pwc.com/east-africa-dti-survey

Strengthening Cyber Defences: The Road to Resilience in East Africa

Findings from the 2025 East Africa Digital Trust Insights Survey

October 2024

pwc

Welcome to PwC's East Africa Digital Trust Insights (DTI) Survey

Vikas Sharma
Consulting & Risk Services (C&RS) Leader
Eastern Africa

As cyber threats become more sophisticated and persistent, organisations across East Africa are rising to the challenge. Our latest Digital Trust Insights (DTI) Survey for the East Africa region reveals a significant shift in priorities, with 74% of businesses in the region placing cyber risks at the top of their agenda—well above global averages. It's clear that cybersecurity is no longer just an IT issue; it's a critical business imperative.

East African organisations are navigating a complex landscape, where regulatory compliance, third-party breaches, and social engineering attacks are testing their resilience. In response, 44% of businesses are focusing on regulatory alignment, and many are making bold investments to modernise their infrastructure and upskill their teams.

This report also dives into the promise and risks of emerging technologies like GenAI, which is poised to transform security operations but introduces new vulnerabilities that leaders must be prepared to manage. Despite these challenges, East Africa's leaders are showing strong collaboration and engagement at the board level, positioning the region as a leader in cybersecurity readiness.

Through in-depth survey data and expert analysis, this report provides valuable insights into the strategies and investments shaping the future of cybersecurity in East Africa. Whether you're looking to strengthen your defences or explore new innovations, we hope these findings will inspire actionable steps toward greater resilience.

We invite you to explore the findings and reach out to me or any of the PwC experts featured in this report for further discussion on how to turn these insights into tangible results for your organisation.

Key findings

Threat outlook and emerging technologies

74% of organisations prioritise cyber risks, with threats like third-party breaches, social engineering, and hack-and-leak operations identified as key concerns.

Regulatory developments

92% of respondents report that cybersecurity regulations have challenged, improved, or strengthened their security posture, compared to 78% globally, underscoring regional commitment to improvement.

Cyber leadership

East African boards show strong levels of engagement on key subjects such as cyber metrics (59%) and regulatory actions (46%), both considerably higher than the global averages.

Cyber strategy

While 54% of regional firms prioritise critical processes in their cyber strategies, only 29% conduct tabletop exercises, highlighting resilience gaps.

Cyber investment and priorities

34% of organisations plan a 6-10% budget boost for cybersecurity (closely aligned with global trends), including significant investments in modernising cyber infrastructure.

Cyber risk quantification (CRQ)

46% of organisations lack confidence in using CRQ due to concerns about potential legal or regulatory exposure, and 39% due to the complexity of available tools and data quality issues.

Emerging technologies and GenAI

65% of security executives across Africa indicate that GenAI has widened the cyber attack surface, nearly matching the global rate of 67%.

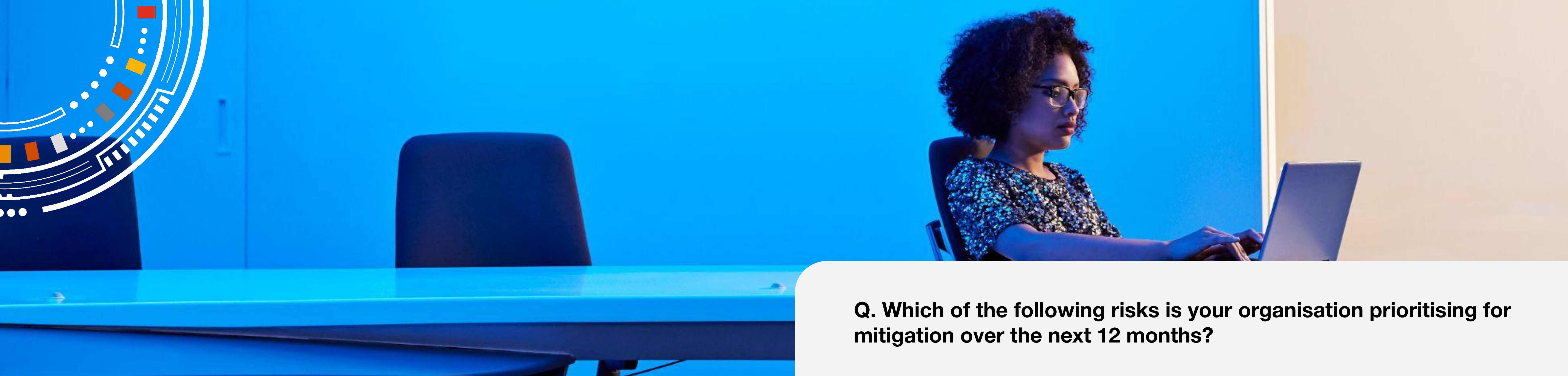
Behaviours

East Africa outperformed global peers by 10-20% across all cybersecurity behaviours, reflecting a robust approach to threat response.

Contents

1

Threat outlook and emerging risks



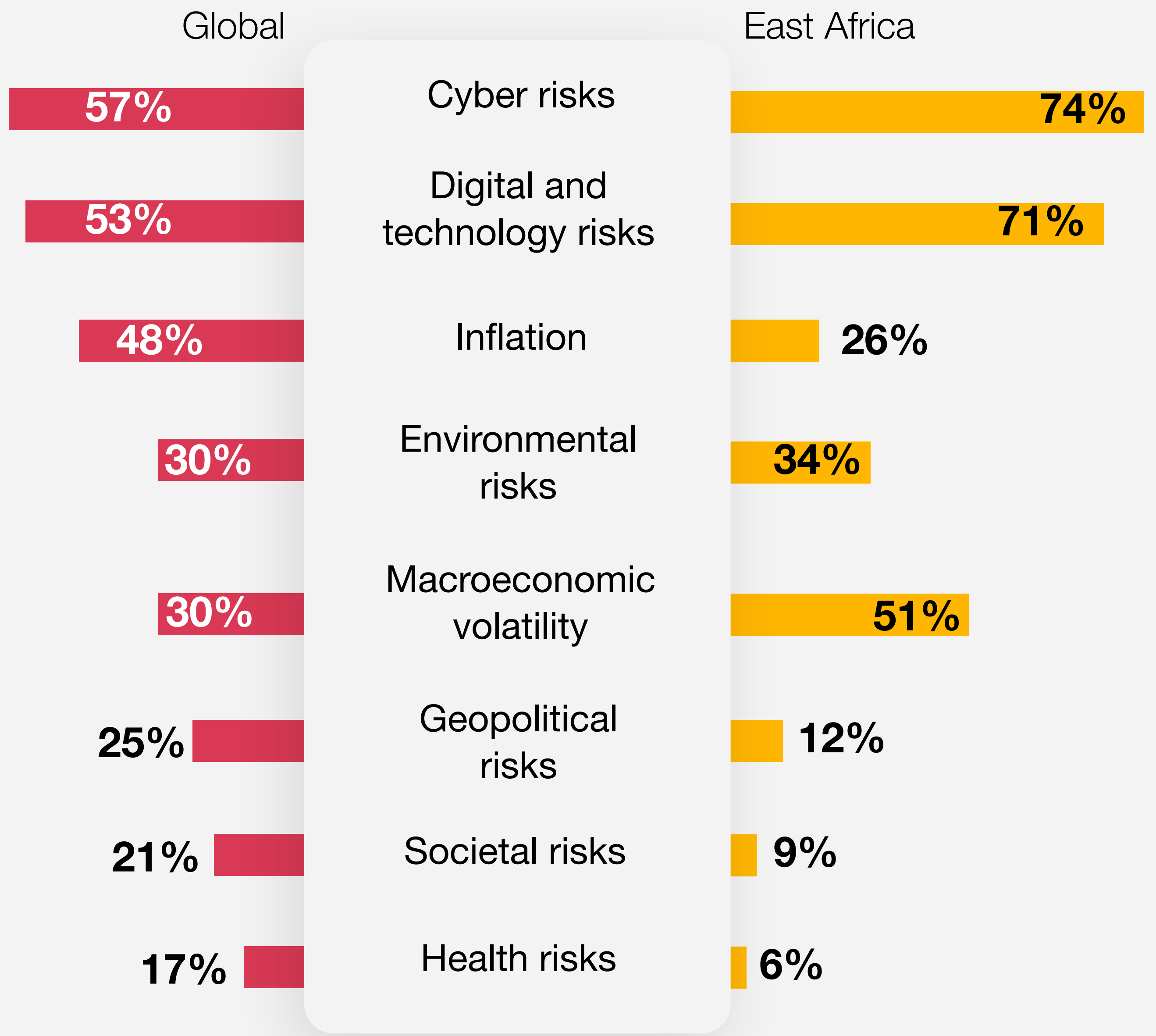
Threat outlook and emerging risks

Adapting to shifting risks

The cybersecurity landscape is continuously evolving, and this survey reveals notable shifts in the risks that organisations are prioritising. Globally, 57% of organisations have identified cyber risks as their top concern, followed by digital and technology risks (53%) and inflation (48%). In East Africa, these concerns are even more pronounced, with 74% of organisations highlighting cyber risks and 71% focusing on digital and technology risks.

A significant distinction in the region is the heightened focus on macroeconomic volatility, with 51% of East African leaders identifying it as a key risk—considerably higher than the global average of 30%. This indicates that economic uncertainty is seen as having a more immediate impact on businesses in East Africa, shaping how they allocate resources and develop their cybersecurity strategies.

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



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

Adapting to shifting risks (cont.)

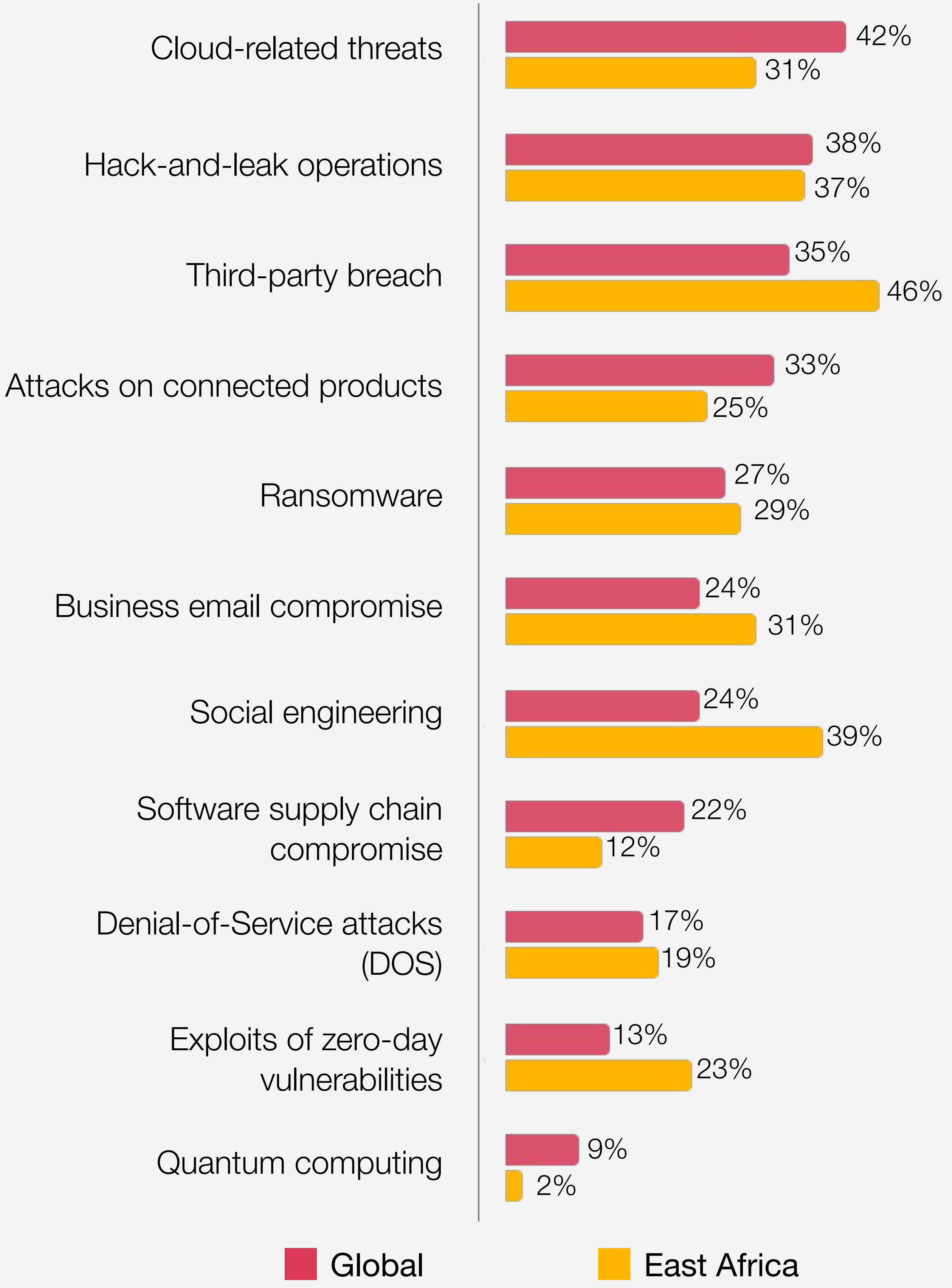
When considering specific cyber concerns, cloud-related threats (42%), hack-and-leak operations (38%), and third-party breaches (35%) dominate at the global level. These broadly reflect the regional results, though with social engineering attacks (39%) perceived as posing a more immediate threat than cloud-related threats by organisations in East Africa.

These findings highlight the growing awareness of supply chain vulnerabilities and the increasing sophistication of cyber attacks that exploit human behaviour.

> "Agility should be at the core of cybersecurity strategies for organisations across East Africa. By concentrating on pressing threats like third-party breaches and social engineering, while adjusting to economic challenges, they can bolster their resilience and secure their long-term defences.

Edward Kerich
C&RS Leader
PwC Kenya

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



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

2

Regulatory developments

Regulatory developments

Leveraging the regulatory guardrails

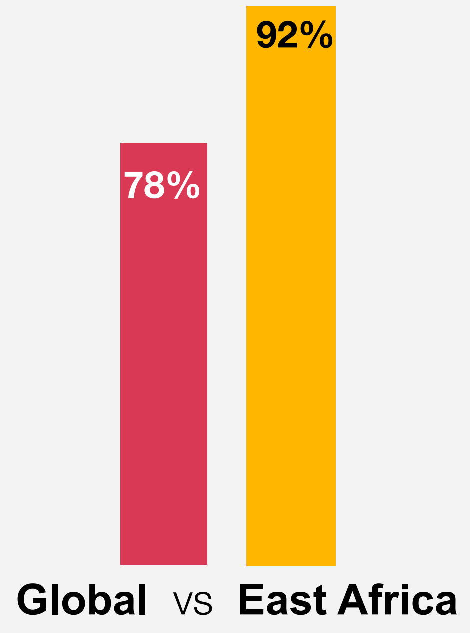
While the regulatory push towards resilience across the digital and physical domains may not be as evident in East Africa as it is globally, data from the survey indicates a positive trend. Despite the complexities of compliance, regulatory requirements in the region are playing a crucial role in driving advancements in cybersecurity capabilities across various industries.

An overwhelming 96% of security leaders and CFOs surveyed across Africa report that cybersecurity regulations have prompted them to increase their investments in security measures over the past year - mirroring global findings. Moreover, in East Africa, 92% of respondents believe that these regulations have effectively challenged, improved, or strengthened their cybersecurity posture.

This contrasts with global statistics, where only 78% of leaders share this belief.

Q. Describe the impact of new cybersecurity regulations on your organisation over the last 12 months

% of respondents who felt these regulations had challenged, improved, or strengthened their organisation's cybersecurity posture.



Source: PwC's Digital trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

Leveraging the regulatory guardrails (cont.)

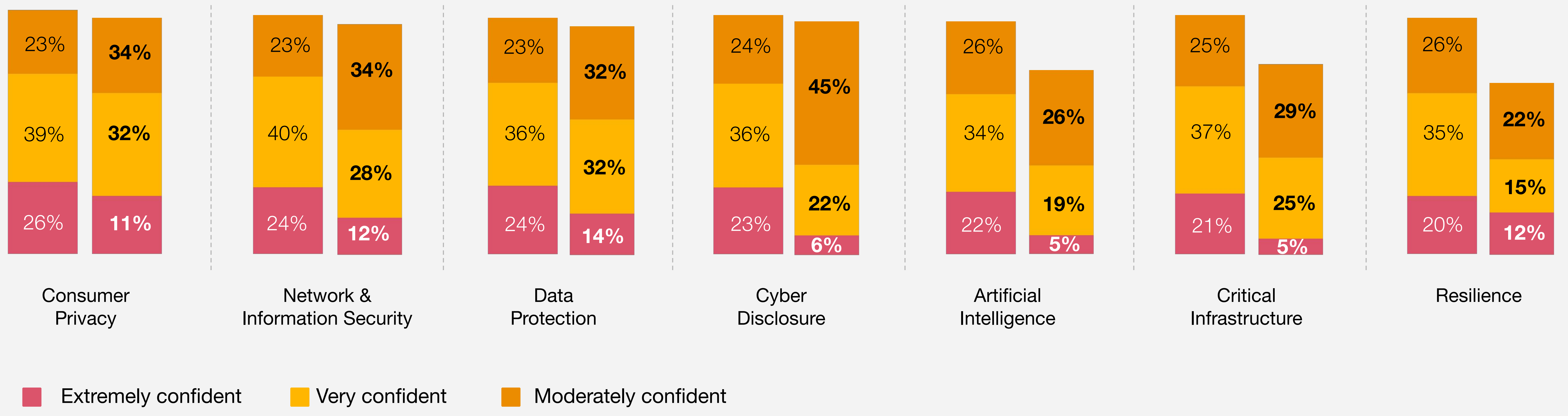
Interestingly, our survey found that a high proportion of respondents in East Africa were either extremely, very, or moderately confident in their organisations' ability to be in compliance with regulations that focus on Data Protection (78%), Consumer Privacy (77%), Network and Information Security (74%), and Cyber Disclosure (73%).

However, confidence levels concerning regulation around Artificial Intelligence (AI), Critical Infrastructure, and Resilience were significantly lower among business and security leaders in East Africa compared to their global peers. Nearly 10% reported being "not at all confident" in their organisation's ability to comply with AI-related regulations, such as the European Union AI Act.

Q. 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 you operate?

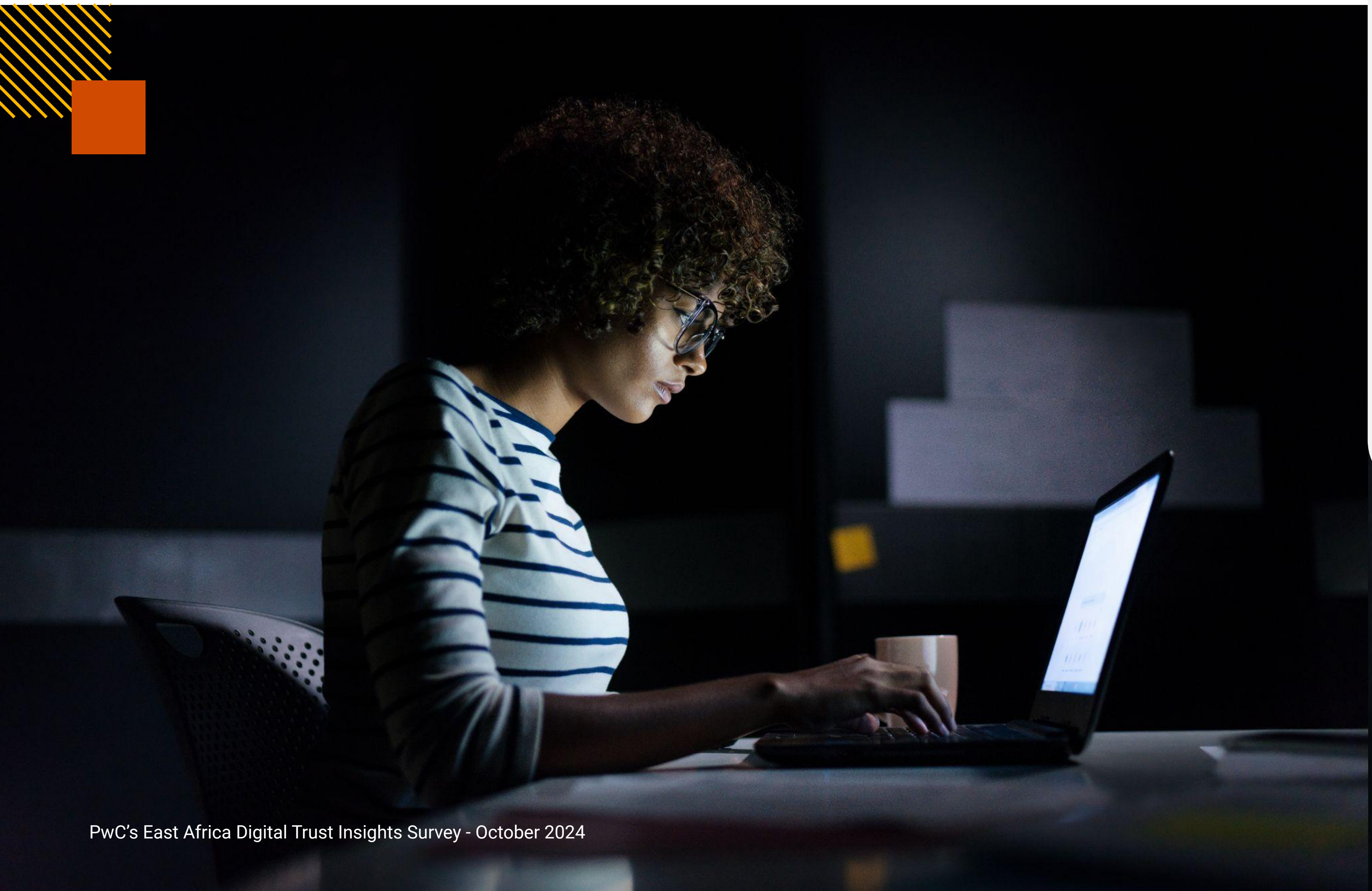
% of respondents who answered "extremely", "very", or "moderately".

Global (L) vs **East Africa (R)**



Leveraging the regulatory guardrails (cont.)

Notwithstanding the nuances of the way the question is phrased (“*ability* to be in compliance with” rather than *actual* compliance), these figures provide a sense of reassurance, emphasising how regulations - even those that target entities outside an organisation’s own geographic sphere of operations - can effectively promote the development of cybersecurity capabilities and help bolster enterprise resilience in the face of an increasingly complex threat landscape.



> “
>
> Regional businesses can build stronger cybersecurity frameworks by using international regulations as benchmarks. Aligning with global standards will not only enhance defences, but also position them to better meet evolving regulatory demands, while fostering trust with stakeholders by showing a commitment to best practices.

Julien Tyack
C&RS Partner (Risk)
PwC Mauritius

3

Cyber leadership

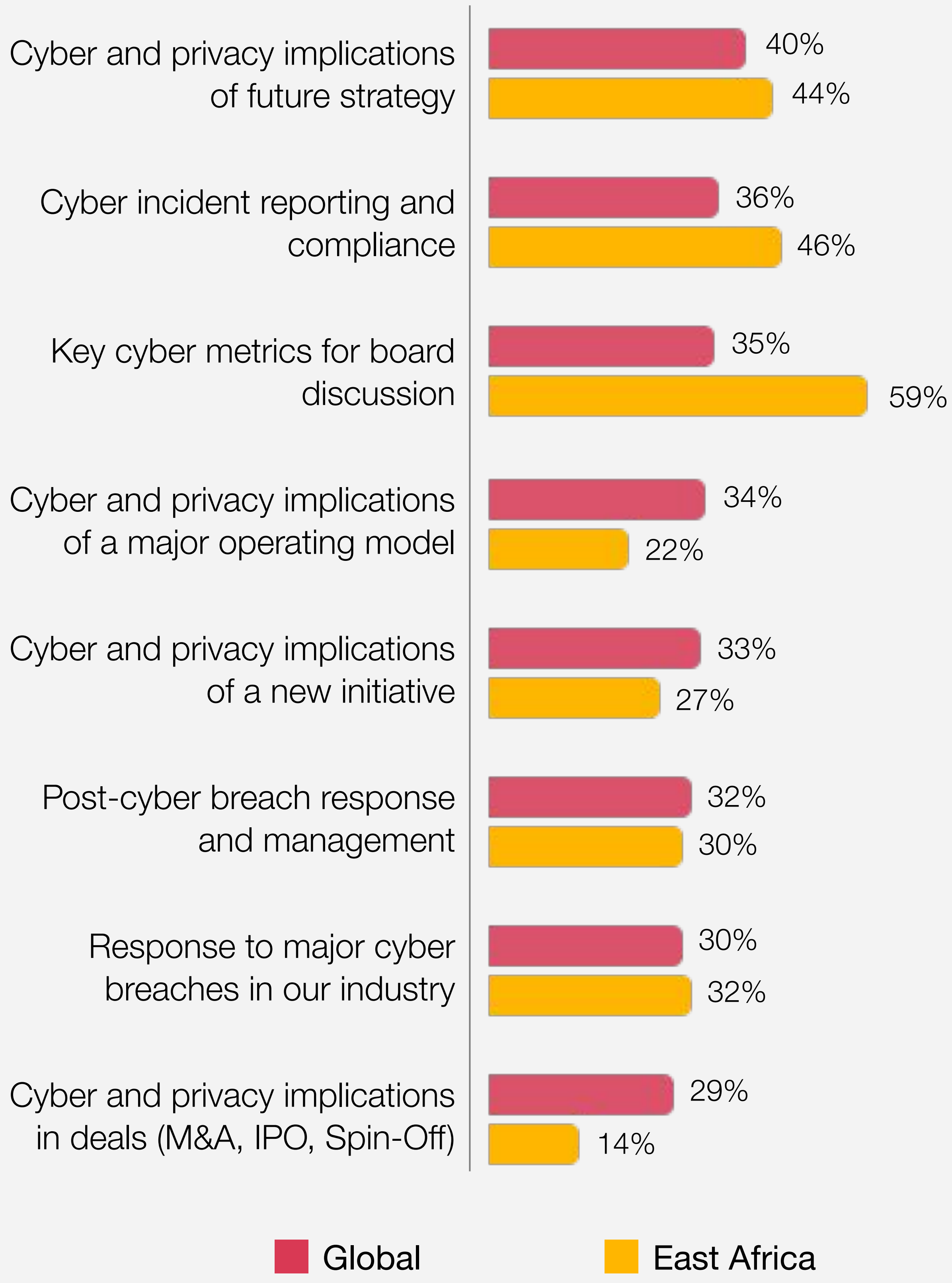
Empowering leaders

Leadership is central to shaping strong cybersecurity strategies, driving resilience, and fostering accountability within organisations. Globally, there is increasing recognition of the importance of leadership teams, particularly at the board level, in actively engaging with cyber and privacy matters. However, the extent of this engagement varies significantly, especially in East Africa, where leadership involvement demonstrates both strengths and areas for improvement.

In East Africa, 59% of organisations report that key cyber metrics are discussed at the board level, considerably higher than the global average of 35%. This marks a positive step towards embedding cybersecurity into leadership conversations. Nevertheless, only 22% of East African organisations involve their boards in discussions about the cyber and privacy implications of major operating model changes, compared to 34% globally. This gap underscores the need for leadership to integrate cybersecurity into broader business transformation strategies.

In terms of specific leadership engagement, East African organisations display a high level of responsiveness to regulatory concerns, with 46% reporting that their CEO gets involved when regulators contact their organisation for cyber incident reporting or enforcement action, for example, surpassing the global average of 36%.

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



Source: PwC's Digital trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

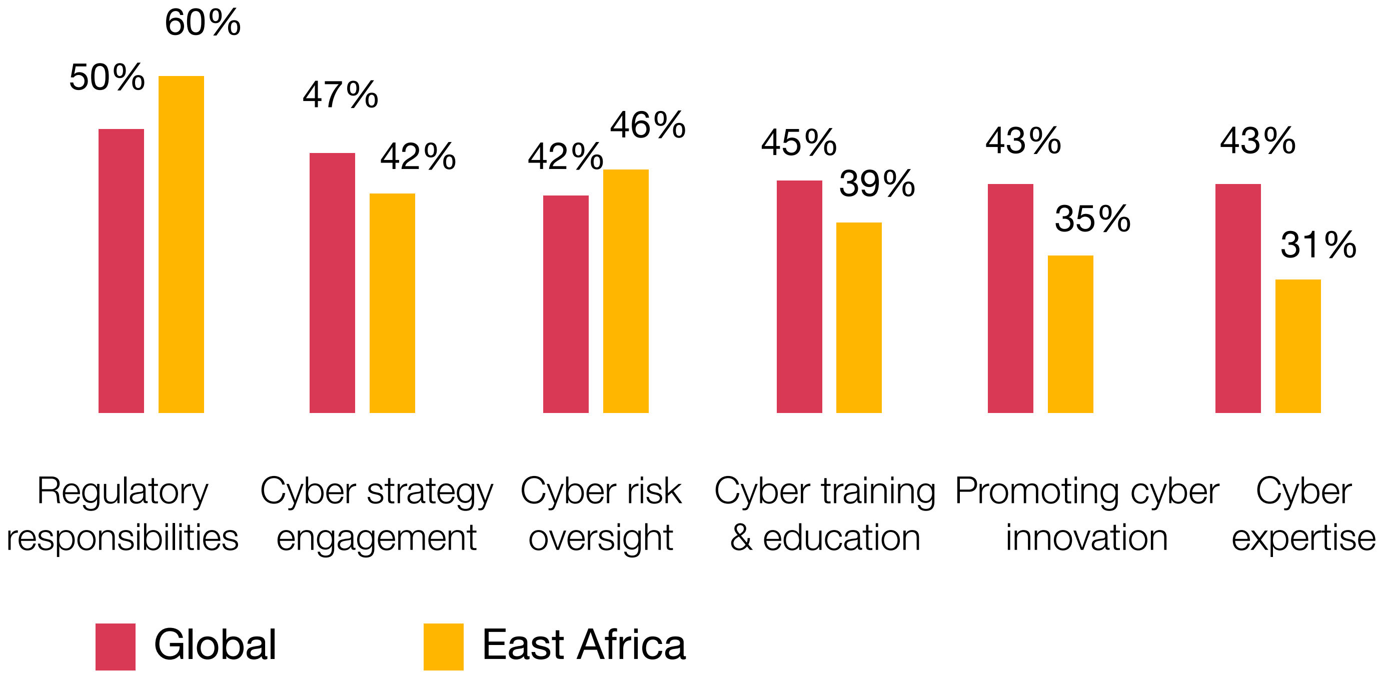
Empowering leaders (cont.)

However, in terms of effectiveness in areas such as promoting cyber innovation and enhancing cyber expertise, boards in East Africa rated lower, with only 35% and 31% considered "very effective".

To further strengthen cyber leadership, East African boards must adopt a more proactive and forward-looking approach. This involves not only focusing on regulatory compliance but also championing innovation and embedding cybersecurity within the overall business strategy. By taking these steps, organisations will be better positioned to build resilience and address emerging cyber risks.

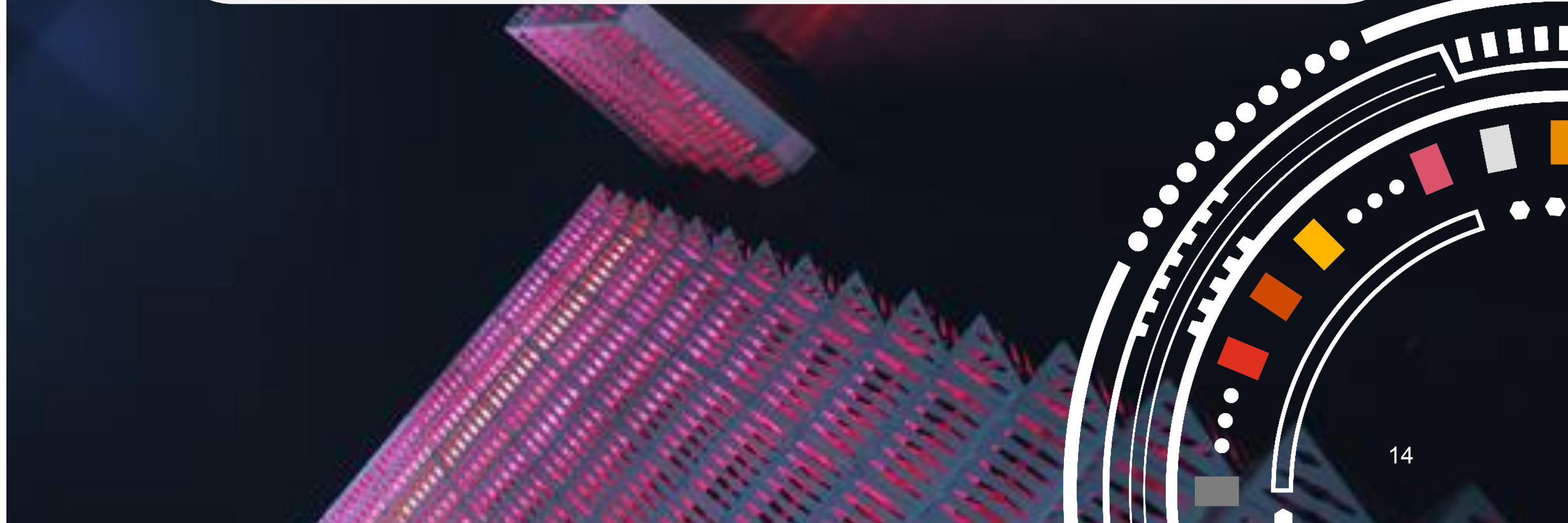
Q. How effective do you think your organisation's board is across the following areas?

% of those who responded "very effective".



> "
>
> In East Africa, progress at the board level is promising, but positioning cybersecurity as a driver of business transformation will be key to managing new risks and enhancing resilience. For effective cybersecurity leadership, organisations must adopt a proactive, innovative stance that integrates security into their broader business strategies.

Vikas Sharma
C&RS Leader
PwC Eastern Africa



4

Cyber strategy

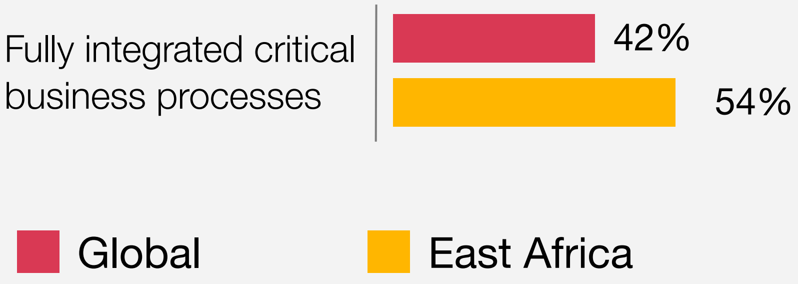
Cyber strategy

Strategic foresight

Organisations globally are recognising that a strong cyber strategy, supported by leadership, is essential for sustaining resilience. However, many are still only partially implementing critical cyber measures, leaving gaps that could expose them to emerging risks. This challenge is similarly reflected in East Africa, where companies are making progress in some areas but still have opportunities for improvement in others.

In East Africa, 54% of organisations have fully integrated the identification of critical business processes into their cyber strategy, surpassing the global average of 42%. However, other key resilience actions remain underdeveloped. Only 29% of organisations in the region are conducting tabletop exercises, and 32% are engaging in peer collaboration—actions that would significantly improve their preparedness for real-world cyber incidents and strengthen collective defences.

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



Source: PwC's Digital trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

Strategic foresight (cont.)

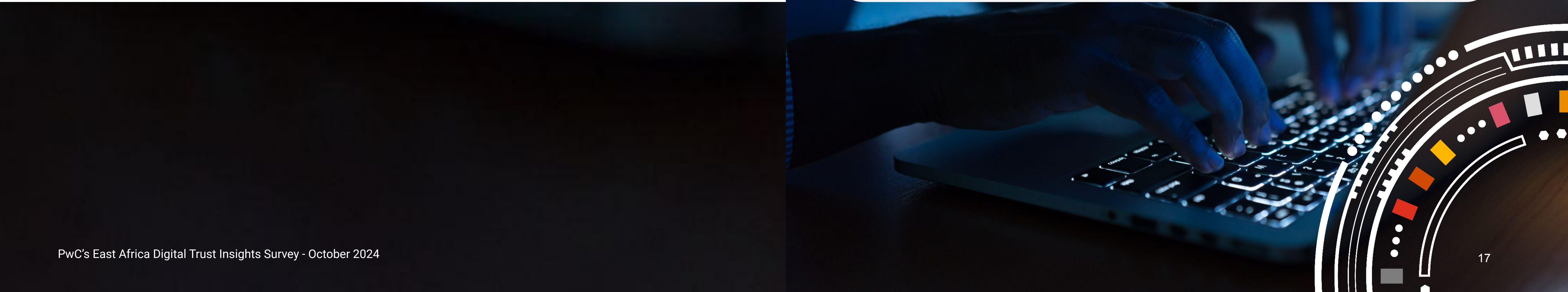
Despite these gaps, East African organisations are excelling in certain areas. For example, 52% of companies prioritise stakeholder reporting, which is crucial for maintaining transparency and trust, particularly with regulators. Additionally, 45% of organisations have established resilience teams, well above the global average of 34%. To fully safeguard against evolving threats, however, companies must go beyond partial implementation and accelerate the adoption of these critical resilience measures.

East African organisations should place greater emphasis on cyber recovery planning and collaboration across industries. By fully incorporating these actions into their strategies, they will be better positioned to address existing gaps and navigate the complex cyber threat landscape.

These efforts are not only key to mitigating risk but also vital for ensuring operational continuity and maintaining stakeholder trust.

> “
>
> To future-proof their defences, East African businesses should focus on advanced resilience strategies like tabletop exercises and cross-industry partnerships, reinforcing both preparedness and stakeholder confidence.

Laolu Akindele
C&RS Partner (Consulting)
PwC Kenya



5

Cyber investment and priorities

Cyber investment and priorities

Investing in resilience

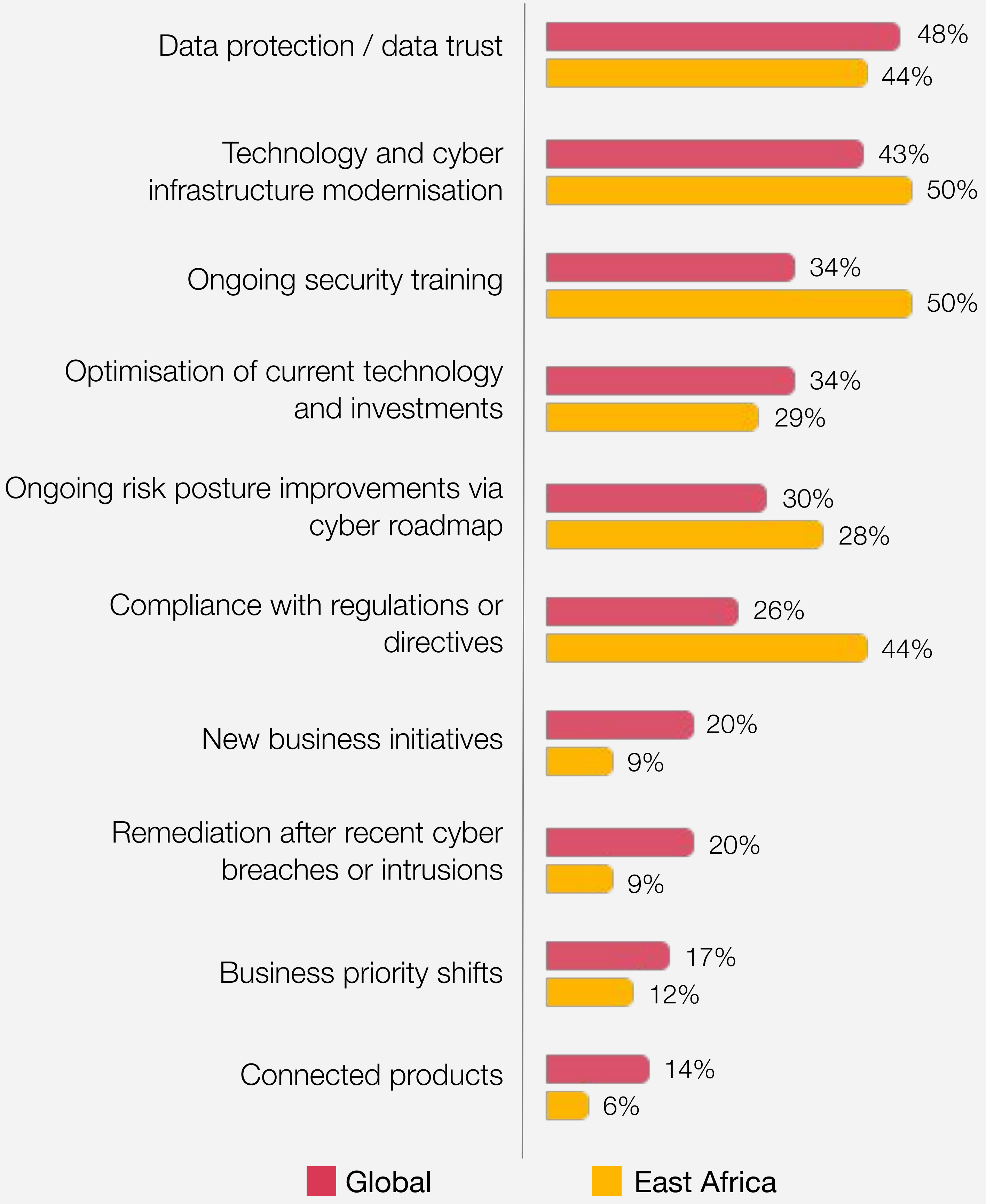
As cyber threats grow in complexity, organisations globally are responding by increasing their cybersecurity budgets. According to the survey, 30% of organisations worldwide plan to raise their spending by 6-10%, and East Africa is closely aligned, with 34% of organisations expecting to increase their budgets by a similar margin.

Globally, regulatory compliance is a priority for 26% of organisations; in East Africa, however, 44% of organisations emphasise compliance. This heightened focus reflects the region's urgent need to navigate an expanding set of local and international regulations that demand more stringent security measures.

In response to these regulatory pressures, 50% of East African organisations are investing heavily in modernising their cyber infrastructure. Outdated systems are increasingly viewed as critical vulnerabilities, particularly as risks such as third-party breaches and social engineering attacks continue to rise in the region.

To complement these infrastructure upgrades, organisations are also focusing on cybersecurity training, with 50% prioritising efforts to build a more cyber-aware workforce. This training includes areas like phishing simulations, incident response drills, and sector-specific security education, all aimed at reducing human error and enhancing the organisation's ability to respond to evolving threats.

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



Source: PwC's Digital trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

Investing in resilience (cont.)

Globally, data protection remains a key focus, with 48% of organisations investing in safeguarding sensitive information. East Africa follows closely, with 44% of businesses focusing on data security. At the same time, the region is placing a strong emphasis on future-proofing its infrastructure and aligning with compliance requirements to prepare for both current and future challenges.

While East African organisations are in step with global trends in increasing cybersecurity spending, they also face the complex intersection of regulatory demands and emerging threats. By investing in modernising their infrastructure and enhancing workforce training, businesses in the region are positioning themselves to build a more resilient security posture. This approach will help them navigate an increasingly complex threat landscape and meet rising compliance expectations.

> Investing in both infrastructure and comprehensive cybersecurity training is crucial for businesses in the region to meet regulatory demands and address emerging threats. Acting now will help build the resilience they need to thrive in a rapidly changing environment.

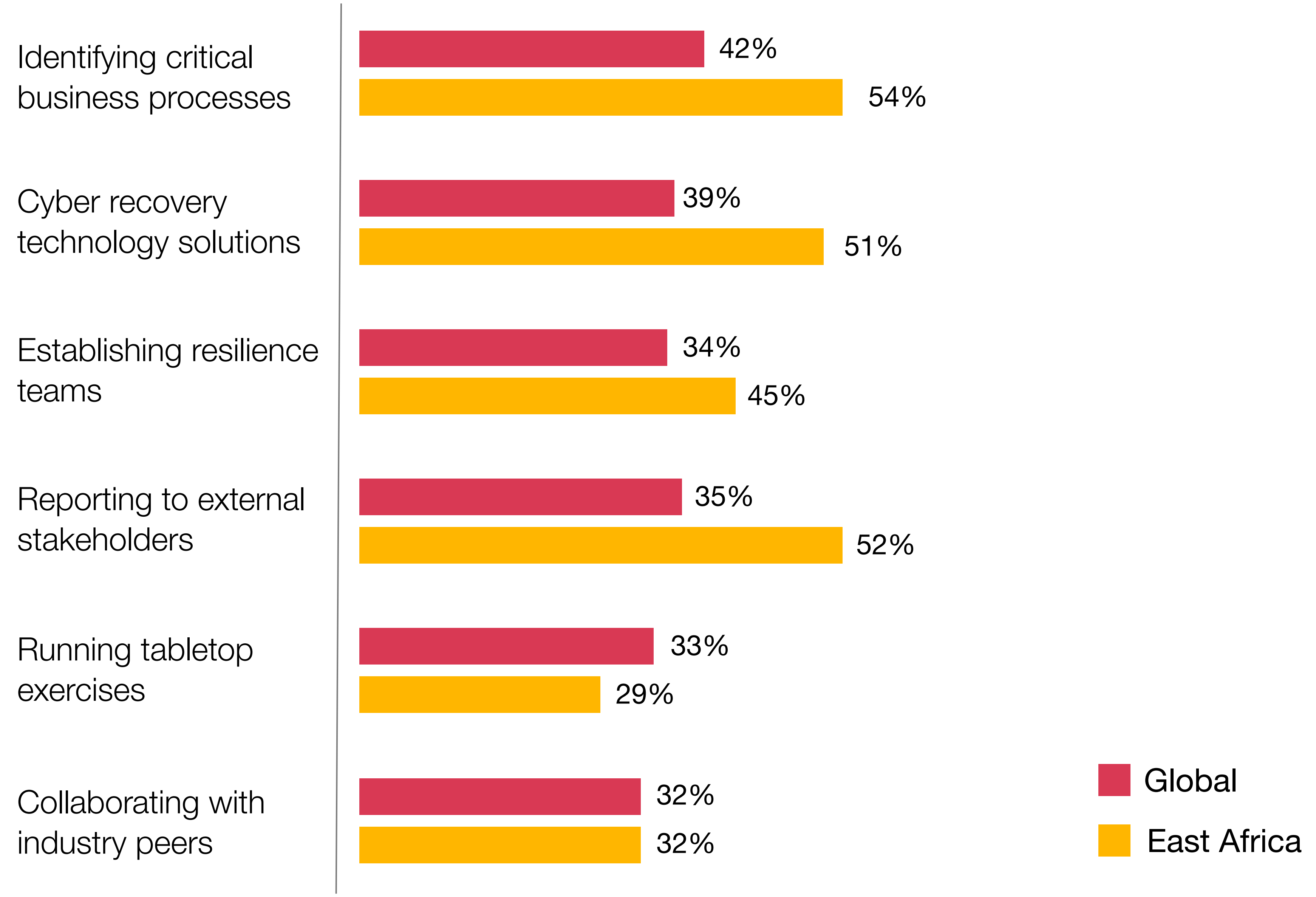
Lyndon Lane-Poole
C&RS Partner (Risk)
PwC Zambia

Snapshot of key resilience actions:

Global vs East Africa

East Africa's cyber resilience initiatives show both strengths and areas where improvement is needed. This snapshot compares key resilience actions between East African organisations and global counterparts, highlighting where East Africa is excelling and where further development is necessary.

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



	Global	East Africa
Identifying critical business processes	42%	54%
Cyber recovery technology solutions	39%	51%
Establishing resilience teams	34%	45%
Reporting to external stakeholders	35%	52%
Running tabletop exercises	33%	29%
Collaborating with industry peers	32%	32%

Source: PwC's Digital trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

6

Cyber Risk Quantification

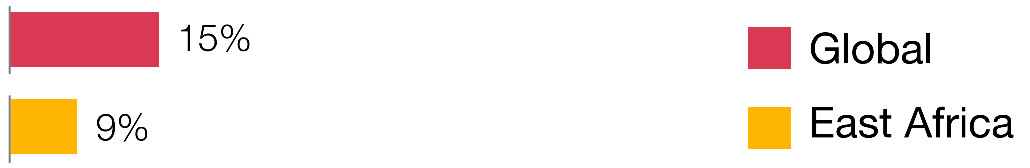
Lost in translation

As cyber threats rapidly evolve in scope and sophistication, Cyber Risk Quantification (CRQ) has become a critical tool that organisations cannot afford to overlook. But despite its widely acknowledged benefits, several challenges have impeded broader adoption: this year's survey revealed only 9% of respondents in East Africa are measuring the financial impact of cyber risks to a significant extent.

That said, across Africa more broadly the numbers are slightly higher (19%) but with an overwhelming majority of those who do in fact measure the impact of cyber risk deploying security posture assessments as their primary method for doing so (86%), rather than scenario-based quantification methods such as FAIR, which calculates the risk by analysing Loss Event Frequency (how often a risk event might happen) and Loss Magnitude (the potential financial impact if it does).

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

% who responded “to a significant extent”.



PwC’s East Africa Digital Trust Insights Survey - October 2024

Much of the hesitancy around using CRQ to quantify the potential financial impact of cyber risk in Africa appears to stem either from uncertainty around the intended scope of risk quantification outputs, (asset - vs business process-level, for example), or data issues such as poor quality, gaps, inconsistencies, or incompatibility.

Our survey also showed that there is perhaps some reticence at board level in Africa to use CRQ due to concerns that the outputs might create potential legal or regulatory exposure (46%), and a lack of confidence in actually using this approach due to the complexity of the tools available (39%).

> “
>
> Quantified risks are more easily understood by management – organisations that don't measure cyber risks, or have not fully developed this capability, are leaving critical intelligence on the table, particularly when it comes to informing board decisions and capital allocation.

Diya Guttoo
C&RS Partner (Consulting)
PwC Mauritius

7

Emerging technologies and GenAI

Be smart, be secure

Despite growing acknowledgement of its transformative potential, Generative AI (GenAI) has yet to gain significant traction in the region. Based on the results of this study, mapped against those of our East Africa CEO Survey conducted earlier this year, investment in this space over the last 12 months has not been matched by a commitment to evolve to the next stage and actually integrate GenAI into existing technological strategies.

This cautious approach reflects a broader regional sentiment around heightened cybersecurity risks associated with GenAI.

Indeed, 65% of the security executives surveyed across the entire African continent reported that GenAI has expanded the cyber attack surface over the past year (against 68% globally), making companies more vulnerable to sophisticated threats. Alongside concerns about data integrity, privacy and compliance, GenAI can also reduce barriers to entry for less sophisticated threat actors, enabling them to craft effective phishing attacks and deepfakes at scale.

Though the picture for East Africa is inconclusive, data from our Africa-wide survey shows that security leaders across the continent are prioritising the use of GenAI in supporting four key aspects of cyber defence, namely: threat intelligence (47%), SOC modernisation (45%), threat detection and response (37%), and security log analysis (37%).

Notwithstanding, several factors may explain the hesitance we are seeing from African businesses in fully adopting GenAI. A reported lack of training resources for employees (45%), insufficient standardised internal policies governing its use (42%), and challenges in integrating the technology with existing systems and processes all contribute.

Additionally, a lack of trust in GenAI among internal leadership and employees continues to be a significant inhibitor (36%).

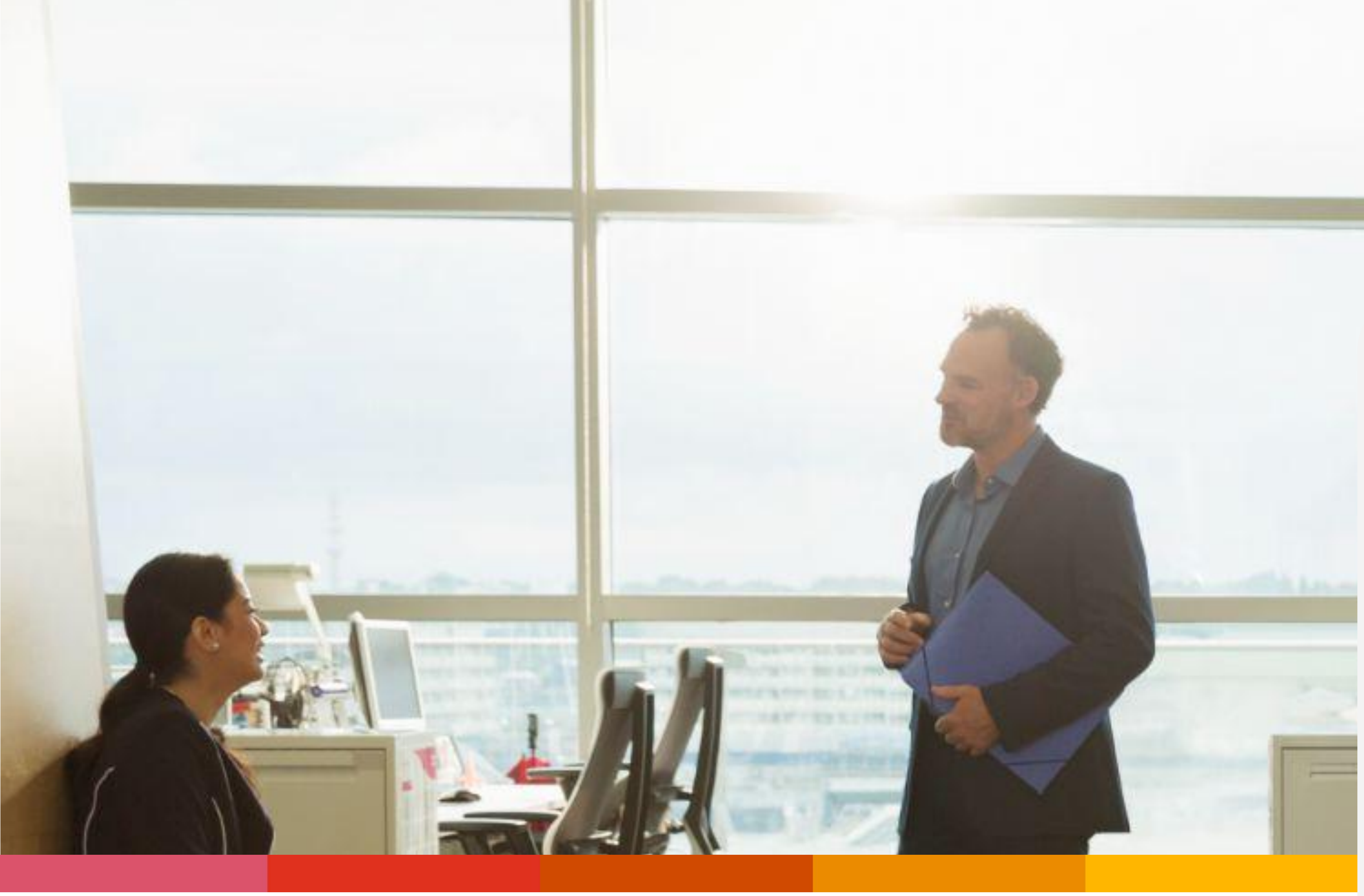
> “
>
> As emerging technologies significantly alter the cybersecurity landscape, business leaders must take an engaged and proactive stance in navigating the complexities introduced by these innovations, making sure their organisations capitalise on new opportunities while also mitigating potential risks.

Jean-Pierre Young
C&RS Partner (Consulting & Innovation)
PwC Mauritius

8

Behaviours

01 SPACE AROUND THE LOGO & COLOUR
02 DYNAMIC LOGO
03 IF THE UNAVOIDABLE HAPPENS



Behaviours

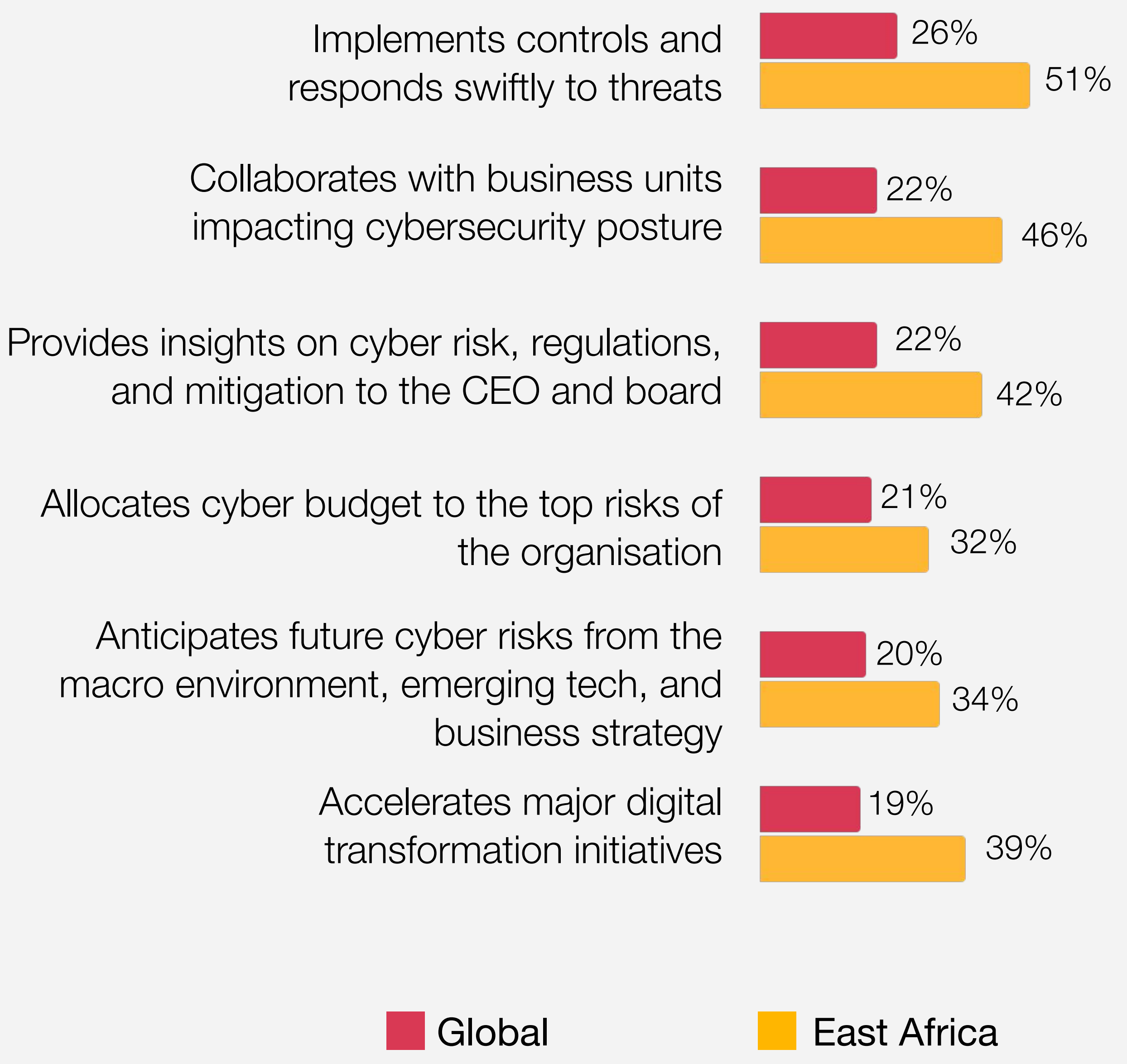
Shared responsibility, collective action

Based on the results of our survey, security leaders in East Africa are almost twice as likely than their global counterparts to put controls in place and respond quickly to threats so their organisations can withstand serious cyber disruptions (51% against the global figure of 26%).

Similarly, they are more than twice as likely to collaborate with other parts of the business that affect the organisation's cybersecurity posture (46% vs 22%). In fact, East Africa outperformed their global peers by 10-20% in every category of this section of the survey that focuses on cybersecurity behaviours.

Q. Please indicate how consistently your organisation's cybersecurity team does the following.

% of respondents who selected "usually (81-100% of the time)".



Source: PwC's Digital trust Insights Survey, Final Results, August 2024 | © 2024 PwC. All rights reserved.

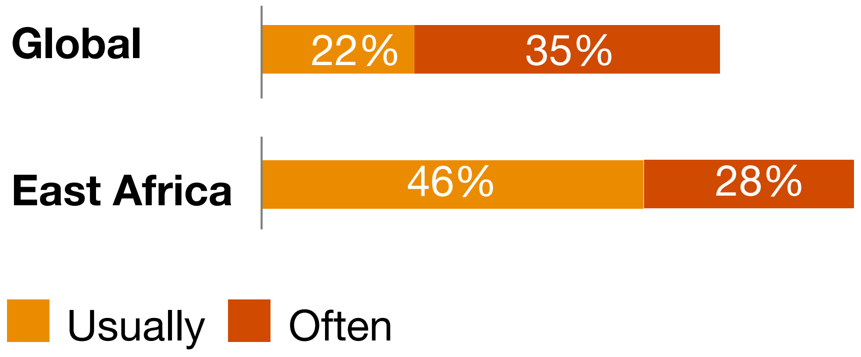
Shared responsibility, collective action (cont.)

This data provides a refreshingly reassuring picture of the mature stance businesses across the continent's Eastern flank are taking when it comes to mitigating and responding quickly to threats. Indeed, quick responses are not just a goal, they are a necessity. Delayed reactions to threats can cost more than just time; they can erode trust and severely disrupt your business. Speed and confidence in leadership should be non-negotiable priorities and it seems East Africa may just be ahead of the game in this respect.

One of the key problems faced by many organisations when it comes to preparing for, protecting against and responding to threats, is that cyber resilience - and resilience programmes more broadly - are too often siloed, with little coordination across functions. In this survey, however, 74% of East African security leaders reported that they "usually" (81-100% of the time) or "often" (61-80% of the time) collaborate with colleagues elsewhere in the business on matters relating to cybersecurity. This underscores a collective understanding that cybersecurity is a shared responsibility, necessitating a unified approach to tackle challenges that transcend individual departments, and even organisations.

Q. Please indicate how consistently your organisation's cybersecurity team collaborates with business units impacting cybersecurity posture

% of respondents that selected "usually (81-100% of the time)" or "often (61-80% of the time)".



> Through collaboration and resource-sharing, security leaders in East Africa can strengthen defences against advanced cyber threats. By partnering with other organisations and government bodies to share threat intelligence and best practices, they will contribute to a more robust digital trust landscape.

Jamila Aroi
C&RS Partner (Risk)
PwC Kenya

9

Methodology

Methodology

The **2025 Digital Trust Insights Survey** is designed to gather the perspectives of business and technology leaders worldwide on the challenges and opportunities for enhancing and transforming cybersecurity within their organisations over the next 12 months. The survey covers key topics such as threat outlook, investments, emerging technologies, regulations, and more.

The final results are based on 4,042 survey responses from 77 territories, spanning a diverse range of industries, sub-industries, and organisation sizes. Of these responses, 89% (3,585) were collected via an external panel provider, while 11% (457) were gathered through PwC's territory network outreach. Responses were collected between 7 May and 12 July 2024.

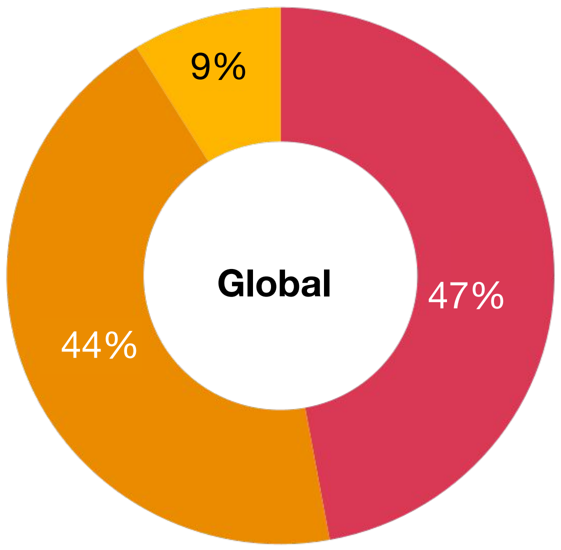
The data shown in this report focuses on East Africa, including responses from Kenya, Mauritius, Rwanda, Tanzania, Uganda, and Zambia.

Due to rounding, percentages may not add to 100%.

More information about PwC's 2025 Global Digital Trust Insights Survey is available here.

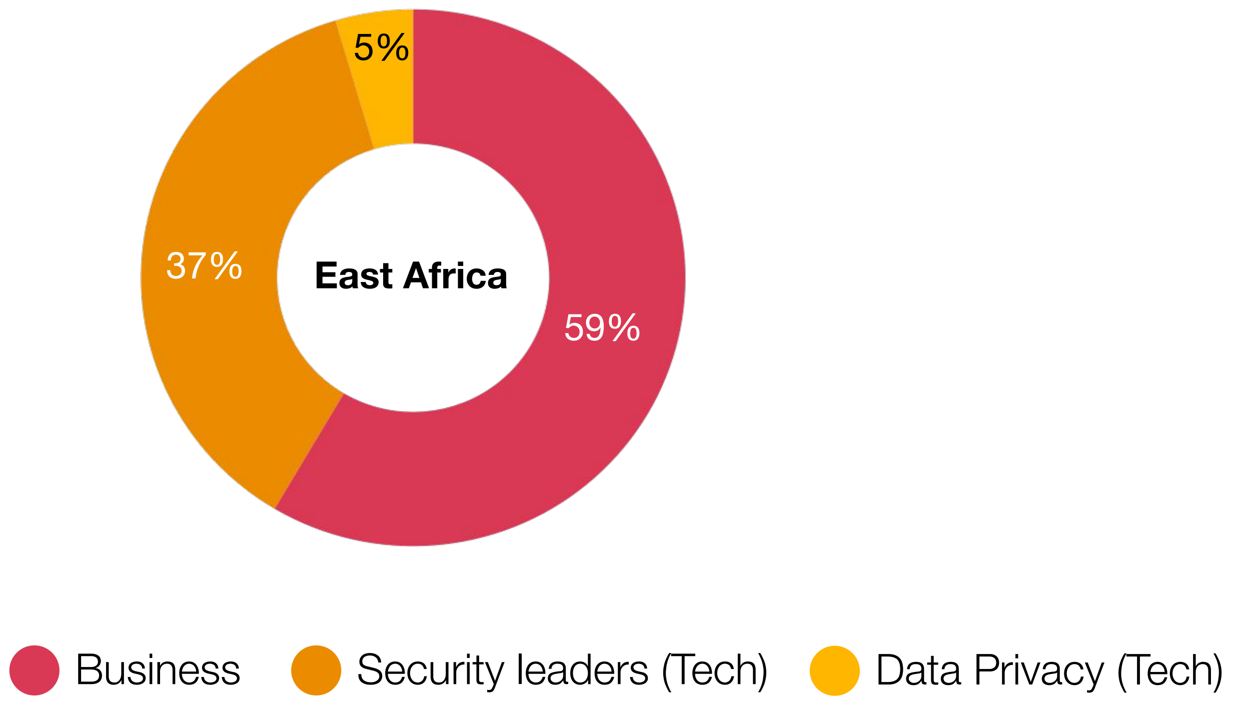
Q. Choose the title that best describes your role.

Base: All respondents= 4042



Q. Choose the title that best describes your role.

Base: East Africa respondents= 65



Your PwC Consulting & Risk Services (C&RS) contacts

Vikas Sharma
C&RS Leader
PwC Eastern Africa
v.sharma@pwc.com

Edward Kerich
C&RS Leader
PwC Kenya
edward.kerich@pwc.com

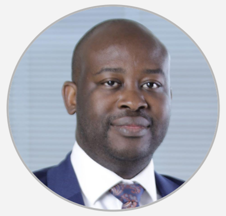
Jean-Pierre Young
C&RS Partner (Consulting)
PwC Mauritius
jean-pierre.young@pwc.com

Lyndon Lane-Poole
C&RS - Partner (Risk)
PwC Zambia
lyndon.l.lane-poole@pwc.com

Uthman Mayanja
Country Leader
PwC Uganda
uthman.mayanja@pwc.com

Julien Tyack
C&RS Partner (Risk)
PwC Mauritius
julien.tyack@pwc.com

Diya Guttoo
C&RS Partner (Consulting)
PwC Mauritius
diya.guttoo@pwc.com



Laolu Akindele
C&RS - Partner (Consulting)
PwC Kenya
laolu.x.akindele@pwc.com

Jamila Aroi
C&RS Partner (Risk)
PwC Kenya
jamila.aroi@pwc.com

Benjamin Mkwizu
C&RS Director
PwC Tanzania
benjamin.mkwizu@pwc.com

Acknowledgements

Insights prepared by the Consulting & Risk Services (C&RS) and Clients and Markets Development (CMD) East Africa teams.

Alex Johnson
Senior Manager
PwC Mauritius
alex.j.johnson@pwc.com

Nelly Lacaze
Senior Manager
PwC Mauritius
nelly.lacaze@pwc.com

Ariane Serret
Senior Manager
PwC East Africa
ariane.serret@pwc.com

Clients and Markets Development Regional Leads in **Kenya, Mauritius, Rwanda, Tanzania, Uganda,** and **Zambia.**

The information provided in this report should not be used as a substitute for consultation with professional advisers. Before making any decision or taking any action, you should consult a professional advisor who has been provided with all pertinent facts relevant to your particular situation. The information is provided as is, with no assurance or guarantee of completeness, accuracy or timeliness of the information and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose.

pwc.com/east-africa-dti-survey

2025 East Africa Digital Trust Insights Survey