with automation and executive reporting)	15%	19%	25%
To a large extent (e.g., established use of cyber risk methods)	29%	38%	45%
To a moderate extent (e.g., exploring through limited use of cyber risk methods)	29%	22%	19%
To a limited extent (e.g., qualitatively through risk assessment and risk prioritisation)	17%	16%	5%
Not at all, but planning to in the next two years	6%	3%	6%
Not at all and no plans to in the next two years	2%	1%	0%
Unsure	1%	1%	0%

Q2 What method of cyber risk quantification is your organisation using?

Global, African (4% more so than South Africa) and South African (9% more so than global) organisations appear to use security posture assessments for cyber risk quantification.

Method that organisations use for cyber quantification (% Ranked top three)

	Global (1,899)	Africa (113)	South Africa (60)
Security posture assessments (e.g., measuring compliance with vulnerability remediation, user access reviews or training completion)	73%	86%	82%
Scenario-based quantification (e.g., FAIR, Monte Carlo)	24%	11%	15%
Other	1%	1%	0%
Unsure	2%	3%	3%

Q3 What challenges, if any, has your organisation faced in quantifying the potential financial impact of cyber risk?

Global and African (6% more so than global) organisations appear to be uncertain about the intended scope of risk quantification outputs when it comes to quantifying the potential financial impact of cyber risk, while South African (4% more so than Africa) and African organisations appear to face challenges with data issues when it comes to quantifying the potential financial impact.

Challenges that organisations have face in quantifying potential financial impact of cyber risk (% Ranked top three)

	Global (1,899)	Africa (113)	South Africa (60)
Uncertainty around intended scope of risk quantification outputs (e.g., asset-level, business process-level or core business units)	45%	51%	45%
Data issues (e.g., poor quality, gaps, inconsistency, incompatibility, complexity)	44%	51%	55%
Legal or regulatory concerns (e.g., risk quantification outputs that create potential legal exposure)	43%	46%	53%
Reliability and trustworthiness of risk quantification outputs	38%	35%	42%
Complexity of risk quantification tools	35%	39%	30%
Insufficient understanding of the consequences of cybersecurity risk	31%	27%	30%
Insufficient fundamentals or infrastructure (e.g., risk library, controls library)	30%	26%	28%
Other	0%	0%	0%

Key: 1st 2nd 3rd

Q4 Please indicate how important or unimportant the following aspects are to your organisation in quantifying cyber risk.

Global, African (7% more so than global) and South African (10% more so than Africa) organisations appear to place extreme importance on prioritising cyber investments in regards to quantifying cyber risk with global placing the same percentage on allocating resources to higher risk areas.

Aspects that organisations selected as 'Extremely Important' in regards to the importance in quantifying cyber risk (% Ranked top three)

	Global (1,899)	Africa (113)	South Africa (60)
To help prioritise cyber investments	46%	53%	63%
To help allocate resources to areas of highest risk	46%	50%	57%
To help evaluate and communicate cyber risks in line with defined risk tolerance	43%	42%	52%
To demonstrate the cyber risk management program's value	42%	50%	58%
To measure and compare threats and incidents on an apples-to-apples basis	41%	35%	43%
To support financial reporting or insurance negotiations	38%	38%	45%
To measure the impact of deals (e.g., M&A, divestiture, etc.) on the risk profile	37%	28%	40%

Key: 1st 2nd 3rd

Q5 Please indicate how important or unimportant the following aspects are to your organisation in quantifying cyber risk.

Global, African (9% more so than South Africa) and South African (2% more so than global) organisations appear to place the evaluation and communication of cyber risk as very important with global placing the same percentage on supporting financial reporting or insurance negotiations and South Africa placing the same percentage on measuring and comparing threats and incidents.

Aspects that organisations selected as 'Very Important' in regards to the importance in quantifying cyber risk (% Ranked top three)

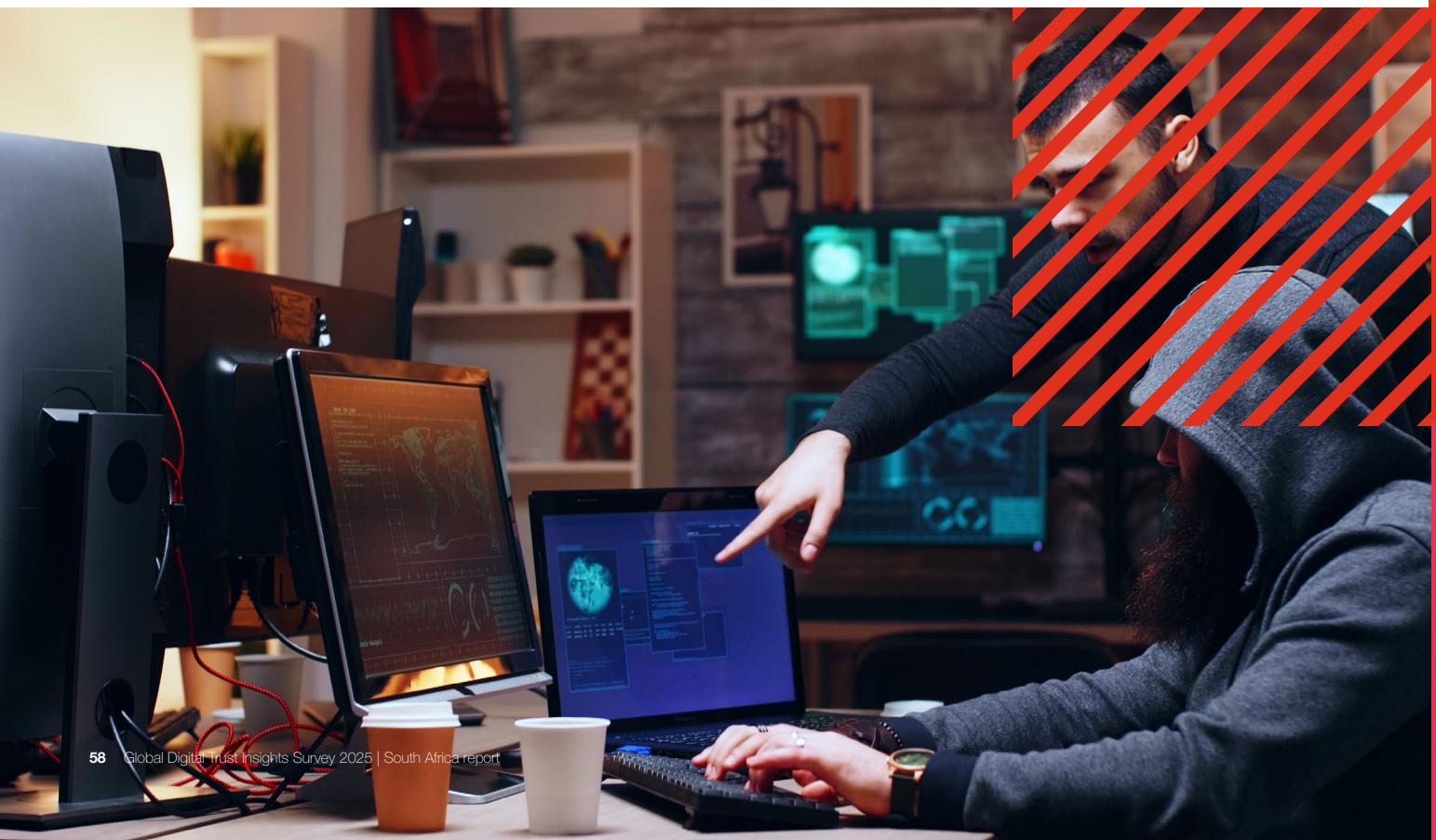
	Global (1,899)	Africa (113)	South Africa (60)
To support financial reporting or insurance negotiations	45%	44%	45%
To help evaluate and communicate cyber risks in line with defined risk tolerance	45%	56%	47%
To demonstrate the cyber risk management program's value	43%	41%	30%
To measure and compare threats and incidents on an apples-to-apples basis	43%	48%	47%
To measure the impact of deals (e.g., M&A, divestiture, etc.) on the risk profile	43%	50%	45%
To help prioritise cyber investments	42%	35%	32%
To help allocate resources to areas of highest risk	41%	42%	40%

Q6 Please indicate how important or unimportant the following aspects are to your organisation in quantifying cyber risk.

Global (2% more so than South Africa), African (2% more so than global) and South African organisations appear to place moderate importance on measuring the impact deals can have on the risk profile.

Aspects that organisations selected as 'Moderately Important' in regards to the importance in quantifying cyber risk (% Ranked top three)

	Global (1,899)	Africa (113)	South Africa (60)
To measure the impact of deals (e.g., M&A, divestiture, etc.) on the risk profile	15%	17%	13%
To support financial reporting or insurance negotiations	14%	16%	10%
To measure and compare threats and incidents on an apples-to-apples basis	12%	15%	8%
To demonstrate the cyber risk management program's value	12%	7%	10%
To help allocate resources to areas of highest risk	12%	4%	3%
To help evaluate and communicate cyber risks in line with defined risk tolerance	11%	2%	0%
To help prioritise cyber investments	10%	9%	3%

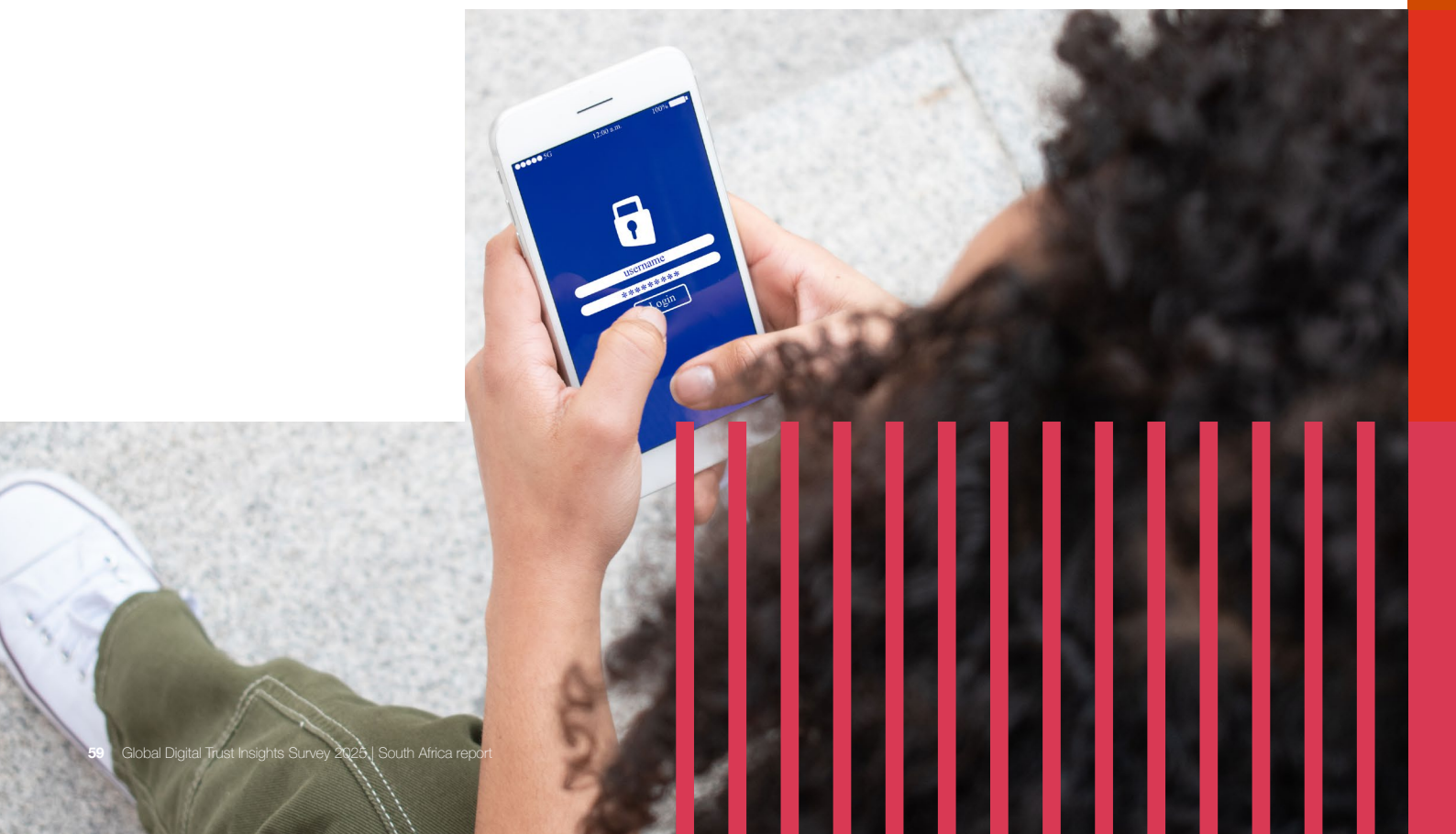


Q7 Please indicate how important or unimportant the following aspects are to your organisation in quantifying cyber risk.

Global (1% more so than both Africa and South Africa), African and South African organisations appear to place no importance on measuring the impact deals can have on the risk profile, with both Africa and South Africa placing the same percentage on the demonstration of the cyber risk management programme's value. Additionally, Africa places the same percentage on financial reporting or insurance negotiations support and South Africa placing the same percentage on the evaluation and communication of cyber risks.

Aspects that organisations selected as 'Not Important' in regards to the importance in quantifying cyber risk (% Ranked top three)

	Global (1,899)	Africa (113)	South Africa (60)
To measure the impact of deals (e.g., M&A, divestiture, etc.) on the risk profile	3%	2%	2%
To measure and compare threats and incidents on an apples-to-apples basis	2%	0%	0%
To support financial reporting or insurance negotiations	1%	2%	0%
To demonstrate the cyber risk management program's value	1%	2%	2%
To help prioritise cyber investments	1%	1%	0%
To help evaluate and communicate cyber risks in line with defined risk tolerance	1%	1%	2%
To help allocate resources to areas of highest risk	1%	1%	0%



Behaviours

Q1 Finally, please indicate how consistently your organisation's cybersecurity team does the following.

Global (18% less than Africa and South Africa), African and South African organisation cybersecurity teams appear to focus most of their efforts on putting controls in place and responding to threats.

Areas where the organisation's cybersecurity team focuses 'Usually (81-100% of the time)' (% Ranked top three)

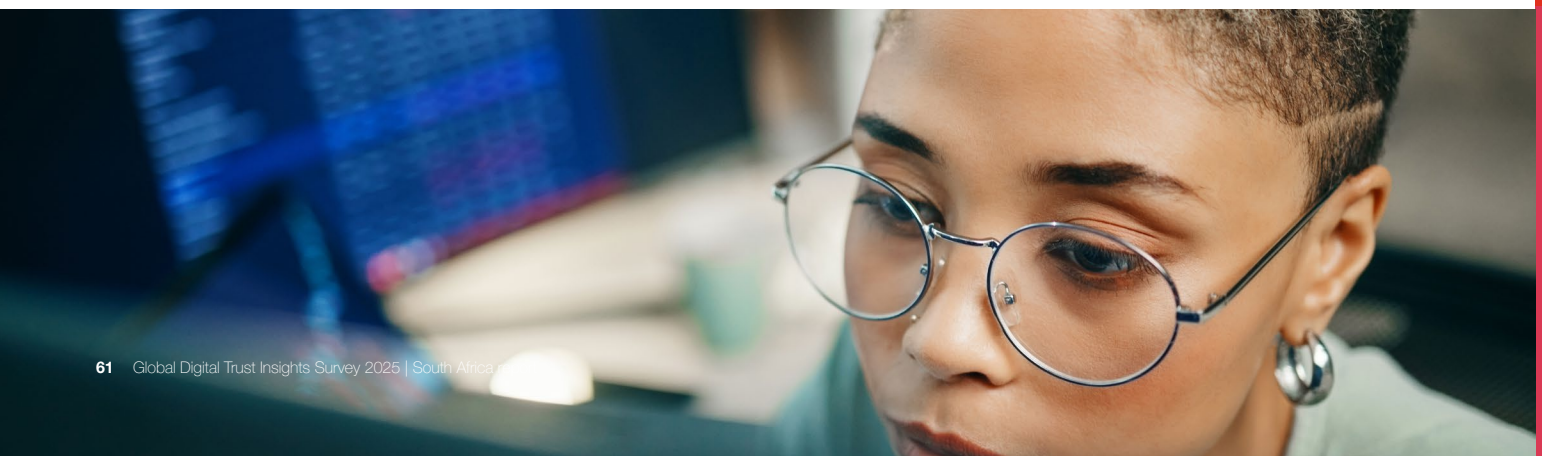
	Global (4,042)	Africa (218)	South Africa (94)
Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions	26%	44%	44%
Collaborates with other parts of the business that affect the organisation's cybersecurity posture	22%	35%	32%
Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board	22%	31%	30%
Allocates cyber budget to the top risks of the organisation	21%	33%	37%
Anticipates future cyber risks given the macro environment, emerging technology and business strategy	20%	29%	26%
Expedites digital and other major transformation initiatives of our organisation	19%	27%	23%

Q2 Finally, please indicate how consistently your organisation's cybersecurity team does the following.

Global, African (4% more so than global) and South African (6% more so than Africa) organisation cybersecurity teams appear to often focus their efforts on expediting digital and other major transformation initiatives, with Africa placing the same percentage on anticipation of future cyber risks and global placing the same percentage on anticipation of future cyber risks, collaborating with other parts of business and putting controls in place and responding quickly to threats.

Areas where the organisation's cybersecurity team focuses 'Often (61-80% of the time)' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Anticipates future cyber risks given the macro environment, emerging technology and business strategy	35%	39%	43%
Collaborates with other parts of the business that affect the organisation's cybersecurity posture	35%	34%	35%
Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions	35%	33%	32%
Expedites digital and other major transformation initiatives of our organisation	35%	39%	45%
Allocates cyber budget to the top risks of the organisation	34%	33%	33%
Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board	34%	34%	36%

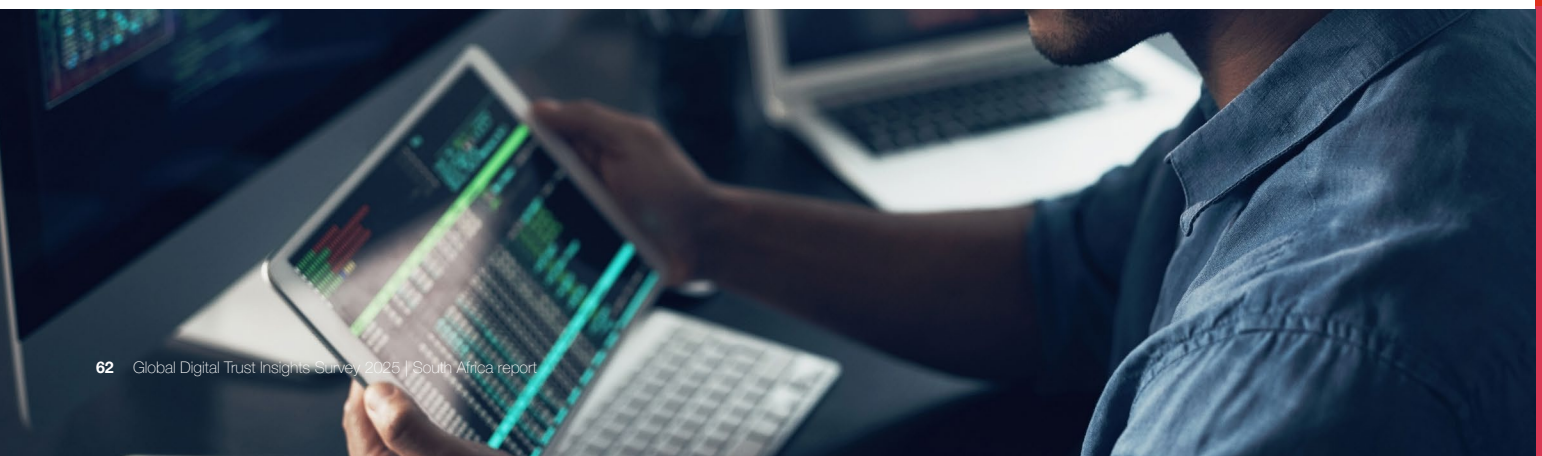


Q3 Finally, please indicate how consistently your organisation's cybersecurity team does the following.

Global (5% more so than Africa) and African organisation cybersecurity teams appear to sometimes focus their efforts on expediting digital and other major transformation initiatives, while South Africa appears to sometimes focus their efforts on delivering insights on changing cyber risk exposure, regulatory developments and mitigation measures to the relevant parties.

Areas where the organisation's cybersecurity team focuses 'Sometimes (41-60% of the time)' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Expedites digital and other major transformation initiatives of our organisation	27%	22%	18%
Anticipates future cyber risks given the macro environment, emerging technology and business strategy	25%	18%	19%
Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board	24%	19%	23%
Allocates cyber budget to the top risks of the organisation	24%	17%	18%
Collaborates with other parts of the business that affect the organisation's cybersecurity posture	23%	18%	17%
Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions	22%	14%	11%



Q4 Finally, please indicate how consistently your organisation's cybersecurity team does the following.

Global (1% more so than Africa) and African organisation cybersecurity teams appear to occasionally focus their efforts on allocating cyber budgets to the top risks with global placing the same percentage on expediting digital and other major transformation initiatives, delivering insights on changing cyber risk exposure, regulatory developments and mitigation measures to the relevant parties, and collaborating with other parts of business. While South Africa appears to occasionally focus their efforts on collaborating with other parts of business.

Areas where the organisation's cybersecurity team focuses 'Occasionally (21-40% of the time)' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board	14%	12%	7%
Collaborates with other parts of the business that affect the organisation's cybersecurity posture	14%	9%	14%
Allocates cyber budget to the top risks of the organisation	14%	13%	9%
Expedites digital and other major transformation initiatives of our organisation	14%	9%	11%
Anticipates future cyber risks given the macro environment, emerging technology and business strategy	13%	10%	7%
Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions	11%	6%	10%

Q5 Finally, please indicate how consistently your organisation's cybersecurity team does the following.

Global (1% more so than Africa and South Africa), African and South African organisation cybersecurity teams appear to rarely focus their efforts on anticipating future cyber risks with global placing the same percentage on allocating cyber budgets to the top risks, collaborating with other parts of business, expediting digital and other major transformation initiatives, and delivering insights on changing cyber risk exposure, regulatory developments and mitigation measures to the relevant parties.

Areas where the organisation's cybersecurity team focuses 'Rarely (0-20% of the time)' (% Ranked top three)

	Global (4,042)	Africa (218)	South Africa (94)
Anticipates future cyber risks given the macro environment, emerging technology and business strategy	5%	4%	4%
Allocates cyber budget to the top risks of the organisation	5%	2%	2%
Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board	5%	2%	1%
Expedites digital and other major transformation initiatives of our organisation	5%	3%	1%
Collaborates with other parts of the business that affect the organisation's cybersecurity posture	5%	3%	0%
Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions	4%	3%	3%

Contacts

Hamil Bhoora

Director
Cyber Security Leader,
PwC South Africa

Johan Pretorius

Director
Cyber Security and SAP,
PwC South Africa

Johan De Waal

Manager
Cyber Security Consultant,
PwC South Africa

Vikas Sharma

Director
Cyber security,
PwC Mauritius

Femi Madariola

Director
Technology Consulting,
PwC Nigeria

Junaid Amra

Director
Forensics Technology Solutions Leader,
PwC South Africa