**CYBERSECURITY ECOSYSTEM IN AFRICA**

***Africa*** is the world's second-largest and second-most populous [continent](https://en.wikipedia.org/wiki/Continent), after [Asia](https://en.wikipedia.org/wiki/Asia). Although it has abundant [natural resources](https://en.wikipedia.org/wiki/Natural_resource), Africa remains the world's poorest and [least developed](https://en.wikipedia.org/wiki/Human_Development_Index) continent. Africa seems to be the "lost continent" of the information technologies (IT). The second largest continent is the least computerized.  ***Cybersecurity*** is the practice of protecting critical systems and sensitive information from digital attacks.

The African Union Commission and Symantec, as part of the Global Forum for Cybersecurity Expertise (GFCE) Initiative, released a report analyzing cyber security trends and government responses in Africa. In addition to the AUC and Symantec this report represents a multi-stakeholder effort, with support from the United States Department of State.

The report explores various cybersecurity trends including the overall professionalization of cyber crimes:

* Rise of Ransomware and Cryptolocker
* Social Media, Scams, and Email Threats
* Smartphones and the Internet of Things
* Business Email Scams
* Vulnerabilities

Africa is a continent on the rise. It is growing quickly in terms of population, the economy, and global influence. Today, Africa is home to 1.21 billion people (up from just 800 million in 2000), with a median age of just 19.5 years, the youngest population in the world. With this prominence of youth comes a diverse population that is looking for productive employment, social engagement, free expression, and increased global connectivity. While the downturn in world commodity prices has hit African economies hard, nearly every African nation is poised to grow over the coming years. Some will continue on a trajectory putting them among the fastest growing economies in the world. Technology adoption continues to rise as well, with mobile device ownership growing exponentially, social media use increasing, and the Internet of Things (IoT) quickly becoming a reality. Even the most conservative metrics show that Africa is poised to make great gains and help fuel global growth into the future. Along with this rapid economic growth, comes a burgeoning e-commerce industry that is poised to expand to an estimated $75 billion USD by the year 2025.

With this growing prosperity and digitization however new risks and vulnerabilities arise that could undermine progress. Chief among these risks is the global rise of cybercrime. As the African Continent’s economy moves online, citizens, their computer systems, and the Continent’s information technology (IT) infrastructure become enticing targets for an increasingly professional cadre of cybercriminals. The growth of cybercrime is by no means just an African problem. In fact, in 2013, the total global direct cost of cybercrime reached an estimated $113 billion USD. In South Africa alone, 73% of adults reported experiencing cybercrime, which is estimated to have cost the South African economy 337 million USD. Compounding the problem is the fact that many Africans are still using outdated, or in many cases pirated, software. Nearly one quarter of users in Africa are currently using the operating system Windows XP that was first released in 2001, and for which software patches were discontinued in 2014.

On the 1st of June 2021, the President of the Republic of South Africa signed the Cybercrimes Act 1 into law. This is the law which criminalizes unlawful activities taking place in cyberspace.

As a flurry of tech startup investment driven by the pandemic tailed off in the second quarter of 2022, funding for startups fell globally by [23%](https://www.bloomberg.com/news/articles/2022-07-13/venture-capitalists-face-a-reckoning-as-funding-and-deals-slow), the largest drop in over a decade. In Africa, however, [that funding doubled](https://www.bloomberg.com/news/articles/2022-08-03/africa-defies-global-trend-with-funding-for-startups-surging) over the same period. The continent has seen a wave of venture capital from within and without, and increasing numbers of ‘unicorns’ – startups valued at over $1 billion.

For investors, the continent is steadily becoming a safer bet, but certain concerns remain, not least of which is the cyber-reliance of many African nations and businesses. [A 2021 report by Interpol suggests](https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf) that the continent’s GDP is reduced by up to 10% (equivalent to $4.12 billion in 2021) by cybercrime alone. If emerging markets like Nigeria, South Africa, and Kenya are to continue drawing investment, they’ll need to match business innovation with more effective security measures.

***Understanding the Threat Landscape:-***

In order for Africa to realize its full potential, policymakers will need to implement effective policies and awareness initiatives to stem the rising tide of cyber threats. Unfortunately, these same policymakers, technicians, and other experts have long noted the lack of detailed and reliable threat information regarding cybercrime threats in the region. Such information is invaluable in assessing and managing cyber risks by providing governments a more complete and nuanced understanding of how criminals and other actors are targeting and exploiting cyber-related vulnerabilities.

To help address this information gap, the African Union (AU) and Symantec Corporation, through the Global Forum for Cyber Expertise (GFCE) and with the support of the U.S. Department of State, are engaged in a public-private partnership to develop a report that collects and presents detailed policy and technical data on the state of cybersecurity in Africa. The research includes surveys sent to every African nation on current cyber capabilities and trends, as well as regional cybersecurity threat data from Symantec’s Global Intelligence Network. Governments and other interested parties can utilize this information to identify gaps and to strengthen protection, prevention and response mechanisms to confront the diverse range of cyber threats. This report also will be an excellent opportunity for AU Member States to illustrate the significant advances and accomplishments in the areas of cybersecurity and combating cybercrime. Moreover, the results of the research will serve to guide future capacity building efforts for AU Members.

***The Threat of Mobile Malware:-***

Initial findings indicate that due to the borderless nature of cybercrime, many of the trends we see globally also are affecting Africa, including the explosion of ransomware and social media scams, and the proliferation of new malware and website vulnerabilities. However, because of how the IT infrastructure evolved in Africa, several of these cybercrime trends will become especially acute and pose a significant danger. Mobile malware, for instance, is a huge problem in Africa today and will continue to be a major threat into the future. Globally, the number of new vulnerabilities identified in mobile software grew a staggering 214% in 2014. Over the past decade, Mobile phone networks have transformed communications in Africa. Most importantly, mobile phones have allowed African communications networks to leapfrog the entire landline generation of development and go directly to the digital age. Globally, smartphones are an increasingly attractive target for cybercriminals who are investing in more sophisticated attacks that are effective at stealing personal data or extorting money from victims. The steady rise of mobile malware that mainly targets Android systems is also of concern given 89% of the smartphone market share in Africa runs on that platform.  For example, according to Symantec data, more than one out of every seven mobile devices in Nigeria is currently infected with mobile malware. Africa also leads the world in money transfers using mobile phones, with 14% of all Africans receiving money through mobile transfers. And with some of the world’s largest mobile money transfer services, such as Kenya’s Mpesa, cybercriminals will continue to heavily target mobile devices in Africa.

With a young population that is rapidly adopting new technologies, Africa is on the verge of an Internet boom. These advances also bring with them new risks. To keep pace, initiatives by African Nations should seek to combat cybercrime and improve their overall cybersecurity posture. It will take a concerted effort from international governments, industry, and civil society to reduce cybercrime and improve cyber protection and resilience so that Africa can reach its full potential in the global economy.

***The Cost of a Continental Skill Shortage:-***

Cyber skill shortages remain an issue in many Global South markets, meaning the impact of common threats is effectively magnified when they hit organizations in these nations. Having the expertise on hand to reduce time-to-response and take decisive, effective remediation action can be the difference between a bullet point on a threat report and a fully-fledged attack.

Many cyber professionals will think of WannaCry, a ransomware attack which affected over 200,000 devices in 2017, as a threat of the past, its relevance consigned to the months after its first appearance. For countries in Latin America and the Caribbean, however, it remains a prevalent and punishing tool, and continues to target thousands of systems: the [highest number of WannaCry attacks](https://www.itpro.co.uk/security/ransomware/367659/wannacry-five-years-on-part-two) are consistently seen in Brazil, Ecuador, and Chile. Why is so much damage still being wrought by a ransomware strain which was largely thrown into obsolescence in the Global North years ago? Think tanks [like the RUSI](https://rusi.org/explore-our-research/publications/commentary/ransomware-now-threatens-global-south) attribute it to a lack of IT professionals and the slow uptake of new security standards in regions which are otherwise enjoying rapid digitalization.

The discordance between internet penetration rates and cyber security capabilities is even more pronounced in Africa. An [estimate made in 2018](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3142296) suggested that there were only 7,000 certified security professionals in the continent, one for every 177,000 people. In the US, comparatively, the figure was one for every 330 people. Even adjusting for Africa’s reduced internet penetration rate, the figure remains one professional for every 45,140 internet users.

The result of this is that [9 in every 10 African businesses](https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf) are said to operate without necessary cyber security protocols in place. If the continent continues to draw investment without making big strides in its cyber security measures, its rapidly growing base of potential victims (Africa’s internet using population numbers over [650 million](https://www.internetworldstats.com/stats.htm), massively outstripping [North America’s 350 million](https://www.internetworldstats.com/stats2.htm)) will draw increasing numbers of cyber-attacks.

***Attackers Destabilize the Market:-***

There is already evidence that attackers are beginning to take notice. [Interpol cites a report](https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf) claiming that in the first months of 2021, African organizations saw the highest increase in ransomware attacks of any region. But it is the efficacy, rather than frequency, of attacks on Global South nations which will be most concerning to investors seeking stability.

Last year in South Africa, several major trade ports were brought to a halt by a ransomware attack on Transnet and, just a few months later, the country’s justice department was brought down in a similar attack. [In Costa Rica](https://www.itpro.co.uk/security/ransomware/367704/ransomware-group-conti-threatens-to-overthrow-costa-rican-government) earlier this year, the ransomware group Conti successfully locked down several government systems and threatened to overthrow the presiding government if ransom payments were not made, leading President Chaves to declare a national state of emergency. Organizations operating critical national infrastructure are particularly attractive to attackers, as the disruption caused by their downtime makes it easier to extort a generous ransom. These attacks are also high-profile, often internationally so.

High-profile attacks can greatly affect the confidence of investors and potential business partners. A [KPMG report](https://assets.kpmg/content/dam/kpmg/pdf/2016/03/SG-Advisory-CS-Cyber-Risks-in-Emerging-Markets.pdf) on cyber risks in emerging markets explains: “Those suppliers handling confidential third-party data in emerging markets that are able to demonstrate strong security posture around that data are likely to be more attractive and potentially able to win more business.” Organizations in countries with generally weaker cyber security practices should be looking at tools to put the concerns of potential partners and investors at ease. Ideally these should be AI-driven tools which not only stop old, known threats, but also those headline-grabbing novel attacks and zero days.

***Protecting Progress:-***

Many Global South governments are now taking steps to address cybercrime concerns, and bring legislation up to global standards. Last year, South Africa’s President Cyril Ramaphosa signed the Cybercrimes and Cybersecurity Act, placing new breach reporting responsibilities on organizations. Similar acts were passed in nations such as [Zambia](https://www.parliament.gov.zm/node/8832) and [Ecuador](https://www.dataguidance.com/opinion/ecuador-cybersecurity-bill-overview) the same year.

International cooperation on the issue of cyber security is also more common: the [Convention on Cyber-security and Personal Data Protection](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection) adopted by the African Union's 55 member states in 2014 has now been ratified by thirteen nations, while in July of this year, delegates from Bangladesh, Bhutan, India, Myanmar, Nepal, Sri Lanka, and Thailand gathered for the inaugural BIMSTEC (Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation) meeting on [cyber security cooperation](https://bimstec.org/?event=first-meeting-of-the-bimstec-expert-group-on-cyber-security-cooperation-met-in-new-delhi-on-14-15-july-2022).

These are important steps, but legislation and discussion will do little if organizations do not take action in their wake. As we stressed in our [recent blog](https://darktrace.com/blog/a-new-home-front-the-part-we-all-play-in-a-modern-cyber-war) on modern cyber warfare, the involvement of the private sector in government directives is crucial to tackling widespread cyber threats. Togo’s Minister of Digital Economy stressed this fact when he [announced](https://finance.yahoo.com/news/togos-cybersecurity-center-serve-whole-092100079.html) the new African Centre for Coordination and Research in Cybersecurity last month: “Our partnership model with the private sector is an innovative approach that we want to showcase to inspire other countries for safer cyberspace on the continent.”

The economic significance of cyber resilience has become undeniable. With proper security investment, emerging markets and Global South nations can hold onto the billions being lost to cyber-attack costs, and continue to focus on business growth and innovation.

The ability to protect the data of partners and clients is today one of the fundamentals behind every business decision. Today’s fluid financial markets provide a plethora of access points for malicious actors to penetrate systems and acquire data. These have to be protected. A system is only as strong as its weakest point. Therefore, as communication and financial networks become globalised, impregnable cybersecurity is becoming a prerequisite for investment in any territory. However, cybersecurity on the African continent remains challenging and many companies are unprepared for cyber attacks.

In addition, only a handful of countries have laws in place to protect consumers and businesses. The Global Cybersecurity Index (2021) shows that of 54 African countries assessed, only 29 have introduced cybersecurity legislation. In 2022, 52% of companies in Africa believed that they were unprepared to handle a large-scale cyber attack. The reality is grimmer; Interpol’s Africa Cyberthreat Assessment Report found that more than 90% of businesses on the continent were operating without the necessary cybersecurity protocols.

***African businesses not prioritizing cybersecurity:-***

African organizations are not giving cybersecurity the priority it deserves and this inadequate security is directly affecting business for enterprises, as well as countries. According to Techcabal, Africa is losing $4 billion annually to cybercrime. However, cybercrime hurts companies beyond their financials, leading to data loss, theft of intellectual property and financial and/or personal information, and damage to brand and reputation.

Africa’s poor cybersecurity also means the region is now targeted by cybercriminals as the “soft underbelly” of global business networks. In Africa, many countries have seen a rise in digital threats and malicious cyber activities.

Ironically, Africa’s rapid technological evolution makes the region an attractive target for cybercriminals. This is slowly changing, though, with countries such as Kenya and Zambia implementing new cybersecurity laws.