

Africa Business Agenda: Technology Perspective 2023

How CEOs in Africa perceive the threats and opportunities presented by new technology adoption

April 2023



Contents

Introduction	3
New technology adoption in Africa	4
Companies in Africa need to view cyber risks as the number one business threat	7
Opportunities from increased technology adoption	9
Conclusion	10
Contacts	11



Introduction

Globally, CEOs have a genuine interest in considering how technology impacts their businesses, according to our recently published *PwC 26th Annual Global CEO Survey*. The concerns of disruption and emerging technologies of 282 sub-Saharan Africa CEOs who participated in the survey are shared in this publication on tech-enabled transformation, which is the third of six in PwC's Africa Business Agenda series.

Insights from the survey reflect that business leaders are most concerned with the rise and importance of technology automation, data, and the shift to the cloud. CEOs are also recognising cyber risks that come with deploying new technologies, where their client interface could potentially be exposed to cybercriminals.

Finally, the results of the survey highlight that companies cannot invest in technology without considering people and processes. It's the trifecta of people, processes, and technology (supported by a strong cybersecurity framework) that will result in a successful, efficient, and value-driven tech-enabled transformation.

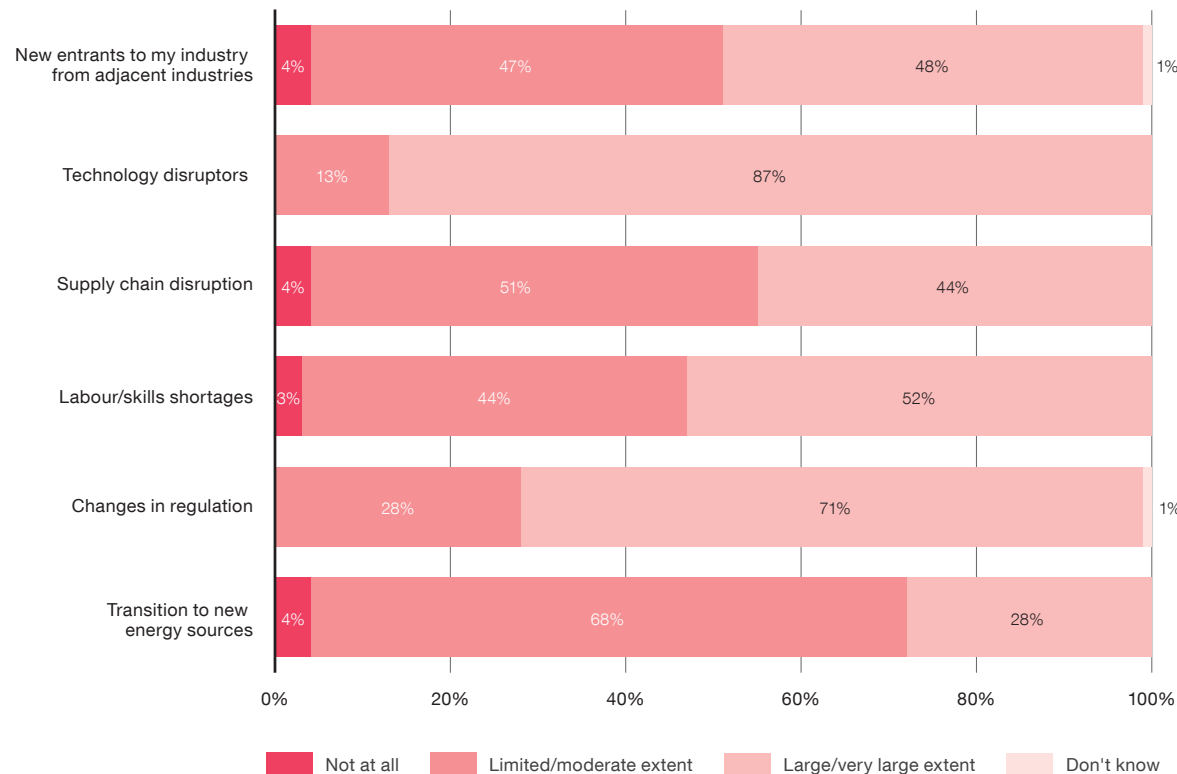


New technology adoption in Africa

In the financial services sector, 87% of CEOs in Africa say they're seeing a significant technology disruption to their business models as opposed to 50% globally.

To what extent do you believe the following will impact (i.e., either increase or decrease) profitability in the industry over the next ten years?

Africa FS



Source: PwC's 26th Global CEO Survey



Most organisations are investing in improved technology capability, with this process typically having started during the early days of the COVID-19 pandemic in 2020, necessitated by a rapid shift in customer behaviour to digital capabilities. Organisations were forced to start investing in their digital capabilities and build their client-facing assets. This focus on client engagement solutions started to highlight the importance of data and the shift to cloud.

Mark Allderman – Technology Transformation Capability Leader, PwC Africa

As organisations are trying to drive growth, they're looking more at adopting cloud solutions, resulting in massive investments in front-end capabilities. This is happening in automation solutions and platforms, allowing increased engagement across platforms, in all industries; giving organisations greater strength beyond the traditional industry boundaries.

How digitalisation is impacting business productivity and performance

The advent of technology and digitalisation has revolutionised the way businesses operate. With the proliferation of digital tools, organisations have become more efficient and productive, resulting in improved overall performance.

Increasing technology adoption can result in additional opportunities for workers to spend more hours on value-added activities, instead of mundane repetitive tasks. However, this increase in efficiency comes with concern about potential job losses for people that perform manual tasks for core processes. The rapid increase in deploying technology capabilities also opens up opportunities for employment in new and developing roles, such as data scientists. This creates opportunities for companies in Africa to start growing these capabilities.

A potential impediment in sub-Saharan Africa is the lack of opportunities for workers to acquire new skills needed for rapid technology adoption resulting in anxiety and fear. Most CEOs understand the importance of allaying fears by formally introducing programmes aimed at upskilling their workforce to be equipped to work in this tech-enabled environment.



Technology can enhance employee productivity and improve customer service. However, as technology continues to evolve, the skills of employees must also change, from merely capturing and analysing data to interpreting and acting on the insights.

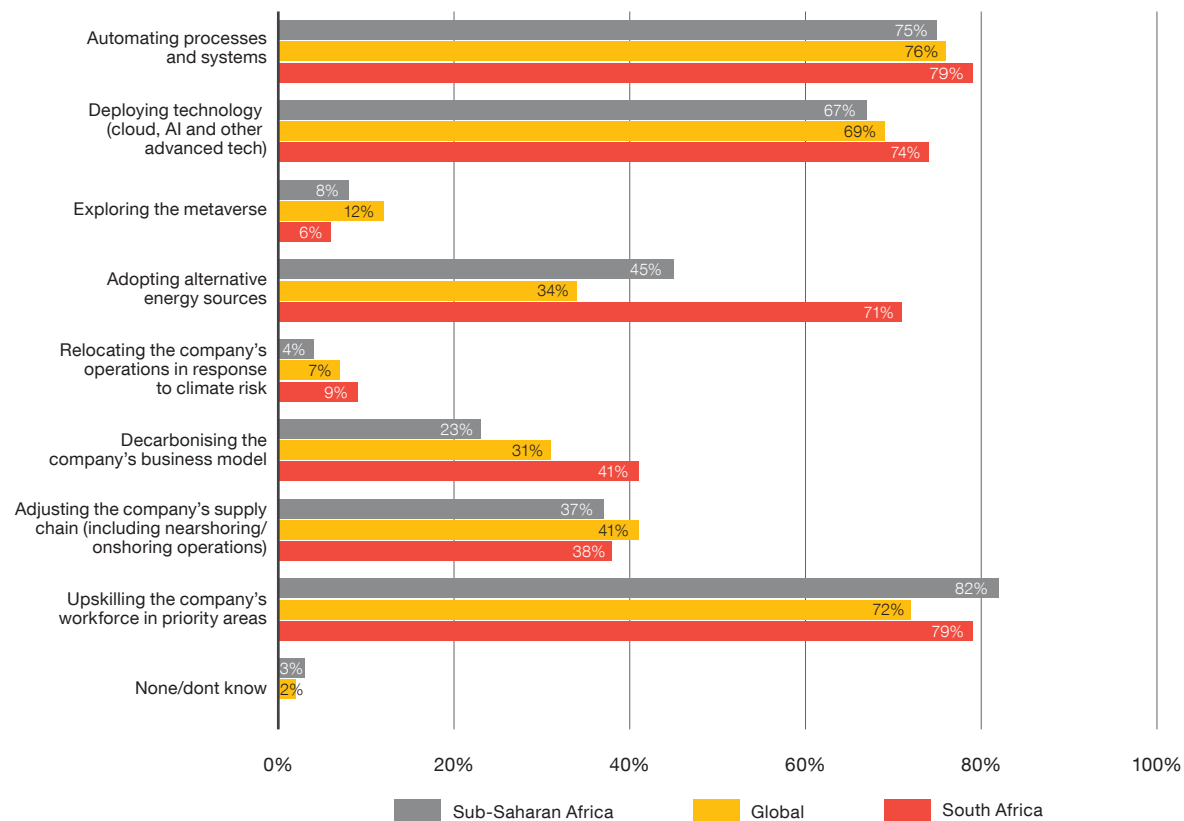
Femi Osinubi – Partner and West Africa Technology Leader, PwC Nigeria





The impact of digitalisation on business performance is significant, and organisations must leverage digital tools to improve productivity. However, the success of any digital transformation strategy hinges on performance management, employee upskilling, and a people-first approach. Furthermore, in Africa, digitisation must be approached carefully, considering the limitations of the African market. By doing so, organisations can achieve better results and improve overall business performance.

Which of the following investments, if any, is your company making in the next 12 months?



Source: PwC's 26th Global CEO Survey



What would help is if organisations start being on the offensive against cybercrime, instead of being reactive and defensive. Once an incident takes place, it becomes difficult to reclaim your interface. A big step in the right direction would be to appoint specialists. The role of the chief information security officer is important in this regard.

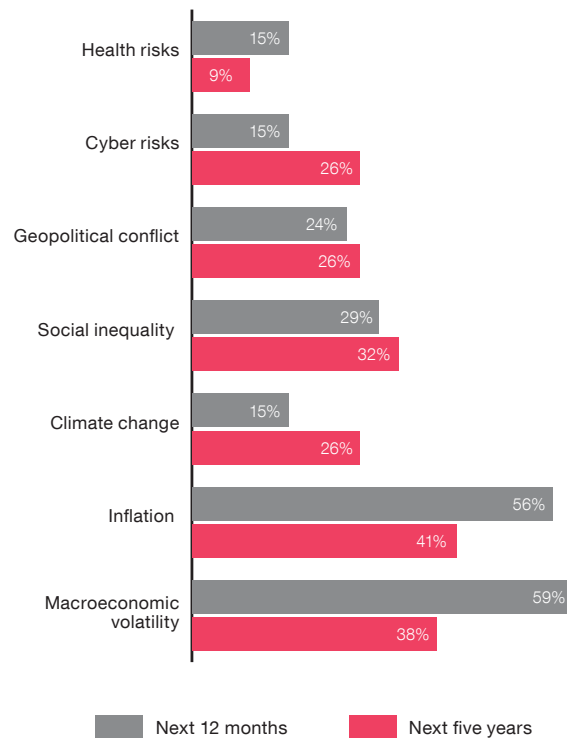
Hamil Bhoora – Cyber Security Competency Leader, PwC Africa

Companies in Africa need to view cyber risks as the number one business threat

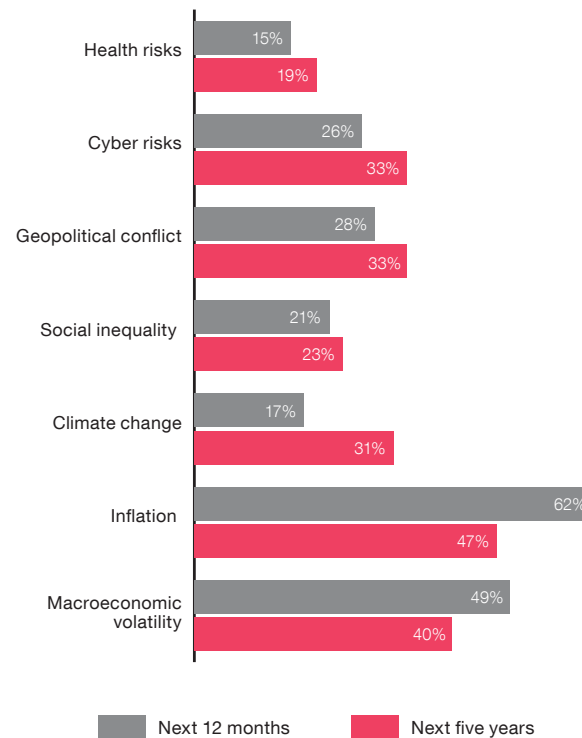
Twenty-six percent of CEOs in Africa believe their companies will be exposed to cyber risk in the next 12 months, and 33% in the next five years. This indicates that among CEOs in Africa, cyber risks are not considered a major risk compared to other factors such as inflation and macroeconomic volatility. This has a lot to do with boards typically focusing on immediate threats that are deemed to be more of a concern.

How exposed do you believe your company will be to the following key threats in the next 12 months and 5 years? (Social inequality: including those stemming from income, gender, race and ethnicity)

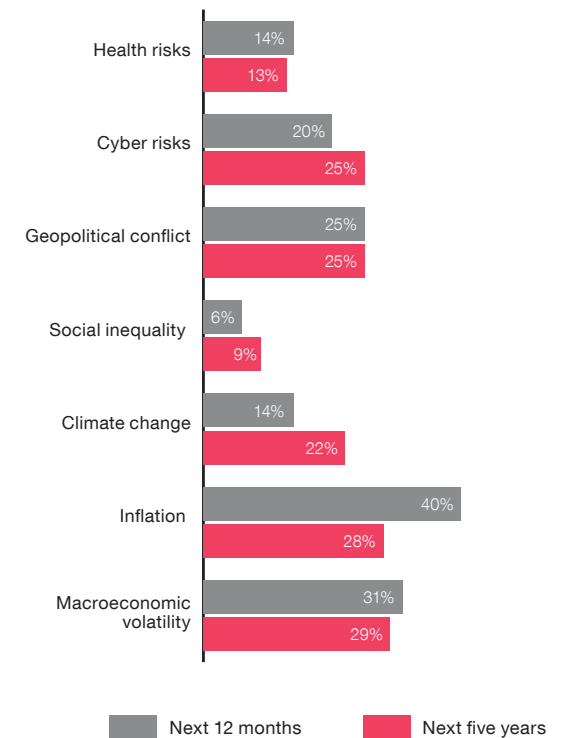
South Africa



Sub-Saharan Africa



Global



Source: PwC's 26th Global CEO Survey

As companies seek to increase their technology adoption, digitisation and automation, many are facing the significant risk of cybercriminals. The manufacturing and mining sectors are extremely vulnerable to cybercriminals, as they focus on increasing their adoption of smart technologies and Industrial Control Systems (ICS) which are housed within operational technology networks, but are often coupled with low cybersecurity investments. While organisations across all industries have been traditionally attacked, which has led to both financial and reputational harm, the financial services sector, although not immune to cyber-crime, has a more mature cybersecurity posture and increased cybersecurity investments accordingly.

A trend identified by PwC is the increased potential for attacks that affect the operations of an organisation due to the adoption of smart technology. Previously, attacks were focused on corporate or back office systems which house technologies such as enterprise networks and ERP core business applications.

Over and above the cyber threats to operational technology networks, we have seen a significant rise in malicious compromises in organisations that have migrated their technologies to cloud service providers. We have seen from many cyber breaches that, although cloud implementation partners are sound in deploying cloud technologies, they do not often prioritise cybersecurity as a key control when deploying a cloud environment.

A related challenge is that many companies are dealing with each incident as it happens in isolation, instead of having a holistic approach looking at overall prevention, which means there is no long-term sustainable strategic plan. Such a strategic plan is necessary to enable the company to withstand the cyber risks and external threats a whole lot better, especially as there would be long-term governance executive buy-in in place, allowing the team responsible for dealing with cybersecurity to manage the situation more efficiently with appropriate risk mitigations in place.

However, what would help is for companies in Africa to change their mindset and start viewing cybersecurity differently in that cybersecurity should be seen as a business risk and not just a technology risk. This can be paired with an initiative that looks at establishing the following:

- A clear cybersecurity strategy aimed to protect all digital assets of an organisation that is linked to the IT and organisational strategy.
- A clear short and long term cybersecurity roadmap which addresses all the current and future cybersecurity people, process and technology requirements.
- Forming architectural review boards with the mandate of managing new technology that comes into the organisation.

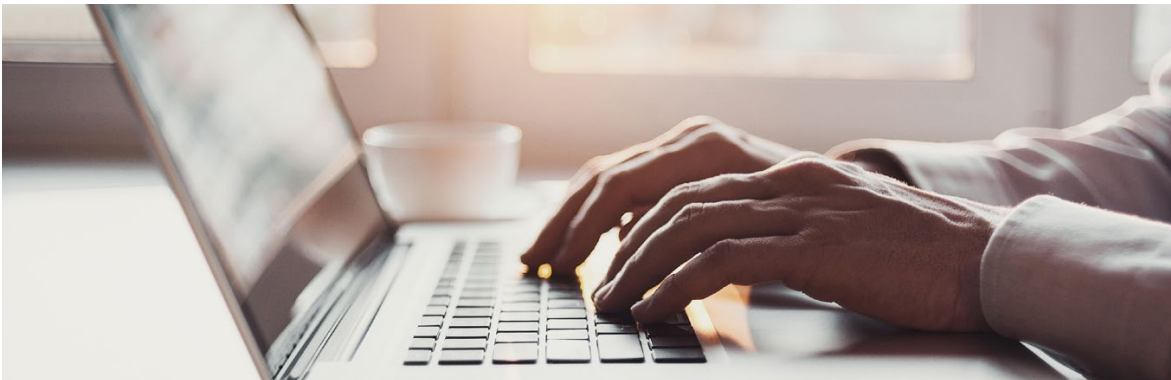


Opportunities from increased technology adoption

While technology adoption rates are low in Africa, it is worth noting that increased investment in adoption can result in more opportunities for job creation and new skills acquisition, as well as opening up new business areas and adding more value.

With increased technology adoption, there are broader levels in which users can interface with the technology, including three-dimensional interfaces, distributed finance, and blockchain. As the rest of the world catches up with regions such as the US, Europe and East Asia, the adoption of these types of capabilities is likely to rise a lot quicker than expected. Because of the position it occupies as an early adopter, the financial services sector, through central banks, is coming to the party with digital currencies, which, among other things, will lead to a rapid rise in non-fungible tokens, also for use within ecosystems such as large gaming platforms. With these developments accelerating, it is likely that in our next annual global CEO survey, we will see an increased adoption of platforms such as the Metaverse, ChatGPT and OpenAI.

This ties in with the need for training developers properly from school to tertiary education, so that we can have a situation where we act responsibly in the way we deploy technology. This means private companies working with government and governance authorities to ensure that proper standards are set and met. The same approach can be adopted when it comes to cybersecurity.



A security mindset and posture needs to be embedded into developer thinking during training at university so that they can do it with cybersecurity in mind. Cybersecurity in organisations needs to be considered in business decisions and technology deployments as including it after the fact makes it more complicated and expensive, and sometimes impossible, to plug the holes.

Yusuf Ryklief – Senior Manager, Cyber Security and Privacy, PwC South Africa

Conclusion

The Africa Business Agenda: Technology perspective 2023 publication reveals that even though the rates of new technology adoption are low in Africa, CEOs do acknowledge the importance of catching up with the rest of the world in the technology race. Even with the concern around potential job losses for unskilled workers, CEOs acknowledge that technology adoption can improve work quality and increase efficiency in the workplace while reducing costs. It can also enable remote work, provide upskilling opportunities, and enhance work-life balance leading to overall benefits for both CEOs and workers.

Organisations can derive value from digital transformation, especially if they understand how technology and data can add value to their business, and do this in a sustainable, manageable and controlled way. Data can change the way CEOs look at business, especially when used appropriately to understand the value their businesses can drive for their customers.

This presents an opportunity to upskill workers and bring them at par with the rest of the global workforce. This has the potential of a knock-on effect that will see some of these skills being utilised to uplift communities from which the workers come.

Managing technology adoption presents an opportunity to mitigate the risk in safeguarding operations against potential cyber attacks. CEOs will need to show a willingness to prioritise cybersecurity even amongst the burden of dealing with challenges that they deem to be more urgent, such as tough economic and operating conditions and, for those in South Africa, load shedding.



Contacts



Mark Allderman

Technology Transformation Capability Leader, PwC Africa

Tel: +27 (0) 21 529 2063

Email: mark.allderman@pwc.com



Femi Osinubi

Partner and West Africa Technology Leader, PwC Nigeria

Tel: +234 1 271 1700

Email: femi.osinubi@pwc.com



Junaid Amra

Forensics Technology Solutions Leader, PwC Africa

Tel: +27 (0) 31 271 2302

Email: junaid.amra@pwc.com



Dave Ives

Partner, Technology, Data and Alliances, PwC South Africa

Tel: +27 (0) 11 797 4945

Email: dave.ives@pwc.com



Hamil Bhoora

Cyber Security Competency Leader, PwC Africa

Tel: +27 (0) 11 797 4102

Email: hamil.bhoora@pwc.com



Ntuthuzelo Mgole

Manager, Cyber Security and Privacy, PwC South Africa

Tel: +27 (0) 11 797 4945

Email: ntuthuzelo.mgole@pwc.com



Yusuf Ryklief

Senior Manager, Cyber Security and Privacy, PwC South Africa

Tel: +27 (0) 21 529 2095

Email: yusuf.ryklief@pwc.com





www.pwc.com

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 327,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2023 PwC. All rights reserved

(23-29507)

