Cyber Research Conference 25 | CYBERSECURITY RESEARCH SOCIETY
Securitas Per Investigationem

International journal of Cybersecurity Research and Informatics

Conference Paper:

The Digital Landscape in Africa and the Role of Artificial Intelligence (AI) Tools for Threat Identification

Authors: [1]Toluwalase Akorede Kadiri [2]Dr. Iretioluwa Akerele [3]Shalom Bulus
Affiliations: Cybarik
Corresponding e-mail(s): [1]kadrinate@gmail.com [2]iretioluwaaakerele@gmail.com [3]Bulusshalom2@gmail.com
Accepted: 11th May 2025; Published: 12th September 2025

THE DIGITAL LANDSCAPE IN AFRICA AND THE ROLE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS FOR THREAT IDENTIFICATION

Abstract

In the second quarter of 2024 alone, cybersecurity organization Check Point revealed that African organizations suffered 2,960 cyberattacks (the world's highest weekly average number of attacks), a 37% increase compared to 2023.

The lack of cybersecurity policies and digital education is the main reason malicious actors thrive in African organizations. This is reflected in Knowbe4's 2023 report, which revealed that over 6 in 10 Africans are ignorant about ransomware, the weaponized encryption malware that affected 1 out of 30 African companies in the second quarter of 2023. The looming growth of artificial intelligence (AI) and machine learning (ML) tools is likely to widen the attack landscape for threat actors. However, the tools can also improve threat identification, containment, and overall security posture.

This study explains the prevalence of cyberattacks in 11 African countries (Algeria, Angola, Ethiopia, Egypt, Kenya, Lesotho, Morocco, Nigeria, South Africa, and Senegal) in 2023 and 2024. The research documented 23 attacks, including the attack scope, vulnerability exploited, and impact of intrusion on organizational assets, affecting African organizations across six sectors (government institutions, financial services, power and energy, education, media, and telecommunications). The study also provided practical security recommendations to fight cybercrimes in Africa.

Keywords: Cyberthreats, Vulnerabilities, Artificial Intelligence, Machine Learning

INTRODUCTION

Digital services and internet penetration are growing in Africa. In 2022, Internet users in Africa reached approximately 570 million, more than double the figure since 2015, with a 43% Internet penetration rate in 2021 (Galal, 2024). The technological growth, however, opens African organizations to sophisticated digital threats. In 2023, Reddy et al., (2023) revealed that cybercrime costs African countries over $ 3.5 billion annually.

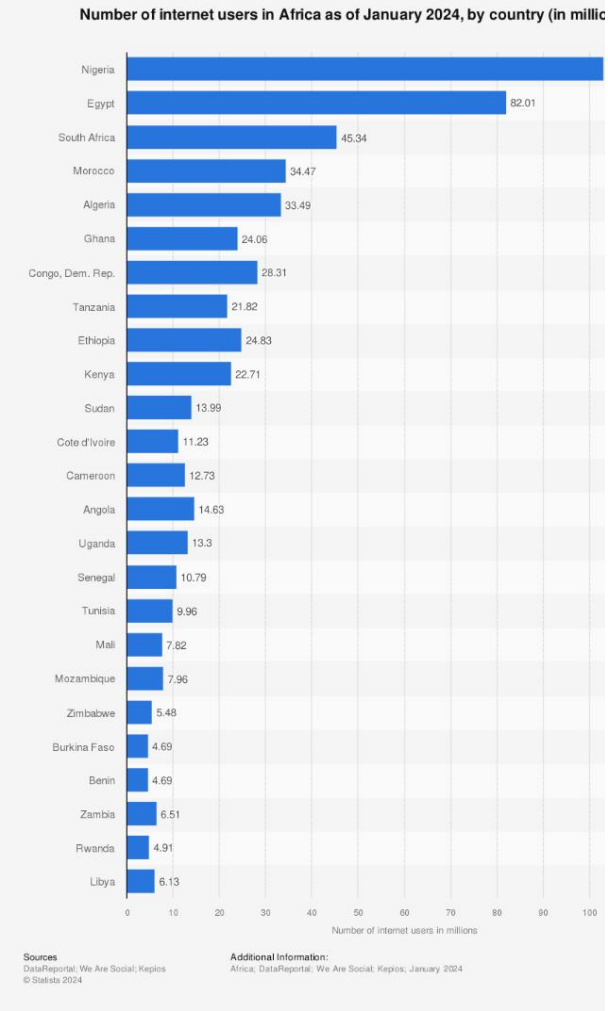


Figure 1.0: Internet penetration in Africa. Source: Statista

The Malabo Convention—the legal framework addressing cybercrime and data protection in Africa signed by African Union (AU) countries in 2014—revealed that only 15 out of 55 African countries have established cybersecurity strategies, while less than 10% of African organizations have risk quantification or monitoring technologies (Ajijola, A-H., & Allen, N., 2022; Thaver, 2022).

In September 2022, KPMG released its Africa Cyber Security Outlook, and it revealed the following: one in five survey respondents don't have a formal information security function; one in five businesses in Africa don't have clearly defined strategies and frameworks to prevent security and privacy risks; one in four African businesses surveyed has an inconsistent approach to mitigating data privacy risks; one in four African organizations have matured in-house security operations center (SOC) for proactive threat monitoring (KPMG, 2022)

Similarly, in 2023, KnowBe4's African Cybersecurity & Awareness Report 2023 revealed that Africa's phishing baseline was 36.7%, meaning over one in three employees is likely to comply with a fraudulent request or click a malicious link (Collard et al., 2024).

The report also examined the effectiveness of cybersecurity training in Africa. While over half of the survey respondents received cybersecurity training, less than a third (21%) of the security training recipients "strongly agreed" the training was adequate; 17% were unsure about the training effectiveness; 10% "strongly disagreed" the training was efficient (Collard, 2023). The result of the security training poll partly explains why African employees are susceptible to malware attacks and costly mistakes (Collard, 2023).

Furthermore, KnowBe4's 2023 report examined the awareness depth of AI and ML technology in African organizations in Botswana, Egypt, Mauritius, Kenya, and South Africa. Per the survey of 800 adults in the aforementioned countries, nearly three-quarters (74%) have misjudged a communication (email or direct message), a photo, or a video to be true; over 5 in 10 of the respondents are aware of deepfakes; more than 3 in 10 don't know what a deepfake is; over 2 in 10 were unsure or had little understanding of deepfake technology (Collard, 2023). The report suggests that African employees are vulnerable to deepfake scams despite the increasing growth of AI and ML in the region.

The lack of national cybersecurity frameworks, inefficient security awareness and culture, and poor investment in security tools show that African organizations are ill-prepared to fight cybercrimes. The

substantial growth of advanced computing systems like AI and ML will likely expand the already porous vulnerability surface, giving cybercriminals unfettered access to sophisticated tools to deepen their nefarious operations in African organizations.

This paper examines cyber breaches in African organizations in 2023 and 2024 to improve cybercrime documentation and awareness in Africa. The paper also proposes preventive measures, highlighting the role of AI in weathering cyberattack storms.

Methodology

This paper covers cyberattacks in Africa in 2023 and 2024. The researchers compiled the report by searching daily for cyber-attacks publicly disclosed on social media pages, verified news outlets, and press releases from the affected organizations. A separate independent researcher validated the authenticity of every claim before documentation. After vetting, the results were compiled in a spreadsheet titled the 2024 African Cybersecurity Report (ACR 2024).

The spreadsheet contains the scope of cyber-attacks, attack description, vector, root cause, impact; action taken by the affected organizations, and corrective measures the affected organizations implemented. **31** cyber-attacks were recorded on the spreadsheet across **11** African countries: Algeria, Angola, Egypt, Ethiopia, Kenya, Lesotho, Morocco, Namibia, Nigeria, South Africa, and Senegal.

The cyberattacks recorded in the spreadsheet cut across the following sectors: government institutions, financial services, power and energy, education, media and telecommunications, aviation, and the automobile niche. Threat actors exploited vulnerabilities like software flaws and security misconfigurations, human weaknesses, such as negligence and third-party intrusion, and weak security controls. The major threats were hacking, ransomware attacks, insider risk, and Distributed Denial of Service (DDoS) Attack. All the pieces of data are visualized in the appendix section.

Discussion and Analysis

The ACR 2024 is a microcosm of the state of cybersecurity in Africa. Between Q1 2023 and Q3 2024, the **finance sector** accounted for 22% of all successful cyberattacks on African organizations, making it the second-most targeted sector behind government institutions (Bezborodko, 2024). The ACR 2024 report follows this trend, as over one-third of the recorded attacks (12 out of 31) affected financial institutions. Furthermore, the ACR 2024 data about the financial sector buttresses the Check Point 2024 report, which showed that attacks on financial services grew by 40% between Q3 2023 and Q3 2024, facing 1,696 attacks weekly on average (Check Point, 2024). The cyber assault on the finance industry happened through varying attack vectors, such as fraud and forgery, hacking, ransomware, and insider fraud.

The ransomware attack on a bank in Angola occurred in February 2023 (FrSebastião, 2023). The attack caused the unavailability of the bank's computer system for "several days," as the Alpha Black Cat ransomware group threatened to release the stolen data illegitimately (FrSebastião, 2023).

In March 2023, a Nigerian fintech company reportedly lost ₦2.9 billion through "illegal transfers from different bank accounts" (Abiodun, 2023). The breach allegedly occurred through a hacking spree, which began on February 13, 2023, with transfers to 28 bank accounts in 63 transactions (Bolu, 2023). After discovering the violation, the company filed a suit in a Lagos court to recover the stolen funds (Abiodun, 2023). The breach lighting struck the company again in May 2024, when an alleged security breach allowed unauthorized entities to divert approximately $24 million to several bank accounts (Chukwu, 2024).

A Nigerian bank experienced an insider attack in May 2024. The employee who was the manager of the electronic products team used their authority as the last line of authorization to divert funds totaling $40 billion for almost two years unnoticed (Olowogboyega & Oladunmade, 2024). The theft was eventually flagged after a customer complaint forced the financial institution to investigate the discrepancies. The stolen funds were allegedly diverted to the bank accounts of 1,190 allies (Olowogboyega & Oladunmade, 2024).

In 2023, crypto criminals stole $3.7 billion from cryptocurrency platforms through hacking incidents (Chainalysis, 2024). Unsurprisingly, a crypto-focused fintech company in Nigeria was breached in February 2022, although the intrusion was revealed in May 2023. A group of hackers called The Syndicate—a team of seven individuals (an Uber driver, two Bureau de Change traders, a senior special assistant to a Nigerian governor, a driver, and a musician)—spearheaded the breach. The Syndicate received helping hands from a gubernatorial candidate for the New Nigeria People's Party in the 2023 governorship election in Nigeria. The candidate was arrested in November 2023 for theft, the conversion of cryptocurrency wallets, and unauthorized fund diversion (Abiodun, 2024). The company lost over ₦140 million to the hack, causing them to release a whitepaper explaining their customer repayment plan (Olayiwola, 2023).

In 2022, Ekeh et al. (2022) explained the prevalence of using SIM cards and Bank Verification Number (BVN) for banking frauds. In July 2023, the Nigerian Police Force (NPF) arrested two fraudsters (Yusuf Ademola and Adesina Olawale Abiodun) adept at hacking BVNs and SIMs for internet banking fraud (Uba, 2023). Before their arrest, they swindled over 1,000 bank accounts (Uba, 2023).

Kenya, like Nigeria, is a haven of banking fraud, having experienced over $600 million in loss linked to card fraud and corruption between 2021 and July 2023 (Ndege, 2024). In April 2024, a Kenyan bank allegedly lost $2.1 million to debit card theft. The anecdotal explanation for the theft is that the attackers conducted the transactions in batches to prevent alerting the relevant authorities (Ndege, 2024).

Fraudulent activities are an everyday menace in the Nigerian banking sector. In Q1 2023 and Q2 2023, the sector recorded a combined 39,035 fraud activities (FITC, 2023). A commercial bank in Nigeria had its fair share of losses because of fraud-related transfers, withdrawals, and unsanctioned reactivation of bank accounts, losing ₦5.46 billion, as the company's June 2023 interim financial statement revealed (ICIR, 2023). Similarly, a Nigerian payment infrastructure company lost ₦30 billion to chargeback fraud in November 2023 (Olowogboyega, 2023). Current and former employees allegedly exploited vulnerabilities in the company's system, causing some merchants to fraudulently file and receive chargebacks (Olowogboyega, 2023).

The banking breach wave reached Lesotho. On December 11, 2023, a bank in Lesotho experienced a “cyber-security incident on its systems” (Greig, 2023). The incident forced it to suspend some of its systems to prevent further infiltration, causing payment delays (Greig, 2023).

On June 13, 2023, a South African finance institution revealed that the Russian ransomware group encrypted its servers, log files, and documents on or about May 21, 2023 (DBSA, 2023). While the ransomware gangs accessed personal information, including contact details, telephone numbers, physical and email addresses, and financial information about stakeholders, the bank said the security incident posed limited consequences (DBSA, 2023).

Attacks on **government-related** institutions were the second-highest targeted category in ACR 2024 (7 out of 31). The data

corroborated Positive Technologies' 2024 report, which revealed that government agencies faced 29% of successful attacks on African organizations between Q1 2023 and Q3 2024 (Bezborodko, 2024). The cyber onslaught on government parastatals is likely tied to the political instability in Africa, where military revolutions have rocked several African countries since 2020 (Statista, 2024). There's a lingering sense that adversaries launched cyberattacks as defense strategies against opposing countries.

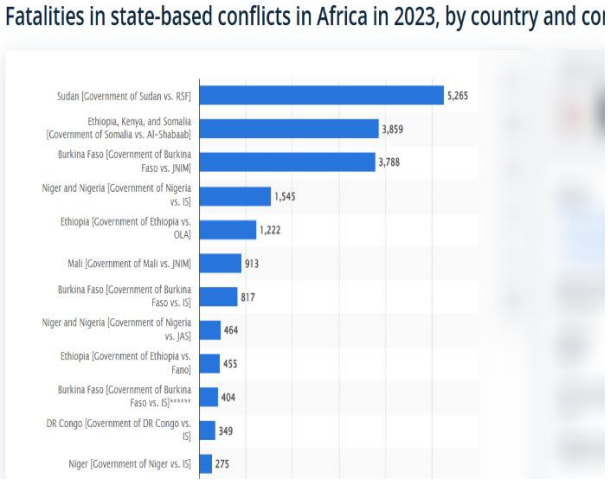


Figure 2.0 The fatalities in Africa countries in African countries in 2023. Source: Statista

In May 2023, a hacker group nicknamed "Mysterious Team" attacked dozens of government websites in Senegal because it wanted to "liberate Senegal from dictatorship" and thwart a potential third-term presidential bid of President Mackey Sall in Senegal (Digwatch, 2023). Self-acclaimed Sudanese cyber-warriors Anonymous Sudan claimed responsibility for the outage on a government portal in Kenya in July 2023. The portal grants access to over 5,000 government services, including media houses and mobile banking services (Mwai & Nkonge, 2023). The group, which allegedly has links with Russia, launched a distributed denial of service (DDoS) attack on Kenya because it has been "attempting to meddle in Sudanese affairs and released statements doubting the sovereignty of our government" (Mwai & Nkonge, 2023).

In March 2023, an Ethiopian data center suffered a cyberattack that compromised technological assets, forcing an emergency shutdown (Endale, 2023). In April 2024, two Egyptian brothers were arrested and subsequently sentenced to two years for hacking the ministry housing consumer database (Jain, 2024). The exploit allowed them to defraud unsuspecting victims, including stealing KD 11, 000 from a Kuwaiti citizen's account through WhatsApp (Jain, 2024).

The Nigerian government also witnessed cyber wrath in 2023 and 2024. On July 12, 2023, a hacker named Alister Crowley under the moniker "Anon Ghost," who also claimed they operated from the Maldives, defaced a government-owned website in Nigeria, calling for "Update your security" in one of the defamatory messages on the website (The Cable, 2023). The phone number of a sitting governor in Nigeria was hacked in February 2024 (Asare, 2024). In March 2024, the identity database in Nigeria was reportedly exposed to the dark web because of the negligence of the managing government agency that gave unverified third parties unfettered access to sensitive information of Nigerians (Abdulganiy, 2024).

In Q3 2024, the **communications** industry suffered the fourth-highest average weekly attacks (2,433), a 57% increase from Q3 2023 (Check Point, 2024). The ACR 2024 spotted a similar trend, as three out of the 31 documented cyberattacks affected media companies, the joint-third most breached sector alongside the Internet Service Providers (ISPs) niche. The three attacks on media outfits further highlighted the increasing growth of nation-state threat actors and DDoS as an attack vector in Africa, especially in 2023.

A Morocco-based media organization attributed "geopolitical tensions" as the culprit for the abnormally massive flow of traffic it received (Hespress, 2023). A media company in Algeria blamed geopolitical issues for the "'severe' cyber attacks" it

faced in February 2023, alleging that it was attacked from Israel, Morocco, and some parts of Europe (The New Arab, 2023). A South African news website faced a distributed denial of attack (DDoS) in August 2023 (The Wire, 2023). The website received malicious traffic that forced it to shut down shortly after publishing a story explaining that Indian Prime Minister Narendra Modi was "unhappy not to be welcomed by his South African counterpart when he landed [in Johannesburg, South Africa]." (The Wire, 2023).

The average weekly attacks on **Internet Service Providers (ISPs)** grew from 648 to 923 between Q1 and Q3 2024, a 42.8% increase. The ACR 2024 recorded three cyberattacks on ISPs in Africa, highlighting the growing ubiquity of cyber threats in the telecommunications industry.

A South Africa-based ISP experienced a ransomware attack in February 2023. A mobile network operator company in Kenya was allegedly interrupted when Anonymous Sudan launched a retaliatory attack on a government-owned portal in Kenya (Mwai & Nkonge, 2023). In August 2024, the NPF arrested two students for allegedly hacking the Application Programming Interface (API) of an ISP provider in Nigeria to steal airtime and data worth ₦1.9 billion (Dania, 2024). In December 2024, the Hunter International ransomware group attacked a state-owned telecom operator in Southern Africa (Rukanga, 2024). The attackers reportedly stole sensitive data, including the personal and financial information of ministries and senior government officials, and customer records. The hackers reportedly leaked the data on social media to mount pressure for ransom payments (Rukanga, 2024)

The **research and education sector** experienced the highest global average weekly attacks between Q3 2023 and Q4 2024, increasing by 119% (Check Point, 2024). The ACR 2024 recorded cyber violations involving two education centers.

The first case involving the education sector happened in Kenya. After taking over the Facebook page of a Kenya-based university and changing the profile picture, the hacker wrote, "Hello everyone here I just want to clarify about this account that was hacked, to be honest, I was just having fun so don't take the posts I publish seriously, once again I'm sorry." The suspected hacker demanded Sh68,000 before returning the account—it was unclear if the university complied with the hacker's request (Shatuma, 2023).

In May 2023, a Nigerian university suffered a similar website hacking fate. The school maintained that unwanted trespassers had access to only "inconsequential records" from the front-end server (Johnson, 2023). The attacks on both universities solidify the recurring theme that educational institutions have a porous internal system.

The impact of generative AI—the advanced computation technique that generates previously unseen content, such as text, images, or audio, from training data—on the automotive industry is a two-edged sword. On one hand, GenAI optimizes research & development (R&D), innovation time and costs, and customer support, leading to faster production times, advanced computerized car features, and personalized car experiences for consumers (Sing, 2023). On the other hand, it integrates multiple digital products that increase the threat and vulnerability landscape, music to the ears of threat actors. For instance, high- and massive-scale incidents in the automotive industry doubled in 2023 compared to 2022, with 95% of cyberattacks executed remotely (Upstream, 2024).

The aviation niche is adding innovative technological tools to improve operational efficiency (Ukwandu et al., 2022). The integration of electronic-enabled aircraft, smart, interconnected airports, and the heap of sensitive data it stores make it a juicy target for nation-state actors, Advanced Persistent Threat (APT) groups, and hacktivists (Ukwandu et al., 2022; Aviation

ISAC, 2024). In 2020, 61% of all identified cyberattacks targeted airlines, as the aviation industry lost around $1 billion yearly to fraudulent websites alone (Eurocontrol, 2021).

The automobile and aviation sectors were represented in ACR 2024. Both industries contributed to a combined three cyberattacks. In February 2023, the South African arm of a German automobile manufacturer suffered a ransomware attack that affected the company's system and backups in Johannesburg (MyBroadband, 2023). South Africa's tech-focused news outlet, MyBroadband, believed a "relatively new ransomware strain called Faust [was used] to encrypt the company's files and lock it out of corporate systems" (MyBroadband, 2023). Faust is a variant of the Phobos ransomware group, which emerged in 2019 (Lin, 2024).

In East Africa, in February 2023, Medusa—a notorious cyber-terrorist group that launched in 2021—illicitly encrypted the files of an airport in Kenya. The attack reportedly "had no 'significant' operational and financial impact," per an official of the airport (Maombo, 2023). The official also said it was unclear if Medusa duplicated stolen files (Maombo, 2023). The attack, however, affected the airport's website for several days before the threat group released 514 GB of stolen data that included procurement plans, site surveys, invoices, receipts, and physical plans. Medusa allegedly gained access to the internal network using the identity card and passport of an internal employee (Maombo, 2023).

The cyberattack on the aviation industry extended to Nigeria. In April 2024, a Nigerian airline released a statement warning intended customers to be vigilant because hackers cloned its website to defraud unsuspecting travel hopefuls (Babalola, 2024).

Globally, the attack on utility organizations grew by 200% in 2023, as attackers targeted critical infrastructure to spread malware (Armis, 2023). Alongside the automobile sector, the utility industry was the least represented sector in the ACR 2024 report.

The only documented attack in the industry in ACR 2024 occurred in March 2023, when an unknown hacker group used a Cobalt Strike tool and DroxiDat—a new variant of the SystemBC payload—to attack a power generator in southern Africa (Baumgartner, 2023). While the attackers profiled systems and established remote connections in the internal environment, they neither delivered ransomware nor malicious software (Baumgartner, 2023).

Recommendations

1. Improve security awareness and culture

African organizations currently have a low-moderate status regarding their security culture because of a lack of an established cybersecurity framework to address emerging threats (Collard et al., 2024). In 2022, almost a third of African organizations surveyed in the Africa Cyber Security Outlook lacked an updated security strategy (KPMG, 2022).

The slow adoption of a national cybersecurity strategy is another blocker negatively affecting threat detection and security awareness. For instance, less than one-third of African countries have a national cybersecurity strategy (Ajijola, A-H., & Allen, N., 2022), suggesting a lack of financial and human investments in digital security (Ajijola, A-H., & Allen, N., 2022).

The trickle effect of negligence is an ignorant populace devoid of security consciousness. For example, over half of the Africans (52%) surveyed in KnowBe4's African Cybersecurity & Awareness Report 2023 revealed that lack of awareness or training was the root cause of their security errors (Collard, 2023). Similarly, 7% of African employees are comfortable sharing personal information, while 4% will share

their data if properly compensated (Collard, 2023).

The ignorance about basic cybersecurity principles and lack of a national cybersecurity strategy partly explain why social engineering was the main cause of breaches amongst African individuals, as shown in Figure 2.0 below, in Q2 2023 (Bezborodko, 2024).

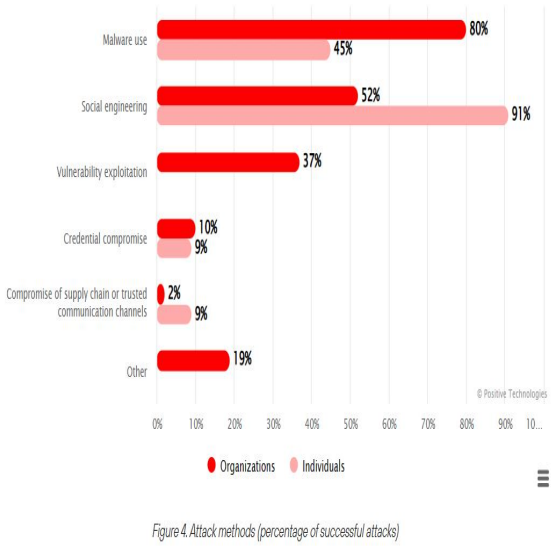


Figure 4. Attack methods (percentage of successful attacks)

Figure 3.0. Social engineering was the second-highest attack method in Q2 2023 in Africa. Source: Positive Technologies

Security training, however, is a proactive measure that addresses the human weaknesses affecting African employees. Effective awareness training campaigns implement a continuous learning model that considers the scope and context of the organization (Bada et al., 2019). Effective security training also reduces the cost of data breaches. For instance, organizations with defined high-level employee training spent $4.15 million on breaches compared to $5.10 million for organizations with low-level employee training (IBM Security, 2024).

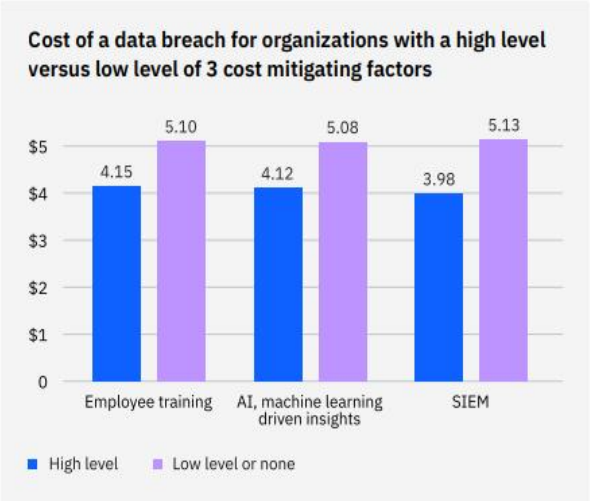


Figure 28. Measured in USD millions

Figure 4.0. High-level employee training saves costs. Source: IBM

While security training is the architecture that helps employees guard against internal and external threats, security culture provides the ideas, policies, standards, and customs that influence cybersecurity in organizations (Thaver, 2022). The culture ensures the dynamic threat landscape doesn't affect the security awareness level of employees. Organizations must make cybersecurity their standard culture and behavior as much as investing in awareness and training sessions to close the knowledge gap prevalent amongst Africans.

2. Invest in AI tools for advanced threat identification

In Q2 2024, Africa faced the highest average number of cyber-attacks per organization weekly, a 37% increase from Q2 2023 (Check Point, 2024). Malware (e.g., ransomware, Remote Access Trojans, loaders, and spyware) and DDoS attacks were the attack vectors threat actors routinely used to attack African organizations (Positive Technologies, 2023).

While investing in a human firewall will proactively shrink the fragilities bad actors can exploit, advanced technological tools can use ML and deep learning capabilities to analyze large datasets and automate threat detection and remediation (Rizvi, 2023). The

2024 Cost of a Data Breach Report highlighted the impact of weaving AI and automation into security. In 2024, companies that invested in AI and ML-driven technical controls spent over 1 million less on data breaches on average (IBM Security, 2024).

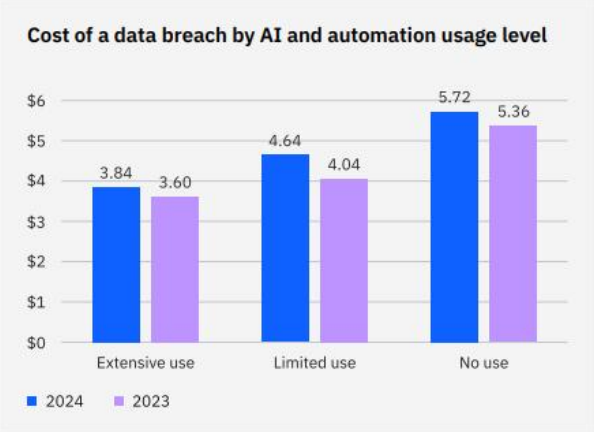


Figure 5.0. How AI helped organizations with data breaches in 2024. Source: IBM

3. Invest in a backup system

Proactive cybersecurity measures are necessary for threat identification. However, breaches are inevitable. This is why organizations must invest in tools and policies, such as a disaster recovery plan (DRP), to minimize the impact of cyberattacks and quicken recovery when breaches inevitably happen.

DRP focuses on restoring technological assets after a breach or disruption (Kesa, 2024). It considers the context of the organization alongside the potential impact and severity of disruptive incidents. Based on the findings, the DRP creates a functional plan to safeguard critical IT assets and data integrity. Similarly, data backup creates multiple copies of data in files for protection against accidental or intentional data loss, system failures, hardware malfunctions, and cyber-attacks (Kesa, 2024).

Conclusion

Africa's growing internet penetration and perceived lack of national security frameworks make it attractive for cyber breaches. This paper examined the extent of security breaches in African organizations in various sectors. While there's no one-size-fits-all approach to prevent breaches, implementing AI technology for threat identification and remediation alongside investment in security awareness and training are proven strategies that will improve the security posture of African organizations.

Limitations of research

A gap identified in this research is the lack of detailed information about the modus operandi of threat actors after breaches. The researchers depended on deductive reasoning and statements from law enforcement agencies to validate the authenticity of attacks. This means that it was difficult to determine the exact technique, tactic, and procedures (TTP) of cyberattacks used for this research paper. Furthermore, the lack of a national breach notification database means it's likely some breaches eluded the researchers during the compilation period.

REFERENCES

- Asare, A. (2024). Scammers hack Cross River gov's phone number, use it to seek assistance. *Daily Post.* Scammers hack Cross River gov's phone number, use it to seek assistance - Daily Post Nigeria
- Abiodun, B. (2023). Hackers steal ₦2.9 billion from Flutterwave accounts, motion granted to freeze accounts connected with stolen funds. *Techpoint Africa.* https://techpoint.africa/2023/03/05/hackers-have-stolen-2-9-billion-from-flutterwave/
- Abiodun, B. (2024). Hack or mismanagement? Inside Patricia's troubling customer fund crisis. *Techpoint Africa.* Hack or mismanagement? Inside Patricia's troubling customer fund crisis (techpoint.africa)
- Abdulganiy, M. (2024, March 19). Revealed: How NIMC exposed probated data of 100m Nigerians to dubious verification agents. *The Cable*. REVEALED: How NIMC exposed private data of 100m Nigerians to dubious verification agents | TheCable
- Ajijola, A-H., & Allen, N. D. F (2022, March 8). African Lessons in Cyber Strategy. African Center for Strategic Studies. African Lessons in Cyber Strategy – Africa Center for Strategic Studies
- Armis (2023). The anatomy of cybersecurity: A dissection of 2023's attack landscape. Armis Blog. Anatomy of Cybersecurity | Armis
- Aviation ISAC (2024). *CISCO survey results.* https://22499298.fs1.hubspotusercontent-na1.net/hubfs/22499298/CISO%20Survey%20Results%20-%202024.pdf
- Babalola, Y. (2024, April). Fraudsters clone Air Peace website, dupe customers. *Leadership News*. Fraudsters Clone Air Peace Website, Dupe Customers
- Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. Apollo - University of Cambridge Repository. Think Mind. https://doi.org/10.17863/CAM.40856
- Baumgartner, K. (2023, August 10). Unknown actor targets power generator with DroxiDat and Cobalt strike. Kaspersky Blog. https://securelist.com/focus-on-droxidat-systembc/110302/
- Bezborodko, A. (2024, November 09). *Cybersecurity threatscape for African countries: Q1 2023–Q3 2024.* Positive Technologies. Cybersecurity threatscape for African countries: Q1 2023–Q3 2024

- Chainalysis (2024, February). *The 2024 Crypto Crime Report*. *[FINAL] The 2024 Crypto Crime Report
- Check Point (2024, October 18). *A closer look at Q3 2024: 75% surge in cyber attacks worldwide*. Check Point Team. A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide - Check Point Blog
- Check Point (2024, July 16). *Check Point research reports highest increase of global cyber attacks seen in last two years—a 30% increase in Q2 2024 global cyber attacks.* Check Point Team. Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks - Check Point Blog
- Collard, A. (2023). *KnowBe4 African Cybersecurity & Awareness Report 2023*. 2023-KnowBe4-African-Cybersecurity-Awareness-Report-Research_EN-GB.pdf
- Collard, A., Colbert, M., Huisman, J., Kraemer, M.J., Kron, E., Malik, J., Schwartz, J., & Tnee, P. (2024). *Phishing by Industry Benchmarking Report*. 2024 Phishing By Industry Benchmarking Report.
- Dania, O. (2024, August 02). [ICYMI] Two students arraigned for hacking MTN computers. Punch Newspaper. Two students arraigned for hacking MTN computers
- DBSA (2023, June 12). Notification of Security Compromise. https://www.dbsa.org/press-releases/notification-security-compromise
- Digwatch (2023, May 23). Senegalese government websites under suffer major cyberattacks. *Digital Watch Observatory.* Senegalese government websites suffer major cyberattacks | Digital Watch Observatory
- Chukwu, N. (2024, May 16). Exclusive: Flutterwave loses ₦1 billion in security breach. *TechCabal.* Exclusive: Flutterwave loses ₦11 billion in security breach
- Endale, A. (2023, March 11). “Massive” cyber attack crashes African Union’s systems. *The Reporter*. "Massive" Cyber Attack Crashes African Union's System (thereporterethiopia.com)
- Ekeh, G. E., Afolabi, Y.I., Uche-Nwachi, E. O., Ekeh, L. K., & Eze-Udu, E. (2022). Awareness of BVN, SIM swap and clone frauds: Methods and Controls. Science World Journal, Vol 17 (No 2) 2022. Awareness of BVN, SIM swap and clone frauds: Methods and controls | Science World Journal (ajol.info)
- Eurocontrol (2021, July 05). Eurocontrol Think Paper ₦12 – Aviation under attack from a wave of cybercrime. Eurocontrol blog.

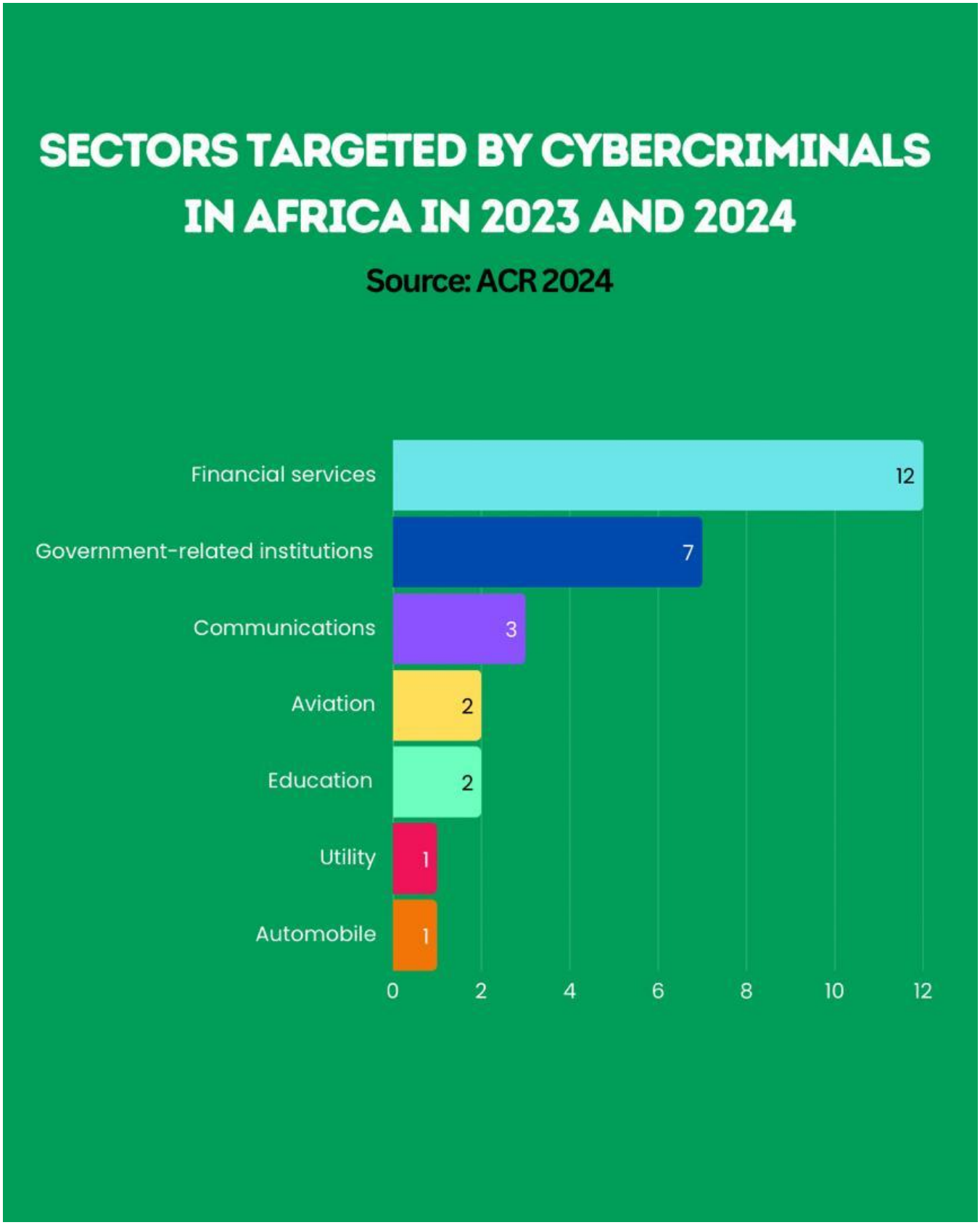
https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime

- FITC (2023). Reports on fraud and forgeries in Nigerian banks. Fraud and Forgery 2023 2nd Quarter.cdr (techpoint.africa)
- FrSebastião, J. (2023. February 18). Banco Sol suffers computer attack. *Menos Fios.* https://www.menosfios.com/en/banco-sol-sofre-ataque-informatico/
- Galal, S. (2024, March 13). Number of internet users in Africa as of January 2024, by country. Statista. Africa number of internet users by country 2024 | Statista
- Greig, J. (2023, December 15). Central Bank of Lesotho facing outages after cyberattack. *The Record.* https://therecord.media/central-bank-lesotho-cyberattack-causes-outages
- Hespress (2023, February 16). MAP websites targeted by a DDOS cyberattack. *Hespress.* MAP websites targeted by a DDOS cyberattack (hespress.com)
- IBM Security (2024, July). *Cost of a data breach report 2024.* *Cost of a Data Breach Report 2024
- ICIR (2024, March 05). EFCC links banks to 70% of financial crimes in Nigeria. EFCC links banks to 70% of financial crimes in Nigeria (icirnigeria.org)
- Jain, S. (2024, April 10). WhatsApp scam exposed: Egyptian brothers imprisoned for hacking consumer database. *The Cyber Express.* WhatsApp Scam Takedown: Egyptian Hackers Imprisoned
- Johnson, H. (2023, May 11). Babcock university confirms hack of school website. *Punch Newspapers.* Babcock university confirms hack of school website (punchng.com)
- Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. World Journal of Advanced Research and Reviews, *18* (03), 970-992. https://doi.org/10.30574/wjarr.2023.18.3.1166
- KPMG (2022, September). *Africa Cyber Security Outlook*. KPMG Africa Cyber Security Outlook 2022
- Lin, C. (2024, January 25). *Another Phobos ransomware variant lunches attack-Faust.* Fortinet Blog. https://www.fortinet.com/blog/threat-research/phobos-ransomware-variant-launches-attack-faust

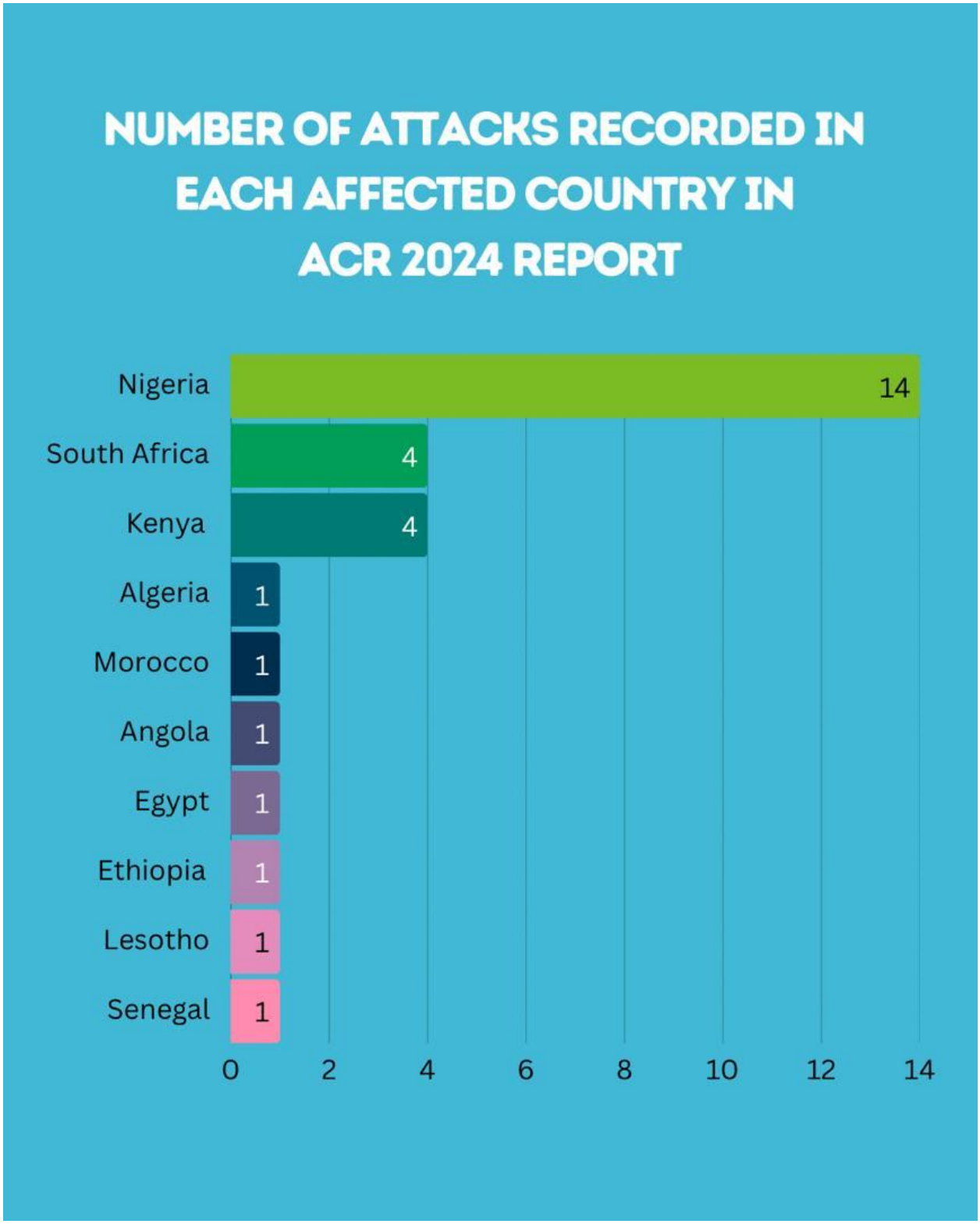
- Maombo, S. (2023, April 12). KAA confirms data breach, says no sensitive data leaked. https://ntvkenya.co.ke/news/kaa-confirms-data-breach-says-no-sensitive-data-leaked/
- MyBroadband (2023, February 21). Porsche South Africa suffers ransomware attack. *MyBroadband* https://mybroadband.co.za/news/security/481087-porsche-south-africa-suffers-ransomware-attack.html
- Mwai, P. & Nkonge, A. (2023, July 23). Kenya Cyber-attack: Why is e-Citizen down? *BBC*.Kenya cyber-attack: Why is eCitizen down? (bbc.com)
- Ndege, A. (2024, April 17). Exclusive: Kenya's Equity Bank hit by $2.1 million debit card fraud, 19 suspects arrested. *TechCabal*. Exclusive: Kenya's Equity Bank hit by $2.1 million debit card fraud
- Olayiwola, B. (2023). Patricia Token White Paper. Patricia.Patricia Token White Paper - Patricia's Journal | Patricia (mypatricia.co)
- Olowogboyega, O. (2023, November 02). Exclusive: Payments giant Interswitch loses ₦30 billion to chargeback fraud, launches recovery response. *TechCabal*. Exclusive: Interswitch loses ₦30 billion to chargeback fraud, begins recovery (techcabal.com)
- Olowogboyega, O. & Oladunmade, M. (2024, May 31). Exclusive: First Bank employee on the run after diverting ₦40 billion; bank begins recovery. *TechCabal*. Exclusive: First Bank employee on the run after diverting ₦40 billion
- Positive Technologies (2023, July 28). *Cybersecurity threatscape of African countries 2022-2023*. Cybersecurity threatscape of African countries 2022–2023 (ptsecurity.com)
- Reddy, P., van Dale, R., Ngambeket, G., & Epstein, G. (2023). *Cybersecurity in Africa—a call to action.* Cybersecurity in Africa—a call to action
- Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and protection. International Journal of Advanced Engineering Research and Science (IJAERS), *10* (5). https://dx.doi.org/10.22161/ijaers.105.8
- Rukanga, B. (2024, December 17). Sensitive data leak after Namibia ransomware attack. *BBC*. Namibia ransomware: Sensitive data leaked after telecoms firm hacked
- Shatuma, L. (2023, May 07). Kabarak University Facebook hacker demands Sh68,000 to return page. *Star.* Kabarak University Facebook hacker demands Sh68,000 to return page (the-star.co.ke)

- Statista (2024, July 04). *Fatalities in state-based conflicts in Africa in 2023, by country and conflict detail.* Statista Research Team. Worst wars in Africa 2023 | Statista
- Thaver, Y. (2022, June). *Impact of Cyberextortion on Africa*. KnowBe4. IDC-Sponsored-Impact-Cyberextortion-Africa-Research_EN-US.pdf (knowbe4.com)
- The Cable (2023, July 12). Ogun government website hacked. *The Cable.* https://www.thecable.ng/just-in-ogun-government-website-hacked/#google_vignette
- The New Arab (2023, February 13). Algeria's official news agency alleges website attacked from Israel, Morocco, parts of Europe. *New Arab.* Algeria news agency says site attacked from Israel, Morocco (newarab.com)
- The Wire (2023, August 24). South African news website says it faced cyber attacks after publishing report on Modi. *The Wire.* https://thewire.in/media/south-african-news-website-says-it-faced-cyber-attack-after-publishing-report-on-modi
- Uba, A. (2023, July 05). Police arrest two for hacking into over 5,000 bank accounts in Lagos. *The Guardian.* Police arrest two for hacking into over 5,000 bank accounts in Lagos | The Guardian Nigeria News - Nigeria and World News — News — The Guardian Nigeria News – Nigeria and World News
- Upstream (2024). *Global automotive cybersecurity* report. https://info.upstream.auto/hubfs/Security_Report/Security_Report_2024/Upstream_2024_Global_Automotive_Cybersecurity_Report.pdf?
- Ukwandu, E., Ben-Farah, M., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-security Challenges in Aviation Industry: A review of Current and Future Trends. Information, *13*(3), 146. https://doi.org/10.3390/info13030146.

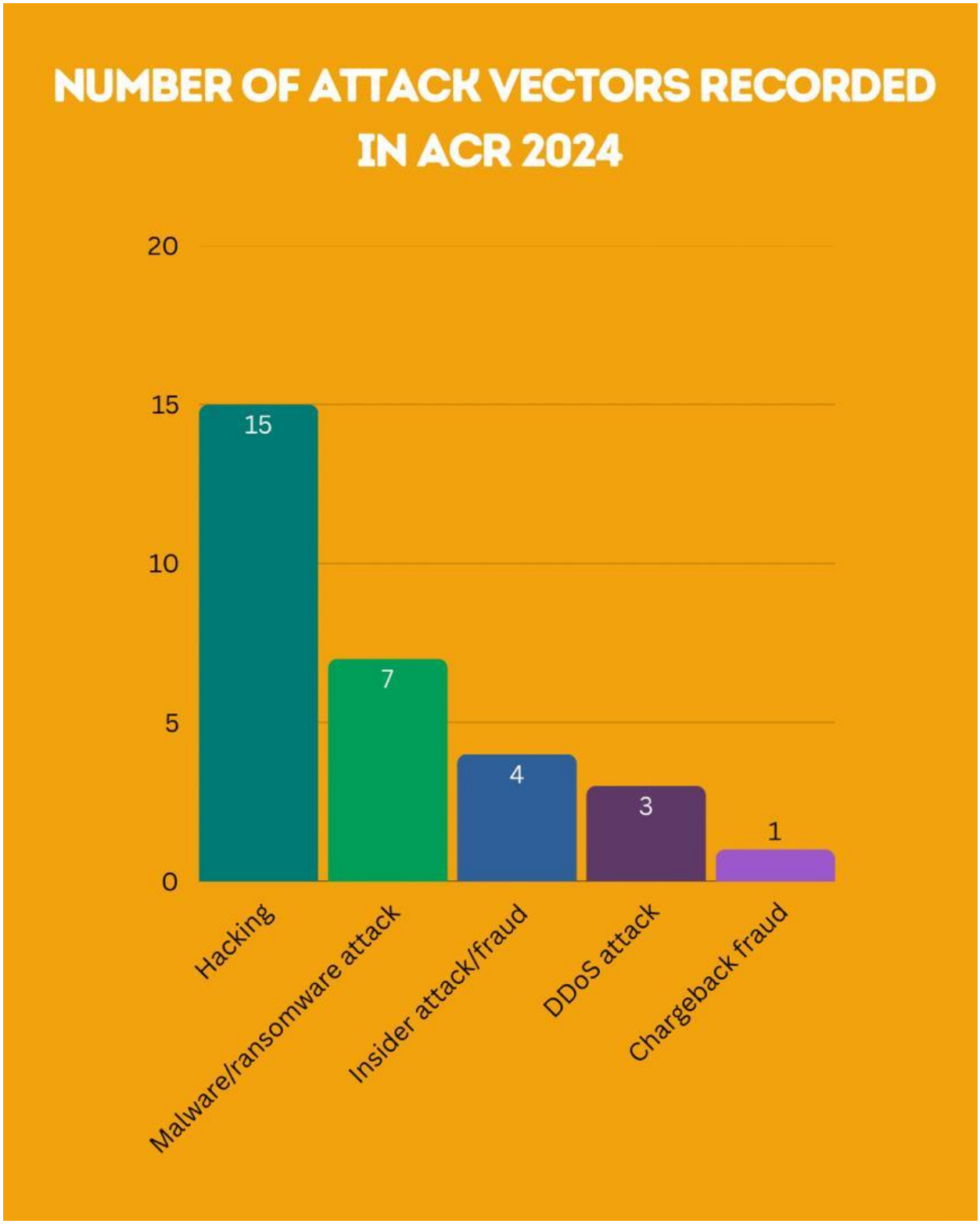
Appendix



Appendix a: The sectors targeted during in 2023 and 2024 in ACR 2024 report



Appendix b: The number of attacks per country



Appendix c: The attack vectors/vulnerabilities exploited in ACR 2024