KPMG

Africa Cyber Security Outlook

September 2022

Foreword

John Anyanwu

Partner and Head,
Cyber Security,
KPMG in Nigeria and
Africa Cyber Lead

Marcelo Vieira

Partner and Head of
Cyber Security,
KPMG in Southern Africa

Anthony Muiyuro

Cyber Lead
KPMG East Africa

While the African continent continues to face many challenges including poverty and political conflict, multiple economies in the region have shown tremendous growth. Numerous countries have demonstrated a rapid post-pandemic recovery with an increase in consumption and adoption of digital technologies at the grassroot level.

Whilst these technologies have enabled faster growth, they have also led to challenges related to cyber security. Research reports suggest that African enterprises are a favourite target for cyber attackers.

The cyber security landscape across the African continent is highly dynamic and is rapidly evolving, propelled by widespread digitalisation across business sectors.

While regaining strength in the aftermath of COVID-19, organisations have been forced to rethink their ways of working while leveraging digital initiatives, aimed at streamlining operations and ensuring business continuity. However, this drive for digitisation remains to be matched by adequate investments in protecting assets and data from cyber threats. Realising the importance of digitalisation and increased risk of data breaches, various governments are rapidly introducing legislation and adopting frameworks to ensure consumer privacy and data security for protecting public interest.

All these factors, combined with an ever-expanding threat horizon, create a perfect storm for organisations that are forced to meticulously measure the opportunity cost of every investment in a world of economic uncertainty. Organisations are rebuilding their cyber strategies to meet these demands and to ensure integrity and resilience of operations.

Furthermore, with the increasing risk in digital supply chains, new risk mitigation initiatives are being strategised by organisations globally. Agile cyber security measures enhance an organisation's risk resilience, thus enabling organisations to harness new opportunities for revenue growth and business success.

It is against this backdrop that we have the privilege of presenting our inaugural Africa Cyber Security Outlook report, exploring the nature of the cyber challenges faced by organisations in our continent and seeking solutions through a uniquely African lens.

We would like to thank the technology, security and business leaders who have lent their voice to this initiative so that we may learn from each other and stand together in these uncertain times.

Table of Contents

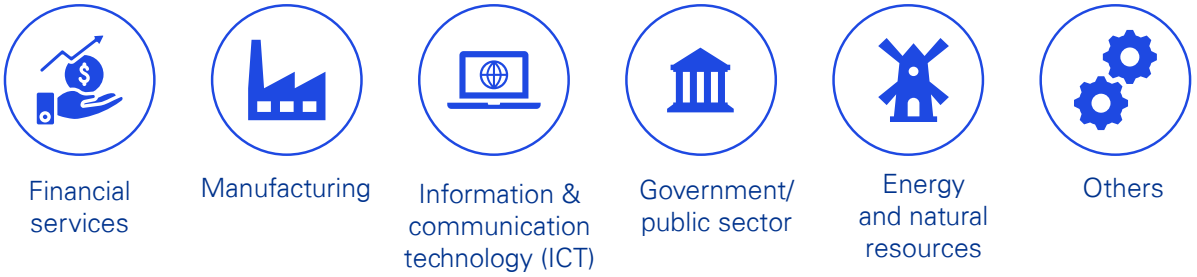
01

Profile of survey respondents

Profile of survey respondents

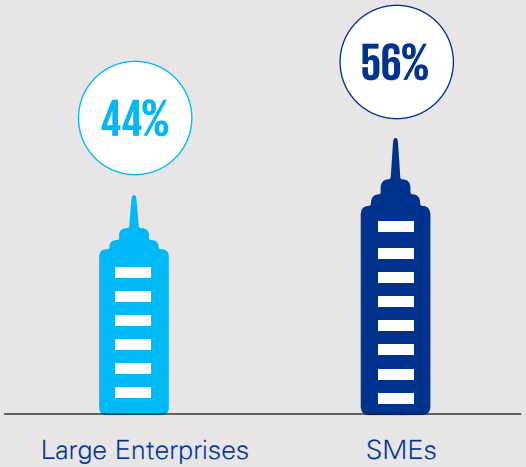
KPMG's inaugural Cyber Security Outlook surveyed about 300 respondents from across Africa, understanding their current state and future priorities. The survey covered respondents spanning various industry sectors considering both large enterprises and small and medium enterprises (SMEs).

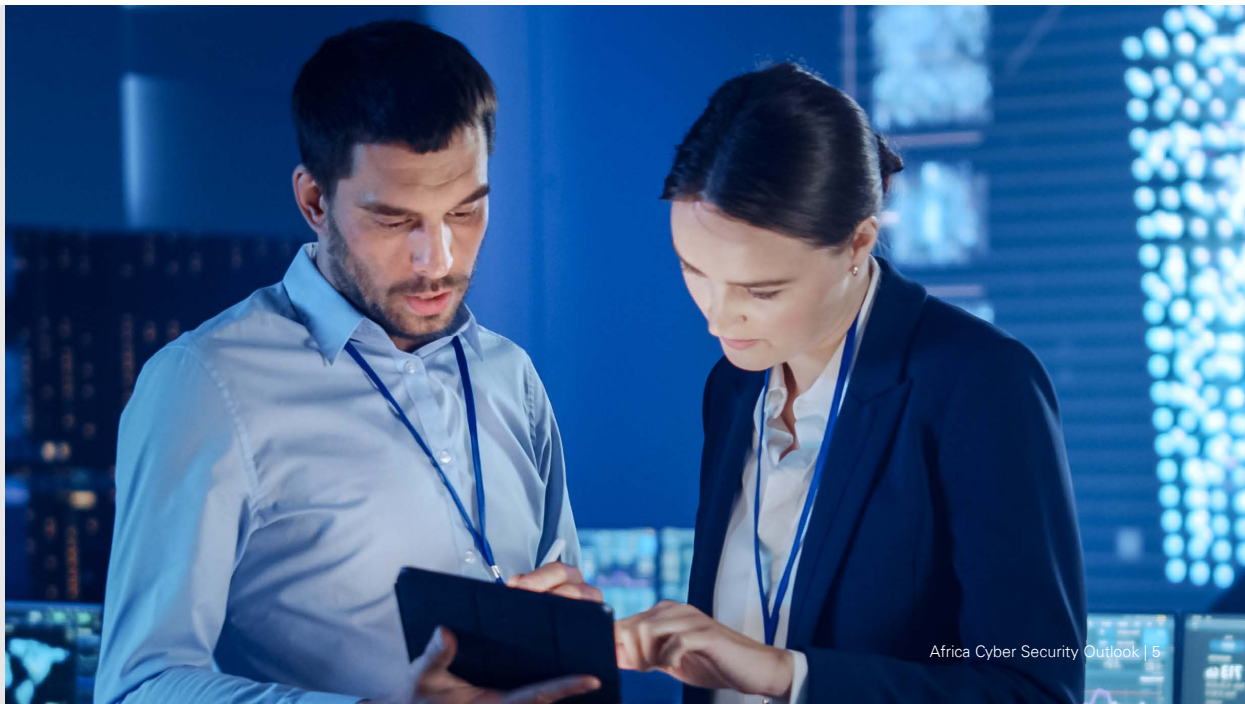
Business sectors of responders



Regional breakdown of respondents

Organisational profile (%)





02

Cyber security: building tailored strategies

Africa: a changing cyber security landscape

Africa is the world's second largest continent with huge diversity and disparity across countries. The region continues to encounter numerous socio-economic challenges such as water and food scarcity, inadequate healthcare and political instability. These challenges are further compounded by the impact of a rapidly changing climate. However, in recent years, Africa has emerged as a fast-growing digital behemoth, driven by policy reforms and leadership initiatives. The region has the youngest population in the world, which is playing a key role in its digital growth journey. Organisations are building infrastructure and services to enable digital services at a pace never seen before.

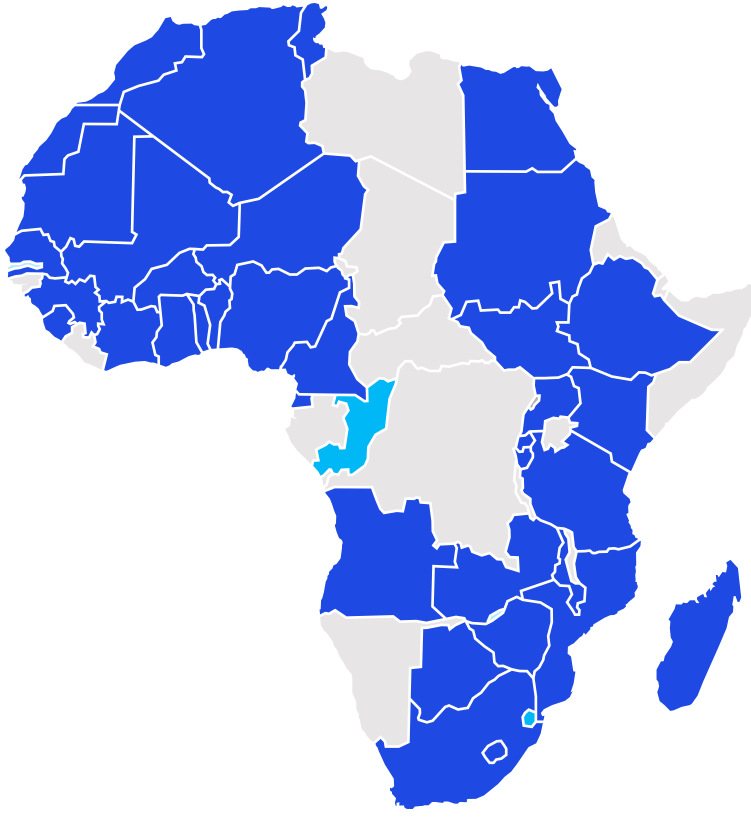
The penetration of the internet and smartphones has accelerated the adoption of digital technologies, aiding efficient service delivery. Lockdowns imposed during the COVID-19 pandemic have led to an increase in remote connectivity services, as organisations put measures in place to continue business operations. According to the Global System for Mobile Communications Association (GSMA), the number of unique mobile subscribers in Sub-Saharan Africa will reach 615 million by 2025.[1]

The proliferation of digital services has led to an explosion in digital ecosystems, broadening the attack surface and increasing the associated risks. With these developments, managing security and privacy in a dynamic and vulnerable environment remains a major challenge for African enterprises.

The recent large-scale cyber attacks and cross-jurisdictional issues in pursuing the perpetrators have made it painfully clear that the challenges with borderless cyber crime can only be solved through joint efforts of multiple governments. The fight against crime within the confines of regional borders is a lost battle in most cases.

According to the United Nations Conference on Trade and Development, 39 out of the 54 African countries have established cyber security legislation, while 2 have draft legislation under development. However, more remains to be done as 13 countries have not yet started the process to draft cyber security and further promote multi-jurisdictional collaboration. The adoption of cyber security policies and regulations across Africa stands at 72 percent, which is the lowest across the globe.[2]

National cyber security legislation adoption in Africa[2]



Legend

- Countries with cyber legislation
- Countries with draft cyber legislation
- Countries with no cyber legislation

[1] The Mobile Economy Sub-Saharan Africa 2021
[2] UNCTAD Cybercrime Legislation Worldwide

Encouragingly, at a regional level, there are various cyber security initiatives that aim to address the continent's surging cyber-related threats and challenges. Beginning in 2019, the EU collaborated with the Economic Community of West African States (ECOWAS) commission and initiated the West African Response on Cyber Security and Fight against Cybercrime (OCWAR C) and adopted a regional cyber crime and cyber security strategy.[3] Also, the African Union Mechanism for Police Cooperation implemented the cyber crime strategy 2020-24 that seeks to enhance coordination, develop specialised police capacities, and harmonise legal and regulatory frameworks.[4] The Foreign, Commonwealth & Development Office of the United Kingdom, in collaboration with governments and the public sector, is working on initiatives to develop cyber security capacity, awareness and skills across multiple African countries.

Even though these regional efforts are noteworthy, there is a significant gap in their implementation and adoption in national level cyber security strategies. The challenges in catalysing broad-based national level coordination and cooperation are resulting in a highly dynamic regulatory landscape, impeding the adoption of cyber security policies in Africa. So what does this mean for organisations grappling with countless variables to maintain an effective security posture? In the following section, we present the results of our survey to better understand the current pain points for organisations at a strategic level and make pragmatic recommendations on building an effective cyber security strategy.

[3] Economic Community Of Western African States (ECOWAS)
[4] Africa Center for Strategic Studies

Is your cyber security strategy fit-for-purpose ?

27%

of respondents have a strategy linked to a specific threat profile with measurable KPIs.

As the digital footprint expands and the number of cyber threat incidents continue to rise, organisations are realising the importance of enforcing measures driven by a focused strategy.

According to our survey, about 75 percent of respondents have reported having strategies that were either regularly refreshed or had been built in alignment with the organisation's threat profile with measurable KPIs. Designing a strategy with built-in feedback loops can enable the organisational leadership to fine-tune the implementation of cyber security practices while delivering effective oversight.

Interestingly, a higher proportion of organisations with operations across multiple countries in Africa have established clearly defined frameworks and strategies compared with those that operate in only one country. This signifies that organisations that have been subject to a dynamic legislative and cyber risk landscape are inclined towards building a more holistic cyber strategy that can be adopted as a standard across geographies, while considering local regulations and risks. It is also crucial that organisations regularly review and update their strategies to mirror the ever-shifting goalposts.

Our results indicate that this strategic effort is not in vain, as organisations with a mature strategy are 50 percent less likely to fall victim to a major cyber incident. This should motivate the one in four respondents, who did not have a recently updated cyber strategy and were reliant on ad hoc and responsive efforts. The pitfalls of this ad hoc approach cannot be understated, and organisations following this approach are more likely to experience serious consequences as a result of a cyber incident.

How would you describe your strategic cyber security outlook?

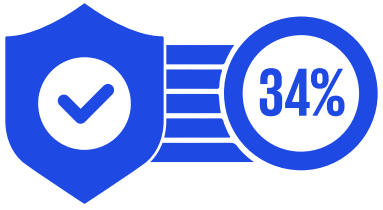
75%

have a strategy that is regularly refreshed or has been built in alignment with the organisation's threat profile with measurable KPIs.

25%

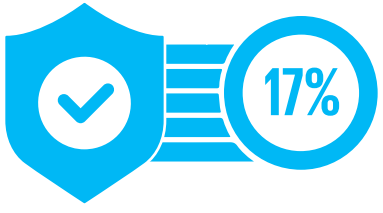
do not have a recently updated strategy and are reliant on ad hoc and responsive efforts.

What is your organisation's approach to implementing independent information security oversight?

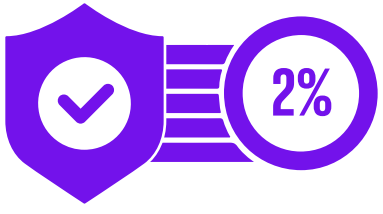


We have a fully independent cyber and information security function reporting directly to the organisational leadership. Risk management and internal audit provide independent oversight.

Information security is incorporated into IT security and reports to the CIO or equivalent. Risk management and/or internal audit provide(s) independent oversight.



We have no formal information security function, and IT security efforts are fully managed out of IT with little to no independent oversight.



Other formal structures are in place.

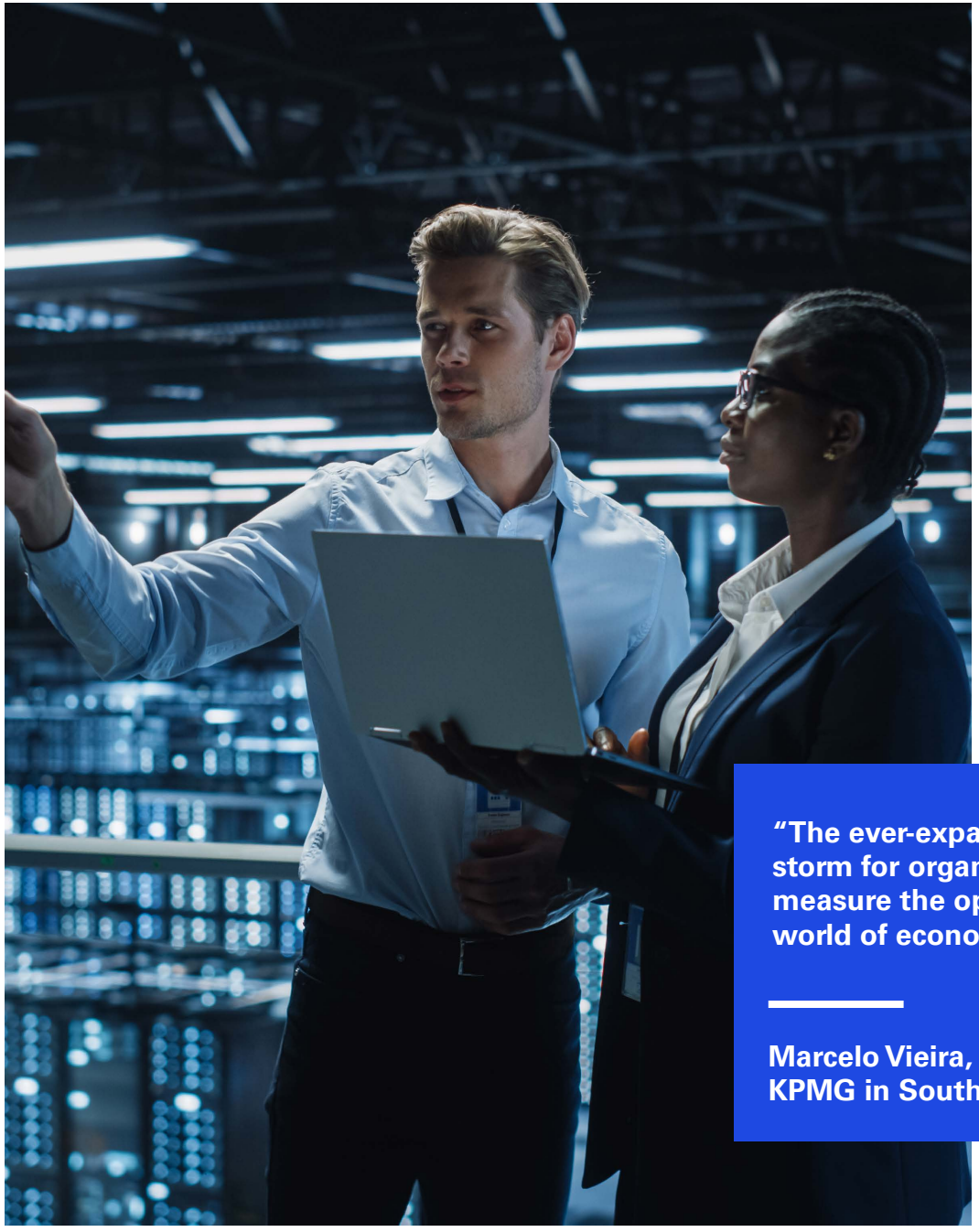
34%

of respondents have a fully independent cyber and information security function with oversight through risk management and internal audit.

IT security teams are generally responsible for securing IT infrastructure from cyber attacks and threats. Information security, on the other hand, provides independent oversight and support to prioritise the security of information, and enforce security controls to mitigate information risk. Given that information is the fuel that drives modern business, it is imperative for the information security function to cut across all business functions. Establishing an independent information security function is thus touted as a critical success factor for mature information risk management.

According to our survey, about 47 percent of respondents stated that their organisations have incorporated the information security function into IT security. While there is no one-size-fits-all approach in structuring relevant teams, it is a commonly held view that incorporating the information security function as a part of IT operations may have inherent conflicting goals. Fundamental differences in the expected outcomes of the functions may drive IT to primarily focus on uptime and availability, while security functions also place a premium on confidentiality and integrity. It is same with DevOps, where developers tend to be incentivised on speed to market and not security, with predictable consequences. Finding the right balance is key to ensure that cyber security becomes baked into the culture of the organisation.

On the bottom end of the scale, about **one in five respondents from our survey highlighted the absence of a formal information security function.** While the lack of resources may prevent smaller organisations from establishing an independent oversight structure, it remains crucial for business leaders to implement a framework to ensure that information security oversight is exercised diligently. In this case, a little is a whole lot better than none whatsoever!



A cyber security strategy for a changing world

Cyber security should be a key consideration in building digital trust and play an integral part in the corporate strategy. It should not be an afterthought. As organisations collaborate to build cyber security strategies to secure information and business assets, it is crucial that the strategy also considers key assets, the threat landscape as well as the legal and regulatory frameworks. In this section, we explore a practical approach in building a fit-for-purpose strategy.

"The ever-expanding threat horizon creates a perfect storm for organisations that are forced to meticulously measure the opportunity cost of every investment in a world of economic uncertainty."

Marcelo Vieira, Partner and Head of Cyber Security in KPMG in Southern Africa

A sound organisational approach to cyber security strategies and governance includes building upon principles such as:

1. Understanding crown jewels

You cannot protect what you do not know. A 'crown jewel analysis (CJA)' seeks to identify information assets critical to accomplishing an organisation's mission. This analysis aims to inform the strategic and tactical security measures required to protect the organisation at rest and in transit — across all touch points.

All information assets are not equal; some require more protection than others. Treating all information assets as high value has the benefit of securing all assets to a similar level; however, resources may be wasted on maintaining and certifying information security controls that do not require it. Ideally, the approach should be balanced against the cost and effort in maintaining security controls across all systems.[5]

2. Evaluating the cyber threat landscape

While a common set of cyber risks affect most businesses, unique business processes and information assets result in countless threat permutations.

By examining this landscape in detail, organisations can tailor cyber strategies to meet these complex demands. Threat assessments should not only consider traditional on-premises infrastructure, but consider Operational Technologies, cloud environments and crucially- any third party/ supply chain cyber threat exposure.

3. Assessing current state maturity

Within this asset and threat context, organisations should comprehensively evaluate cyber security measures and build visibility across the business risk exposure.

To assess the current state maturity, organisations can perform cyber audits against leading frameworks and standards, penetration testing, vulnerability assessments, and cyber attack simulations. This will enable the leadership to better understand the maturity of their current security capabilities and future needs.

4. Documenting and aligning cyber strategy

In formulating a cyber strategy, organisations need to ensure it is aligned to the core business strategy, while adhering to the legal and regulatory responsibilities of the business.

The strategy should aim to embed security into business processes in a way that enables the organisation to maintain pace. Organisations should transition from traditional security thinking around confidentiality and availability of data and begin thinking about striving to ensure integrity and resilience.

5. Putting it into practice

Chief Information Security Officers (CISOs) can simplify the process of obtaining stakeholder buy-in by defining these strategic initiatives into an achievable priority and resource-based roadmap to success. The CJA, threat profile and current state maturity assessment are crucial inputs for a pragmatic roadmap.

Ensure that key organisational stakeholders are part of the process to obtain commitment to a security strategy that can protect organisational and customer data, as well as manage risk, and is sensitive to short- and long-term business priorities.

Reformulate thinking in the executive suite as it relates to security by focusing on practical enterprise risk rather than expense and speed.

6. Monitoring cyber security effectiveness

Effective governance requires actionable insights into cyber risk exposure at a business unit/product level. This includes reporting about the effectiveness of operational controls through continuous auditing and continuous monitoring (CA/ CM) processes.

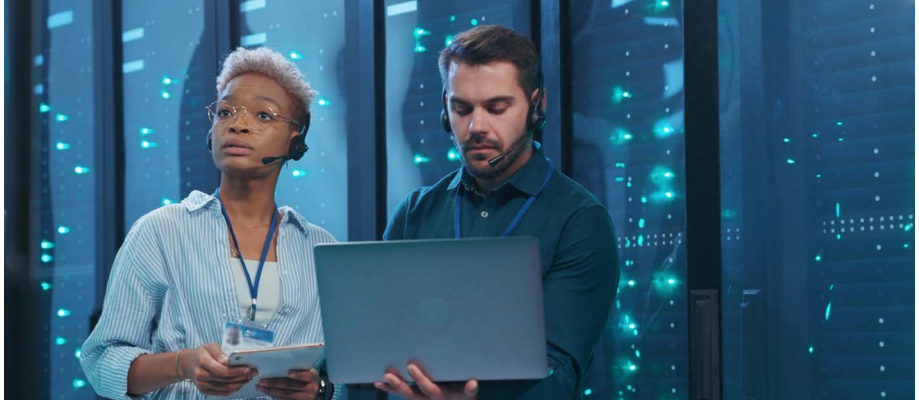
Implementing monitoring solutions based on organisational needs and budget, can help drive effective cyber security programmes. State-of-the-art concepts such as cyber mesh can be employed to monitor and secure critical endpoints. By exploring the use of frameworks and KPIs, organisations can establish closed feedback loops. Cyber security functions can then analyse KPIs for providing actionable security insight to organisational boards.

[5]Cybersecurity considerations 2022, KPMG

03

Safeguarding privacy in the face of growing threats

Cyber criminals — changing tactics?



According to an Interpol report, from January 2020 to February 2021, South Africa witnessed 230 million cyber attacks, while the numbers for Kenya and Morocco were recorded at 72 million and 71 million, respectively.[6] These threats ranged from ransomware to business email compromise attempts. Cyber criminals in this modern era are changing tactics to include data exfiltration and actively target personal information. This approach is mostly used as leverage to compel organisations to meet their demands. Failure to comply with such demands often results in public data exposure and negative media publicity, which often lead to a significant impact on consumer privacy and far reaching reputational and regulatory consequences.

Another key factor in this proliferation is the increase in consumer demand for personalised experiences across an explosion of digital touch points; all this before the Metaverse has truly hit the mainstream consumer market. In the same vein, this has provided an additional attraction for cyber criminals who are also motivated by the potential economic value in compromising and selling data dumps on the dark web for cryptocurrency payments.

All factors considered, it has therefore never been more challenging to safeguard the personal information of staff and customers. A large percentage of the respondents in our survey have reported having clearly defined frameworks and proactive data protection measures. However, that being said, many organisations are still grappling with controls and measures to effectively implement local and international privacy requirements.

20%

of respondents felt that organisations did not have clearly defined strategies and frameworks to mitigate security and privacy risks.

Citizens religiously guard their privacy rights, highlighting the positive trend towards increasing consumer awareness around data privacy. Effective data governance policies can bear fruits in the long run such as improved risk, security and data management across the enterprise. The pre-emptive action to prevent personal information breaches can, thus, lead to improved customer privacy controls and enhanced brand recognition.

According to our survey, one in five respondents from organisations surveyed across Africa did not have clearly defined strategies and frameworks to mitigate security and privacy risks. As per a report by Gartner, organisations in the MENA region are expected to increase their security spending in 2022 due to a surge in cyber security attacks, threats to cyber-physical systems and malicious nature of ransomware.[7] The key areas that are expected to witness an increase in spending include cloud, application and data security, identity access management, and infrastructure protection. Organisations that are catching up on cyber investments should strongly consider privacy-by-design principles in their security investment roadmap.

[6] Africa Cyberthreat Assessment report
[7] Gartner report

Linking cyber security and privacy

The COVID-19 pandemic triggered an increase in online education and remote working by 97 percent and 66 percent, respectively, as per an Ericsson report.[8] As we look towards the future of remote work and continual explosion of data generation and usage, it becomes increasingly evident that data privacy and cyber security are inextricably linked. This raises a strong need for joint efforts between data and cyber security teams to establish effective cyber security and data protection policies. This need often extends across the internal borders of business.

The collection and storage of data by related entities or partnerships adds to the complexity across the already tricky privacy landscape. For instance, the COVID-19 pandemic prompted healthcare providers across Africa to collect personal information, demographics and other healthcare data for sharing medical records, tracking people's movement to enable contract tracing. This necessitated collaboration between multiple private and public sector entities.

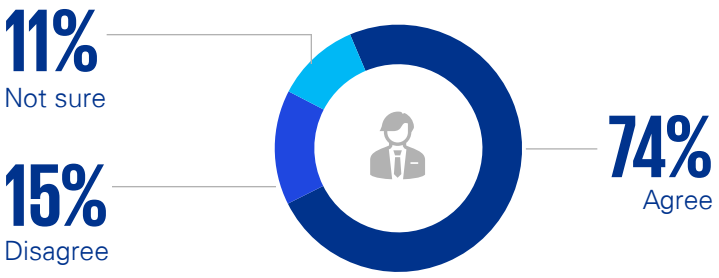
Clear ownership and accountability for information protection and cyber security is therefore crucial to ease the burden on those tasked with the implementation and operation of controls.

Organisations that aggregate, compare and analyse data to better service their consumers have become a proverbial goldmine for cyber criminals. The electronic systems and digital frameworks underpinning these algorithms capture a vast number of data points, rendering them as attractive targets for people acting with malicious intent. Thus, it is crucial to integrate cyber security frameworks and processes across all data endpoints, considering physical and logical security management from the source of its generation, transmission and ultimately its storage. Understanding all of the touchpoints of the full information cycle should not be underestimated. We often pour all our efforts to secure information on corporate servers, but neglect to consider that the same sensitive information may be shared by executives on a popular chat application, for example.

[8]Ericsson report

Consistency is key

There is a standard approach to proactively identify data privacy risks on systems and products.



According to our survey, about three in four respondents from organisations felt that they had a standard approach for proactively identifying data privacy risks across systems and products. Measures such as privacy by design which emphasise building security into the products at a process level, rather than retrospectively applying privacy measures, help in to building strong organisational focus on privacy. Organisations compliant with existing data privacy frameworks are poised for a head start in achieving compliance across the dynamic regulatory landscape. Moreover, safeguarding personal information can help organisations mitigate identity theft, and prevent fraudulent account takeovers as well as phishing attacks and extortion attempts.

Conversely, that leaves about one in four respondents stated that their organisation applies an ad hoc or non-consistent approach to mitigating data privacy risks. The evolving cyber and privacy regulatory landscape is driving businesses to develop an understanding of the information they collect and process, to a level never seen before. Organisations need to ensure privacy compliance with a myriad of emerging privacy laws as applicable to their operations, such as the Protection of Personal Information Act, 2013 (POPIA) and Data Protection Act in Kenya, Botswana, Ghana and Egypt. Not to mention the GDPR!

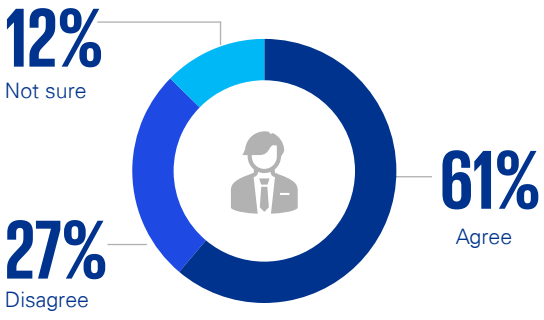
Organisations must maintain vigilance, consider the nuances and harmonise privacy controls to enable compliance across multiple geographies to ensure that the challenge does not become insurmountable.

Comprehensive data protection and privacy measures are therefore non-negotiable foundations for trust in the modern world.

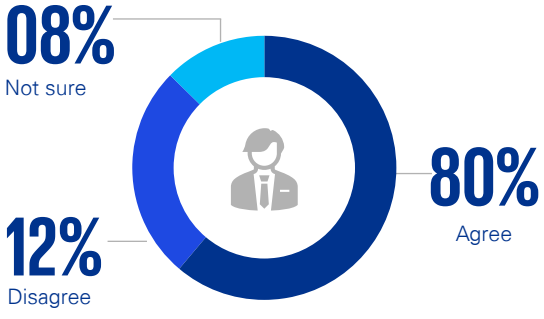
Key considerations for effective data governance

- Define a relevant and up-to-date data map to understand the flow of information in the organisation, including third parties
- Monitor the data pipeline for compliance and anomalies
- Establish feedback loops to monitor KPIs and report to relevant governance committees
- Ensure high visibility and transparency while processing data across regions
- Embed appropriate frameworks and controls, with real-time effectiveness measurement

Does your organisation have a clear data protection/governance approach, led by a data protection officer?



Has your organisation established clearly defined strategies and frameworks to mitigate security and privacy risks?



According to our survey, about three in five respondents observed that their business had implemented a clear data protection/governance approach.

This demonstrates the significant efforts taken by the cyber leaders 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. Privacy measures and data protection practices can also translate to competitive advantage for businesses operating in the modern digital landscape.

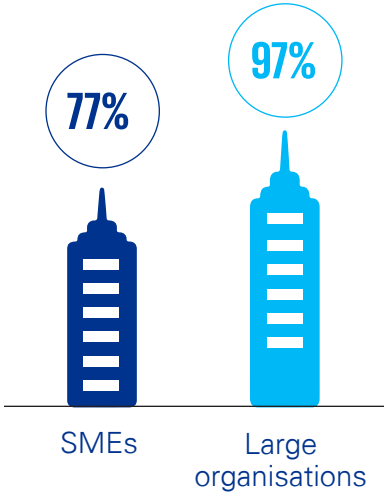
In this backdrop, the role of data protection officers has gained immense significance for providing strategic insight into responsible and effective data handling practices, setting up data protection controls and enforcing privacy frameworks. Data protection officers are also responsible for conducting data protection impact assessments, liaising with supervisory authorities and risk mapping. The data protection function drives confidence about the privacy and data protection landscape, enabling businesses to build digital trust across their value chain.

About four in five respondents have established robust frameworks and well-defined strategies to mitigate security and privacy risks.

Organisations are now aware of the impending threats and the risk of exposure to cyber threats. To achieve robust cyber security, organisations must focus on holistically developing their cyber capabilities. A planned implementation of the cyber strategy is crucial for successfully executing strategies in the face of challenges such as skill and budget shortages prevailing across Africa. Defining the scope of cyber security across an organisation's operations is crucial, while setting up zero-trust solutions to detect and combat modern threats and vulnerabilities.

Fine-tuning KPIs based on an assessment of the effectiveness of deployed safeguards can enable organisations to further strengthen their existing strategies. A robust and strategic approach to cyber strategy can thus enable organisations to pre-empt and counter cyber attacks that have the potential to cause significant monetary, reputational and operational damages to organisations.

Organisations that have established clearly defined strategies and frameworks to mitigate security and privacy risks



Respondents from large companies across the African landscape have reported a relatively mature approach to privacy and cyber security compared with SMEs. Building skills around cyber security and information risk can help large organisations augment their approach to cyber security. Organisations must build a human firewall by continuing to spread awareness among their workforce and third parties regarding cyber security, empowering them to report suspicious activity and navigate changing threats.

Core security practices such as identifying points of vulnerability and prioritising the risk/protection levels across assets can better ensure the protection of intellectual, personal and cyber physical assets, while also maintaining a balance in capex.

Based on the results of our survey, SMEs tend to lag behind larger corporates. These organisations typically have to make do with a much smaller pool of resources. However, they may be in a position to rapidly enhance their information protection maturity by leveraging the experiences and good practices of their larger counterparts.

Irrespective of their size, organisations are now more aware of and are working to ensure data privacy and protection to build trust and safeguard consumer privacy.

04

Cyber security talent: a call to arms

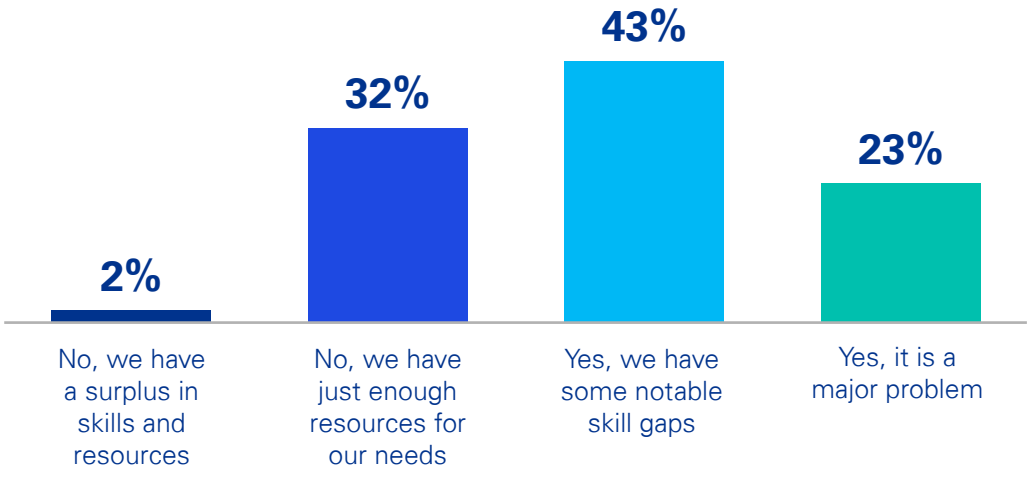
Are cyber skills really that scarce?

According to the State of Cyber Security 2022 report by the Information Systems Audit and Controls Association (ISACA)[9], talent poaching, inadequate financial incentives, and limitations to career growth and development emerged as key threats causing the shortage of cyber resources across organisations. The increasing complexity of cyber attacks has led to a need for highly specialised cyber security resources across technical and non-technical domains. The study also observed that after the 'Great Resignation' trend, employees are demanding increased work flexibility and higher wages.

According to our survey, about two in three enterprises encounter challenges in recruiting and retaining qualified cyber professionals. However, challenges often lead to opportunity as the increased attrition initiated by the 'Great Resignation' also created a competitive market for talent to staff cyber teams.

There is no doubt that a surging demand for cyber security across most sectors is leading to a dearth of cyber security professionals. At a global level, an estimated 3 million cyber security job vacancies remain unfilled.[10]

Is your organisation facing challenges in recruiting and retaining the right talent?



Furthermore, this gap is expected to widen to 10 million vacancies in the near future. The advent of remote work has allowed global multi-national corporations (MNCs) to expand their talent pool, enabling them to tap into geographically diverse regions. This has exacerbated the skill shortage across the talent pool in Africa, the access to which is now being contested on a global level.

Outsourcing cyber security functions to managed security service providers is emerging as a viable alternative for organisations. However, outsourcing cyber security processes involves the risk of exposing data to a third-party service provider, prompting the need for effective planning and control before making outsourcing decisions.

About one in four respondents felt that sourcing talent was a major problem. Organisations need to work towards cultivating talent pipelines by partnering with universities, developing in-house talent and offering attractive remuneration.

According to the State of Cyber Security 2022 report by ISACA, respondents felt that rudimentary soft skills, cloud computing expertise, security controls and coding skills are the key cause of the skill gap while recruiting cyber resources. Organisations have to think creatively to solve these talent challenges. In many cases, this involves a hybrid approach between insourced and outsourced resources.

[9] Cybersecurity Jobs Report
[10] State of Cyber security 2022

Typical cyber security resources in organisations must possess deep knowledge of threat and incident management, be adept at intrusion detection and network security monitoring management, and be able to implement cyber security controls and frameworks, among others. However, there still exists a huge dearth of resources that possess these skill sets. This is no easy challenge facing recruiters.

Our survey indicates that across Africa, organisations within financial services, government/public sector, and ICT sectors are prime targets for cyber attacks. It is no surprise then that they also face the most acute demand for cyber skills and resources.

According to a Carnegie report, the financial sector in the African landscape has been the largest employer of cyber security professionals due to the critical nature of operations across financial institutions.[11]

Percentage of organisations that have enough cyber resources for their needs based on the sector

24%	29%	36%	38%	47%	48%
Financial services	Government/ public sector	ICT	Fast-moving consumer goods	Energy and natural resources	Manufacturing

[11] Carnegie Report

Organisations bullish on cyber skills resourcing

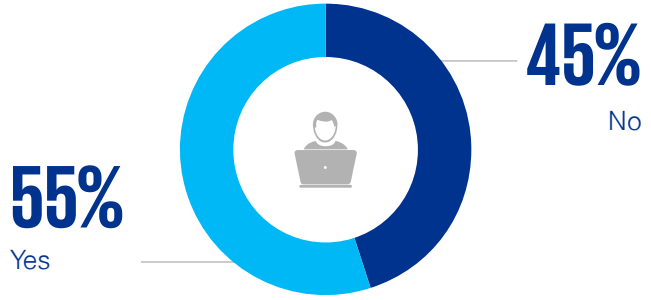
The shortage in cyber resources translates to high cost of onboarding qualified cyber security professionals due to a highly competitive marketplace. **Smaller organisations face increased difficulty in accessing and recruiting qualified cyber talent, compared with larger enterprises,** due to budget constraints, inherent uncertainty in career trajectories and understaffing of teams.

Despite the shortage, about 55 percent of respondents from our survey stated that their organisations plan to recruit cyber security resources in the next 12 months. Approximately 58 percent of these respondents observed that their organisations plan to onboard at least one to two cyber resources, whereas about 25 percent plan to onboard three to five resources within the next 12 months.

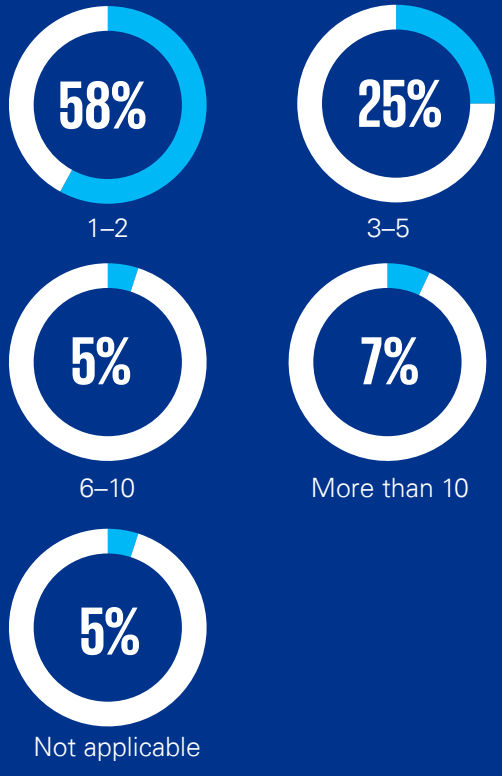
Recruiters need to take cognisance of the highly competitive market and look past traditional degrees to help ascertain a candidate's skill set and cultural fit to ensure their ability to manage understaffed teams. In addition, training and retaining key talent has been identified as instrumental in building high performing cyber security teams.

According to our survey, a higher proportion of SMEs reported recruiting cyber resources as a major problem, compared with large enterprises.

Is your organisation planning on recruiting cyber security resources in the next 12 months?



If yes, how many cyber resources are you planning to add to your organisation?



Setting up high-performance cyber security teams

Based on an interpretation of results across our survey, it is evident that the skill shortage across organisations will persist for the foreseeable future. Organisations are now required to develop and attract cyber resources despite the widespread shortage. The following are a few practices that might be considered for this:

1. Revamping recruitment processes and criteria

The current recruitment strategies must be modified to include innate flexibility around years of experience, exposure to tech stacks and the requirement for non-traditional degrees, subject to finding appropriate talent. Streamlining of recruitment processes could benefit organisations and candidates alike, by simplifying the process for candidates and improving the operational efficiency for companies.

People with in-demand skill sets like data analytics, risk management and cloud as core technical disciplines can be hired and then 'converted' into well-rounded cyber professionals. Such a move would help overcome the lack of diversity in cyber security, encouraging new skills, backgrounds, perspectives and opinions to look at the same problem from multiple angles.

2. Offering competitive salaries and benefits

Apart from competing in terms of salaries for hiring and retaining talent, organisations can explore innovative strategies for offering competitive benefits and conducive work environments to employees.

Benefits such as meals, healthcare, sponsored training, freebies, flexible work practices and loan repayments could help organisations position themselves better, while offering competitive and comparable salaries. Thinking outside the box, organisations can also subsidise green energy projects, invest time in social projects, etc. by aligning their actions with employees' environmental, social and governance (ESG) aspirations.

3. Collaborating to expand the talent pool

According to a survey by the World Economic Forum (WEF), the youth in South Africa, aged 15–24 and from marginalised backgrounds, are eager to upskill themselves. However, they lack the financial stability to do so.

Organisations can use this as an opportunity to cultivate their talent pipelines by partnering with educational institutions to sponsor education in the cyber security domain. Organisations can also hold internal skill mapping exercises to identify and upskill talent around cyber security.

4. Developing in-house talent

Investing in training and development programmes, and promoting cyber certifications, among other measures such as onboarding fresh talent, could be an effective way to develop in-house talent pipelines.

Organisations in Africa are offering vacation work programmes that can be leveraged to identify and build the cyber resource pool. Organisations can offer multiple career paths by bifurcating technological and managerial roles within cyber security to offer a broader choice to candidates, enabling them to upskill in their areas of interest. Additionally, organisations can facilitate internal transfers to enable job shadowing to provide on-the-job training opportunities to interested candidates.

5. Embedding advanced tech for security

Organisations with substantially large cyber security spending budgets can stay abreast of cyber risks by adapting next-generation technologies such as bots, automation and artificial intelligence (AI) to enhance the overall security monitoring.

By taking on tasks that previously required human intervention, automation can reduce the workload, increase efficiency, improve consistency, accelerate responses and help provide comprehensive decision support to security professionals.

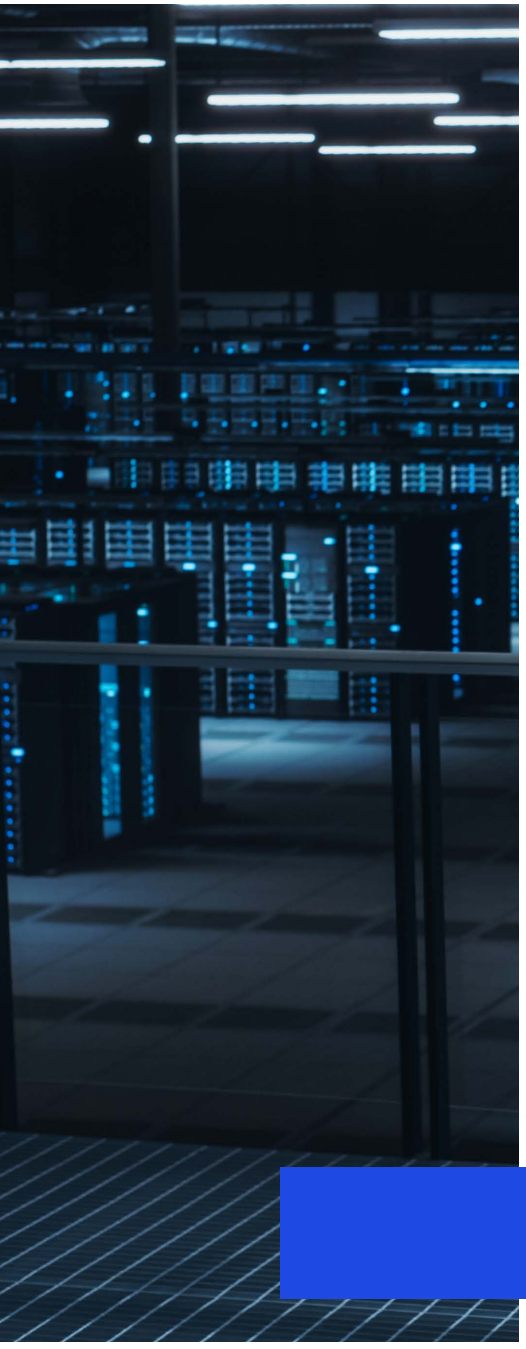
6. Outsourcing cybersecurity

Organisations can consider outsourcing their security needs to managed security service providers. They can completely outsource the cyber security function while navigating through the risk of outsourcing cyber security to a third party.

However, organisations might adopt a hybrid stance towards outsourcing, wherein the responsibility of securing core systems can be retained internally by prioritising the level of security required across functions.

05

Cyber attacks: the what, when and how?



Do African businesses carry a target on their back?

Organisations are witnessing a surge in cyber attacks such as network security compromise, malware, ransomware, cryptojacking and socially engineered malware. According to the WEF Global Cyber Security Outlook 2022,[12] an organisation faced an average of 270 attacks in 2021, a 31 percent year-on-year increase compared with 2020. There has also been a massive 151 percent increase in the volume of ransomware attacks over the first six months of 2021.

The increase in cyber incidents is driven by various factors such as monetisation of cyber attacks, attractiveness of personal information assets for syndicates, easy access to cyber attack tools, credential sales by initial access brokers, and availability of ransomware-as-a-service offerings. According to the Verizon Data Breach Investigations Report (DBIR) 2021,[13] the global uptrend in cyber incidents is primarily driven by organised crime perpetrators acting out of financial motivation, followed by admin-orchestrated and state-affiliated threat actors. The recent global crisis involving Russia and Ukraine could further propel cyber attacks as the war extends to the cyber-physical space, potentially leaving collateral cyber damage in its wake.

An estimated 2.5 quintillion bytes of data is being generated every day across the globe.[14] Hackers now have access to more sensitive data, with increased attack surfaces. The shift of the economy to a remote and hybrid working culture is also prompting cyber criminals to attack potentially weaker network and endpoint defences. In addition, according to an Interpol report, African businesses continue to face cyber threats in the form of online scams, digital extortion, business email compromise, ransomware, and botnets.

The increase in cashless payments, work-from-home enablement, and relatively low public-private partnership activity across Africa have resulted in an increase in cybercrimes after the COVID-19 pandemic.[15] South Africa's healthcare and banking sectors have faced distributed-denial-of-service (DDoS) attacks, while its maritime infrastructure has also been disrupted in the wake of cyber threats. Cities such as Johannesburg have been subject to data breach and ransomware attacks on key social services such as bill payments, social advices and emergency service networks. Countries such as Kenya have faced ransomware attacks on supply chain networks that were interconnected using cyber-physical systems.

---

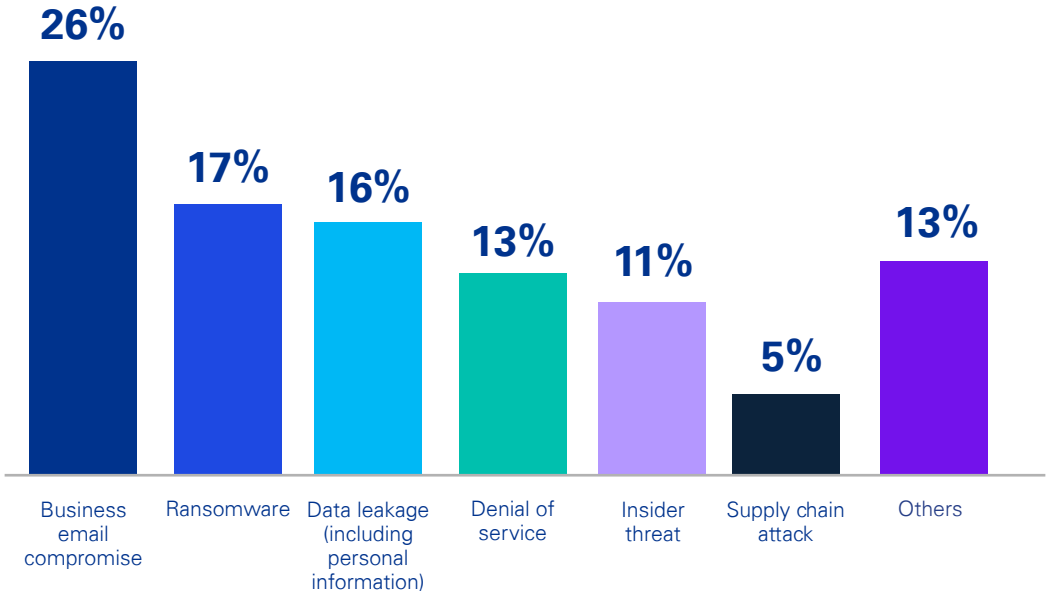
[12] Global Cybersecurity Outlook 2022
[13] Data Breach Investigations Report 2021
[14] Cybercrime and cybersecurity statistics
[15] Interpol Cybercrime Analysis Report

According to our survey, 46 percent of businesses with an ad hoc approach to cyber security have fallen victim to an attack. This is significantly higher than the 28 percent of respondents with robust cyber security and privacy programmes. Respondents have fallen victim primarily to cyber incidents such as business email compromise, ransomware, data leakage and denial-of-service attacks.

Business email compromise incidents are socially engineered attacks aimed at exploiting an organisation's business processes to fraudulently trigger payments to the attacker's account. It is not a surprise that business email compromise ranks as the top attack vector. A large factor in a successful attack is the failure of the human firewall.

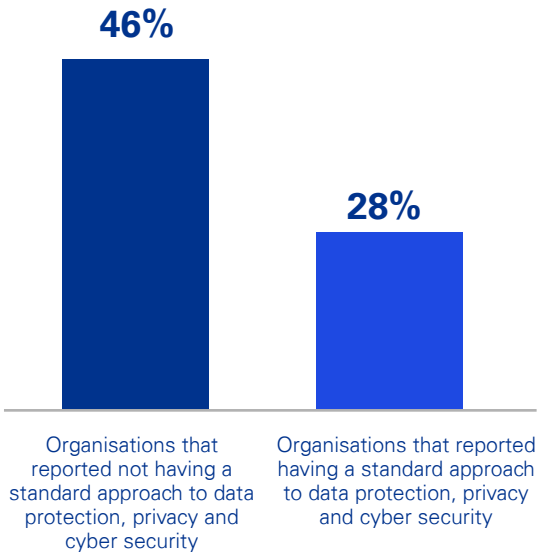
It is a well-worn cliché that humans are the weakest link in the security chain — with good reason. Consistent vigilance supported by strong process controls, underpinned by segregation of duties, remains an effective countermeasure against this form of social engineering.

Nature of cyber attacks faced by African companies



Others include threats such as intrusion or hacking, credential stuffing, phishing, malware and website redirects.

Strategic profile of cyber attack victims



According to our survey, about one in three organisations in Africa have experienced a cyber attack in the last 12 months. An analysis of the types of attacks reveals that while business email compromise stands out, attack types are pervasive across the board. This requires organisations to develop a strong security framework covering technical and human-focused defence/response strategy.

Ransomware: the big bad extortion

Organisations, whether small or large, must ensure seamless collaboration among key resources for coordinating and executing incident response plans. This is the type of problem that can`t be resolved with technology alone. A well-oiled response machine requires people and effective processes.

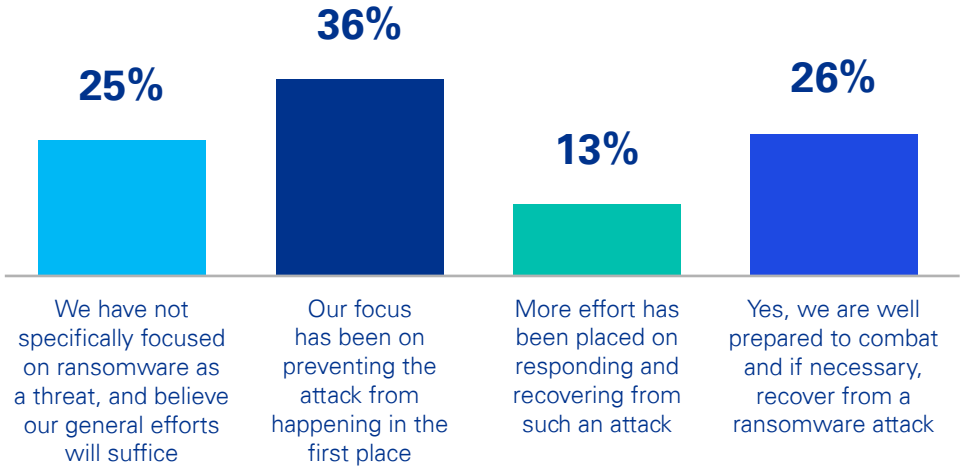
In the same way elite athletes rely on muscle memory for optimal performance, cyber incident response teams (CIRTs) can benefit significantly through regular crisis/ incident management simulations. Simulations or 'tabletop' exercises are a regular feature of mature cyber security culture, helping organisations improve their ability to detect network attacks earlier, enabling faster containment to prevent escalation. The drill should identify gap detection software and intelligence gathering to keep them on top of potential threats worldwide.

According to our survey, only one in three respondents is confident that CIRTs in their organisations are equipped to effectively deal with a major incident.

One in five data breaches can be attributed directly to a successful phishing attack[16]. Given this risk, the majority of African business still are not confident that their security awareness training program is bearing fruits.

[16]DBIR 2022 Report

Have you implemented a coordinated ransomware defense and response plan?



According to our survey, only one in four respondents feel that their organisations are prepared to combat and respond to cyber threats such as ransomware, whereas one in four respondents felt that organisations lacked focus on ransomware in the belief that general efforts would suffice.

In the centre of the two extremes, are organisations that have chosen to focus more attention on either preventing, or responding to a potential ransomware incident. The former option is certainly supported by conventional wisdom, following the mantra of "prevention is better than the cure." However, there is an emerging school of thought that subscribes to the cliché "its not a case of if, but when you will fall victim to an attack". They have therefore concentrated their efforts on ensuring that, no matter the extent of the incident, recovery processes will enable an effective return to business. While there are merits to both approaches, the sweet spot has to be somewhere in the middle. As responsible leadership, when is the last time you have sought to obtain the necessary assurance that your business can survive a ransomware attack?

Incident readiness: a playbook for your worst day

According to our survey, more than half of respondents across Africa that have recently fallen victim to cyber attacks, still lack confidence in the effectiveness of their cyber security incident response teams.

According to our survey, respondents from more than half of the organisations across Africa still lack confidence in the effectiveness of their cyber security awareness training. Mitigative measures such as performing log correlations, conducting threat intelligence studies and analysing anomalous user behaviour patterns to identify the root cause of cyber incidents, can help in building confidence in cyber security practices. Repeat attacks are on the rise and have been resulting in increased identity theft and account takeover fraud. The lack of action to pre-empt such threats and establish a strong line of defence, could leave organisations exposed to such repeat attacks.

To ensure cyber readiness, organisations must proactively approach, pre-empt and mitigate cyber threats. This includes assessing the threat landscape to pre-empt threats, while also evaluating the security across existing infrastructure to prioritise endpoints by the level of protection required.

Simple steps such as conducting cyber awareness and training programs, updating systems to the latest security patches, establishing a firewall, maintaining backups and defining role based access can enable organisations to pre empt cyber threats.

Regular assessments of remote working operations and penetration testing, can help evaluate the robustness of an organisation's network security. Simulated exercises to test the response to cyber incidents across business processes could also contribute towards building confidence in cyber response and readiness capabilities.

How confident are you in the effectiveness of your organisation's cyber security awareness training?

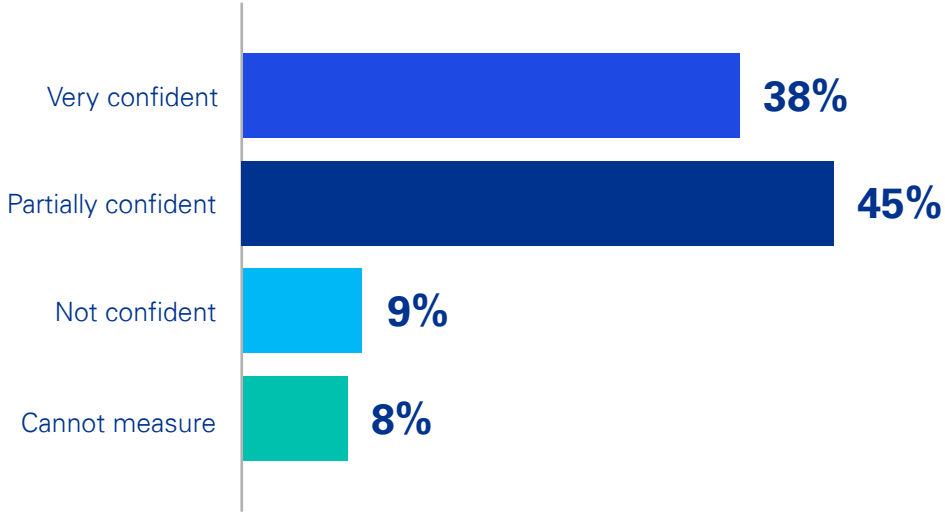
>50% not very confident about cyber security awareness trainings.

According to our survey, large organisations were found to be more confident about the effectiveness of their cyber security response teams compared with medium and small organisations. This gap can be bridged by partnering with managed service providers with the necessary expertise.

Showing more clearly the potential links between physical hazards (for example operational technologies) and cyber issues will build a greater appreciation of the broader impact of an attack and help reduce the risk of an incident in the first place. Incident playbooks can play a key role in supporting CIRTs in the nuances between various cyber attack types, support decision-making and boost the overall effective response times.

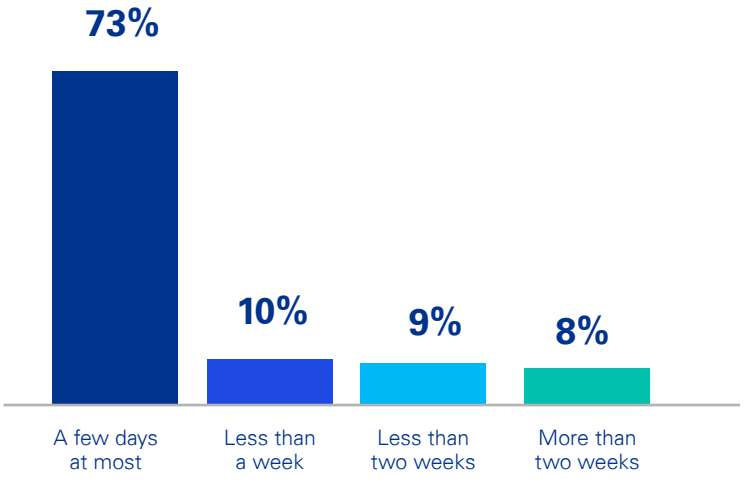
Organisations should also evaluate the implementation of tools such as security orchestration automation and response (SOAR) which may help automate the cyber security function, freeing up resources for more critical tasks.

How confident are you that the cyber security incident response team (CIRT) is equipped to effectively deal with a major incident?



Recovering from a cyber security incident

For respondents that experienced a cyber attack in the last 12 months, how long did recovery efforts take?

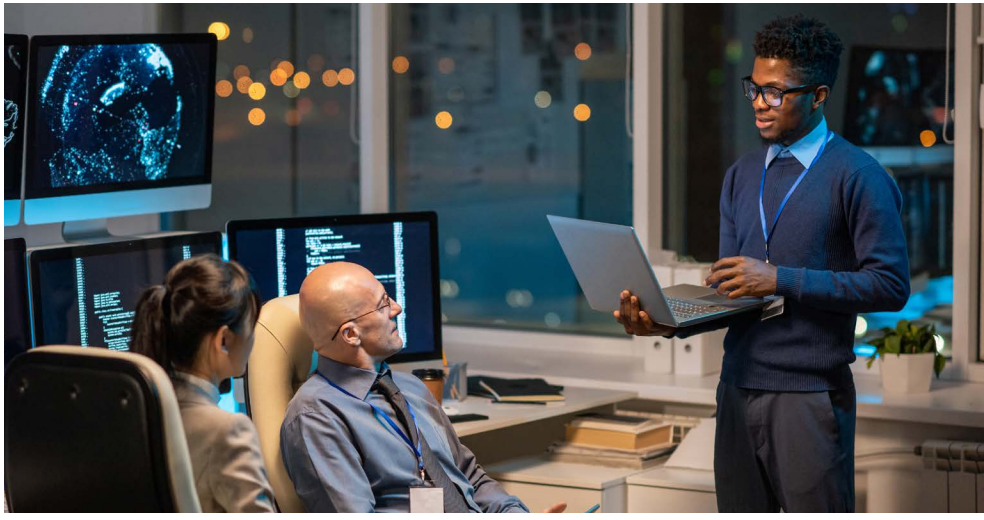


Organisations have traditionally approached cyber security using a prevention-based approach. However, the modern cyber landscape raises a critical question about "When will an organisation's systems be breached", rather than "Will they be breached?." Thus, organisations need to focus equally on defence and response efforts. An effective cyber security incident response plan aims to ensure business continuity, provide data asset protection and prevent potential data loss in the future.

Our respondents report relatively quick recovery turnaround times following a cyber incident. More than 80 percent report recovering in a few days, up to a week.

Whether a few days or more, the financial impact of lost productivity and reputational repercussions can be devastating. Incident response efforts must be well integrated with business continuity efforts to limit the impact on your staff and customers. Transparency often pays off in the court of public opinion. It is therefore crucial that public relations and/or communications departments are well briefed and ready to manage the message.

According to our survey, about two in three respondents from organisations across Africa were confident of quick recovery from cyber attacks Nevertheless, organisations must build commensurate confidence in the overall cyber awareness and incident response function to drive digital trust and positively influence consumer perception.



06

Building effective SOCs

According to our survey, one in four organisations across Africa leveraged ad hoc security solutions that provided only limited security alerts.

Why, and how to establish SOCs

Organisations are establishing security operation centres (SOCs) in various operating models such as virtual SOCs that leverage a team of remote professionals for monitoring security controls and multi-function SOCs in which internal teams perform SecOps in addition to current work roles. Hybrid SOC deployments include a team of internal and external third-party contractors for performing SecOps, while dedicated SOC formats include maintaining an internal team focused exclusively on security operations. Whichever model you choose will largely depend on your risk profile and resource budget. There is no 'one-size-fits-all' approach; however, it remains crucial to ensure that the chosen model has a clear mandate and open lines of communication, and is subject to regular effectiveness assessments.

According to our survey, about one in four respondents highlighted that their organisations have established mature in house security operations centers signifying their focus on proactive monitoring of operations. Organisations that have successfully pre-empted or defended against cyber attacks can further strengthen their SecOps practices by employing dedicated internal SOC teams for cyber threat and incident risk management. They can also organise sensitisation training to educate cyber teams about the impact of its decisions and the negative consequences that an organisation may face in the event of a cyber breach.

According to our survey, about one in four respondents claimed that their organisations are leveraging ad hoc security solutions that provide limited security alerts. Organisations relying on ad hoc solutions for security response must consider implementing a more robust toolset, capable of correlating disparate events into a risk aware alerting mechanism, for example an enterprise system information and event management (SIEM) solution. These solutions can improve network and endpoint visibility by establishing continual monitoring, leveraging AI-enabled threat detection and other intelligent solutions. By automating routine tasks, organisations can reduce errors that occur as a consequence of repetitiveness in tasks. Mapping and regularly assessing systems is crucial for establishing feedback loops for continual improvement.

Which of these adequately describe your organisation's security operations centre (SOC)/ cyber security team?

[17]IDG Research

In transitioning from an ad hoc toolset to a SIEM, organisations must consider the system integration landscape to lay out the objectives of deploying the SIEM. More mature systems can, for example, collerate events between enterprise systems and supporting infrastructure solutions to identify complex indicators of compromise (IOC's). Organisations must design fit to purpose SIEM solutions that intelligently monitor activity, while disregarding noise across devices.

About, one in four respondents from our survey indicated that their organisations outsource SOCs to managed security service providers or maintain hybrid SOCs. Large organisations can augment existing solutions leveraging outsourced solutions, whereas SMEs can leverage outsourced/hybrid SOCs to put in place security operations while keeping costs in check.

According to IDG research, about 78 percent of senior IT leaders believe their organisations lack sufficient protection against cyber attacks despite increased IT security investment. Interestingly this points to the fact, that maintaining effective cyber security measures does not solely depend on investments in cyber security tools, but also involves the need for robust cyber security strategies and security operations[17].

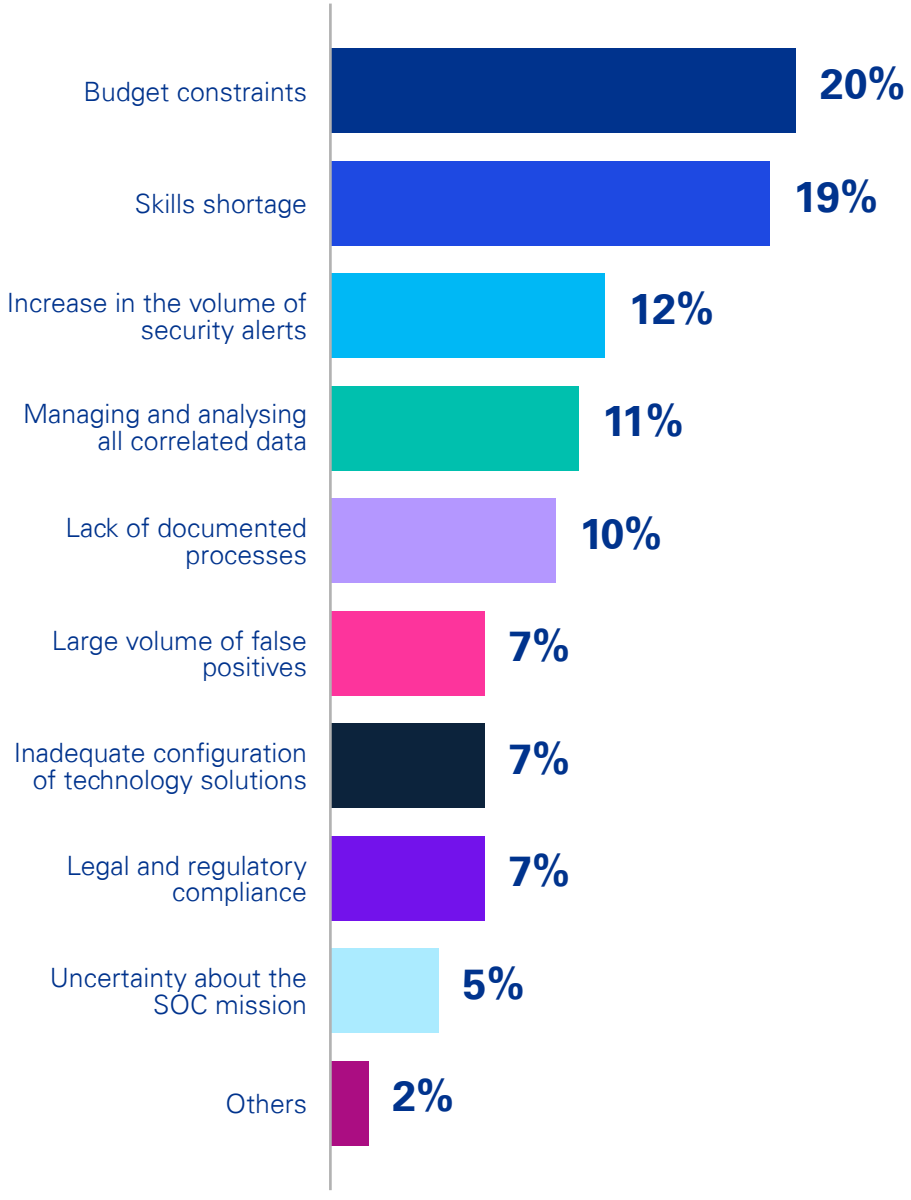
As per our survey, the primary challenges faced by African organisations in operating effective SOCs, have been budgetary constraints, followed by skill shortage and an inability to effectively deal with the increase in the volume of security alerts.

According to our survey, budgetary constraints, skill shortage and an increase in the volume of security alerts were among the top concerns for more than 50 percent of respondents. Regardless of the current economic challenges, budget constraints will always be a challenge as businesses weigh the opportunity cost of every spending decision. The average cost of deploying and operating SIEM solutions is around US$50,000, reaching as high as US$1 million for the first year and about US$0.5 million each consequent year to keep the solution running.[18]

An effective SOC requires more than just the latest and greatest technology solutions. Skilled resources are required to effectively steer the ship — configure tooling, handle incident response, investigate and triage alerts, offer subject matter expertise, and more. The shortage of cyber talent makes it difficult to staff well-resourced teams. As mentioned previously, outsourcing can assist in managing capex and overcome skill gaps; however, it should not come at the expense of reduced process accountability and oversight.

According to our survey, 12 percent of respondents noted challenges in handling the increased volume of security alerts. However, this challenge can be mitigated by automating security processes and applying threat intelligence to flag only crucial cyber events based on key indicators of compromise.

What are your top challenges in operating an effective SOC?



[18] Peerspot

Establishing an effective SOC capability

The transformation of enterprise IT infrastructure and networks has led to the emergence SOCs as a centralised security capability that offers high visibility into the estate.

01. Defining SecOps processes

The development of a mission and detailed documentation of security practices is a fundamental step in setting the right tone and operational framework for SOCs. Organisations must define and document a focused SOC strategy that includes details about cyber event monitoring, analysis, threat intelligence and prescribed responses to establish effective SOC processes.

02. Security operations training

SOC teams should keep abreast of the latest threats together with tools, techniques and procedures (TTPs) employed by threat actors. Training can also consider targeting a wide range of stakeholder groups, including business users, leadership and SOC teams to help ensure effective incident detection and response practices. Red vs Blue teaming, or the more collaborative Purple Team exercises are a proven way to upskill team members while identifying process inefficiencies.

03. Driving collaboration amongst stakeholders

Effective collaboration among teams, supported by deploying adequate platforms, procedures and frameworks for facilitating such collaborations, is crucial for operationalising SOC teams. Developing purpose-driven roles and responsibilities, underpinned by effective communication channels both within the SOC and among business stakeholders, can go a long way towards achieving that.

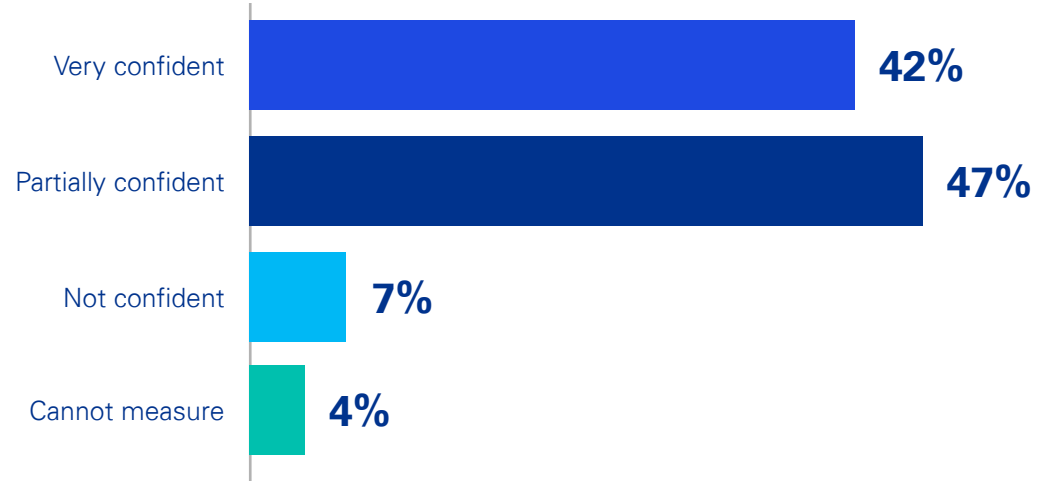
04. Deploying adequate SOC tools

SOCs must be equipped with adequate tools based on their suitability to an organisation's existing network and IT infrastructure, and a prioritisation of threat profiles and key information assets. Organisations can consider using tools such as endpoint detection and response (EDR), SOAR and SIEM to centrally establish event monitoring, analysis and response processes.

05. Automating the security environment

To ensure seamless security operations, organisations must identify repetitive and manual SOCs processes, and leverage AI and automation tools to automate SOC functions, wherever feasible. Practices such as infrastructure and network monitoring, anomaly detection and vulnerability scanning are known to be good candidates for automation due to the high volume and repetitiveness of these tasks. This helps in dealing with sudden spikes in the volume of security alerts across the cyber landscape, enabling professionals to focus on relatively crucial incidents at a given point in time.

How confident are you about the cyber security controls implemented by your organisation to detect and mitigate the threat of a cyber incident?



According to our survey, more than half of the respondents from organisations were still not very confident in the cyber security controls implemented by their organisation to detect and mitigate the threat of a cyber incident.

Building confidence in outsourced cyber security operations

Organisations either establish internal cyber security operational teams, outsource cyber security operations or leverage a hybrid approach. It is important, however, to keep in mind that while you can outsource a process, you can never fully outsource a risk. It is very likely that the outsourced service provider faces similar staffing and skill challenges that their clients do. It is therefore crucial that outsourced or hybrid models are managed with effective oversight, at a process governance as well as a technical level. A structured 'Purple Team' exercise based on likely attack vectors and indicators of compromise (for example the MITRE ATT&CK framework) can be instrumental in assessing technical and process capabilities. When conducted in a 'dawn raid' style, it can provide valuable insight into the real-world readiness of the SOC function, whether internal, outsourced or hybrid.

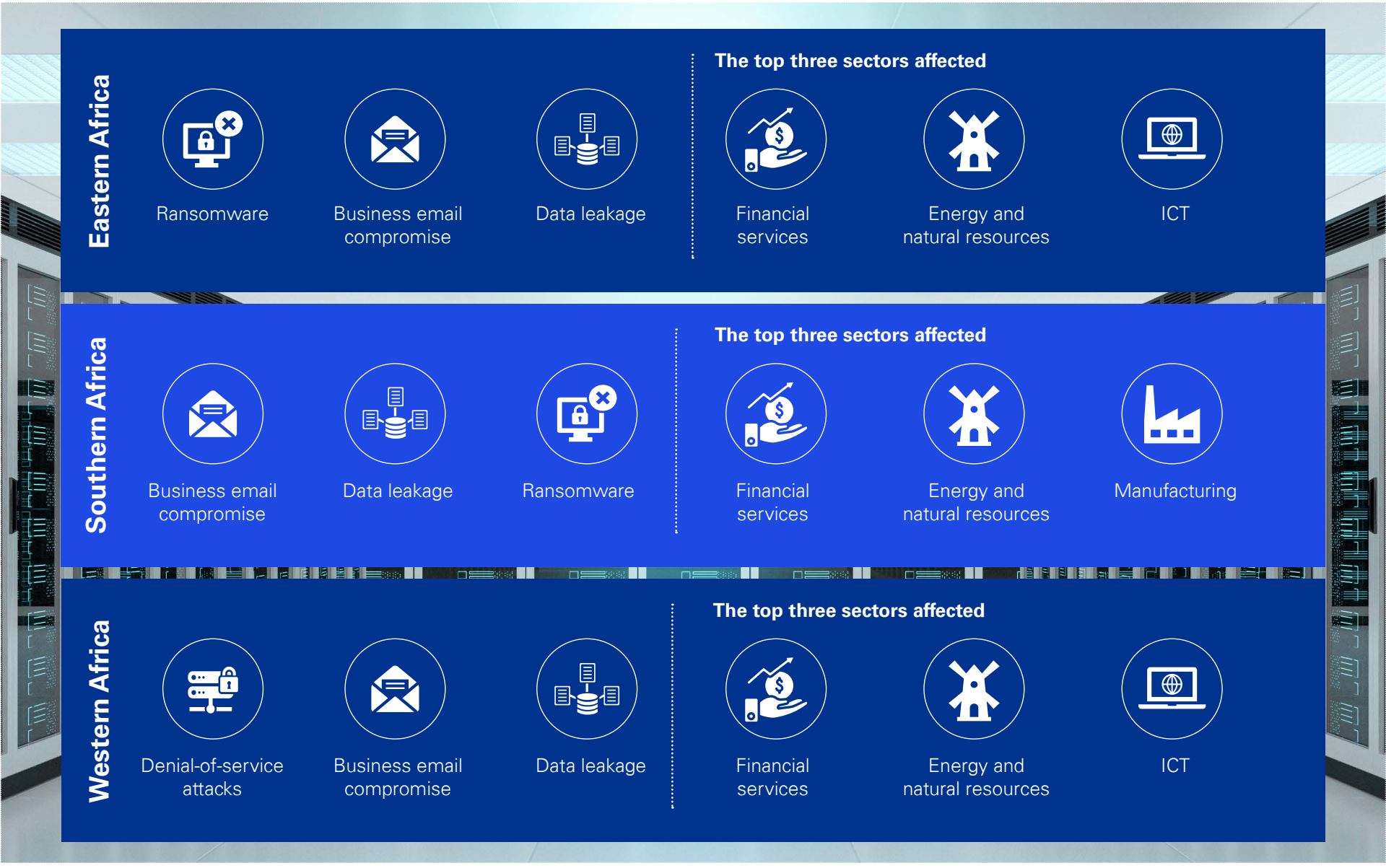
"Knowing what has happened in the past, and what is happening now on your systems, is key to understanding how to defend your IT environment in the future. Immediate triage of alerts and potential compromises, provide actionable intelligence to support decision-making."

Anthony Muiyuro, Cyber Lead KPMG East Africa

07

Regional analysis

Cyber attacks and affected sectors across Africa



According to our survey, organisations across East Africa have been driving the highest adoption of digital transformation, with 89 percent of the respondents stating that their organisation is undergoing digital transformation or has already implemented large-scale transformational projects.

Countries across East Africa have a prime focus on the adoption of ICT in their economic landscape. For instance, Kenya has weaved ICT-focused economic policies into its cyber security strategy to promote socio-economic development across the region. Countries such as Rwanda and Uganda are also in the process of drafting legislation about cyber security. In addition, Rwanda has been known to periodically conduct cyber attack simulations, involving government and private stakeholders, to test the effectiveness of cyber security controls and policies.

According to our survey, 31 percent of the respondents from East Africa report that their organisations have been victims to cyber attacks. This translates to the highest proportion of cyber attacks being reported among the African regions. However, it is heartening to note that organisations in East Africa have taken cognisance of the cyber risk landscape and have a sharp focus on cyber security, regionally, with about 77 percent of the organisations having well-defined and regularly reviewed cyber strategies or having strategies with measurable KPIs.

The sharp focus on cyber security by East African organisations can primarily be attributed to the rapid development and adoption of digital technology across business sectors with limited expertise and awareness around technology and digital infrastructure. The digital transformation of East Africa has been driving an influx of workers and regional tourism. These factors combined with the setting up of key banking institutions across countries such as Kenya, Uganda and Rwanda, have exacerbated cyber threats in the region.

89%

of the respondents in East Africa noted that their organisation is undergoing digital transformation.

31%

of the respondents from East Africa report that their organisations have been victims to cyber attack. This translates to the highest proportion of cyber attacks being reported among the African regions.

According to our survey, organisations across West Africa are closely following Eastern African countries in the adoption of digital transformation, with 82 percent of the respondents stating that their organisation is undergoing digital transformation or has already implemented large-scale transformational projects.

Countries in West Africa are now interconnected and are involved in widespread digital adoption. The countries have adopted a series of cyber security measures to supplement the ICT growth across the region. Additionally, the region has witnessed collaborations with partners such as the Global Forum on Cyber Expertise (GFCE), Cybersecurity Alliance for Mutual Progress (CAMP), Council of Europe (CoE), and United Nations Conference on Trade and Development (UNCTAD) to establish cyber security controls. Countries such as Ghana have established the Cybersecurity Act, 2020, creating the Cyber Security Authority (CSA) to further the development of cyber security in the country.[19]

According to our survey, 23 percent of the respondents from Southern Africa report that their organisations have been victims to cyber attacks. This translates to the lowest proportion of cyber attacks being reported among the African regions. Organisations in Southern Africa have taken cognisance of the cyber risk landscape, with about 74 percent of the organisations having well-defined and regularly reviewed cyber strategies with measurable KPIs.

As the digital transformation across countries in Southern Africa approaches maturity, countries in the region are taking commensurate steps to build cyber resilience. Recent developments in cyber security and privacy legislation have been important drivers for the increase in cyber security and compliance. Initiatives such as the Cyber Security Capacity Center for Southern Africa (C3SA)[20] are driving cyber initiatives through research and active collaborations among countries in Southern Africa. It is encouraging to see cross-regional collaboration between countries through national forums aimed at building cyber expertise.

[19] CSA
[20] C3SA

82%

of the respondents in West Africa noted that their organisation is undergoing digital transformation.

23%

of the respondents from Southern Africa report that their organisations have been victims to cyber attack. This translates to the lowest proportion of cyber attacks being reported among the African regions.

08

Global viewpoint

Lessons for Africa in emerging global trends

Countries across the world are now coming together to collaboratively defend against and mitigate cyber threats. Governments are adopting national cyber security frameworks to accommodate cross-border information sharing and investigations to offer and leverage international cooperation. About 66 countries have signed/ratified the Budapest Convention for defending against cyber crime and achieving international collaboration and information sharing to pre-empt and mitigate cyber threats.

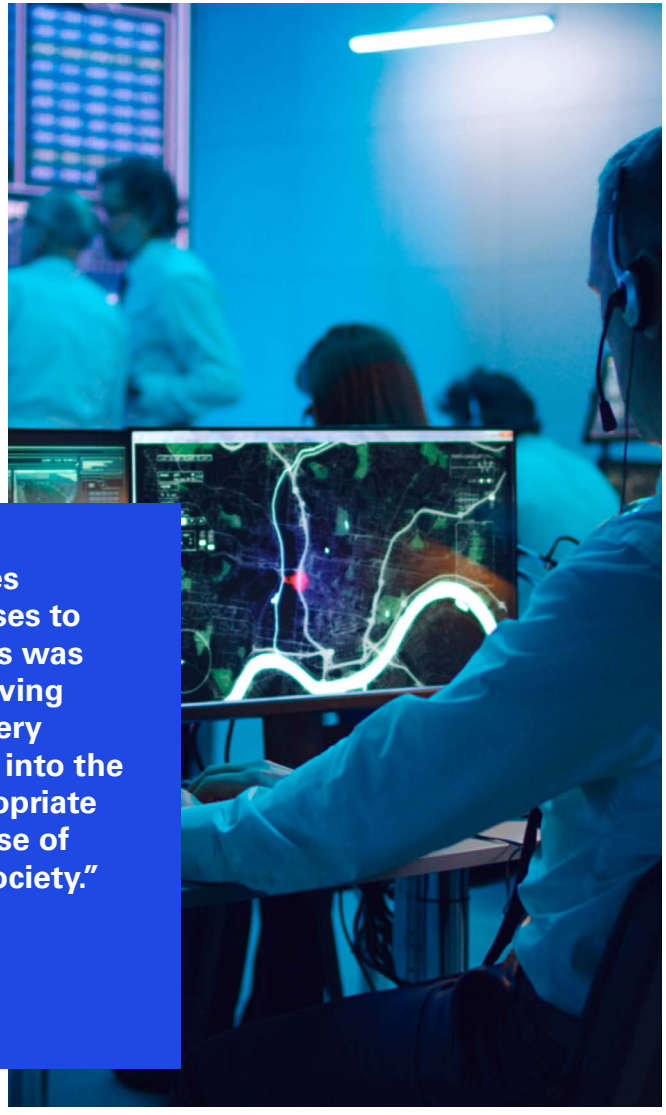
Governments are also focusing on setting up virtually accessible computer security incident response teams (CSIRTs) to enable real-time information sharing and to ensure the availability of a designated point of contact in each country to counter cyber threats. CSIRT America is one such organisation that has been working towards uniting countries in the western hemisphere to deploy and operate CSIRTs for improved response to global threats through international cooperation and collaboration.

There has been a global push to enter public-private partnerships to help mitigate and counter cyber threats. The US Chambers of Commerce, the UK National Cyber Strategy and the Government of India are known to encourage public-private partnerships. These partnerships aim to encourage information sharing on threats to organisations and promoting best practices and dialogue. This could assist them to better interpret and analyse the nature of cyber threats, thus working in collaboration to secure operations and facilitate seamless cooperation towards cyber security.

Cyber threat landscape at a glance

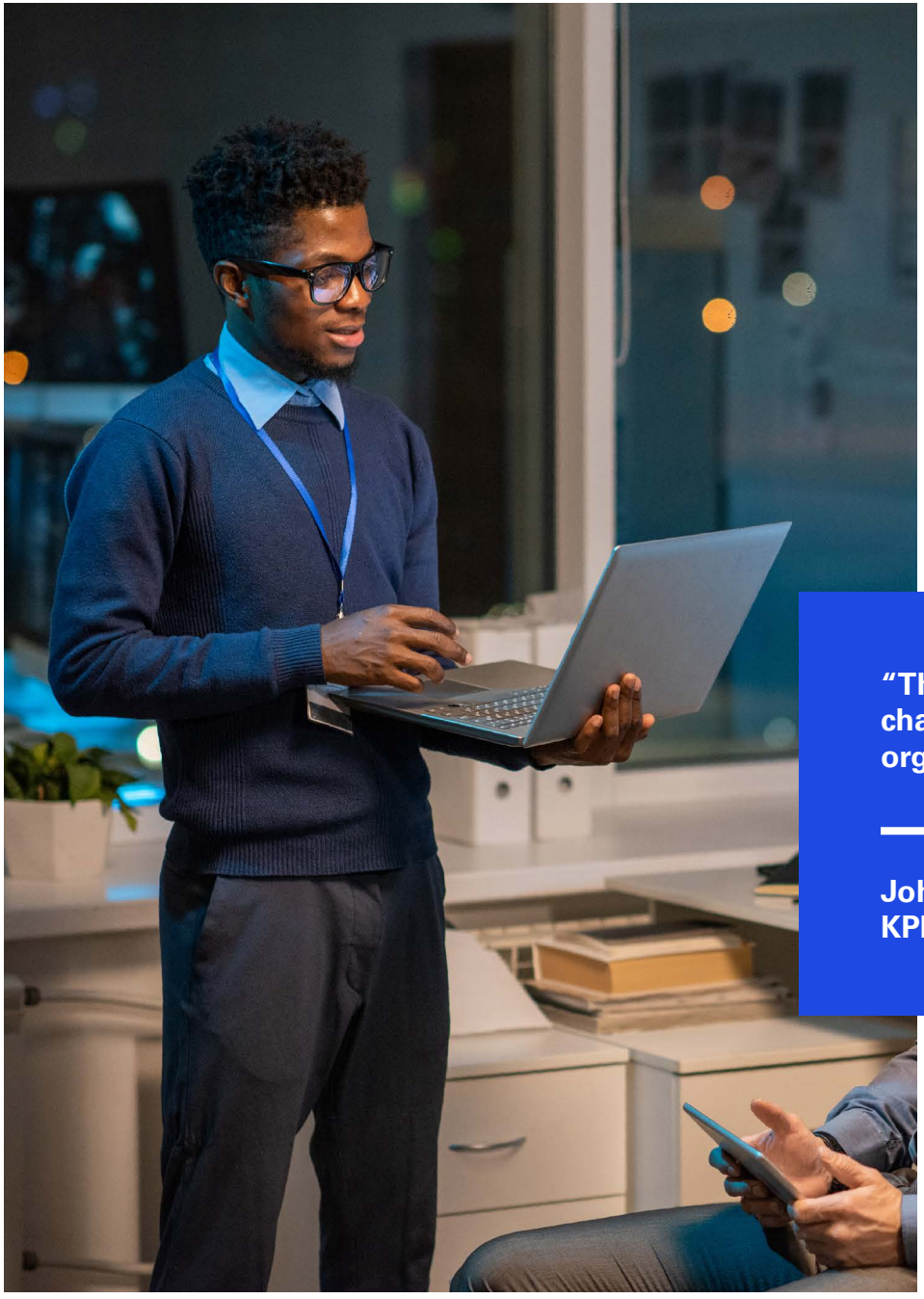
Rising cybercrime shows no sign of slowing. In February 2022, the conflict between Russia and Ukraine prompted widespread state-sponsored cyber attacks across both countries. This warfare extended to target banks, government bodies and crucial financial institutions. These attacks have resulted in operational delays and unplanned downtime for organisations across the EU. African organisations operating within these regions need to take cognisance of the impending cyber threats across these regions and take measures to counter state-sponsored terrorism.

African nations are no longer protected by obscurity and make the list of the most targeted countries across the world. The US, the UK and Saudi Arabia have been identified as leaders across the global cyber security landscape. African governments can learn from these countries to explore cyber legislations and their impact. This can help in drafting well-rounded legislations that have been tailored to the quirks and cogs of the local landscape and culture. For instance, cyber awareness training can be customised around the local culture to counter socially engineered attacks.



"The pandemic brought significant opportunities for both businesses worldwide and cyber criminals. Whilst the pandemic forced businesses to digitalise and transform the way they operate, the pace at which this was completed presented weaknesses in defences to cyber criminals. Having said that, the power of digital technology continues to transform every aspect of our lives, making digital trust absolutely critical today and into the future. Organisations must build digital trust by implementing appropriate security and governance frameworks, plus the responsible, ethical use of tech and data as we continue to embrace technology in every day society."

Akhilesh Tuteja, Global Cyber Security Leader, KPMG International



Organisations need to work in congruence with states to implement national cyber security policies. Organisations also need to focus on partnerships, frameworks and cooperative information sharing to equip themselves to pre-empt and defend against cyber threats while maintaining a focus on enabling privacy. Organisations must also counter threats by achieving a balance between proactive and reactive responses. Old but time-tested methods such as maintaining backups might come in handy.

Business email compromise and ransomware have emerged as commonly exploited channels. By maintaining preparedness for such threats, organisations can position themselves at advantage while countering them. We have observed that organisations are now approaching cyber security head on and building their cyber processes to ensure cyber security and build digital trust.

"The increasing risk across digital value chains requires new mitigation strategies by organisations globally."

John Anyanwu, Partner and Head, Cyber Security, KPMG in Nigeria and Africa Cyber Lead

09

Key takeaways and next actions

Key insights and actions

01. Governments and organisations across Africa are working to implement regulations and nurture the cyber talent pool

Cyber security is among the top threats to economic activity and is one of the key challenges affecting business sustainability. Africa's digital landscape is maturing, driven by an increase in remote working after the pandemic, increased adoption of digital technology across business sectors, expanding mobile internet usage, and increased reliance on connectivity and smart technology. This has led to a proportionate increase in cyber threats in the form of business email compromise, ransomware, data leakage, espionage, supply chain disruptions and other malware targeted at mobile devices. In response to the outbreak of cyber threats, organisations and governments in Africa are now focused on implementing legislations and frameworks to mitigate cyber security and data privacy risks. They are also focused on developing the talent pool of cyber security professionals, driving public awareness about cyber security, and driving collaborations with national and international stakeholders to pre-empt and mitigate threats. Organisations must keep up with the changing times to ensure that they are not left behind.

02. Organizations need to integrate cyber focus into their core strategy

There has been a significant increase in cyber threats with organisations constantly facing challenges to uphold consumer privacy and data security across the African landscape. As organisations take steps towards countering these threats, they need to focus on building clearly defined cyber strategies that are linked to KPIs and KRIs, with measurable outcomes, aligned to the core business strategy. Organisations also need to dedicate a budget towards cyber security to ensure an adequate war chest to combat the threats. Organisations need to adopt strong complementary cyber security and privacy frameworks to execute strategies to maintain digital trust.

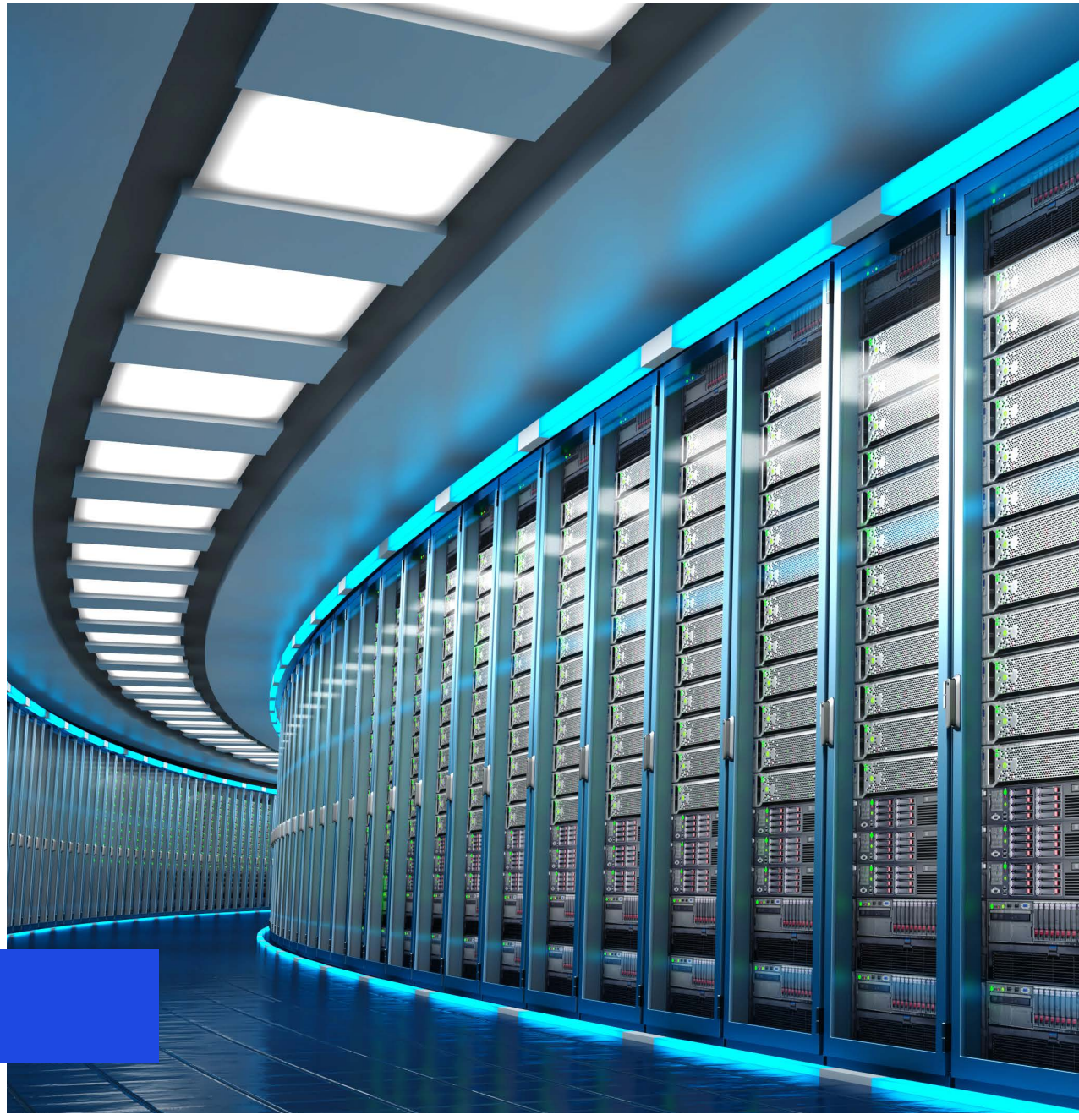
03. To tackle resource shortage, organisations need to be innovative in their hiring

The cyber skills and resourcing chasm in Africa has further broadened during and after post the pandemic. This gap needs to be addressed through public-private partnerships, training programmes and certification initiatives at a grassroots level. The majority of the organisations are inclined towards hiring cyber professionals within the next 12 months. They must be prepared to innovate their hiring strategies, offer competitive salaries with added benefits and revamp recruitment criteria for effective resourcing. They must also evaluate outsourcing cyber security and technological innovation as a means to stay abreast of cyber threats. In addition, the modern workforce becomes increasingly cognisant of their organisations' ESG efforts. Responsible and ethical behaviour is a key driving force behind attracting and retaining top talent.

04. Proactive threat identification and defence is critical for effective prevention, mitigation and response

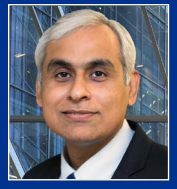
Organisations need to proactively monitor critical information assets and underlying systems to counter threats. They need to actively train CIRTs leveraging, regular crisis/incident management simulations and Purple Team exercises.

Organisations across Africa need to build confidence in their cyber security controls and measures. Effective, fit-for-purpose security operations can drive consistent cyber security practices while navigating through constraints such as budget shortages and cyber skill shortages. In addition, technologies such as EDR, SOAR and SIEM solutions can be leveraged to limit the manual workload on overstretched teams. Well-exercised cyber incident response and recovery plans will enable the CSIRTs to effectively navigate a crises, should the worst come to pass.



Key contacts

KPMG team



Akhilesh Tuteja
Global Cyber Security Leader
KPMG International
E: atuteja@kpmg.com

Dani Michaux
EMA Cyber Security Leader
KPMG in Ireland
E: dani.michaux@kpmg.ie

John Bowen
Africa COO
KPMG South Africa
E: john.bowen@kpmg.co.za

John Anyanwu
Partner and Head, Cyber Security
KPMG in Nigeria & Africa Cyber Lead
E: john.anyanwu@ng.kpmg.com

Marcelo Vieira
Partner and Head of Cyber Security
KPMG South Africa
E: marcelo.vieira@kpmg.co.za

Marcel Kopoin
Head of Advisory
KPMG Francophone Sub-Saharan Africa
E: mkopoin@kpmg.ci

Nancy Mosa
Partner, Head of Technology Assurance
KPMG East Africa
E: nmosa@kpmg.co.ke

João Madeira
Partner and Head of Cyber
KPMG Angola
E: jmadeira@kpmg.com

Anthony Muiyuro
Cyber Lead
KPMG East Africa
E: amuiyuro@kpmg.co.ke

Samuel Aluko
Cyber Lead
KPMG Ghana
E: samuelaluko@kpmg.com

kpmg.com/socialmedia