KPMG's Africa Cyber Security Outlook 2022 Survey: Addressing Cybersecurity – Africa's economic opportunity!

KPMG Africa today launched the Africa Cyber Security Outlook 2022 survey which unpacks the state of cybersecurity across the continent - highlighting that the cyber landscape in Africa is highly dynamic and rapidly evolving – propelled by widespread digitisation and matched by adequate investments in protecting assets and data from cyber threats. In fact, 74% of Africa's large companies reported a relatively mature approach to privacy and cyber security.

"While the African continent continues to face many challenges including poverty and political conflicts, multiple economies in the region have shown tremendous growth with a number of countries demonstrating rapid post pandemic recovery with increased consumption and adoption of digital technologies at grassroot level," says John Anyanwu, Partner and Head of Cyber Security at KPMG Nigeria & Africa Cyber Lead.

The survey has identified key areas of focus for Africa including: the integration of cyber security into core business strategy, more robust and risk focused regulation, proactive threat identification and defence and a focus on the cyber talent pool.

Strategy, governance, and cyber defence

Cyber strategy in Africa is more mature than ever before, with 75% of companies having strategies that were either regularly refreshed or had been built in alignment with the organisation's threat profile with measurable KPIs. Furthermore, 61% of companies have implemented a clear data protection/governance approach, with 80% reporting the establishment of robust frameworks and well-defined strategies to mitigate security and privacy risks.

"This demonstrates the significant efforts taken by leaders in organisations to secure the processing of data across the expanding digital landscape. As organisations undergo digital transformation, it is crucial that they envision data protection and privacy as a key strategic component and we are starting to see a massive shift across the African continent," says Marcelo Vieira, Partner and Head of Cyber Security for KPMG South Africa.

Interestingly, the report also highlights those organisations in Africa with a global footprint have been able to achieve more clarity in strategic cyber security direction compared with those operating solely within Africa. Similarly, those that operate across multiple countries in Africa have established clearly defined frameworks and strategies compared to organisations with presence in only one country.

"Irrespective of organisational size, companies are working to ensure data privacy and protection to build trust and safeguard consumer privacy. Organisations that report having a mature approach to cyber security strategy have been subject to half the number of cyber incidents reported across organisations that have not proactively dealt with cyber strategy," states Vieira.

"Organisations must build commensurate confidence in the overall cyber awareness and incident response function to drive digital trust and positively influence consumer perception. To ensure cyber readiness, organisations need to develop a strong security framework covering technical and human-focused defence/response strategy," states Vieira. "In fact, the stats speak for themselves where 46% of those that don't have a standard approach to data protection, privacy and cyber security fell victim to cyber-attacks, compared to 28% who have robust security in place."

Oversight & management

"Cyber criminals in this modern era are changing tactics to include data exfiltration, targeting personal user information and targeting organisations that attempt to aggregate, combine, compare and analyse data to better service their consumers. Therefore, today, there is a much larger focuses needed on not only mitigating threats but in the way, organisations are set up to deal with them," says Anthony Muiyuro, Cyber Lead at KPMG East Africa.

The approach should focus on a few key principles including understanding crown jewel information assets, evaluating the current and emerging threat landscape, documenting and aligning a fit for purpose cyber strategy, placing it into practice and monitoring effectiveness.

“Our research show that organisations are still largely not confident in their ability to deal with cyber threats, with 47% of them only partially confident. Therefore, organisations must rigorously evaluate their security measures to identify areas for improvement. One effective way of achieving this is through conduction of ‘purple teaming’ as an approach for building confidence in established cyber security controls and responses and ensure robust security oversight. 34% of respondents have a fully independent cyber and information security function with oversight through risk management and internal audit, with 47% still maintain this function within the IT function.

“This function should be a strategic focus, cut across all business functions. Therefore, establishing an independent information security function is touted as a critical success factor for mature information risk management,” mentions Muiyuro.

Cyber talent
“More than 50% that have recently fallen victim to cybercrime, still lack confidence in the effectiveness of their cyber security incident response team’s action during a major cyber security incident and so there is no doubt that a new focus on building cyber skills is critical – the need for highly specialised cyber security resources with skills for cyber leadership, securing and testing systems should be prioritised.

75% of companies encounter challenges in recruiting and retaining qualified cyber professionals and only one in three have access to a sufficient talent pool. Despite this however, some industries are well geared towards cyber skills, with the highest percentage of adequate skills being in the manufacturing (48%) and ENR (47%) sectors, followed closely by the FMCG and ICT sector. The financial services and public sector have been prime targets for cyber-attacks and demonstrate an acute demand for cyber resources, largely due to the high level of regulatory oversight required.

While there is currently a shortage – there is no doubt that Africa is taking this seriously with 55% planning on recruiting cyber security resources in the next 12 months, with 58% planning to onboard at least 1 - 2 resources and 25% looking at 3- 5 resources.

“We need to change the way we recruit in this sector by improving the recruitment process and requirements, looking at non-traditional degrees, offering competitive salaries and of course looking at external collaborations with educational institutions to build skills, develop in-house talent and outsourcing of skills to those in the know. Without this shift, we may be left behind,” says Anyanwu.

Africa at a glance
While East Africa has driven the highest adoption of digital transformation, with 89% of organisations undergoing digital transformation, they are also the largest proportion of cyber-attacks amongst the African regions (31% reported cyber-attacks).

“While 39 out of the 54* African countries have established cyber security legislation, Africa’s adoption of cyber security policies and regulations stands at 72%, which is the lowest across the globe. This, together with the outcomes of our research indicates that there is a very real need to rapidly advance agile cyber security measures to enhance risk resilience and enable organisations to harness new opportunities for revenue growth and business success, while ensuring business continuity. Of course, this comes with its own budgetary and resource challenges but as a continent, we need to become innovative in our approach and lean into experts that can tighten controls and improve Africa’s cyber resilience for increased economic benefit,” concludes Anyanwu.

*United Nations Conference on Trade and Development

Note to editors:
The latest survey draws insights from 300 respondents from across Africa (East, West and Southern Africa), spanning various industry (Financial Services, ICT, Government, Energy and Natural Resources, Manufacturing, to name a few) from both large (44%) and small-to-medium enterprises (SME – 56%) - exploring the nature of cyber challenges faced by organisations as well as seeking solutions through a uniquely African lens.