Photo by Vukheta Mukhari
Kearney, Johannesburg

Cybersecurity in Africa—a call to action

KEARNEY

Executive summary

The African cybersecurity market was valued at $2.5 billion in 2020 and is projected to increase in value to $3.7 billion by 2025, which encompasses the amount that organizations are investing into their cybersecurity capabilities. It is estimated that the region loses more than $3.5 billion annually due to direct cyberattacks, and billions more from missed business opportunities caused by the resulting reputational damage from the attack. It is therefore crucial that the region steps up coordinated efforts to address growing cybersecurity risks.

The region's growing strategic relevance, due to its economic development and evolving digital landscape, makes it a prime target for cyberattacks. Cyber resilience is generally low, and countries have varying levels of cyber readiness. Specifically, countries in the region lack the strategic mindset, policy preparedness, and institutional oversight needed to address cybersecurity issues. The absence of a unifying framework, even among the most prepared countries, makes regional efforts largely voluntary. This leads to an underestimation of value at risk and significant underinvestment.

In addition, because cyber risk is perceived to be an information technology (IT) problem rather than a business problem, regional businesses do not have a comprehensive approach to cybersecurity. The region's nascent cybersecurity industry faces shortages of homegrown capabilities and expertise. Products and solutions are fragmented, and there are few comprehensive solution providers.

There are four drivers that will increasingly expose Africa to outsized cyber risk:

— The growing interconnectedness and flow of people, goods, and information across the region with the realization of the African Continental Free Trade Area (AfCFTA) will intensify systemic risk. This means the region will only be as strong as its weakest link.

— Widespread socioeconomic difficulties—accelerated by the COVID-19 pandemic, food crises, and inflation—have led to diverging national priorities and a varying pace of digital evolution, which will continue to foster a sustained pattern of underinvestment.

— Countries' hesitancy to share threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.

— Technological advances will render threat monitoring and responses more complex, particularly given the rise of encryption and multi-cloud operations, the proliferation of Internet of Things devices, and the convergence of operational technology (OT) and IT environments.

Responses to these cybersecurity challenges must be comprehensive and collaborative. They will require input from multiple stakeholders to deal with large-scale cyber threats and enable Africa's unobstructed leap into the global digital economy. Foremost, it will require an active defense mindset that sees countries working together to defend and leverage Africa's resources.

The ideal regional cybersecurity defense playbook needs to address a four-point agenda (see figure 1 on page 2).

Figure 1

The regional cybersecurity defense playbook should address four key points

Source: Kearney analysis

1. **Elevating cybersecurity on the regional policy agenda** calls for the immediate implementation of Kearney's Rapid Action Cybersecurity (RAC) Framework at the national level, which will harmonize cyber resilience across the region. The framework is a comprehensive 11-point action agenda that will help national governments address gaps in strategy, policy, legislation, governance, and capabilities related to cybersecurity. In addition, the African Union (AU) has taken steps to extend collaboration on cybersecurity across the region by establishing its legal framework—the African Union Convention on Cyber Security and Personal Data Protection—which at the time of writing had been signed by 16 countries but ratified by only 13.[1] To enforce the adoption of the framework across African countries, the AU needs to implement both the incentive mechanism and sanctions/restrictive measures for non-compliance.[2] The African Union Commission (AUC) chairperson's annual report could consider including a review of each country's progress toward achieving the milestones set by the RAC Framework.

2. To **secure a sustained commitment to cybersecurity** and address investment gaps, African countries need to collectively spend around $22 billion on cybersecurity between 2022 and 2026. That's the equivalent of about 0.25 percent of total regional annual gross domestic product (GDP).[3]

3. Concerted efforts need to be made to **fortify the ecosystem** by advocating for businesses to adopt a risk-centric, layered-defense approach to dealing with cyber threats. This includes instilling a culture that enables the sharing of threat intelligence; extending cyber resilience measures across the supply chain; and encouraging the development of regional public–private partnerships (PPPs), industry alliances, and international partnerships.

[1] Status update by African Union (March, 2022)
[2] Kearney analysis (2022)
[3] Kearney analysis: benchmarking with mature markets (such as US, UK, Germany); Gartner, Oxford economics, World Bank

4. Finally, because cybersecurity is a continuously evolving challenge, the region must **build the next wave of cybersecurity capabilities**. This requires cultivating the future generation of security professionals and driving R&D around innovative technologies that can address emerging and unforeseen threats. Corporate boards and chief information security officers (CISOs) have important roles to play in creating a defense-in-depth culture in their organizations. They must help to elevate cybersecurity topics to agendas at board level and establish the CISO function as an independent reporting function. Given the magnitude and complexity of the region's challenges and its unique context, Africa must embrace a game-changing approach based on greater cohesion and collective use of resources to achieve a cyber-resilient future.

The region's growing strategic relevance, due to its economic development and evolving digital landscape, makes it a prime target for cyberattacks.

Africa: a target for cybersecurity threats

Regional cybercrime and the future of cyber threats

The African continent has seen a steady increase in Internet penetration since 2015, fueled by greater access to electricity, the decreasing costs of Internet-connected devices, and an increased focus on the Internet of Things (IoT) (see figure 2 on page 5). By 2021, Internet access across Africa had grown to more than 28 percent, with mobile penetration forecasted to exceed 90 percent by 2023.[4,5] Investment in the region's cybersecurity market is forecasted to grow from $2.5 billion in 2020 to $3.7 billion in 2025—a compound annual growth rate (CAGR) of 7.9 percent.[6,7] Despite this investment it's estimated the region loses more than $3.5 billion annually due to direct cyberattacks, and billions more from missed business opportunities caused by the resulting reputational damage from the attack.[8,9]

A cross-country analysis of cybercrime trends indicates that significant cybercrime activity can take place where there is at least 10 to 15 percent Internet penetration.[10] That means Africa is precariously poised at a point of risk and opportunity on its digital journey.

Rapid growth of the IoT and the "bring your own device" (BYOD) trend within organizations has increased the number of devices and applications that are vulnerable to persistent advanced threats and makes it harder for IT teams to monitor and track data flow. The COVID-19 pandemic has exacerbated this problem, forcing employees to work from home and companies to turn to online operations, which exposes them to more cyber threats. During 2020, 61 percent of IT teams globally stated that they had seen an increase in the number of attacks targeting operations.[11]

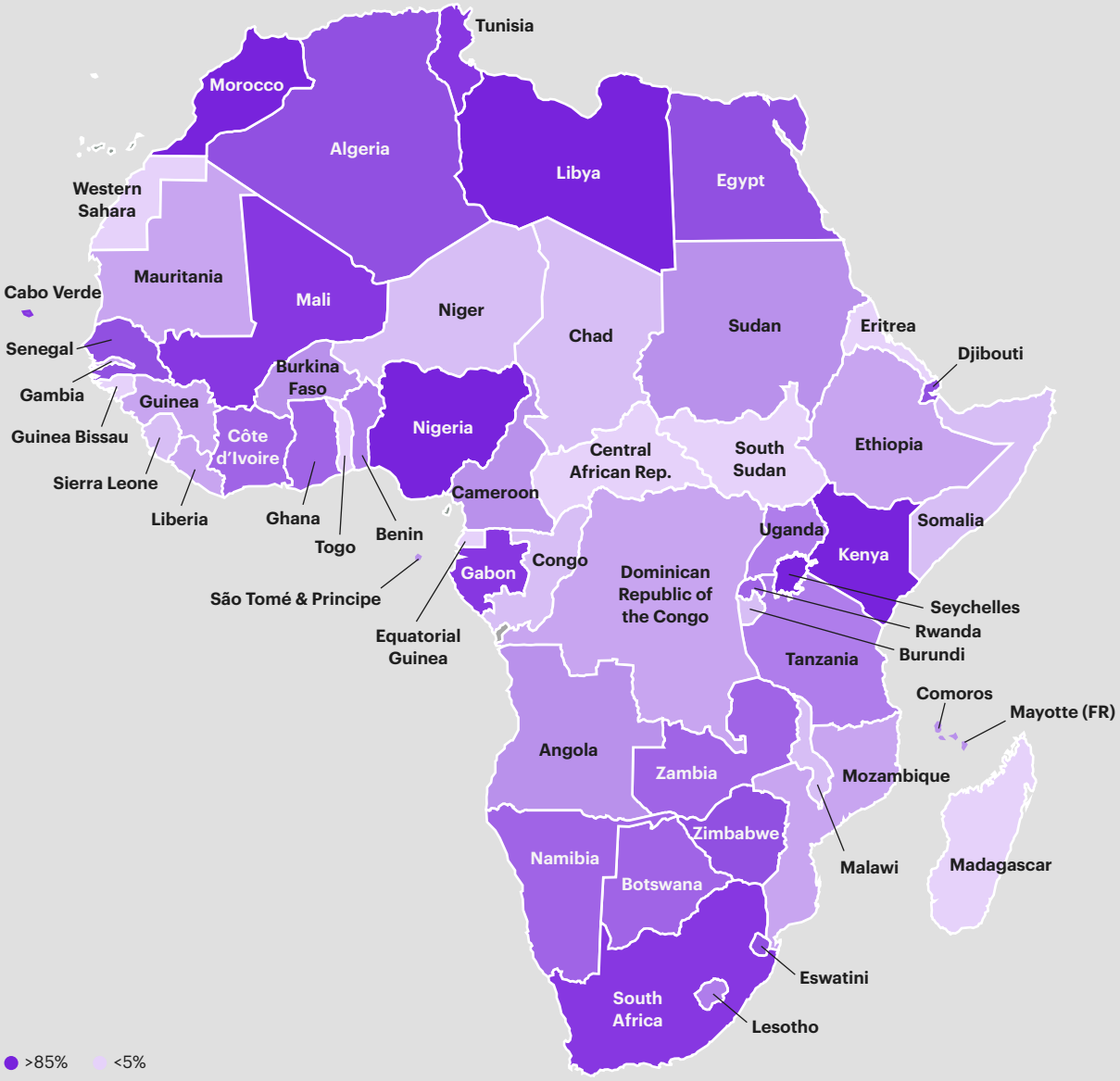
Through cyberattacks hackers can gain access to a group of connected systems by overrunning the point of least resistance. This means managing system interconnection plays a vital role in preventing cybercrime. In the African region specifically, increasing trade and capital flows, and the rapidly escalating use of digital technologies, will increase the need for cyber resilience, with the growing interconnectedness intensifying systemic risks. The varying pace of digital evolution across the region is compounding the need for greater cyber resilience, as it creates pockets of underinvestment in cybersecurity that increases the likelihood of unguarded exposure points.

[4] GSMA (2021)
[5] Informa (2022)
[6] Markets and Markets (2020)
[7] Mordor Security (2020)
[8] Interpol (2021)
[9] Cyber threats are considered attempts made to damage or disrupt critical data and information through methods such as spyware, malware, and phishing.
[10] EU Cyber Direct (2021)
[11] Sophos (2021)

Figure 2

The African continent has seen a steady increase in Internet penetration

Share of Internet users in Africa as of December 2020, by country



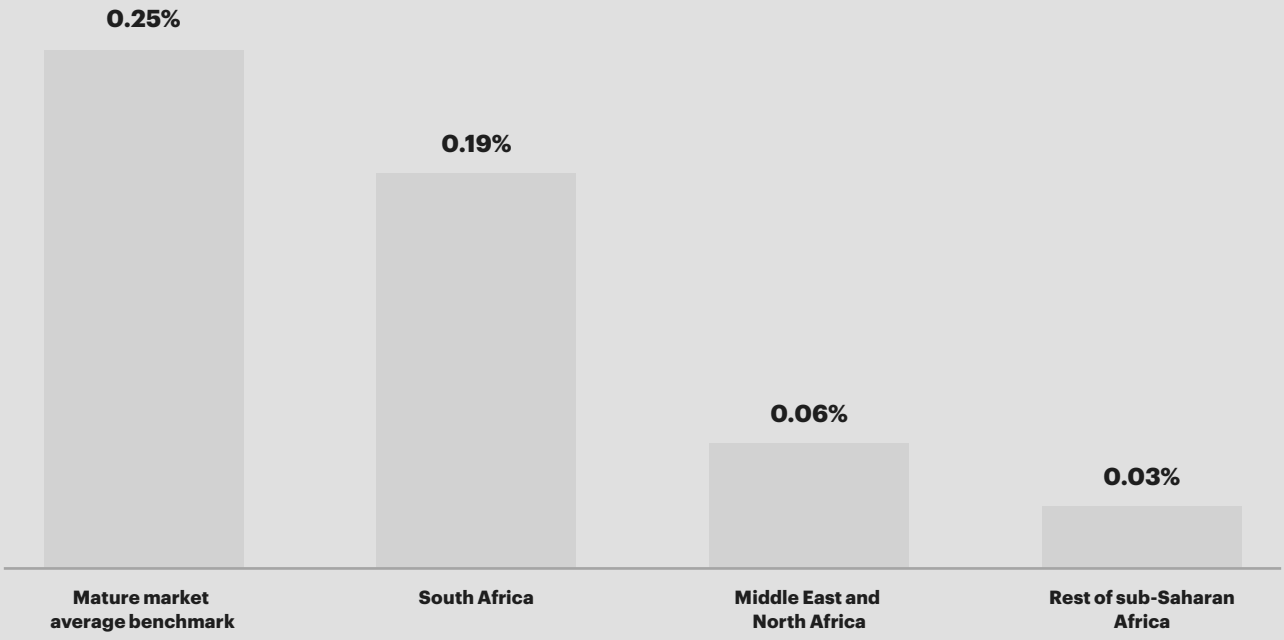
85.20% Zimbabwe	**55.70%** Kenya	**29.20%** Sudan	**13.80%** Malawi
84.20% Djibouti	**54.80%** Libya	**28.90%** Cameroon	**13.40%** Niger
73.00% Egypt	**52.50%** Nigeria	**28.60%** São Tomé & Principe	**13.20%** Chad
72.20% Zambia	**52.20%** Mauritius	**26.50%** Angola	**13.10%** Burundi
72.10% Namibia	**52.10%** Seychelles	**0.25%** Equatorial Guinea	**12.80%** Sierra Leone
68.50% Botswana	**47.70%** Morocco	**21.80%** Comoros	**12.80%** Somalia
68.40% Ghana	**46.50%** Tunisia	**21.40%** Burkina Faso	**12.40%** Guinea-Bissau
67.40% Côte d'Ivoire	**45.30%** Reunion (FR)	**20.30%** Mauritania	**11.90%** Togo
62.70% Rwanda	**45.10%** Cabo Verde	**20.30%** Mozambique	**11.30%** Central African Republic
60.00% Uganda	**39.30%** Gabon	**19.00%** Gambia	**10.10%** Madagascar
59.80% Mayotte (FR)	**38.60%** Mali	**18.90%** Guinea	**7.90%** South Sudan
57.50% Saint Helena (UK)	**37.80%** South Africa	**17.90%** Ethiopia	**6.90%** Eritrea
57.00% Tanzania	**37.60%** Algeria	**17.90%** Congo, Democratic Republic	**4.60%** Western Sahara
56.70% Lesotho	**31.60%** Eswatini	**14.70%** Liberia	
56.70% Benin	**30.50%** Senegal	**14.70%** Congo	

Note: Data for all countries not available.

Sources: World Bank data (2020); Kearney analysis

Figure 3

South Africa is a regional leader in cybersecurity spending but needs to step up investment to reach the mature market average benchmark level



Sources: Gartner, Oxford Economics, World Bank; Kearney analysis

South Africa is a regional leader in spending on cybersecurity. However, like other countries in the region, it needs to step up investment to raise cybersecurity spending to the mature market average benchmark level, which includes the United States, United Kingdom, and Germany (see figure 3). If each African country spends around 0.25 percent of GDP annually on cybersecurity, this would be in line with spending in mature markets. Our estimates suggest that this translates to $4.2 billion annually for the region.

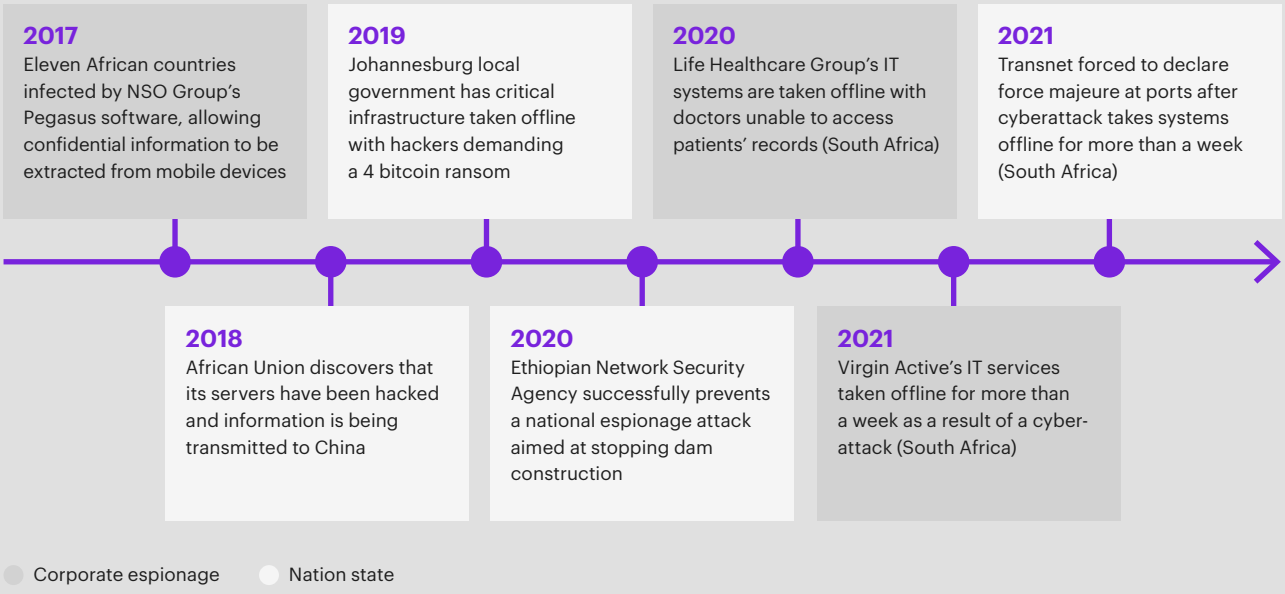
Until recently, many African countries' exposure to large-scale cyberattacks was limited to unsophisticated methods and criminal groups, but this dynamic is shifting and accelerating. For example, cybersecurity company Kaspersky noted a 767 percent increase in targeted ransomware attacks (attackers using specialized strategies to target specific companies) in South Africa between 2019 and 2020, with more than 66 percent of South African organizations reporting random attacks. The firm also noted that 42 percent of victims paid the ransom (at an average of $447,000), but only 24 percent were able to restore all their files. The total cost of recovery averaged $1.85 million per firm.[12] Most cyberattacks in Africa continue to be unsophisticated, with common methods being phishing and distributed denial of service. However, the region is experiencing an increasing number of corporate espionage and nation-state attacks (see figure 4 on page 7).

[12] Kaspersky (2021)

Figure 4

The region is experiencing an increasing number of corporate espionage and nation-state attacks

Non-exhaustive



Source: Kearney analysis

The threat to individuals, companies, and national security in Africa continues to grow as digital adoption, advancements related to the Fourth Industrial Revolution, and Internet connectivity adoption increase without reciprocal growth in cybersecurity infrastructure, tools, and understanding. Cybersecurity is not a matter from which African countries can isolate themselves. The interconnectivity of systems results in the interconnectivity of the security threat to member states. The following sections of this report will dive into the immature policy environment that exists in the African region, shortages of skills and capabilities, and the dangers of lacking a holistic approach to cyber resilience.

Cybersecurity is not a matter from which African countries can isolate themselves. The interconnectivity of systems results in the interconnectivity of the threat.

Lack of investment and strategies weakens cyber readiness

The modern world is increasingly interconnected, and a region's cybersecurity strength now depends on the ability of all connected nation states to collectively fight cyber threats. To better understand the range of cybersecurity maturity among African countries and identify the biggest gaps, we selected five countries considered to have a high cybersecurity readiness, according to the International Telecommunications Union's Global Cybersecurity Index (GCI), and that are strategically important given the size of their economies. See the country selection process in the Appendix (figure A on page 32). These included:

1. **Nigeria**
2. **South Africa**
3. **Egypt**
4. **Morocco**
5. **Kenya**

We then conducted a cyber maturity assessment on the five selected countries to gain an understanding of the broader cyber risk (see figure 5). The assessment covered five criteria identified as crucial to cyber maturity: strategy; legislation; governance and operational entities; sector-specific and international cooperation; and awareness and capacity building. The analysis considered each country's published cyber strategy, and mapped the various bodies enabled to deal with cyber threats. It also considered the countries' successes in increasing cybersecurity capabilities, and any cooperation programs that had been ideated or launched. See the detailed breakdown and category definitions in the Appendix (figure B on page 33).

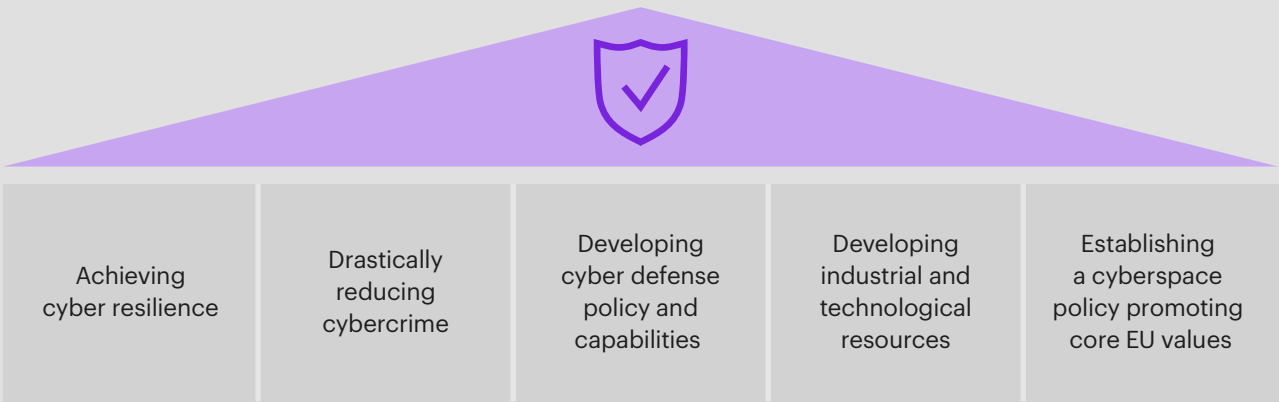
Figure 5
A look at the cyber maturity of five select countries shows that African cyber resilience is low

Source: Kearney analysis

Through the five selected countries, the analysis showed that Africa's cyber resilience is low, particularly around strategy, governance and operational entities, and cross-sector cooperation. The AU has attempted to create a unifying policy through its legal framework (the African Union Convention on Cyber Security and Personal Data Protection), but at the time of the analysis this had been signed by only 16 countries, and implementation hadn't begun. Unified strategy development and capabilities in assessing cyber readiness and reporting incidents are missing, which limits the collective preparedness of the region and its ability to capitalize on shared knowledge. The absence of an implemented, unifying, regional governance framework makes it difficult to collaborate and share intelligence across countries. Businesses also underestimate the value at risk, resulting in a lack of adequate preparation.

Africa faces challenges in pulling together a unifying framework, largely because of the inherent absence of a single power to legislate or veto budgets and appointments. In contrast, the European Union (EU)—which has a strong legislative framework and a powerful secretariat—has placed cyber resilience very high on its agenda and has developed a cohesive regional cybersecurity strategy that became enforceable in 2018 (see figure 6). The General Data Protection Regulation (GDPR) is a good example of effective regulation as it requires a personal breach to be reported to the competent national supervisory authority, and in certain cases to be communicated to the individuals whose personal data has been affected by the breach. The GDPR also includes stringent penalties for enterprises that fail to comply. Similar frameworks can be found in other regions. Examples include the ASEAN Cybersecurity Cooperation Strategy 2021–2025 and the Organisation of American States Cyber Security Program (established in 2016).

Figure 6
The European Union has developed a cohesive regional cybersecurity strategy



Source: Kearney analysis

Due to the non-physical, cross-border nature of cybercrime, preventing and combatting it requires international cooperation. Without a structured African cooperative framework that can be readily implemented, and that holds member states accountable, the region will remain vulnerable. As a starting point, the leading countries in the region can agree on a plan of action to protect themselves according to the unifying framework. Once this is established, it can create a space for other countries to join in and follow, with the objective of protecting as many countries as possible.

Africa's nascent cybersecurity industry faces a skills shortage

The Latin America, Middle East, and Africa (LAMEA) cybersecurity market, which encompasses the amount that organizations are investing by deployment size (cloud-based and on-premises), is expected to reach a value of $40 billion in 2027, up from $19 billion in 2020.[13] Increases in cloud adoption mean that countries and organizations are more exposed to cyber threats, as their data is often hosted by third-party services. This is especially relevant in the African context, as companies are trying to rapidly adapt to digital platforms and integrate their services through cloud-based applications.

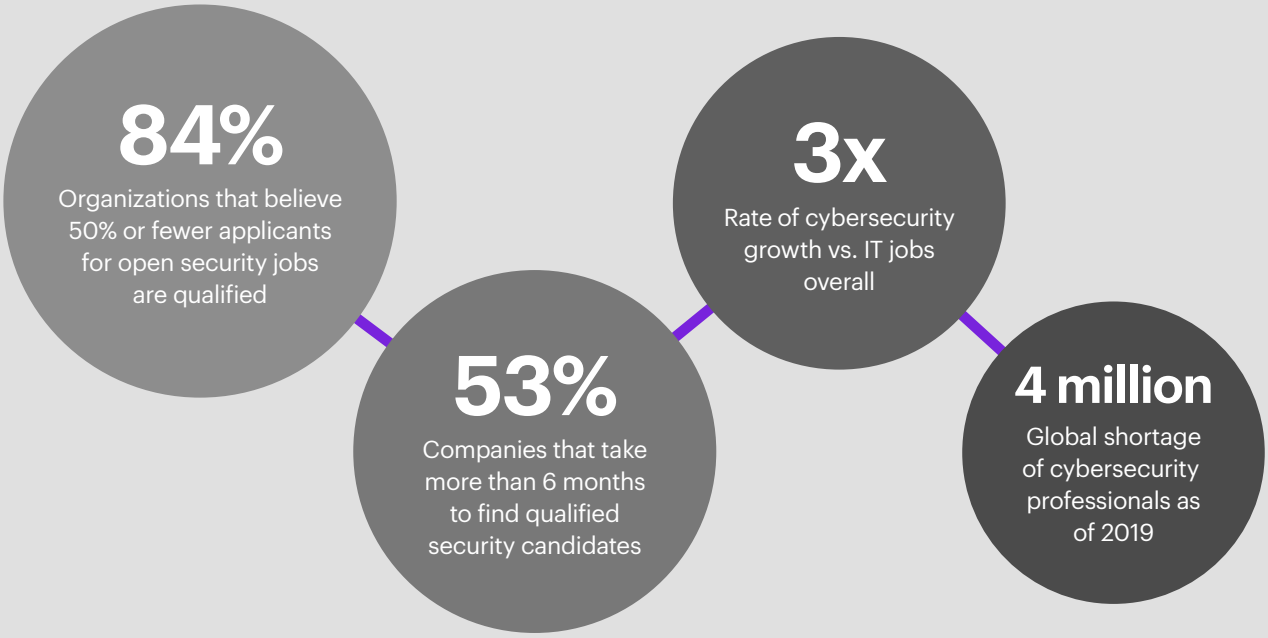
Cybersecurity product portfolios are also varied, and few companies in the region offer solutions that cover the entire capability value chain. Organizations face the challenge of navigating a complex web of vendor relationships to design their cybersecurity programs. Despite having access to a multitude of product vendors and service providers, security solutions aren't often tailored to specific industry needs. This makes it difficult for companies in Africa to secure their digital platforms as they use cloud-based applications to grow. As the market matures, it brings with it the potential for investments and early-mover advantage for companies that develop industry-specific cybersecurity solutions. Companies can use this opportunity by adopting a more rigorous approach to cybersecurity, then work on closing the current skills gap.

When it comes to the cybersecurity skills and professionals, organizations worldwide are battling to close the talent gap amid the rise of technologies such as cloud computing, mobile, and the IoT. Currently, 82 percent of IT professionals believe there is a shortage of skills in the cybersecurity workforce.[14] Considering that this scarcity is global, local organizations will have to compete with their international counterparts to hire skilled workers. This further exacerbates the skills–demand gap for cybersecurity in the African context.

[13] Cybersecurity Market, Allied Market Research (2020)
[14] Intel Security

Figure 7

Organizations strongly believe there is a cybersecurity skills gap, and that it is not being filled fast enough



Source: Kearney analysis

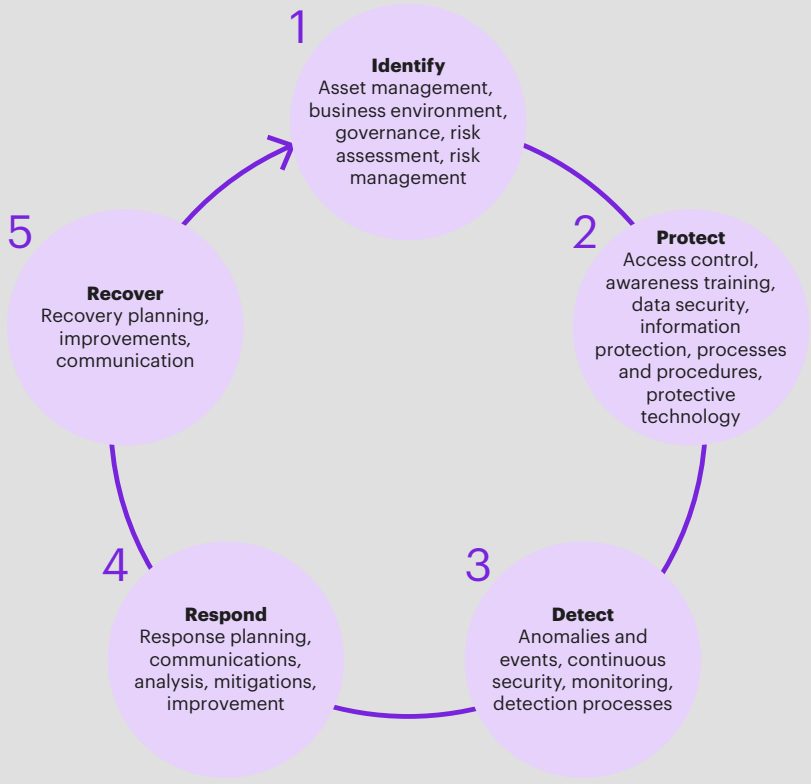
Figure 7 further shows that companies do not believe that the skills gap is being closed quickly enough, with a staggering shortage of 4 million cybersecurity professionals globally as of 2019. Additionally, as of June 2022, only around 156,000 people worldwide were Certified Information Systems Security Professionals (CISSPs), with the United States, the United Kingdom, Canada, and China accounting for more than 70 percent of that number.[15] In the African context, the number of CISSPs is significantly lower, at about 1,200, representing 0.8 percent of the total number worldwide. However, countries in Africa and elsewhere in the world are trying to close the gap with specific initiatives.

In South Africa, for example, the Absa Group is working to address the skills gap by setting up academies in association with the World Economic Forum's Cybersecurity Learning Hub.[16] These academies would focus on data encryption and cybersecurity courses. Their initial target is to produce 300 graduates a year, scaling up the number of intakes as the academies grow.

Despite some attempts to narrow the cybersecurity talent gap, there is no holistic approach to cyber resilience due to misconceptions about the cyber risks themselves.

[15] ISC² (2022)
[16] World Economic Forum, Cybersecurity Learning Hub (2021)

Figure 8
The National Institute of Standards and Technology framework recommends five functional capabilities for achieving comprehensive cybersecurity defense



Sources: 2021 Data Breach Investigation Report, National Institute of Standards and Technology; Kearney analysis

Misconceptions about cyber risks led to a piecemeal approach to building cyber resilience

Corporate stakeholders often have a myopic view of cyber risk, seeing it as an IT issue rather than a business risk. As a result, they see technology investment as the key to mitigating cyber risk. However, more than 82 percent of data breaches in 2022 involved a human element (for example, misconfigured databases or human mistakes that enabled cybercriminals to access organizations' systems).[17] Systems architecture, people, processes, and organizational culture are the greatest tools organizations can employ to improve their cybersecurity. Without a strong vision for cyber-risk management, many organizations either underestimate or overestimate their cybersecurity requirements. A structured approach optimizes finite resources to deliver protection that's appropriate to the risk they represent. Otherwise, as is often the case, little thought is given to how systems are designed or deployed, and the entire organization must undergo costly remediation to protect assets.

The National Institute of Standards and Technology (NIST) framework recommends five functional capabilities for achieving comprehensive cybersecurity defense: identify, protect, detect, respond, and recover (see figure 8). While businesses in the region are largely focused on the identify, protect, and detect functions of the cybersecurity life cycle, more research and investment is needed in the recover and respond spheres.

[17] Verizon (2022)

In addition, our interactions with small and medium-size enterprises (SMEs) indicate that they generally do not see cybersecurity as a top priority. Although these firms are not usually the main target, many cybercriminals use supply chain linkages or shared data to infiltrate partnerships between smaller companies and larger organizations. Large companies are attacked more frequently than small companies, but small companies are significantly more likely to record data loss or system failure after an attack.[18] Because SMEs account for more than 90 percent of all businesses in Africa and more than two-thirds of all employment, their susceptibility to breaches is a major cause for concern.[19] With a proliferation of cyberattacks being observed throughout Africa, large and small businesses need to develop holistic, cyber-centric strategies.

Large companies are attacked more frequently than small companies, but small companies are significantly more likely to record data loss or system failure after an attack.

[18] *2021 Data Breach Investigation Report*, Verizon
[19] London Stock Exchange Group (2021)

Cybersecurity challenges will escalate in Africa

Section 2 highlighted how African countries are fast becoming targets for cyberattacks, and how a low level of preparedness makes the region particularly vulnerable. As the threat landscape escalates, the region needs to urgently address the problem.

In the rapidly evolving cyber landscape, four drivers must be addressed, which will be the focus of this chapter.

— The growing interconnectedness and flow of people, goods, and information across the region due to the realization of the AfCFTA will intensify systemic risk. This means the region will only be as strong as its weakest "cyber link."

— Widespread socioeconomic difficulties—accelerated by the COVID-19 pandemic, food crises, and inflation—have led to diverging national priorities and a varying pace of digital evolution, which will continue to foster a sustained pattern of underinvestment.

— Countries' hesitancy to share threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.

— Technological evolution will render threat monitoring and responses more complex, particularly given the rise of encryption, and multi-cloud operations, the proliferation of Internet of Things devices, and the convergence of OT and IT environments.

These characteristics will aggravate the current situation in the region. If they are not addressed, the value at risk for Africa is significant. In addition, cybersecurity concerns have the potential to derail the region's innovation agenda, a key part of the AU's Vision 2063 goals. Africa is also increasingly becoming a strategic player in geopolitical tensions—an important factor given that cyber warfare is on the increase. The threat is not only external but internal, which justifies the need for more collaboration. Indeed, even neighboring countries in Africa can use cyber threats to weaken other countries during tensions or commercial fights.

Cybersecurity concerns have the potential to derail the region's innovation agenda, a key part of the AU's Vision 2063 goals.

Cybersecurity challenges will become more complex

When it comes to systemic risk, the region will only be as strong as its weakest "cyber link"

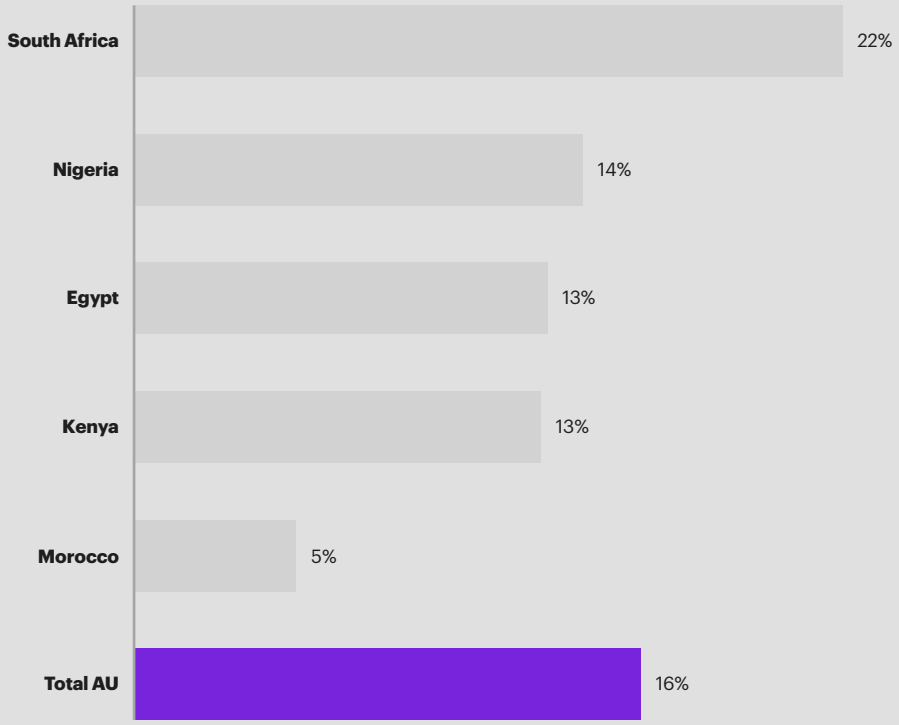
At the time of writing, the AfCFTA agreement had been signed by 54 of the 55 member states of the AU, and ratified by 43 signatories. The momentum that the agreement has gathered is a tribute to the potential impact it could have for the African and global economies. The agreement's long-term vision is the complete unification of Africa's economies, creating a single continental market where people and investments move freely. While potential benefits for Africa and its people are significant, a transformation with far-reaching deregulation naturally creates holes for exploitation. Many of these challenges have taken center stage during negotiations between signatories and are leading to the development of unified governance frameworks addressing several trade-related issues. However, in the absence of a homogenous standard for cybersecurity, the AfCFTA ambitions will increase the exposure of all member states to cyber risk, regardless of their own standards.

Figure 9 highlights the level of intracontinental trade in the AU. This accounts for 16 percent of Africa's total trade. Another note to the connectivity across the continent is the extensive footprint of banks and other key companies. Ecobank and Ethiopian Airlines are two standout pan-African businesses, serving 58 percent and 71 percent of AU nations, respectively. Other notable corporations that serve approximately 30 percent of the continent include Standard Bank, Attijariwafa Bank, MultiChoice, MTN, ShopRite, and Jumia.

Interconnectedness brings systemic risk. Recent cyber heists have game-changing implications for regional systemic risk, demonstrating that threat actors don't need to attack a core system to exploit its weaknesses.

With growing intra-regional trade and business linkages across African countries, there's a high risk of contagion in the event of cyberattacks across the region.

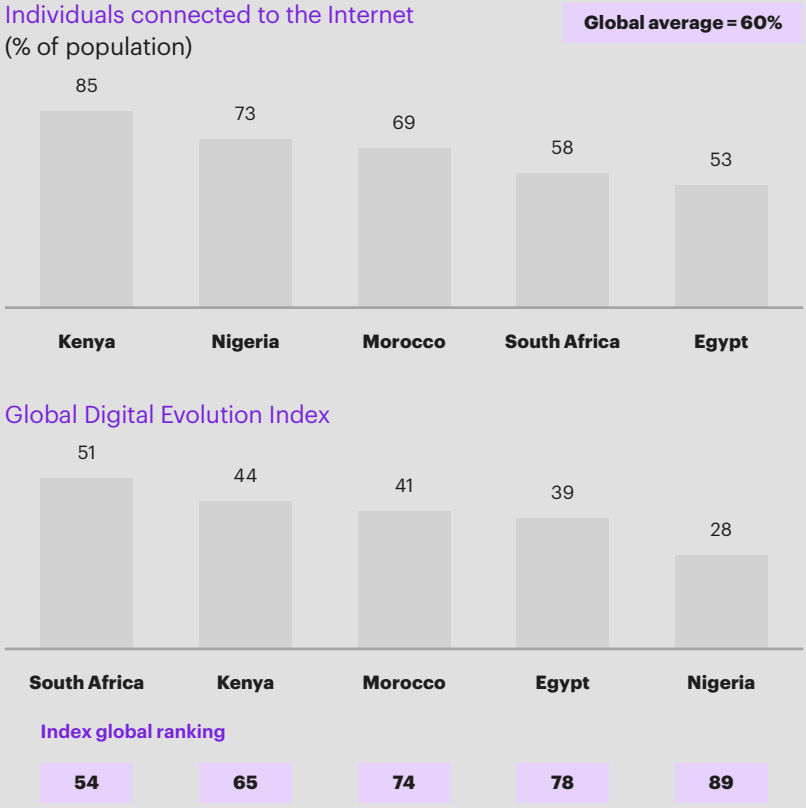
Figure 9
Intracontinental trade represents 16% of Africa's total trade



Source: Kearney analysis

Figure 10
There is a digital divide in the African region

Network Readiness Index (rank)	
South Africa	**48.9 (68)**
Egypt	**47.8 (73)**
Kenya	**46.9 (77)**
Morocco	**39.71 (93)**
Nigeria	**36.7 (109)**
AU average	**~30**



Notes: As a key indicator of how well countries are doing in the digital world, the World Economic Forum's NRI, also referred to as Technology Readiness, measures the propensity for countries to exploit the opportunities offered by information and communications technology (ICT).

Sources: *Tufts Digital Intelligence Study 2020 report*, World Economic Forum; Kearney analysis

The varying pace of digital evolution will foster sustained underinvestment, which was only worsened by the COVID-19 pandemic

Despite the growing interconnectedness of the region, African countries have varying degrees of network readiness. The pace of digital evolution also varies across countries. Figure 10 shows how the five countries in the maturity assessment rate according to the World Economic Forum's Network Readiness Index (NRI)—which measures degree of readiness to exploit opportunities offered by information and communications technology (ICT)—and The Fletcher School's Digital Evolution Index (DEI)—which measures the pace of digital growth across supply, demand, institutional environment, and innovation.[20,21] It shows a contrasting picture between the NRI and DEI ratings, and the Internet penetration of each nation, revealing key issues with the region's digital development. The NRI and DEI both rank South Africa and Kenya as leaders in the region, while South Africa falls short in distributing Internet access to its population.

South Africa highlights a stark inequality that has not yet been effectively addressed, with around 42 percent of the country unable to access its digital development. This under-connected portion of the population is driving a digital capability gap in the continent's third-largest economy. Cybersecurity incidents will proliferate without enough skilled ICT specialists and a low level of technological literacy.

This is in contrast to Nigeria, which has a comparatively well-connected population yet low digital maturity, meaning there are more direct cybersecurity risks. Ranked 89th in the world and last in Africa for its digital maturity, Nigeria has 146 million individuals connected to the Internet while the country lacks the technological infrastructure to adequately mitigate cyber risk.[22] This dangerous combination is resulting in Nigeria's continual loss of up to $500 million annually from cybercrime.[23]

[20] The Portulans Institute and World Economic Forum
[21] The Institute for Business in the Global Context, The Fletcher School, Tufts University
[22] Of the nations measured by the study (this includes 15 of the 55 AU member states)
[23] Nigerian Communications Commission

Each African nation has its own unique history and context, which help to define priorities. Few place cybersecurity as a major national priority. Among these differing African contexts, all nations except for Nigeria, South Africa, Egypt, Morocco, Kenya, Mauritius, and Rwanda are considered to have weak levels of cyber maturity.[24] This difference in priority is again made clear by the low level of ratifications in the AU's 2014 Convention on Cyber Security and Personal Data Protection.

The COVID-19 pandemic has presented a difficult reality for governments in the region. From the second quarter of 2020, the continent's leaders were entirely focused on their respective pandemic responses. At the same time, cybercriminals doubled down on the opportunity presented by the rapid structural changes that were occurring, such as working from home and increased reliance on crucial networks in the finance, healthcare, and public sectors. These critical risks should have already been identified and mitigated during the transition, but a global lack of focus on the issue has led to exponential growth in cybercrime since 2019. During one week in late March 2020, 310,000 devices were hacked in South Africa alone.[25] This trend was not local to Africa, with cyberattacks on the global financial services industry increasing by more than 238 percent between February and April 2020.[26] The events of 2022 have resulted in food supply shortages for several nations, while high global inflation rates have put further pressure on national budgets.

The flurry of cybercrime in the African region since the start of the pandemic has again highlighted the need for a more unified response to threats in the region.

Lack of formal structures and cross-border agreements for sharing threat intelligence lead to porous cyber defense mechanisms

Most African governments and businesses lack the means, strategies, and sometimes the willingness to collaborate when it comes to sharing incident information or threat intelligence, which is crucial for forensic investigation and prevention. The lack of intelligence sharing is a global issue stemming from limited mandates to share specific information about cyber incidents across intelligence agencies. With the growing sophistication and increasing pace of cyberattacks (for example, zero-day exploits and advanced persistent threats), sharing intelligence and best practices, along with establishing a joint incident response, can alleviate the region's overall risk (see sidebar: Cisco and Interpol collaborate to combat cybercrime on page 18).[27]

Furthermore, Africa lacks a governing framework to introduce incident reviews on a regional level. In the absence of these formal structures that facilitate cooperation, intelligence agencies and prosecuting authorities will not be able to effectively respond to and mitigate cyber threats, as cybercrime is highly transnational by nature. PPPs such as the collaboration between Interpol and digital communications technology company Cisco to combat cybercrime, represent an opportunity for African states to circumvent political blockers and increase cross-border cooperation and threat intelligence sharing.

Technological evolution and digital transformation in Africa is becoming increasingly complex

The evolution and adoption of technology will continue to add complexity to the effective monitoring of and responses to cyber incidents due to the:

— Increasing reliance on digital currencies

— Proliferation of smartphones and connected IoT devices

— Democratization of IT and data, especially in organizations—for example, the increase in workforce mobility, work-from-home policies, and BYOD work arrangements

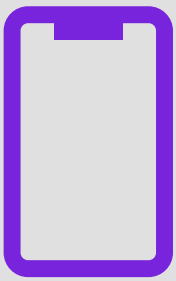
[24] Global Cyber Security Index, ITU (2021)
[25] Kaspersky Statistics 2020
[26] VMware report "Modern Bank Heists 3.0", May 2020
[27] Interpol (https://www.interpol.int/en/News-and-Events/News/2017/INTERPOL-and-Cisco-collaborate-to-combat-cybercrime)

Cisco and Interpol collaborate to combat cybercrime

In 2017, Cisco and the International Criminal Police Organization (Interpol) announced an agreement to share threat intelligence as the first step toward jointly fighting cybercrime. This not only will allow for quick threat detection around the world but will also pave the way for potential collaboration on training and knowledge sharing. Cisco's agreement with Interpol supports the programs that target pure cybercrime and cyber-enabled crimes to assist member countries with identifying cyberattacks and their perpetrators.

Persistent SIM swap attacks in East Africa

Hackers are taking an increasing interest in SIM swap attacks on mobile money users. In 2018 alone, 25 percent of Kenya's population experienced this type of fraud. The attacks involve hackers first gaining information about ideal targets through connections with corrupt employees within mobile money provider organizations. This information is then used to register fake SIM cards on the network, which removes the genuine SIM card and transfers control to the fraudulent SIM. The corrupt employee then resets the victim's mobile money PIN, which can be controlled through the new, fraudulent SIM. Following this, the victim's account can be drained almost instantly.



Each of these trends is accompanied by fast growth in innovation and technical complexity. Despite the benefits of adopting new technologies, it is essential that governments and cyber watchdogs facilitate the provision of proportional efforts and resources to ensure that policies and monitoring methods remain up to date.

Increasing reliance on digital money

The GSMA reported that in Africa in 2021 the mobile money market consisted of 36.7 billion transactions across more than 621 million accounts, with a total transaction value of $701.4 billion. This represents 70 percent of the global mobile money market and equates to 26 percent of the continent's GDP.[28]

Africa's dominance of this market is no surprise given that mobile technology has enabled economies to function under difficult conditions such as rolling blackouts, hyperinflation, and limited access to data connections. The technology has also been found to be susceptible to multiple types of attacks, including:

— Authentication attacks (most mobile money systems are only secured by four- or five-digit PINs)

— Identity theft

— Unstructured Supplementary Service Data technology vulnerabilities

— Phishing

— Brute-force attacks

— Denial-of-service attacks

— Agent-driven fraud

— Unauthorized SIM swaps (see sidebar: Persistent SIM-swap attacks in East Africa).

An adjacent concept is cryptocurrency and blockchain technology. While this is more peripheral in Africa compared to mobile money, it still brings risks to African governments, organizations, and individuals. The African region is only beginning to recognize the threat posed by virtual currencies, with almost no policy alignment across member states. This alignment is vital to reduce the opportunities for criminals to benefit from unregulated activities. This is a growing concern as Africa lags further behind other regions in terms of unifying an approach to mitigating risks.

[28] State of the Industry Report on Mobile Money 2022, GSMA; Statista

For African individuals, financial losses to scammers are mounting. Within the space of a year, two of the world's largest cryptocurrency-enabled pyramid schemes were unearthed on African soil, namely Mirror Trading International and Africrypt. The former achieved the infamous accolade of 2020's largest cryptocurrency scam globally, with an estimated theft of $588 million. Africrypt collected the same accolade in 2021 with the theft of a staggering $3.6 billion.[29]

Attacks against African businesses have increased over the past year, aimed at stealing computer power for cryptocurrency "mining" operations. Around 74 percent of all malware attacks detected in the EMEA region in 2020 were caused by so-called "coin miners."[30] The involvement of insiders in these attacks is on the rise, reducing businesses' ability to detect the breaches. They are often carried out by employees with high-level network privileges and the technical skills needed to turn their company's computing infrastructure into a currency mint.

The rise of digital payments poses perpetual threats to African citizens and organizations. They create environments in which bad actors can use social engineering as a technique to gain advantage—such as by deceiving people into revealing passwords and other personal information to gain access to computer systems. This reinforces the importance of ensuring that digital evolution considers the human aspect as well as the technological. As it stands, trends in these types of crime can only worsen as Africa moves toward a more connected future.

Proliferation of smartphones and connected devices

The regional consumer IoT market is expected to grow. South Africa will lead the way, with a forecasted revenue of 11.35 percent CAGR between 2023 and 2027, driven by investment in the telecommunications, manufacturing, logistics, transport, and government sectors.[31] Future growth is anticipated in the financial services, energy, agriculture, and healthcare sectors. Mauritius, Seychelles, Rwanda, and Kenya have also prioritized investment in IoT technologies.

Africa's slow pace of technological development relative to the rest of the world will mean it can leapfrog into many advanced technologies, such as it did in skipping straight to smartphones over wired telecommunications. This is expected to be the case with IoT technology.[32]

IoT endpoints tend to be unsophisticated devices. They represent easy targets for attackers who seek to exploit the weakest link in a connected network, making the whole network vulnerable. In this context, a secure access policy and software-defined segmentation is vital. To implement effective application segmentation, it is crucial to understand how application components communicate with each other, what infrastructure services they depend on, and how the component clusters are grouped. Rich telemetry and unsupervised machine learning can be used to achieve this. Recognizing application dependency will enable the development of effective segmentation policies, helping to contain breaches by ensuring that attacks cannot spread.

Africa's slow pace of technological development relative to the rest of the world will mean it can leapfrog into many advanced technologies.

[29] Moneyweb
[30] The Nippon Telegraph and Telephone Corporation
[31] https://www.statista.com/outlook/tmo/internet-of-things/south-africa
[32] IoT adoption in Africa, Intelligent CIO

Democratization of IT and data, especially in businesses with remote operations

The need to operate businesses remotely during the COVID-19 pandemic has led to the rise of virtual organizations, which provide remote access to core systems that employees need to carry out their day-to-day activities from home. This has led to a rise in client portals as well as mobile and web-enabled applications. Cyberattacks specific to computing and web applications accounted for 67 percent of all attacks in 2020 globally—marking 22 percent growth from 2019.[33]

To ensure business continuity during the initial waves of the pandemic, companies had to quickly migrate toward architectures that provided convenient remote access to their systems and data. Any oversights in the implementation of these new operating models may result in vulnerabilities that can be exploited in the future. However, even best practice corporate cybersecurity systems are vulnerable to social engineering, as home-based employees become easy entry points for attackers. This makes it equally important for businesses to both increase their employees' threat awareness and implement adequate cybersecurity technologies.

While the number of people working from home increased dramatically due to the pandemic, BYOD and workforce mobility trends have been on the rise for the past decade, including across the African continent. The popularity of BYOD work arrangements has grown rapidly in East Africa, where they are seen as a means of supplementing technology to improve efficiency and increase employees' freedom. Kenya has seen this trend for some years, driven by a shift to task-based organizational cultures, where what you do is more important than where you do it. Kenyan authorities have communicated the cyber risks associated with this trend, as the country has experienced a steep rise in corporate espionage and fraud as far back as 2014.[34]

Underestimating value at risk leads to underinvestment in cybersecurity

It's crucial to adopt a value-at-risk mindset to mitigate threats effectively. Senior-level decision-making and resource allocation must be based on assessments of what high-value assets are at risk from a cyberattack and the potential impact of a breach. Current assessments that are based on average historical data do not account for increases in sophisticated attacks.

Quantifying the value at risk from cybercrime is challenging, and organizations around the world lack competencies in this area. One of the biggest challenges is understanding the nature of threats to high-value assets and appropriately prioritizing resources toward mitigating them. No organization can afford to use every defense mechanism in its arsenal, nor is it practical. However, resources must be allocated according to the magnitude of the threat and the value at risk.

Cyber threats grow with technological advancement, meaning it's paramount that governments future-proof their critical infrastructure. This includes cultivating an environment that encourages ICT providers to invest and grow local capabilities. Governments and businesses must urgently develop and implement forward-looking cyber strategies that demonstrate an understanding of value at risk. The interconnected nature of cybercrime means Africa needs a unified cybersecurity framework that addresses cybersecurity within countries and across the continent.

[33] The Nippon Telegraph and Telephone Corporation
[34] University of Cape Town conference paper, Salah Kabanda (2017)

Call to action: active cyber defense for resilience to cyber threats

Africa needs a comprehensive agenda to address its low cyber resilience, deal with the scale of cyber threats, and ensure Africa's unobstructed leap into the digital economy. Cybersecurity programs often take a siloed approach to defending infrastructure, even though vulnerabilities extend across peer companies and vendors, and adversaries plan and execute sophisticated attacks across several targets at once. This section provides a four-point agenda with which policymakers and key stakeholders can work together to heighten awareness about cybersecurity and adopt a stance of active defense (see figure 11). The agenda focuses on flipping the asymmetry between defenders and attackers by encouraging defenders to cooperate and take advantage of the region's collective resources.

Elevate cybersecurity in the regional policy agenda

The region's policymakers have agreed that closer coordination through the AU platform is essential. However, given varying levels of preparedness and differing national priorities, cybersecurity needs to be prioritized in regional and national policy agendas by steering the implementation of Kearney's RAC Framework, and elevating cybersecurity to the top of agendas in regional economic dialog to achieve alignment within the AU.

Figure 11
The regional cybersecurity defense playbook should address four key points

Source: Kearney analysis

Steer the implementation of a Rapid Action Cybersecurity (RAC) Framework

A few African countries have already defined their national cybersecurity strategy and implementation road map. However, the pace, urgency, and harmonization of cybersecurity policy thrusts across the rest of the region remain too slow.

The AU has taken steps to increase collaboration on cybersecurity across the region by establishing the African Union Convention on Cyber Security and Personal Data Protection legal framework. The framework has been signed by 16 out of 55 member countries but only ratified by 13.[35] Such a system, based on the loose collaboration of national agencies and voluntary exchanges, is unlikely to go far enough to safeguard Africa. Therefore, a tighter coordination mechanism is needed. Implementing Kearney's RAC Framework, which focuses on addressing countries' weaknesses in cyber resilience, is the first step toward establishing harmony across the region (see figure 12). The framework includes 11 strategic imperatives aimed at fixing cybersecurity basics across the region. National governments should soon take the lead in implementing the framework with support and guidance from the AU.

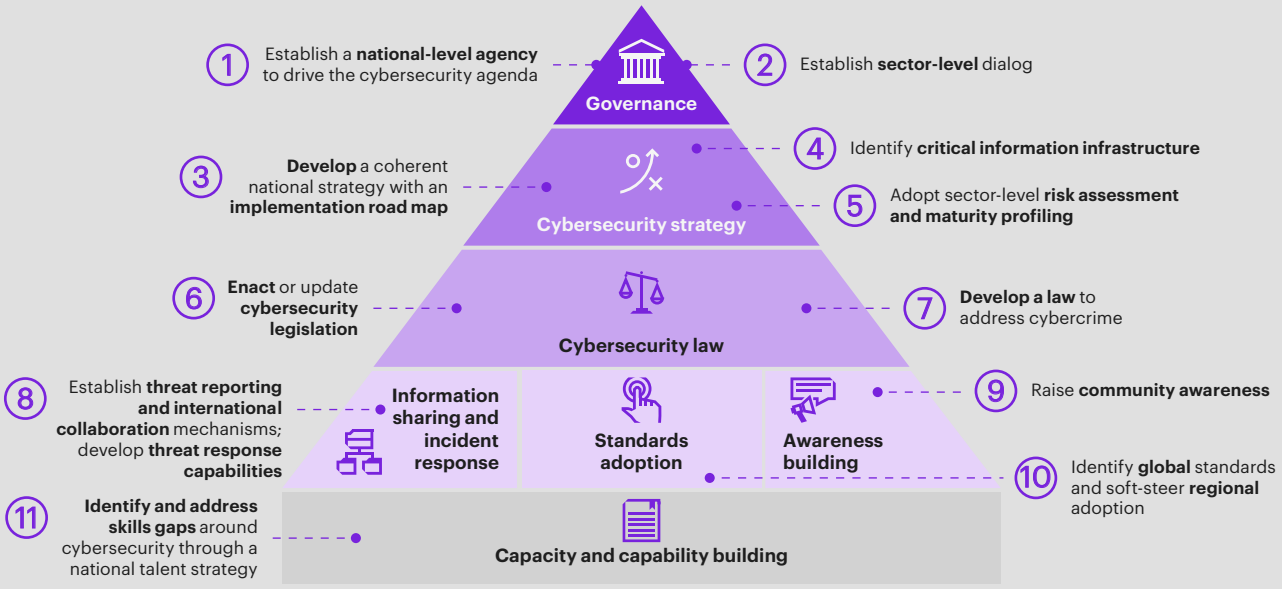
[35] Status update by African Union (March, 2022)

Governance

Several African countries have identified national agencies that can drive their cybersecurity agenda. In others, the process is still ongoing, with computer emergency response teams (CERTs) serving as the de facto agency in charge of cybersecurity. It is essential to define who within each country is responsible for managing cybersecurity strategy and ensure they are given sufficient authority to drive action across sectors and government departments. While centralized and decentralized models exist, establishing an independent national agency with the mandate to define and supervise the security agenda will foster a strong enforcement mindset and provide a central point of coordination.

Figure 12

Implementing Kearney's RAC Framework is the first step toward establishing harmony across the region



Source: Kearney analysis

Cybersecurity strategy
Each country must define a national cybersecurity strategy with a sharp vision, a defined scope, detailed objectives, and an implementation road map. It's crucial that this approach is based on the identification, analysis, and evaluation of risks. Risk assessments should be carried out at national and sector levels. A vital part of the strategy will be defining and identifying vital sectors and crucial information infrastructure (CII) while engaging with CII owners at the outset, and developing special mechanisms to protect CII and ensure business continuity. A clear set of sector-specific risk mitigation mechanisms needs to be put in place. Assessing and prioritizing high-value assets and determining the breach probability for each should be at the core of such risk assessments.

Cybersecurity law
To address the evolving nature of cybercrime, each country must define or update pragmatic cybercrime laws and strengthen local law enforcement to bring cybersecurity legislation in line with global standards. The legal framework should provide CII owners with clarity on their obligations to proactively protect their assets from cyberattacks. Given the borderless nature of the cybercrime environment, international cooperation on legislation should be considered alongside local laws.

Out of 55 African countries, only 29 have passed legislation to promote cybersecurity. The only existing multilateral treaty addressing cybercrime is the Budapest Convention on Cybercrime, proposed by the Council of Europe in 2001. This treaty includes provisions for cross-border assistance between law enforcement agencies on cybercrime that's separate from more cumbersome mutual legal assistance treaty arrangements. The 11 African countries that have signed the Budapest Convention are Benin, Burkina Faso, Cabo Verde (Cape Verde), Ghana, Mauritius, Morocco, Niger, Nigeria, Senegal, South Africa, and Tunisia. The AU cooperates with the Council of Europe Cybercrime Programme Office via its Global Action on Cybercrime Extended project. This project aims to strengthen the ability of states worldwide to apply legislation on cybercrime and electronic evidence, and enhance their abilities to effectively cooperate with other nations in this area. Further adoption and alignment of the African Union Convention on Cyber Security and Personal Data Protection with the Budapest Convention could bring strategic and operational benefits to the region. To enforce the adoption of the framework across African countries, the AU needs to implement an incentive mechanism, as well as sanctions and restrictive measures for non-compliance.

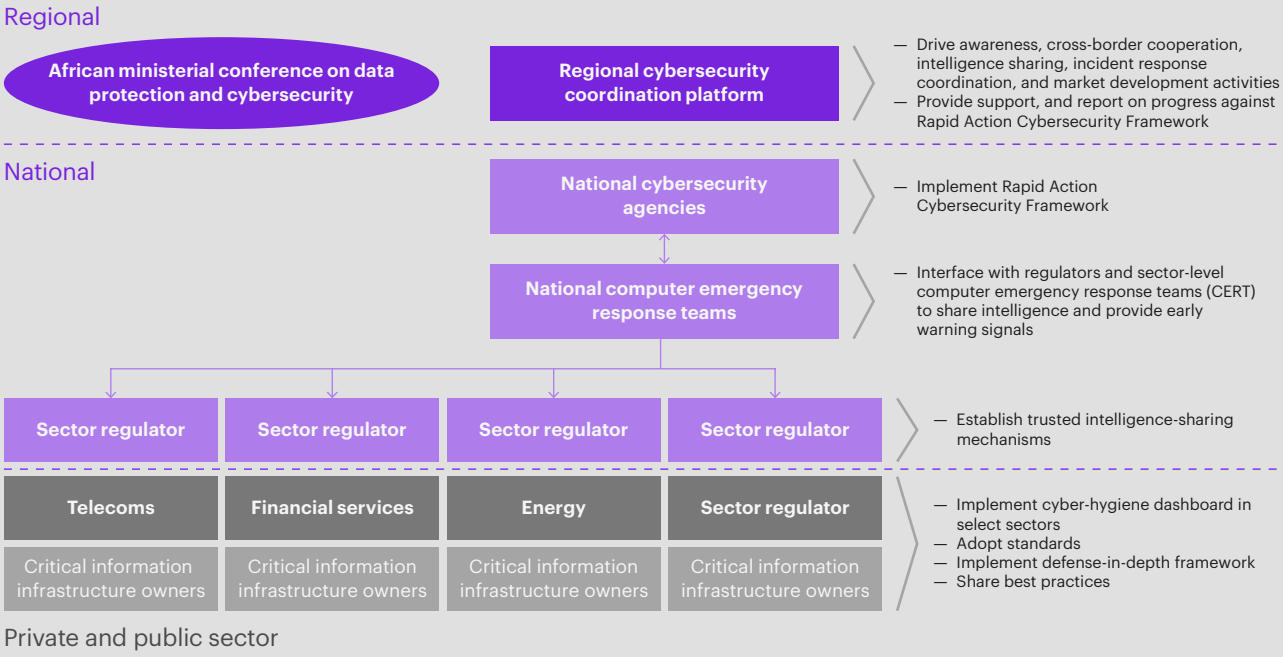
Information sharing and international collaboration
Information sharing among stakeholders is a powerful mechanism for better understanding a constantly changing environment. Sharing views on emerging threats, risks, and vulnerabilities with aspects of national security provides powerful insight into how the threat landscape evolves. It is crucial to properly define the information-sharing mechanism and the underlying rules, including non-disclosure agreements, traffic-light protocol, antitrust rules, and law enforcement access. A good way to start is to introduce methods for sharing information within sectors. However, this should be extended to encourage cross-sector communication, especially considering the multitude of interdependencies between sectors, such as between the banking and telecom sectors for mobile payments. Given that a country's cyberspace is by no means isolated from that of the rest of the world, international partnerships are essential to help nations fight cyber threats together.

Standards adoption
National cybersecurity agencies have a pivotal role to play in driving adoption and harmonization of standards across the African region. To begin with, they can encourage alignment with standards such as ISO 27001 and guidance such as the National Institute of Standards and Technology Cybersecurity Framework. The region can benefit significantly from collaboration at sector level to establish best practices related to specific concerns such as the convergence of OT and IT. This collaboration can help to set the agenda for the wider adoption of standard specifications for sharing threat intelligence, such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII).

Awareness building
It's become vital to raise awareness about threats and vulnerabilities and their impact on society. With greater awareness, individual and corporate users can learn how to behave and protect themselves in the online world. The public and private sectors have a joint responsibility to define the target problems of awareness-raising campaigns and identify mechanisms to address them. Initiatives such as Safer Internet Day, International Youth Day, and the European Union Agency for Cybersecurity's (ENISA's) security month have helped increase social awareness and modify online behavior.

Figure 13

A regional operational coordination platform is needed to interface with various national agencies



Source: Kearney analysis

Capacity and capability building

The region must adopt a forward-looking talent strategy to address the capacity and capability gaps highlighted earlier. Cross-regional collaboration efforts to train together with industry can enable countries to tap into each other's strengths and quickly boost the talent level.

A regional operational coordination platform is needed to interface with various national agencies.

Elevate cybersecurity to the top of the agenda in regional economic dialog

In addition to the AU Ministerial Conference, a regional operational coordination platform is needed to interface with various national agencies. As shown in figure 13, the regional cybersecurity governance framework would be designed to boost awareness and cross-border cooperation, and facilitate market-development activities such as the adoption and harmonization of standards. Sharing information via a coordination platform can help improve cyber threat detection, enable region-wide deterrence, and provide counterstrategies. In the context of the AfCFTA, identifying cyber-safe trading partners based on their ability to meet minimum threshold requirements on time will help elevate cybersecurity on the economic agenda.

Most importantly, the scope of the annual report provided by the AUC chairperson could consider expanding to include each country's progress based on the RAC Framework, helping to drive attention and progress across the region.

Pursue a sustained commitment to cybersecurity

Two initiatives can help secure sustained commitment to cybersecurity: pursuing country commitments to addressing the cybersecurity spending gap and defining and tracking cybersecurity metrics through a sector-level cyber-hygiene dashboard.

Pursue commitments to address cybersecurity spending gaps

Coupled with the region's digital divide, differing national priorities and perceptions about the value at risk from cybercrime leads to the suboptimal allocation of funds to address cybersecurity. The region needs a sustained and committed approach to investing in cybersecurity as it becomes more digitally connected. From 2022 to 2026, Africa will need to spend around $22 billion (approximately 0.25 percent of total annual regional GDP) to align with international benchmarks (as highlighted in section 1) and secure high-value assets from cyberattacks.[36]

Define and track sector-level cybersecurity metrics

Barriers to trust and transparency emanate partly from a lack of structured mechanisms to collect data, measure performance, and share intelligence. The lack of consistently defined and applied cybersecurity metrics and mechanisms within each country makes it difficult to assess the effectiveness of a cyber program and drive continuous improvement.

In sectors such as financial services, identifying and tracking meaningful metrics can enhance transparency while also improving performance on these metrics over time. A few metrics can help focus the cybersecurity agenda on the areas that matter most (see figure 14). The onus is on regulators to identify metrics that have the most relevance to their respective sectors and ensure these definitions are consistent and up to date. Establishing metrics at the sector level requires a consultative approach that considers sector-level constraints and different business needs.

[36] Kearney analysis: benchmarking with mature markets (such as US, UK, Germany); Gartner, Oxford economics, World Bank

Figure 14
A few metrics can help focus the cybersecurity agenda on the areas that matter most

Function	Management perspective	Metrics
Incident management	How well do we detect, identify, handle, and recover from security incidents?	— Mean time to incident discovery — Number of incidents — Mean time between security incidents — Mean time to incident recovery
Vulnerability management	How well do we manage exposure to vulnerabilities by identifying and mitigating known vulnerabilities?	— Vulnerability scanning coverage — Percentage of systems with no known severe vulnerabilities — Mean time to mitigate vulnerabilities — Number of known vulnerabilities
Patch management	How well do we maintain the patch state of systems?	— Patch policy compliance — Patch management coverage — Mean time to patch
Application security	Can we rely on the security model of business applications to operate as intended?	— Number of applications — Percentage of critical applications — Risk assessment coverage — Security testing coverage
Configuration management	How do changes to system configuration affect security?	— Mean time to complete changes — Percentage of changes with security reviews — Percentage of changes with security exceptions
Cybersecurity spending	What is the level and purpose of spending on information security?	— IT security spending as percentage of IT budget — IT security budget allocation

Source: Kearney analysis

Fortify the ecosystem

The active defense mindset needs to be extended across the ecosystem in each country by not only implementing best practice guidelines in the corporate sector, but also raising cyber awareness across business partners. Three moves can help fortify the ecosystem:

— Instill a culture of transparency in sharing threat intelligence.

— Extend cyber resilience across the supply chain.

— Forge public–private partnerships (PPP) and industry alliances.

Instill a culture of transparency in sharing threat intelligence

Defending a country's digital assets requires close cooperation across stakeholders, including government agencies, the private sector, and end users. Despite general agreement about the need for this cooperation, information sharing remains inadequate both globally and in the region. Legal impediments—some real, some perceived—are obstacles to robust information sharing across private and public sector entities. The US Cybersecurity Information Sharing Act aims to improve cybersecurity by giving private companies liability protection when they share relevant information with federal or private entities, allowing companies to remove information that identifies someone who is not directly related to a threat.

ENISA suggests three types of approaches to sharing information on cybersecurity incidents: traditional regulation, self- and co-regulation, and information and education schemes.[37]

African countries must move beyond regulations and instead focus on education and awareness building. In the initial stages, an awareness-building approach focused on value at risk and driven by national cybersecurity agencies could help create a climate of confidence and trust. It could enable countries to more easily share good and bad practices and experiences and discuss preparedness measures. Keeping the sharing group small and using traffic-light protocols or other rules on how information gets shared can inculcate the right behaviors. In addition, the types of regular table-top exercises, cyber-incident drills, and stress testing that are currently being carried out in South Africa need to be extended to the rest of Africa.

There is also merit in cross-sector communication, given the convergence of sectors in the digital sphere (for example, telecoms and banking). It is also useful to develop an early warning system for CIIs, which requires the cooperation of a wide range of stakeholders and could be the central capability for handling creeping, slow burn, and sudden crises. Having a common language for sharing threat information enables greater standardization. For example, the free, community-driven STIX and TAXII standards help with the automated exchange of cyber-threat intelligence.

Economic incentives stemming from cost savings—such as quicker reaction to threats, and anticipating network failures—and the quality, value, and use of shared information should be touted as the main reasons for building a sharing culture. More robust sharing of private and public network security information and real-time threat information would enable effective strategic and operational decisions. The Cybersecurity Hub in South Africa was established by the Department of Telecommunications and Postal Services in 2015 to enhance interaction and consultation and promote a coordinated approach to engagement with the private sector and civil society. The hub coordinates cybersecurity response activities and facilitates information and technology sharing. It also promotes the use of national standards for threat sharing via various platforms.

[37] *Cybersecurity Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*, ENISA, December 2015

Extend cyber resilience across the supply chain

As cybercriminals often take advantage of SMEs' low readiness levels to infiltrate these businesses' partnerships with larger organizations, the cybersecurity lens must be extended across the entire supply chain.

Building cyber resilience throughout supply chains requires consideration of the management practices of managed services and cloud services vendors. The supply chain represents a significant cybersecurity risk as it has various breach possibilities. For example, a software manufacturer could be breached via malware that modifies source code that is then distributed to enterprises that use the software. Another common compromise vector is the theft of a vendor's credentials that grant remote access to an enterprise the vendor works with, leading to infiltration of the enterprise network from a trusted source. High-profile breaches have included Target, Home Depot, and the US Office of Personnel Management. In addition, ICT services and support are often outsourced to reduce costs and streamline operations.

Small organizations are often targeted because they are more vulnerable, represent a single point of failure, or have disproportionate access to valuable information given their size within a supply chain.

It is essential to institutionalize a multi-stakeholder supply chain risk assessment process that engages as many supply chain members as possible. Vital business relationships must be graded according to the consequences of losing their services and be regularly reviewed for relevance and interactions between subsequent identified supply chain members. This is technically challenging as some of the most complex supply chains have many external partners. However, by adopting a security-by-design mindset as part of a cybersecurity strategy, businesses can help avoid the piecemeal implementation of cybersecurity solutions, which will reduce the future need for costly and often ineffective retrofitting. Additionally, monitoring data flow across supply chain links can reveal potential indicators of compromise and provide insight into potentially risky behavior.

Forge PPPs and industry alliances

The public and private sectors can benefit from working together on cybersecurity initiatives. The private sector controls much of the critical infrastructure that is vulnerable to cyber threats. Some companies with such infrastructure have already defined cybersecurity strategies and governance, giving them unique expertise and experience in dealing with potential threats.

Cooperation between industry and government agencies on cybersecurity initiatives can use both sectors' unique yet complementary strengths. According to the Intelligence and National Security Alliance, the mission of cybersecurity PPPs is threefold. First, these partnerships must identify and detect behaviors of concern. Second, PPPs must ensure that actors from both sectors comply with the standards of the partnership. Third, and most importantly, PPPs must provide a mechanism for a response after a cyber threat. This entails examining attacks and addressing any necessary shortcomings in the current defense system.

Furthermore, effective PPPs should ensure that policymakers understand the cybersecurity developments in the private sector and their policy implications. PPP programs have supported numerous objectives, including sharing best practices and threat intelligence, harmonizing standards, ensuring greater inclusion of SMEs, and R&D into emerging threat vectors. For example, the Government of Mauritius developed a PPP-based collaboration framework as part of its National Cybercrime Strategy to facilitate better collaboration and cooperation among stakeholders. The collaborative approach helped drive cybersecurity resilience and protect CII. The evolution of Mauritius's PPP model demonstrated that flexible PPP arrangements are more beneficial than rigid approaches. These models better reflect the complexities of processes and hierarchies in the public and private sectors.

PPPs have typically focused on three objectives: workforce development, R&D, and information sharing. The main private sector parties in these partnerships generally come from local or global institutes of higher learning, research institutes, and cybersecurity solution vendors, including those specializing in cyber insurance.

Industry alliances have also emerged around niche areas such as IoT security, which regional companies could benefit from. These alliances focus mainly on solving security concerns around IoT through collaborative research and by shaping standards. African countries should collaborate with these international industry alliances or explore regional alliances focused on their specific needs. Some of the key emerging alliances include the IoT Cybersecurity Alliance, the Industrial Internet Consortium, and the Cyber Threat Alliance.

African countries need to drive the growth of African cybersecurity workforce capabilities.

Develop next-generation cybersecurity capabilities

Cybersecurity presents a significant economic opportunity for the region given that it is one of the fastest growing segments in the ICT space. A concerted effort to encourage the development of the local industry will allow regional companies to take advantage of these opportunities. African countries need to drive the growth of African cybersecurity workforce capabilities and develop frameworks that ensure greater mobility across the vendor ecosystem.

Because of gaps in capacity and capabilities, the region needs more people to pursue cybersecurity careers, with skills development tailored to the needs of individual industries. Hence, it is important to raise the profile of cybersecurity and develop a clear policy framework for developing capacity and capability, as shown in figure 15 on page 29. National cybersecurity agencies need to lay out a clear strategy around cybersecurity workforce planning, which will help position cybersecurity as a crucial strategic occupation that supports the digital economy. This requires closer coordination with public sector agencies, including education ministries, workforce development agencies, and economic development agencies. There is also a need to constantly monitor and track specific cybersecurity skills, such as in IT security, OT security, and encryption. Forecasting skills in demand and identifying plans to address gaps will help develop the local cybersecurity industry.

Setting up occupational standards for cybersecurity includes identifying job roles and competencies, and accrediting training programs and suppliers. A vital aspect of cybersecurity capacity is developing multiple educational pathways, ranging from classes that provide foundational skills to higher-level courses, in the following ways:

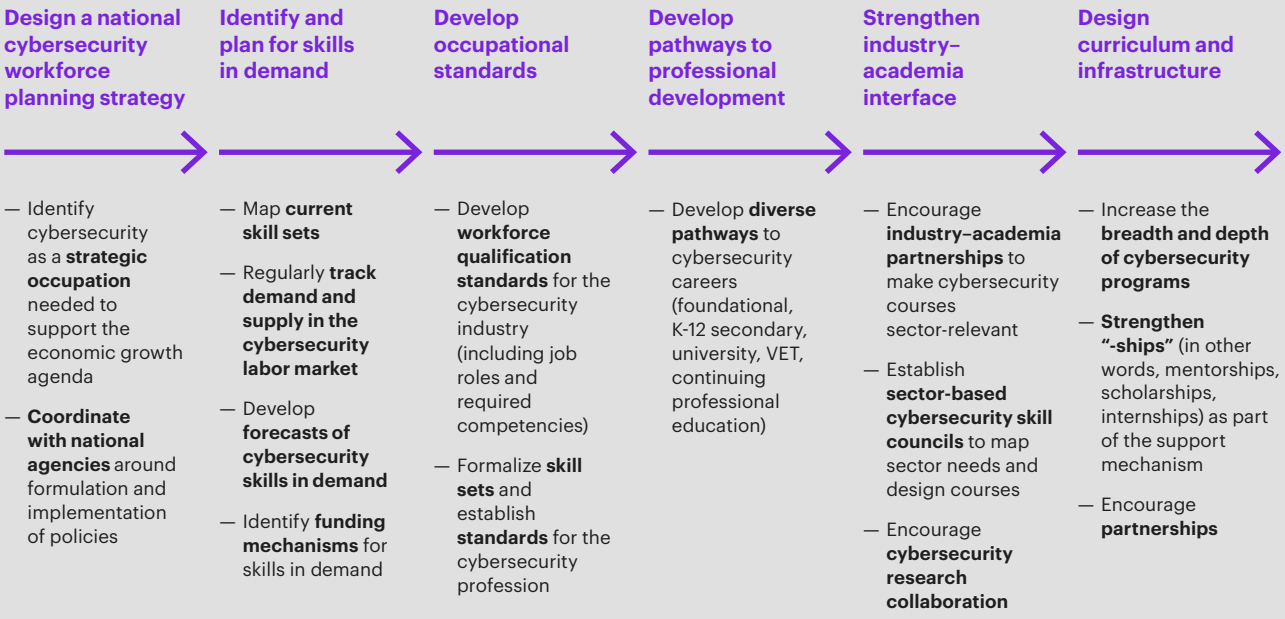
— **K–12:** create awareness via outreach programs to educate the public, including children.

— **Universities:** promote cybersecurity as a career using industry-linking programs, targeted university courses, and innovation opportunities.

— **Industries:** scale up cybersecurity professional development via specialized skill building and conversion programs for professionals.

Figure 15

It is important to develop a clear policy framework for building capacity and capability



Source: Kearney analysis

Encouraging engagement between industry and academia will ensure that programs are tailored to specific industries. Setting up cybersecurity skill councils with industry representation can increase engagement between industry and academia.

In South Africa, financial services provider Absa Group founded the Absa Cybersecurity Academy in 2019 to help address the cybersecurity skills shortage. The program is an externally focused, corporate social responsibility initiative that empowers marginalized South African youths to become certified cybersecurity specialists. It plans to graduate 300 students each year. The academy is also part of the World Economic Forum's Cybersecurity Learning Hub, a joint initiative to provide free cybersecurity training to address the global deficit in the cybersecurity workforce.

The region also needs to strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players. The region could benefit from attracting world-class companies with advanced capabilities to facilitate knowledge exchange and local capability building. To solve today's challenges, institutions need to foster R&D into tackling disinformation and creating cybersecurity solutions for emerging threat vectors in automation, AI, and OT security.

Conclusion and next steps

The region's response to the cybersecurity challenge needs to be comprehensive and forward-looking, engaging an array of stakeholders to deal with threats and support the region's leap into the vanguard of the digital economy. No country, company, or individual can surmount the cybersecurity challenges alone. Every stakeholder has a role to play in creating a safe environment. The crucial shift from traditional, suboptimal cybersecurity to strong cyber resilience will require moving beyond protecting against attacks to building resilient assets and processes. The practices, procedures, and processes used to build and maintain digital systems will determine the success or failure of the next big attack. Enhancing Africa's cybersecurity capabilities and profile will foster the region's business ecosystem and attract external businesses (especially digital ones) to invest in the African economy.

In section 3, we highlighted a four-point agenda of concerted actions required to tackle the core of the problem:

1. Elevate cybersecurity on the regional policy agenda.

2. Secure a sustained commitment to cybersecurity.

3. Fortify the ecosystem.

4. Build the next wave of cybersecurity capability.

Figure 16 shows some actions that are required immediately. In the short term, national governments across Africa should implement the 11-point agenda highlighted under Kearney's RAC Framework. The AUC chairperson's annual report should be expanded to include a review of progress for each country, which will increase awareness about cybersecurity and raise the bar in terms of preparedness.

Figure 16
Some actions are required immediately

Call-to-action agenda	Regional	National
Elevate cybersecurity on the regional policy agenda	— Set up a regional cybersecurity coordination platform. — Track national progress via the AU chairperson's annual report.	— Implement the 11-point RAC Framework. — Establish a sector-level governance mechanism.
Secure a sustained commitment to cybersecurity	— Track cybersecurity investments against the agreed commitment. — Report on national cybersecurity spending.	— Engage with private sector stakeholders to stimulate cybersecurity investment. — Set up a cyber-hygiene dashboard for crucial sectors to define and track key performance indicators at the sector level. — Recommend standards for voluntary adoption.
Fortify the ecosystem	— Adopt voluntary certification of vendors and develop recommended lists. — Foster cross-border and international cybersecurity cooperation. — Encourage PPPs across the region.	— Adopt voluntary certification of vendors, and develop recommended lists. — Establish and incentivize trusted sharing mechanisms. — Formalize security maturity assessments as cyber certification for the private sector. — Set up industry alliances. — Encourage PPPs.
Build the next wave of cybersecurity capabilities	— Develop cross-border capabilities to prevent cybercrime. — Support regional start-ups to boost the development of advanced solutions and address white spaces. — Set up regional R&D funds for cybersecurity, with contributions from member countries.	— Align the cybersecurity talent strategy with the national workforce planning agenda. — Identify and plan for skills that are in demand. — Develop career pathways around cybersecurity. — Foster R&D around emerging threat vectors. — Anchor world-class capabilities to facilitate knowledge exchange.

Source: Kearney analysis

Figure 17

Corporate boards and CISO stakeholders will play an important role

Call-to-action agenda	Corporate board	Chief information security officer
Elevate cybersecurity on the regional policy agenda	— Table cybersecurity as a crucial agenda item for boards of directors. — Establish the CISO as an independent function with board-level reporting.	— Establish group-wide cybersecurity strategies, governance, processes, and culture. — Implement information security management systems that comply with ISO 27001. — Establish working definitions for high-value assets and identify primary threat vectors.
Secure a sustained commitment to cybersecurity	— Set up a cybersecurity investment framework. — Embed a value-at-risk mindset in decision-making.	— Benchmark and track cybersecurity spending vs. IT budget. — Establish cybersecurity metrics and monitor them regularly. — Conduct cyber risk posture assessments. — Review opportunities to trim security product portfolio. — Conduct regular scenario analyses of value at risk.
Fortify the ecosystem	— Instill a risk-centric culture.	— Engage with peers in and across sectors to share threat intelligence and best practices. — Extend cybersecurity policies and processes across the supply chain. — Participate in industry alliances focusing on emerging threat vectors.
Build the next wave of cybersecurity capabilities	— Elevate cybersecurity capacity building as a strategic imperative.	— Engage in capacity and capability-building initiatives. — Interface with academic institutions to design curriculums and programs aligned with industry needs. — Explore investments in emerging security technologies such as artificial intelligence and blockchain.

Source: Kearney analysis

A sustained and committed approach to investing in cybersecurity is needed as the region becomes more digitally connected. From 2022 to 2026, Africa will need to spend around $22 billion (around 0.25 percent of annual regional GDP) to align with international benchmarks and secure the high-value assets that may be at risk from cyberattacks.

Corporate boards and CISOs have important roles to play in creating a defense-in-depth culture in their organizations (see figure 17). These roles include elevating cybersecurity on the board of directors' agenda and establishing the CISO function as an independent reporting function. CISO responsibilities include establishing group-wide strategies and governance, and conducting value-at-risk assessments. In addition, cybersecurity resilience needs to be extended to business partners by providing continuous education and including them in internal risk audit assessments.

Forging industry alliances and engaging with educational institutions to develop industry-relevant cybersecurity courses will help build a robust local industry and address capacity and capability gaps.

Given the varying levels of readiness across African countries, the magnitude of required change, and the complexity of creating a coherent region-wide approach to cybersecurity, a system based on a loose collaboration of national authorities and voluntary exchanges is unlikely to be enough. Only a radical agenda and active defense stance with multi-stakeholder engagement can defend the region and capitalize on its collective resources.

Addressing cyber threats is about resilience, but it is also a business enabler. If the cyber profile of Africa increases, many external businesses, chiefly in the IT and Ops domains, will be willing to invest in Africa—provided adjacent investments in communications and IT infrastructure are made. Even the local business ecosystem will benefit. Therefore, the cyber threat itself presents an opportunity for the continent—not only to defend and foster a more protected cyberspace but also to enable businesses to thrive in the digital economy.

Appendix

Countries with the highest cybersecurity readiness were selected through a three-stage process shown in figure A on page 33. In stage 1, only countries listed in International Telecommunications Union's Global Cybersecurity Index (GCI) were selected. In stage 2, the list was narrowed down to five countries with a GDP filter. In Stage 3, industry experts stress-tested the stage 2 outcomes ensuring countries important to Africa's cybersecurity landscape were covered. From this, Rwanda, Algeria, and Ethiopia were identified for further investigation, but were ultimately excluded from the final assessment. For Rwanda, despite the World Bank providing $100 million in financing for digital development in 2021, the country was excluded due to its relatively low GDP. Algeria and Ethiopia were excluded as they rated much lower on the GCI than the top five countries selected.

Strategy: looks at published national strategies that identify the importance of cybersecurity and outline plans to prepare for future threats

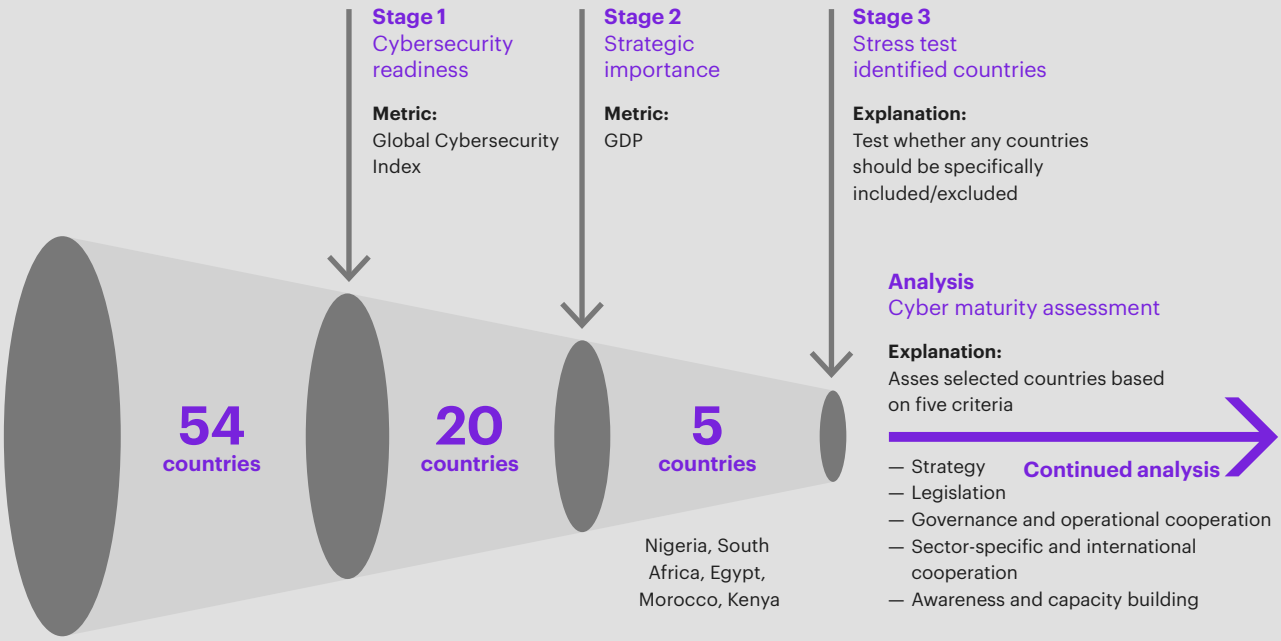
Legislation: based on the existence of legal institutions, policy, and frameworks that deal with cybersecurity and cybercrime

— **Governance and operational entities:** based on the existence of technical institutions and their technological capabilities, frameworks, and other organizations that are mandated to deal with cybercrime

— **Sector-specific and international cooperation:** based on the existence of cooperation during the policy development and implementation phases

— **Awareness and capacity building:** measures based on the existence of partnerships, cooperative frameworks, and information-sharing networks

Figure A
Countries with the highest cybersecurity readiness were selected through a three-stage process



Sources: Global Cybersecurity Index, ITU (2021), GDP Africa, Trading Economics (2022); Kearney analysis

Figure B
Policy maturity by country

Country	Strategy	Legislation	Governance and operational entities	Sector-specific and international cooperation	Awareness and capacity building
Nigeria	— Well-defined strategy to deal with cyberthreats — Poor implementation of strategy	— National Cybersecurity Policy and Strategy (2021)	— National Cybersecurity Coordination Centre (NCCC); Nigerian Computer Readiness and Response Team	— NCCC works across sectors, acting as a communication bridge between private and public sectors	— Identified need for training programs and capability enhancement — Limited implementation
South Africa	— Measures to prevent and punish cybercrime — Not overarching	— National Cyber Security Policy Framework (2015)	— National Cybersecurity Hub, which governs cyber activities	— The National Cybersecurity Hub provides centralized communication between parties	— Limited initiatives launched — Mostly driven by private sector
Egypt	— Well-defined strategy that focuses on government and private sector positioning, with clear objectives	— National Cybersecurity Strategy (2017)	— Egyptian Supreme Cybersecurity Council; Egyptian Computer Emergency Readiness Team	— Programs included in the National Cybersecurity Strategy cooperate with regional and international stakeholders	— Initiatives mostly led by private sector
Morocco	— Has a risk assessment of current infrastructure, and plans to develop capabilities	— National Strategy for Cybersecurity (2012)	— National Control Commission for the Protection of Personal Data; Moroccan Computer Emergency Response Team	— Minimal local cooperation — Part of the international cooperation on regional cybercrime	— Identified need for capability upliftment — Little implementation
Kenya	— Well-defined strategy that focuses on government's positioning as well as capability enhancement	— National Cybersecurity Strategy (2014); Computer Misuse and Cybercrimes Act (2018)	— Ministry of ICT; Cyber Crime Unit, which sits within the National Police Service	— A national coordination center has been proposed but not fully implemented — Multiple regional coordination agreements	— Kenya National Digital Master Plan (2014) is aimed at improving capabilities and upgrading infrastructure

Source: Kearney Energy Transition Institute

Glossary

Figure
Glossary (1/2)

Abbreviation (where relevant)	Term	Definition
4IR	Fourth Industrial Revolution	Conceptualizes a rapid change to technology, industries, and societal patterns and processes in the 21st century due to increasing interconnectivity and smart automation
	advanced persistent threats	A cyberattack where an unauthorized user gains access to a network and remains undetected for an extended period
AfCFTA	African Continental Free Trade Area	A pan-African agreement to create the largest free-trade area in the world, initially eliminating 90 percent of intra-African trade tariffs, and ultimately unifying the economies of the African Union
	agent-driven fraud	Exploitation of customer trust or illiteracy by sales agents, intended to maliciously use the customer's security or access information
	artificial intelligence	The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings
ASEAN	Association of South East Asian Nations	A political and economic union of 10 member states in South East Asia, which promotes intergovernmental cooperation
AU	African Union	A continental union consisting of the 55 African states
AUC	African Union Commission	The African Union's secretariat, which undertakes the day-to-day activities of the union. The leadership structure of the commission includes the chairperson, deputy chairperson, and eight commissioners. They oversee a thematic program that includes peace and security, political affairs, trade and industry, infrastructure and energy, social affairs, rural economy and agriculture, human resources, science and technology, and economic affairs. It is based in Addis Ababa, Ethiopia.
	authentication attacks	Exploiting a weak PIN system to gain access to user accounts
BYOD	bring your own device	A corporate policy whereby employees are encouraged to use their own personal devices for performing their regular duties, rather than company-owned assets
	brute-force attack	Guessing PIN codes to access user accounts
CAGR	compound annual growth rate	The measure of an investment's annual growth rate over time, taking into account the effect of compounding
CERT	computer emergency response team	A group of information security experts responsible for the protection against, detection of, and response to an organization's cybersecurity incidents
CII	critical information infrastructure	Includes ICT systems, data systems, databases, networks (including people, buildings, facilities, and processes), the destruction of which has a debilitating impact on national security, economy, operations, public health, or safety
CISO	chief information security officers	Senior-level executives responsible for developing and implementing information security programs, including procedures and policies designed to protect enterprise communications, systems, and assets from internal and external threats
	Council of Europe Cybercrime Programme Office	Based in Bucharest, Romania, the office is responsible for assisting countries worldwide in strengthening their legal systems' capacity to respond to the challenges posed by cybercrime and electronic evidence on the basis of using standards from the Budapest Convention on Cybercrime.
	cybersecurity	The practice of protecting vital systems and sensitive information from digital attack
	distributed denial-of-service attack	Blocking a network link to prevent legitimate transactions and create an opportunity for fraud
DEI	Global Digital Evolution Index	A measure of a nation's digital maturity
ENISA	European Union Agency for Cybersecurity	Contributes to the European Union's (EU's) cyber policy; enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes; cooperates with member states and EU bodies; and helps Europe prepare for tomorrow's cyber challenges
GCI	Global Cybersecurity Index	A trusted reference that measures the commitment of countries to cybersecurity at a global level, helping to raise awareness of the importance and different dimensions of the issue. Each country's level of development or engagement is assessed on five pillars: (i) legal measures, (ii) technical measures, (iii) organizational measures, (iv) capacity development, and (v) cooperation. This is then aggregated into an overall score.
GDP	gross domestic product	The standard measure of the value created through the production of goods and services in a country during a year

Source: Kearney Energy Transition Institute

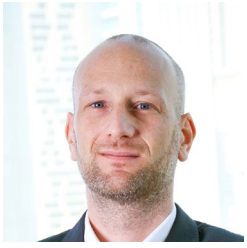
Figure
Glossary (2/2)

Abbreviation (where relevant)	Term	Definition
GDPR	General Data Protection Regulation	A regulation in European Union (EU) law on data protection and privacy in the EU and the European Economic Area
	Global Action on Cybercrime Extended project	A joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe to strengthen the capacities of states worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area
	identity theft	Opening accounts and performing illicit transactions under a stolen identity
ICT	information and communications technology	A diverse set of technological tools and resources used to transmit, store, create, share, or exchange information
INSA	Intelligence and National Security Alliance	The leading nonpartisan, nonprofit trade association for public, private, and academic sector members of the United States intelligence community. It promotes public–private collaboration to strengthen the intelligence community and meet national security objectives. INSA members collaborate to develop creative, innovative, and timely solutions to the intelligence and national security issues facing the United States.
IoT	Internet of Things	The network of physical objects able to connect to and share data with other devices via the Internet
ISO	International Organization for Standardization	The organization that develops and publishes international standards
ISO 27001	International Organization for Standardization 27001	ISO/IEC 27001 is the world's best-known standard for information security management systems and their requirements
IT	information technology	The use of computing devices to process, store, and exchange electronic data and information
K–12	kindergarten to 12th grade	An education system for children that starts at kindergarten (the first year) and ends at 12th grade (the 13th year)
NIST	National Institute of Standards and Technology (US Department of Commerce)	Promotes US innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life. It is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.
NRI	Network Readiness Index	A measure of a nation's ability to exploit advances in ICT
OT	operation technology	Technology used on industrial equipment, assets, and processes to detect or actuate changes through direct monitoring
	phishing	Using social engineering to trick a user into revealing compromising information
PPP	public–private partnerships	A long-term arrangement between two or more public and private sector organizations
RAC Framework	Rapid Action Cybersecurity Framework	Kearney's cybersecurity framework (as highlighted in section 3)
SME	small and medium-size enterprise	A business that maintains revenues, assets, or a number of employees below a certain threshold
STIX	Structured Threat Information eXpression	A standardized language that represents structured information about cyber threats and is used to exchange cyber threat intelligence
	systemic risk	The risk that a cyber event cascades into related ecosystem components, creating adverse effects in public health, safety, the economy, or national security[38]
TAXII	Trusted Automated eXchange of Indicator Information	A collection of services and message exchanges that enable information about cyber threats to be shared across product, service, and organizational boundaries
USSD	Unstructured Supplementary Service Data	An unencrypted, real-time connection between mobile devices that's used to send data or communicate, similar to short message service (that is, SMS)
	USSD technology vulnerabilities	USSD messages that can be intercepted as they are not encrypted
	unauthorized SIM swap	Using social engineering to obtain personal credentials to take control of a person's SIM card, to gain full access to their mobile money accounts
WFH	work from home	A corporate policy whereby employees are allowed to perform their regular duties away from their typical workplace by accessing company networks remotely
	zero-day exploits	A cyberattack that targets a software vulnerability that is unknown to either the software or antivirus vendors, giving the vendor "zero days" to fix the issue as it was only just discovered

[38] *Understanding Systemic Cyber Risk*, World Economic Forum

Source: Kearney Energy Transition Institute

Authors



Rob van Dale
Partner, Dubai
rob.van.dale@kearney.com

Prashaen Reddy
Partner, Johannesburg
prashaen.reddy@kearney.com

Guy Ngambeket
Consultant, Doha
guy.ngambeket@kearney.com

Greg Epstein
Consultant, Johannesburg
greg.epstein@kearney.com

The authors would like to thank Sanket Jakate, Troy Horrell, Abdulla Mulla, and Malcolm Wright for their valuable contributions to this paper.

Kearney is a leading global management consulting firm. For nearly 100 years, we have been a trusted advisor to C-suites, government bodies, and nonprofit organizations. Our people make us who we are. Driven to be the difference between a big idea and making it happen, we help our clients break through.

kearney.com

kearney.com

KEARNEY