



AFRICA CYBERSECURITY REPORT – KENYA 2024/2025

From Risk to Resilience:
AI and the Future of Cyber Risk Management





Africa Cybersecurity Report

Kenya, 2024/2025

From Risk to Resilience:

AI and the Future of Cyber Risk Management



About the Africa Cybersecurity Report

Africa cybersecurity report is a crown jewel of African based intelligence that is released annually by Africa Cyber Immersion Centre (ACIC) in collaboration with its partners. ACIC is Serianu's Research and Development Arm founded in 2017. The report provides an in-depth analysis of unique local trends, threats and attacks. Analysis is drilled down to provide you with industry analysis and priority focus areas for 2026. This report pulls together intelligence from numerous threat sensors, industry experts, regulators and professional associations.



Table of Contents

Abbreviations	4
Editor's Note	5
Acknowledgements	7
Disclaimer	10
Foreword	11
Section 1: Emerging Trends & Priorities for Cyber Resilience - Africa.....	18
Section 2: The Economics of Cyber Resilience - Africa.....	25
Section 3: Cyber Intelligence - Kenya.....	44
Section 4: Survey Analysis - Kenya	54
Section 5: Artificial Intelligence Landscape in Kenya.....	66
Section 6: Decision Assurance - AI for Business Leaders.....	78
Section 7: The Boardroom Cyber Risk Language Divide	82
Section 8: Anatomy of an AI-Powered Cyber Attack	92
Section 9: 2026 Priority and Focus Areas	101
Section 10: Cyber Shujaa Program	117
Appendix.....	119



2026 SPONSORSHIP INVITATION

*Empowering Kenya's Youth. Strengthening Businesses.
Securing the Digital Future.*

Kenya's digital economy is growing faster than its workforce.

As AI, cloud, fintech, and automation reshape industries, organisations face a widening gap in cybersecurity, data protection, and digital skills. At the same time, thousands of talented young Kenyans remain unemployed simply because they lack industry-aligned training.

Cyber Shujaa is closing this gap



Since May 2022
trained over 3358+

Total Placed 2330
in banks, telcos, fintechs & regulators



40+
startups launched by alumni



36%
women participation



National recognition across government and industry



Why Your Organisation Should Partner With Us

1. Access Certified, Job-Ready Talent
2. Strengthen Your Ecosystem
3. Demonstrate ESG & CSR Leadership
4. Build Board & Executive Digital Oversight
5. National Visibility & Brand Leadership



**Empower Youth. Strengthen Businesses.
Build National Resilience.**

We are now scaling to reach

50,000+
youth, women, SMEs & leaders by 2030.



To Partner With Us, Contact:
Nabihah Rishad

nabihah.rishad@serianu.com
nabihah.rishad@cybershujaa.co.ke
+254 725 790 905



cybershujaa.co.ke



**Scan me
for more
information**

A National Digital Workforce Transformation Program by

CHALLENGE
FUND
FOR
YOUTH
EMPLOYMENT



Abbreviations

ACIC	Africa Cyber Immersion Centre
AI	Artificial Intelligence
API	Application Programming Interface
BEC	Business Email Compromise
CISO	Chief Information Security Officer
CVEQ	Cyber Visibility and Exposure Quantification
DDoS	Distributed Denial of Service
DNS	Domain Name System
DPO	Data Protection Officer
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GDP	Gross Domestic Product
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
IMF	International Monetary Fund
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
KPI	Key Performance Indicator
KYC	Know Your Customer
LLMs	Large Language Models
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
OT	Operational Technology
PII	Personally Identifiable Information
SLA	Service Level Agreement
SOC	Security Operations Center
SQL	Structured Query Language
USD	United States Dollar



Editor's Note



“Cyber resilience is built not in isolation, but through collaboration, trust, and shared effort.”

Each year, producing the Kenya Cybersecurity Report is both a technical and human journey. Behind every statistic in these pages are people, researchers, analysts, data partners, and contributors all working tirelessly to understand and explain the evolving digital landscape that shapes our lives and our economy.

This year's report reflects months of collaboration, debate and validation from countless late nights to spirited discussions about what the data really means for Kenya's cybersecurity maturity. The process reinforced a truth that has guided this series since 2012: resilience is not a one-time achievement; it is a continuous commitment.



The 2024/2025 edition tells a story of progress. Kenyan organizations are becoming more aware, more proactive, and more strategic. They are no longer only asking how to stop an attack but how to recover, learn, and strengthen after one. That shift in mindset from fear to preparedness marks real maturity.

The data shows improvement across sectors.

Businesses are investing more in training, building stronger governance structures and embracing frameworks that link cybersecurity to performance.

While threats are growing more sophisticated, Kenya's collective response is growing stronger and more coordinated.

Resilience begins where awareness becomes action. Artificial Intelligence is the defining factor of this new era, both a powerful ally and a potential adversary.



It enables faster detection, smarter prediction, and better automation but it also challenges us to ensure transparency, accountability and human oversight remain at the core of our systems.

This report could not have been possible without the extraordinary effort and generosity of our contributors, industry experts, policymakers, researchers, and institutions that shared their data and insights. Their openness continues to make this report one of Africa's most respected cybersecurity references.

To everyone who participated, thank you. To our readers, may this report inform, inspire and remind us all that resilience is not a destination; it is a shared journey.

Nabihah Rishad

Nabihah Rishad,
Editor-in-Chief,
Africa Cybersecurity Report Series
Product and Research Lead,
Serianu Limited



Acknowledgements

In developing the Africa Cybersecurity Report – Kenya 2024/2025, the Serianu Cyber Threat Intelligence Team received invaluable collaboration and key inputs from key partners as listed below.



Design, Layout and Production: Tonn Kriation

The Serianu Cyber Threat Intelligence Team

Co – Authors



Carol Muchai
Researcher



Riara Wanjiru
Researcher, Top Trends





Barbara Munyendo
Researcher, Cyber
Intelligence



Jackie Madowo
Researcher



Andrew Wambugu
Researcher, Top Technology
Priorities



George Kiio
Researcher, Cyber
Intelligence



Anne Gikaara
Researcher



Daniel Ndegwa
Researcher



Contributors

David Mugonyi, EBS	Director General, Communications Authority of Kenya
Dr. Magdalyne Kamande	Director ICT & Transformation Services, The Nairobi Hospital, and a thought leader in the ICT industry
Audrey Kemuma	Risk Management Thought Leader currently serving as a Corporate Risk Management Advisor for FedEx Corporation - USA
Fidelis Muia	Director, Technical Services, Kenya Bankers Association
Eston Kairu	General Manager - Information Security Governance & Technical Assurance - Equity Group, Chairman - IT Systems, Risk and Security Sub-Committee - Kenya Banker's Association
Mugambi Laibuta, PhD, CIPM	Chairperson, Data Privacy and Governance Society of Kenya (DPGSK)
Dr. Paula Musuva	Assistant Professor, School of Science and Technology United States International University - Africa (USIU-Africa)
Shikoli Makatiani	Director & Board Member, Serianu Ltd
Joseph Mathenge	Chief Operations Officer, Serianu Ltd
John Kuria	Cyber Threat Management Analyst Deloitte, Kenya
Bernard Dulo	Assistant General Manager - Liability and Specialty Lines, GA Insurance
Joan G. Mburu	Chief Information Security Officer, Airtel Kenya
Dennis Musyoka Katusya	Manager - Technology Service Delivery, Mitchell Cotts Group
Deborah Mutungi	Group IT Manager, Sarova Hotels and Resorts
Mercy Kimani	Head of IT, Nation Media Group
Catherine Nyaga-Mbithi	Co-Chair, Institute of Risk Management, East Africa Group and Internal Audit Manager, ABSA Life Assurance, Kenya
Robert Kariuki Mogoi	Chairman, Sacco IT Professionals Association (SITPA)
Amrit Singh Labharam	Kenyan-German Digital Dialogue Advisor at the GIZ Digital Transformation Centre, Kenya
George Kisaka	CEO & Co-Founder, hlola.io
Brian Nyali	Global Security Investigator, Ericsson
Omari Payne	Principal Cyber Security Auditor, Airtel Africa



Disclaimer

The views and opinions expressed in this report are those of the authors and do not necessarily reflect the official position of any specific organisation or government.

As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers should therefore also rely on their own experience and knowledge in evaluating and using any information described herein.

For more information contact:

Serianu Limited

info@serianu.com | www.serianu.com

© Serianu Limited, 2025

All rights reserved



Foreword



“Cyber resilience is not about avoiding disruption, it’s about ensuring we can rise stronger after every challenge.”

When we first published the Africa Cybersecurity Report in 2012, our goal was simple, to help organizations and nations see what was once invisible. At that time, cybersecurity was often viewed as a purely technical concern. Today, it has become a pillar of business continuity, investor confidence and economic stability.

Over the past twelve years, these series have chronicled Africa’s digital transformation, from the early days of mobile innovation and online banking to the era of artificial intelligence and digital regulation. Each edition has reflected the continent’s progress, its vulnerabilities and its growing determination to protect what matters most: trust.



The 2024/2025 Kenya Cybersecurity Report, themed “From Risk to Resilience: AI and the Future of Cyber Risk Management,” marks another milestone in this journey. It shows that Kenya is no longer reacting to cyber incidents; it is learning to predict them, limit their impact and recover faster. In simple terms, the country is saving far more than it loses not just in money but in confidence and capability.

That shift signals a deeper change. Cybersecurity is no longer a cost of doing business; it is becoming an investment in business strength. Organizations are starting to measure their success not by how few attacks they experience but by how effectively they can adapt and keep operating when those attacks occur.

Artificial Intelligence sits at the heart of this transformation powering both

new opportunities and new risks. It is reshaping how we detect and respond to threats but it also reminds us of the need for human judgment, ethical leadership and accountability in every digital decision we make.

As publishers, we are proud of what this report represents, a collective effort of researchers, analysts, and industry experts across Kenya and beyond. It reflects not only data but dedication. Not only findings, but foresight.

The real measure of progress is not how many attacks we prevent, but how quickly we recover and improve after each one.

Resilience is, and will remain, a leadership choice. Kenya’s progress demonstrates that with the right coordination, collaboration and vision, a safer digital Africa is within reach.

William Makatiani

William Makatiani,
Publisher,
Africa Cybersecurity Report Series,
CEO, Serianu Limited



Industry Regulator's Perspective

Communications Authority

By David Mugonyi, EBS,
Director General, Communications Authority of Kenya



I. Cybersecurity Mandate

The Communications Authority of Kenya (CA) continues to strengthen national digital security under its 5th Strategic Plan (2023–2027). Guided by the Kenya Information and Communications Act (KICA) of 1998, the CA is mandated to develop frameworks that support the investigation and prosecution of cybercrime.

To advance this mandate, the government established the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) in 2014 as a multi-agency structure coordinating national cybersecurity response in partnership with law enforcement and international actors.

The Computer Misuse and Cybercrimes Act (CMCA) of 2018 further enhanced this ecosystem through the formation of the National Computer and Cybercrimes Coordination Committee (NC4). The 2024 CMCA regulations expanded the CA's responsibilities to include establishing and operating the Cyber Security Operations Centre (CSOC) for the ICT and telecommunications sector.

II. Global Cyber Threat Landscape Overview

i. Ransomware

Ransomware groups intensified attacks on Critical Information Infrastructure (CII) and public services using Ransomware-as-a-Service (RaaS) models, AI-supported extortion tactics, and blended Distributed Denial-of-Service (DDoS) campaigns. National KE-CIRT/CC advisories urged organizations to maintain offline backups, apply zero-trust segmentation, and update threat intelligence.

ii. Distributed Denial-of-Service (DDoS) Attacks

Threat actors launched large, multi-vector DDoS attacks using Internet of Things (IoT) botnets and amplification techniques exploiting Network Time Protocol (NTP) and Domain Name System (DNS) weaknesses. KE-CIRT/CC recommended cloud-based scrubbing services and AI-supported anomaly detection to manage high-volume attacks.



iii. **Social Engineering and Phishing**

Social engineering threats grew more targeted, including AI-generated voice deepfakes and Business Email Compromise (BEC) campaigns across email, SMS, and voice channels. KE-CIRT/CC advised organizations to adopt phishing-resistant authentication, enforce Multi-Factor Authentication (MFA), and expand user training.

iv. **System Misconfiguration Exploits**

Misconfigured cloud services, weak Application Programming Interface (API) settings, and default credentials remained common causes of breaches. KE-CIRT/CC emphasised secure-by-default configurations, least-privilege access, frequent audits, and Infrastructure-as-Code (IaC) scanning.

v. **Emerging Threats**

Advanced Persistent Threat (APT) groups continued targeting critical infrastructure through spear-phishing, zero-day exploitation and supply-chain compromise. KE-CIRT/CC encouraged segmentation, timely updates, behavioural monitoring, and wider threat intelligence sharing. Capacity-building for constituents also continued.

vi. **Alignment With Global Trends**

Global and national threat patterns remained closely aligned, with similar tactics, techniques and procedures (TTPs) observed across regions.

III. **National Cyber Threat Landscape Overview**

i. **Total Cyber Threats Detected**

Between July and September 2025, the National KE-CIRT/CC detected 842 million cyber threat events an 81.64% decrease from April–June 2025.

Key drivers included inadequate patching, limited awareness of phishing and social engineering, and increased use of AI-enabled attacks.

ii. **Total Cyber Threat Advisories Issued**

During the same period, 19,951,546 advisories were issued a 15.53% increase from the previous quarter.

Advisories focused on patching, MFA, strong password policies, and well-configured firewalls and antivirus tools.

IV. **Administration of the .KE Country Code Top-Level Domain (.KE ccTLD)**

The CA oversees the .KE ccTLD to ensure compliance with national requirements and global best practices informed by the Internet Corporation for Assigned Names and Numbers (ICANN) and its Governmental Advisory Committee (GAC).

Following GAC engagements and national experience, CA issued directives requiring:

1. Monthly publication of reports on phishing, malware, botnets, pharming and spam incidents, including resolution status.
2. Sinkholing mechanisms to block malicious domain names and support threat analysis.
3. Improved WHOIS data accuracy to strengthen cybercrime response.

V. Capacity Development & Partnerships

The CA continues to collaborate with telecommunications operators, regulators, academia and ICT consumers to strengthen national cyber capacity.

Key initiatives include:

- Quarterly National KE-CIRT/CC Cybersecurity Committee (NKCC) sessions
- The Annual Cyber Security Conference
- The National Public Key Infrastructure (NPKI) Forum
- Cybersecurity bootcamps and hackathons
- The Annual Youth Cybersecurity Forum
- Youth mentorship and study tours

These programmes help build a skilled and informed cybersecurity community across Kenya.





01

SECTION 1

EMERGING TRENDS & PRIORITIES FOR CYBER RESILIENCE - AFRICA





Section 1: Emerging Trends & Priorities for Cyber Resilience - Africa

Introduction

Africa's rapid digital growth powered by AI, cloud, APIs, and fintech ecosystems has outpaced existing security safeguards creating faster and more interconnected cyber risks. In 2026, resilience will depend on how well organizations govern AI, secure identities, modernize detection, automate controls, strengthen third-party ecosystems, and elevate board-level oversight. The trends below capture the most critical shifts shaping Africa's cyber resilience agenda.

Top Ten Emerging Trends & Priorities for 2026

1. AI Governance Becomes a Core Risk Discipline

AI misuse, shadow AI experimentation and unreviewed AI-generated decisions are emerging as major sources of risk. Organizations must implement clear oversight, safe-use policies and governance controls to manage AI responsibly.

2. Identity & Access Becomes the Primary Battleground

Most breaches still begin with compromised credentials. Strengthening MFA, privileged access controls, and continuous identity monitoring become essential as digital services scale.



3. Cloud, API & Application Misconfigurations Surpass Traditional Network Risks

With widespread cloud adoption and API-driven integrations, misconfigurations and weak interfaces are now leading causes of data exposure. Cloud governance and API security become mandatory.

4. Automation in Patch & Vulnerability Management Becomes Non-Negotiable

Manual patching can no longer keep pace with attackers exploiting known vulnerabilities. Automated, risk-based vulnerability management becomes the new enterprise baseline.



5. Third-Party & Ecosystem Failures Emerge as the Fastest-Growing Threat Vector

Fintech systems, telco APIs, SaaS tools, and cloud vendors now represent the most fragile points in the value chain. Organizations must strengthen vendor assurance, visibility and integration security.

6. SOC Modernization Accelerates to Counter Machine-Speed Attacks

Traditional SOC's are overwhelmed by noise and fragmented visibility. Behavioral analytics, AI-assisted triage and consolidated monitoring define the modern SOC model for 2026.

7. Shadow AI & Shadow IT Become the New Insider Threats

Unapproved AI tools, rogue SaaS platforms and unmanaged applications create silent exposure points. Monitoring, governance, and controlled alternatives become essential.

8. Boards Shift from Cybersecurity Oversight to Cyber Resilience Oversight

Cyber resilience is now a business and continuity imperative. Boards must demand strategies, evidence-based reporting, crisis readiness, and measurable resilience outcomes.

9. Recovery & Continuity Validation Becomes Mandatory

Ransomware and outages have exposed weaknesses in backup reliability. Routine recovery testing, immutable backups, and evidence-based continuity assurance become central resilience measures.

10. Integration Security Becomes as Critical as Perimeter Security

APIs, vendor connections, and platform integrations now represent the weakest attack surfaces. Strengthening integration security through governance, monitoring, and contractual controls becomes a top regional priority.



Industry Player Perspective

Healthcare

By Dr. Magdalyne Kamande,
Director, ICT & Transformation Services,
The Nairobi Hospital, and a thought leader in the ICT
industry



From Patient to Protocol: Building Cyber-Resilience in Kenya's Digital Health Ecosystem

The theme "From Risk to Resilience" is timely for Kenya. As the country strengthens its place as a digital leader in East Africa, cyber risk management must move from basic defense towards a more adaptive and proactive approach. This shift is especially urgent in healthcare, where digital initiatives such as UHC, KHIS and tools like the Chango app are expanding access to care while introducing new weaknesses.

A patient record is far more than a document. It contains personal identifiers, financial information and sensitive health details that can sell for more than ten times the value of credit card records on illicit markets. Recent analyses indicate an increase in cyberattacks across East Africa, with healthcare becoming a frequent target. Security reports show a rise in ransomware incidents affecting critical infrastructure, including hospitals in Kenya where breaches have exposed thousands of records and disrupted patient registration systems.

The Patient Trust Mandate

At the center of healthcare is patient safety and trust. These values are protected by the Kenya Data Protection Act of 2019 under the Office of the Data Protection Commissioner. The law requires lawful processing, explicit consent and strong protections for sensitive health data. A cyberattack is therefore more than an information technology failure; it violates both legal obligations and the ethical duty to protect patients. The consequences can be severe, for example:

- A ransomware attack that encrypts critical patient records at a national hospital, forcing surgeons to delay essential procedures.
- A refined phishing campaign that compromises a healthcare worker's credentials, leading to the mass theft of sensitive HIV statuses or mental health information, or the alteration of drug dosage records in a national system.
- A connected infusion pump or pacemaker that is altered through an intrusion, turning a life supporting device into a possible threat.



AI as the Catalyst for Building Resilience

To protect the digital evolution of healthcare, Kenya must strengthen resilience. This means the ability to anticipate, withstand, recover and improve. AI plays an important part in this shift.

1. **Proactive Defense:** AI systems can study large healthcare environments in real time and identify unusual activity such as bulk downloads or suspicious device activity before damage occurs.
2. **Smarter Vulnerability Management:** With modern systems and older platforms existing together, AI can locate weaknesses and highlight the flaws that pose the greatest threat to patient safety. Zero Trust controls support this by verifying every access request.
3. **Faster Response and Recovery:** AI enabled automation tools can isolate affected systems within seconds, reducing downtime and allowing analysts to restore services that support patient care.

The Path Forward for Kenya

Strengthening resilience in digital health requires coordinated action:

- Policymakers should reinforce the Data Protection Act by offering clear guidance for sensitive health data and supporting the adoption of AI enabled controls in public health facilities.
- Healthcare administrators should apply security minded planning to all digital health projects and protect high value data such as pediatric records and genomic information.
- Cybersecurity practitioners should develop AI solutions that are practical, understandable and suitable for the ethical demands of healthcare. They should also promote a culture of accountability from frontline staff to research institutions.

A Continuous Commitment

Moving from risk to resilience is not a one-time accomplishment. It requires steady improvement. By applying AI responsibly and placing the protection of human life at the center, Kenya can safeguard its digital health systems and maintain public trust. The goal is a healthcare sector that is technologically strong, safe for patients and dependable at every level.

Industry Player Perspective

Healthcare

By Audrey Kemuma,

Risk Management Thought Leader currently serving as a Corporate Risk Management Advisor for FedEx Corporation - USA



Cybersecurity in Healthcare in an era of Sustainability and AI

In healthcare, cybersecurity is not only a technical responsibility. It is a direct protector of patient safety. A single cyber incident, whether it involves espionage, a denial of service attack on surgical equipment, or interference with remote monitoring tools, can interrupt treatment and endanger lives. Despite this reality, awareness remains limited, especially as healthcare now depends on complex concepts such as Data Governance, Data Security, Data Privacy and Artificial Intelligence. These concepts are often treated as identical, yet each has a distinct role.

Data Governance focuses on managing the availability, accuracy and proper use of information within hospital systems. Data Security protects information from unauthorized access or corruption, while cybersecurity protects the digital systems, networks and devices that process that information. Data Privacy concerns the lawful handling of personal information and ensures that individual rights are respected.

These areas connect but are not the same. A hospital can secure its data from unauthorized access yet still violate privacy rules through incorrect handling of sensitive information. At the same time, a cyber incident can instantly result in a privacy violation. Applying Privacy by Design helps address these challenges by placing protective measures at every stage of system development and information handling.

In healthcare, strong data protection is directly linked to institutional stability. Poor security can lead to information loss, litigation, financial damage and a decline in patient trust. Digital systems, including electronic health records and AI supported diagnostic tools, increase the complexity and must receive equal attention.

Kenya's planned Integrated Healthcare Information Technology System, developed by the Ministry of Health with Safaricom, aims to connect patient records across facilities through a national health cloud supported by AI tools.



This level of integration requires strong protective measures because any breach could affect sensitive information across the entire country.

AI brings both opportunity and risk. It improves diagnosis, treatment planning and predictive care, but it can also be used to execute advanced attacks. This creates the need for responsible governance and clear ethical rules for AI use within hospitals.

The Joint Commission International standard highlights the importance of securing information. It requires hospitals to safeguard confidentiality, security, integrity and privacy of information and to protect systems from theft, damage, ransomware and other threats. The standard also calls for staff training on phishing, password practices, ransomware, device protection and

reporting unusual activity. Hospitals must conduct yearly information security assessments, create response procedures, test systems for weaknesses and evaluate third party vendors to ensure they meet required expectations.

Meeting these responsibilities requires cooperation across clinical teams, leadership, information technology departments, regulators and even patients who depend on the confidentiality of their records.

In conclusion, modern healthcare relies heavily on technology, including AI. As hospitals manage growing volumes of sensitive information, strengthening security is essential. Protecting information protects patients, and sustained trust is critical for every healthcare institution's long-term success.



02

SECTION 2

THE ECONOMICS OF CYBER RESILIENCE - AFRICA





Section 2: The Economics of Cyber Resilience - Africa

Introduction

This section examines the economics of cyber resilience, with the objective of quantifying how different cyber events translate into financial losses, operational disruption, and sector-wide risk concentration across Africa. It provides a data-driven analysis of the most prevalent threat scenario events and loss scenario events, highlighting the sectors most affected and the attack types that generate the highest economic impact. The section demonstrates that while identity compromise, vulnerability exploitation and fraud-related incidents dominate in frequency, ransomware and supply-chain breaches remain the most costly per event.

By presenting incident proportions, loss magnitudes and sector exposure trends, the section emphasizes a central insight: investing in resilience through stronger identity governance, visibility, and recovery capability reduces both the likelihood and severity of cyber losses, making it a strategic economic priority for organizations and national ecosystems.

Summary and 2026 Outlook

Africa's cyber-resilience profile in 2025 reflects both **progress** and **persistence** of exposure.



Across the continent, total cybersecurity expenditure reached **USD 15.3 billion** (0.55 % of GDP) while cybercrime losses totalled **USD 5 billion** (0.18 % of GDP).

This establishes a **3:1 spend-to-loss ratio**, Africa's benchmark for resilience efficiency.

Most Targeted Industries



Financial services



Government



Telecommunications

Leading in Total Impact



Ransomware



Fraud



Third-Party Outages

Despite higher incident volumes, regulatory action, improved SOC coverage, and maturing governance frameworks show measurable progress in resilience capability.

Africa Cybersecurity & Digital Economy Snapshot







Overview

Africa's accelerating digitalization continues to transform economies expanding access, services and productivity while simultaneously intensifying exposure to cyber threats. In 2024/25, the continent's digital economy surpassed USD 2.8 trillion in nominal GDP, with more than 570 million internet users and 855 million mobile-data subscriptions.

Cybersecurity expenditure rose sharply as nations invested in protection, detection, and recovery capacity.

The following table presents the latest cross-country comparison of macro-digital and cyber-resilience indicators across the five in-scope economies, supported by global and regional sources.

Key Indicators by Country

Region / Country	Population (2025 est.)	Nominal GDP (USD)	Internet Users (2025)	Aggregate Cybersecurity Expenditure (USD est.)	Estimated Crime Losses (⅓ of Spend)	Qualified Cyber Professionals (2025 est.)	Mobile Data Subscriptions (2025)
 Africa (Total)	1.55 B	\$ 2.8 T	570 M	\$ 15.3 B (0.55% GDP)	\$ 5.0 B	400 000 (120 000 cert)	855 M
 Nigeria	237.5 M	\$ 285.93 B	109 M	\$ 1.43 B	\$ 0.48 B	75 000 (28 000 cert)	150 M
 Kenya	57.5 M	\$ 136.0 B	29 M	\$ 0.68 B	\$ 0.23 B	27 000 (9 000 cert)	68.8 M
 Uganda	51.4 M	\$ 64.99 B	14 M	\$ 0.33 B	\$ 0.11 B	11 000 (3 500 cert)	38.6 M
 Botswana	2.56 M	\$ 19.19 B	2.1 M	\$ 0.096 B	\$ 0.032 B	3 500 (900 cert)	4.21 M
 Lesotho	2.36 M	\$ 2.09 B	1.1 M	\$ 0.010 B	\$ 0.003 B	900 (180 cert)	2.07 M

Notes

- Qualified professionals include individuals with globally recognized certifications such as CISA, CISM, GIAC, SANS, CISSP, CEH, ISO 27001, and PCI DSS QA, as well as those who have completed accredited bootcamps or structured training programs in cybersecurity, data privacy, or related fields.
- The term "Qualified Cybersecurity Professionals" also encompasses experienced non-certified practitioners with demonstrated expertise in cybersecurity operations, data protection, or information-governance disciplines.



Disclaimer

All figures presented in the table on the previous page are internal estimates developed by Serianu Limited as of October 2025. They are intended for strategic and informational purposes only and may be revised as new or more accurate data becomes available.

Key Findings and Interpretation

- Cybersecurity expenditure reached approximately USD 15.3 billion (0.55 % of Africa's GDP).
- Estimated cybercrime losses stand at USD 5 billion (0.18 % of GDP), maintaining the 3:1 spend-to-loss benchmark.
- Nigeria and Kenya together account for nearly 14% of continental security spend, reflecting advanced fintech and mobile-money ecosystems.
- Skill shortages persist: fewer than one in three cyber professionals hold formal certification.
- Internet penetration growth outpaces defensive investment, leaving a maturity gap across public and private sectors.





Most Affected Industries – Africa











Overview

Across Africa in 2024/25, cyber incidents concentrated within a small number of high-digitization sectors.

Financial services, government, and telecommunications together represented the majority of both incidents and financial losses, while healthcare, manufacturing, and energy showed accelerating exposure as digital transformation deepened.

Percentages represent modeled distributions of incident frequency and relative magnitude of loss across the five in-scope economies.

Industry Distribution of Cyber Incidents and Losses - Africa

Industry / Sector	Number of Incidents (%)	Magnitude of Loss (%)	Summary Observation
 Financial Services (Banking, Insurance, SACCOs/Credit Unions)	22	25	Payment-fraud, credential compromise, and insider threats dominate; heavy regulatory oversight sustains investment.
 Government & Public Sector	16	14	Ransomware, data exposure, and service-availability disruptions frequent; national SOC initiatives expanding.
 Fintech & Digital Payments	12	13	API abuse and mobile-money fraud increasing; rapid growth outpacing control maturity.
 Telecommunications & ISPs	10	11	DDoS, SIM-swap, and signalling-system exploitation common; redundancy programs strengthening.
 Healthcare & Life Sciences	8	9	Ransomware and PII-breach costs rising; legacy-system patching remains inconsistent.
 Cloud & ICT Service Providers	7	7	Misconfigurations and shared-platform risks; multi-tenant controls improving.
 Retail & E-Commerce	7	6	Card-not-present fraud and fake-merchant scams prevalent; payment-gateway monitoring improving.
 Education & Research Institutions	6	4	Phishing, credential theft, and web defacement frequent but lower-impact.
 Manufacturing & Industrial Operations	6	7	OT and supply-chain breaches drive downtime; recovery expenses significant.
 Energy & Utilities	6	4	SCADA and grid-control targeting increasing; regulators mandating resilience testing.

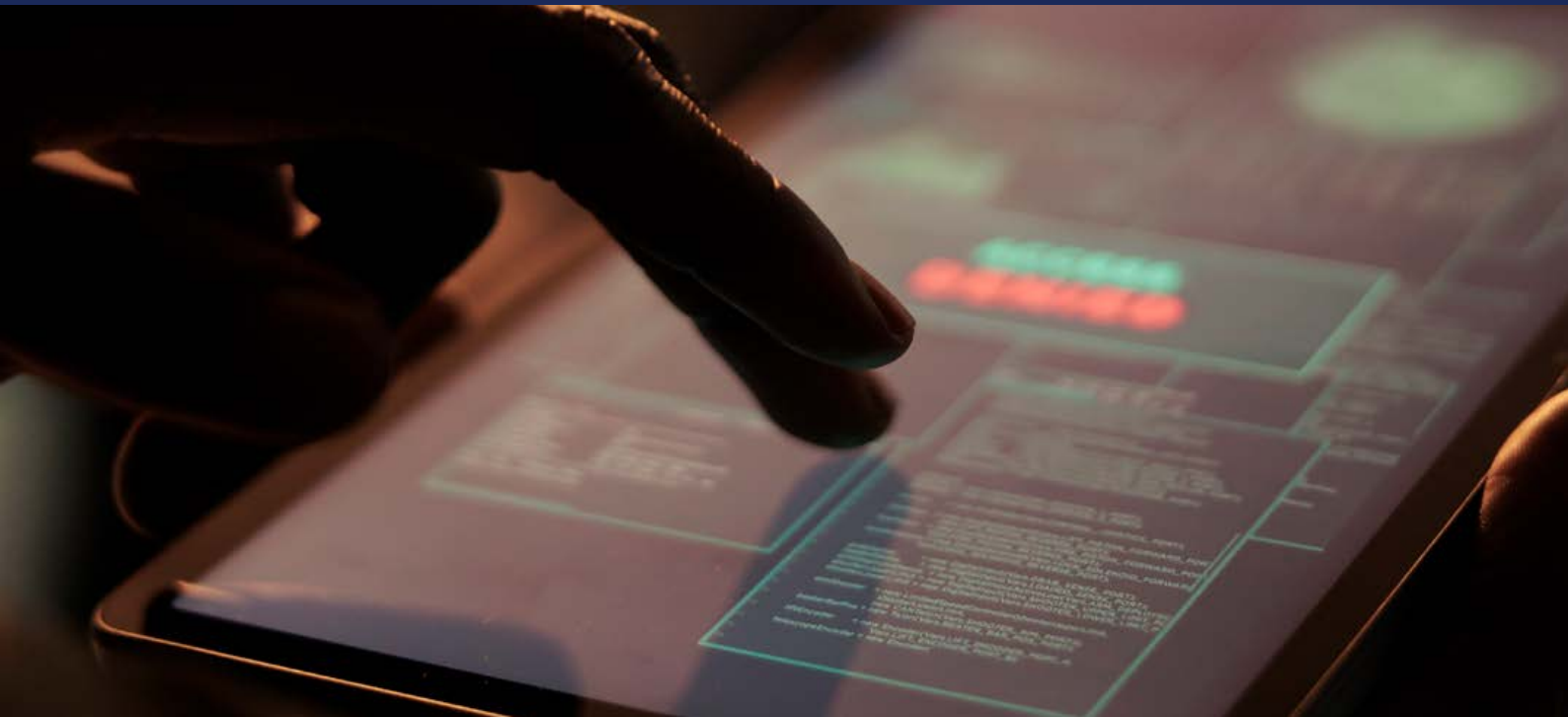


Key Findings

- The top five sectors: finance, government, fintech, telecoms, and healthcare account for 70 % of total incidents and losses.
- Fraud-driven scenarios dominate, while ransomware and supply-chain attacks cause the largest single-event costs.
- Public-sector exposure continues to expand as e-government and cloud-migration projects outpace control maturity.
- Critical-infrastructure sectors (energy, manufacturing) exhibit fewer but higher-impact incidents due to operational-technology vulnerabilities.

Interpretation

Africa's cyber-risk concentration mirrors its digital-adoption curve: the sectors enabling commerce and citizen services attract the most attacks. **Financial institutions** remain the continent's security bellwether, while **healthcare and industrial operations** face rising risks from interconnected systems. Improving **cross-sector visibility, data-governance discipline, and business-continuity readiness** will determine whether rising investment yields measurable resilience gains in 2026.




Top Threat Scenarios – Africa

Overview

Threat activity in 2024/25 was dominated by identity-centric attacks, vulnerability exploitation, and social-engineering campaigns. Attackers increasingly combined phishing, credential theft, and ransomware into hybrid operations targeting financial and governmental ecosystems. The following table reflects modeled proportions of incident frequency and relative loss magnitude across the five in-scope economies.

Top Threat Scenarios - Africa

Threat Scenario Event Type	Number of Incidents (%)	Magnitude of Loss (%)	Summary Observation
 Phishing & Social Engineering	24	18	Primary infection vector; AI-generated content and voice spoofing raise success rates.
 Exploitation of Vulnerabilities & Misconfigurations	18	15	Persistent patch-management gaps in cloud and government networks.
 Credential Theft & Reuse (Identity Compromise)	14	12	Drives fraud and unauthorized transfers; MFA adoption rising but inconsistent.
 Business Email Compromise (BEC)	10	11	High-value fraud via supplier-invoice manipulation and fake approvals.
 Ransomware / Data Encryption for Extortion	5	17	Lower frequency, highest per-event losses; downtime costs dominate impact.
 Distributed Denial of Service (DDoS)	6	5	Disruptive but transient attacks on telecoms and fintechs.
 API & Cloud Exploitation	5	6	Weak authentication and shared-service exposure; API economy expanding.
 Third-Party / Supply-Chain Compromise	4	8	Vendor and MSP intrusions trigger cascading regional effects.
 Malware Deployment & Propagation	8	4	Commodity malware prevalent; relatively low loss per incident.
 Insider-Triggered Incidents (Negligent or Malicious)	6	4	Human error remains significant; analytics improving early detection.



Key Findings

- **Identity-related attacks** (phishing, credential theft, BEC) constitute **48%** of total incidents.
- **Ransomware and supply-chain breaches** generate **25%** of overall loss magnitude.
- **Vulnerability exploitation** remains the leading enabler of persistent access.
- **Cloud and API risks** continue to rise as digital ecosystems interconnect.
- **Insider risk** often accidental, still triggers a meaningful share of events.

Interpretation

- Africa's threat landscape reflects a maturing yet uneven defensive posture.
- Automation, credential abuse, and social manipulation outpace traditional controls.
- Enhancing **identity governance, vulnerability prioritization**, and **real-time telemetry correlation** will deliver the most measurable reduction in both incident frequency and loss severity by 2026.













Top Loss Scenarios – Africa

Overview

Loss scenarios describe the specific cyber events that lead to measurable financial or operational impact. In 2024/25, fraud-related incidents remained dominant in frequency, while ransomware and third-party outages caused the largest per-event financial losses. These patterns reflect Africa’s rapid digital-finance growth and increasing interdependency across cloud, fintech, and government ecosystems.

Top Loss Scenarios - Africa

Loss Scenario Event	Number of Incidents (%)	Magnitude of Loss (%)	Summary Observation
 Payment Fraud	16	14	Most frequent category; fueled by real-time transfers, weak transaction monitoring, and social engineering.
 Online Fraud	14	10	Marketplace scams, e-commerce manipulation, and fake platform activity continue to grow.
 Email Fraud (BEC)	12	8	Supplier-invoice redirection and impersonation schemes widespread.
 Mobile Fraud	10	3	SIM-swap and mobile-money fraud persist despite stronger KYC controls.
 Card Fraud	9	5	Card-not-present attacks prevalent; 3-D Secure adoption improving.
 Data Theft (Operational or IP Data)	9	9	Corporate data leaks and IP exfiltration linked to espionage and insider compromise.
 PII Breach / Data Disclosure	7	6	Regulatory penalties and customer remediation costs rising sharply.
 Data Encryption (Ransomware)	6	18	Fewer incidents, but extreme losses per case; downtime and recovery dominate cost.
 System Outage (Internal or Misconfiguration)	9	12	Infrastructure errors and unplanned downtime cause significant productivity loss.
 Third-Party Outage / Supply-Chain Disruption	8	15	Vendor or cloud-service failures generate cascading impacts across sectors.



Key Findings

- **Fraud-related losses** (payment, online, email) represent **40%** of total incidents and **32 %** of total losses.
- **Ransomware** and **third-party failures** generate **33%** of aggregate loss magnitude despite lower frequency.
- **Operational outages** now rank among top three loss drivers, underscoring gaps in resilience and redundancy.
- **Data-related incidents** (theft, breach, encryption) are rising due to fragmented data governance.

Interpretation

- Africa's 2024/2025 loss profile mirrors its economic digitization, rapid fintech expansion combined with uneven resilience maturity.
- Enterprises face a dual challenge: financial fraud draining liquidity and infrastructure outages undermining operational continuity.
- Investments in payment integrity monitoring, ransomware recovery testing, and third-party risk assurance will deliver the greatest reduction in loss exposure over the next 12 months.



Top Risk Scenario – Africa








Overview

Risk scenarios describe the underlying weaknesses, control failures, or exposures that enable cyber incidents and amplify losses.

In 2024/25, most events were driven by unauthorized access, data integrity failures, and system unavailability, often linked to identity compromise, weak third-party assurance, or incomplete backup strategies.

The table below highlights the top ten risk scenario types across the in-scope economies.

Top Risk Scenarios - Africa

Risk Scenarios Event Type	Number of Incidents (%)	Magnitude of Loss (%)	Summary Observation
 Unauthorized Outgoing Fraudulent Transfer	14	13	Largest single cause of direct monetary loss; driven by BEC and insider compromise.
 Unauthorized Access to Personal & Sensitive Data	13	7	Persistent exposure vector; leads to privacy violations and reputational harm.
 Unplanned Unavailability of Critical Systems	11	13	Infrastructure or attack-related downtime disrupts service continuity.
 Unauthorized Use / Misuse of Applications or Privileges	10	4	Misuse of access rights remains common; detection maturity improving.
 Unauthorized Transfer of Financial / Operational Data	10	9	Data exfiltration and manipulation prevalent in financial and telecom sectors.
 Unauthorized Modification of Financial / Operational Data	9	12	Data integrity attacks distort reporting and fraud detection processes.
 Unauthorized Encryption of Critical Data (Ransomware)	8	16	Low-frequency, high-impact incidents; recovery cost dominates.
 Third-Party System Compromise / Outage	9	14	Vendor or MSP disruptions produce multi-client operational impacts.
 Unauthorized Access to Configurations & Logs	8	4	Enables stealth persistence; low direct cost but high systemic risk.
 Unauthorized Disclosure of Personal / Sensitive Data	8	8	Regulatory fines and remediation programs increasing in frequency.



Key Findings

- **Fraudulent transfers, data manipulation, and system downtime** account for over **40%** of modeled losses.
- **Third-party compromises** and **ransomware** incidents yield the largest per-event losses.
- **Identity and privilege management gaps** remain central enablers of cascading breaches.
- **Data-governance weaknesses** amplify reputational and compliance exposure.

Interpretation

Africa's cyber-risk profile in 2025 reveals a structural challenge: the same vulnerabilities that drive efficiency, interconnected systems and rapid digitization also magnify incident impact. Improving identity assurance, data-integrity controls, and third-party oversight will deliver the highest resilience gains. Organizations should embed continuous testing and immutable-backup frameworks to maintain business continuity under disruption.



Top Loss Cost Types – Africa

Overview

Loss-cost types describe where organizations and individuals spend resources following cyber incidents. In 2024/25, the most common expenditures related to incident response, remediation, and productivity losses, followed by direct financial theft and regulatory or contractual obligations. Percentages represent how often each cost type appeared across modeled incident datasets from the five in-scope economies.

Top Loss Cost Types - Africa

Loss Cost Type	Number of Incidents (%)	Summary Observation
 Response and Remediation Costs	21	Containment, forensics, and system rebuilds occur in nearly all major incidents.
 Productivity and Downtime Costs	18	Business interruption and service degradation remain universal consequences.
 Funds Loss (Direct Fraud / Payment Theft)	16	Monetary theft through unauthorized transfers and compromised accounts.
 Remediation Projects / System Replacement	12	Infrastructure modernization and patch cycles accelerated post-incident.
 Reputation and Brand Damage Costs	10	Market-confidence and stakeholder-trust erosion; longer-term brand impact.
 Regulatory Fines and Legal Settlements	8	Increasing due to stronger enforcement of privacy and financial regulations.
 Contractual and Third-Party Liabilities	6	SLA penalties and partner compensation following service disruption.
 Competitive and Strategic Costs	4	Loss of proprietary information delaying innovation or market entry.
 Customer Retention and Recovery Costs	3	Goodwill refunds, loyalty initiatives, and post-breach outreach.
 Insurance and Residual Transfer Costs	2	Low activation rate; limited cyber-insurance penetration across Africa.








Key Findings

- **Incident-response and downtime costs** appear in over one-third of all cyber events.
- **Direct fraud losses** and **regulatory penalties** show year-on-year growth across finance and telecom sectors.
- **Reputation recovery** costs are now routine, even for operational incidents without data breach.
- **Insurance adoption** remains limited, leaving most organizations self-funding recovery.

Interpretation

Africa's cyber-loss economics reveal that containment and continuity expenditures dominate post-incident spending. Proactive investment in rapid-response playbooks, business-continuity automation, and fraud-prevention analytics can significantly reduce recurring costs. Organizations should treat post-incident recovery budgets as measurable resilience metrics, not exceptional expenses.

Cross-Domain Highlights

Focus Area	2025 Snapshot	2026 Priority Focus
 Economic Exposure	GDP USD 2.8 T • Cyber Spend USD 15.3 B • Loss USD 5 B	Enhance efficiency of spend through automation and joint threat-intelligence sharing.
 Industry Risk Concentration	Finance, government, and telecom 65% of incidents	Extend cross-sector resilience testing and joint incident response protocols.
 Threat Landscape	Identity abuse and ransomware lead impact metrics	Strengthen identity governance and vendor risk visibility.
 Operational Resilience	Outages and downtime now key loss drivers	Integrate continuity metrics into board-level oversight.
 Skills and Capacity	400 000 cyber professionals (30% certified)	Expand regional talent pipelines through initiatives like Cyber Shujaa and university partnerships.

2026 Outlook

1. **Resilience Efficiency Benchmark:** Maintain the 3 : 1 spend-to-loss ratio as a regional indicator of maturity; seek incremental improvement through data-driven investment.
2. **Identity and Access Governance:** Prioritize multi-factor authentication, credential management, and continuous monitoring.
3. **Third-Party Dependence:** Enforce transparency and redundancy for critical service providers and cloud vendors.
4. **Data Integrity & Governance:** Position data accuracy and availability as core resilience metrics in regulatory and board reporting.
5. **Regulatory Convergence:** Advance alignment between national cybersecurity and data-protection laws to strengthen cross-border response and reporting.

Interpretation

Africa is shifting from reactive defense to measurable resilience management. The region's next phase will focus on demonstrating return on security investment through quantifiable risk-reduction and continuity metrics. Collaboration among regulators, enterprises, and technology partners will determine the continent's ability to translate spending into trust and stability by 2026.





Industry Player Perspective

Banking

By Fidelis M. Muia,

Director, Technical Services, Kenya Bankers Association



Turning Intelligent Risk into Strategic Resilience

Kenya's financial sector continues to advance its digital capabilities, and Artificial Intelligence now sits at the centre of both innovation and risk. AI supports personalised services, faster decision making and predictive analytics, but it has also introduced faster, adaptive and increasingly complex cyber threats. Attackers are using AI supported tools to automate intrusions, craft convincing deepfakes and exploit weaknesses at scale. Traditional rule-based risk frameworks cannot match this pace, making resilience the priority for modern institutions.

The Shifting Risk Frontier

AI has broadened the definition of cyber risk. Organisations now face model manipulation, data poisoning, synthetic identities and automated misinformation. Attackers increasingly target the intelligence systems that guide financial decisions rather than the underlying data alone. Because AI systems can be influenced by altered

inputs, a single compromised dataset can distort outcomes across entire platforms. Growing dependence on third party AI services, from cloud analytics to automated support tools, adds further exposure. In this environment, resilience becomes the essential capability that allows institutions to anticipate, withstand, recover and adapt as threats change.

From Risk Management to Resilience Engineering

Financial institutions must move from compliance-based security to resilience by design. This requires a systems lens that connects technology, governance and people.

Resilience begins with visibility into every model, dataset and algorithm in use. It strengthens through adaptability by embedding privacy and security safeguards throughout development. It is reinforced by redundancy so that operations continue even when intelligent systems fail. Above all, resilience depends on people. Skilled staff remain the strongest safeguard in environments shaped by automated tools.



Kenya's Context: Innovation with Responsibility

Kenya's status as a leader in digital finance provides a strong foundation for AI resilience. The country's mobile first financial services, dynamic fintech sector and supportive regulation have expanded financial access nationwide. The same innovative mindset must now support responsible AI governance.

As AI becomes central to fraud prevention, customer engagement and credit decisioning, institutions must strengthen resilience at the same rate. A coordinated defence network that connects banks, fintechs, switches and regulators will be vital. AI driven threats spread across institutions, making collective readiness an essential part of sector stability.

Recommendations for the Financial Sector

1. Institutionalise AI Governance and Model Risk Management

Maintain an updated model inventory, assign clear ownership across development and integrate AI risk into enterprise risk strategies. Independent validation should check fairness, explainability and robustness.

2. Strengthen Collaboration Across the

Sector

AI related threats affect the entire ecosystem. Shared threat intelligence, coordinated simulation exercises and aligned standards for third party AI providers will support a unified defence posture.

3. Invest in Human and Technical Capability

Build teams that understand AI, equip leadership to oversee AI governance and adopt tools such as AI supported threat detection, zero trust access models and continuous monitoring.

A Call to Leadership

AI will continue shaping financial services and influencing the nature of cyber risk. Kenya's sector leaders must decide whether to view AI as a burden or as a capability that reinforces trust and long term stability. Resilience is not achieved by removing all risk but by functioning confidently in uncertain conditions. With strong governance, coordinated readiness and investment in people and technology, Kenya's financial sector can convert intelligent risk into enduring resilience and use that resilience as a strategic advantage.



Industry Player Perspective

Banking

By Eston Kairu

General Manager - Information Security Governance & Technical Assurance - Equity Group,
Chairman - IT Systems, Risk and Security Sub-Committee
- Kenya Banker's Association



From Risk to Resilience: AI and the Future of Cyber Risk Management

An (in)famous bank robber in the 1920's – 1930's known as Willie Sutton was once asked why he robbed banks and his alleged answer was, "Because that's where the money is!"

Fast forward to the present and this quote remains relevant to date and the risk has metamorphosized from guns and fast car chases on local roads to transmission of gigabytes of data at dizzying speeds through a vast global network. This has further been compounded by rapid advancement of Machine Learning (ML) and Artificial Intelligence (AI) in facilitating well-crafted and effective methods of conducting cyber crime to get to where "the money is".

In typical fashion, many a CISO in the Financial Services will immediately perceive this development as a threat. In recent times however, progressive cybersecurity practitioners have taken a broader view and seen this as;

1. A capability that would leapfrog the business ahead of its competitors
2. An opportunity for enhancing their cyber capabilities and build robust and automated controls.

The above perspectives demonstrate the shift between risk reduction to business enablement. Whereas the former school of thought was focused on protecting what was already there, the later provides proper guardrails that the business needs to dream, dare and conquer. This is business resilient cyber risk management.

This shift is not only one of mindset but needs to be considered across people, process and technology. It is not lost on many CISO's that there is a global shortage of an estimated 4.7 million cyber security professionals and therefore, a lot more focus should pivot on the process and technology perspectives.



Enhanced use of machine learning and artificial intelligence to analyze, prevent, detect, respond and recover from cyber incidents will greatly reduce routine tasks, eliminate noise, minimize the risk of human error and give more opportunities for capacity building.

The CISO must evolve and become a master of achieving the perfect balance of protecting the institution while at the same time being a fundamental pillar in its growth and continued existence for decades to come.

Back to the alleged quote by Sutton which eventually evolved into what is now called "Sutton's Law" currently taught in medicine that states that "when diagnosing, one should first consider the obvious. It suggests that one should first conduct those tests which could confirm (or rule out) the most likely diagnosis rather than wasting time and money investigating every conceivable possibility". However, in the AI and ML world, every conceivable possibility is investigated in a matter of milliseconds!



03

SECTION 3



CYBER INTELLIGENCE -
KENYA



Section 3: Cyber Intelligence - Kenya

Open Ports and Exposed Devices

A significant number of exposed devices in Kenya have been detected, with open ports on various services posing security risks. Remote access services, database systems, and network management protocols are especially critical, as they present a direct route to system compromise or network control. Immediate mitigation efforts should focus on securing these high-risk areas while continuing to monitor and manage less critical services.

Statistics

Service Name	Count
HTTP	115,888
SNMP	43,944
UNKNOWN	23,761
SSH	19,077
MIKROTIK_BW	12,152
NTP	11,295
MIKROTIK_WINBOX	11,056
IKE	6,067
TELNET	5,993
DNS	5,560
FTP	5,517
SMTP	3,436
L2TP	2,969
PPTP	1,748
RDP	1,574
OPENVPN	1,308
IMAP	1,195
DCERPC	1,184
PORTMAP	1,166
CWMP	1,010

Analysis

1. Web Services - HTTP (115,888), DNS (5,560)

- **Impact:** Web services are commonly targeted for web application attacks (e.g., Cross-Site Scripting, SQL Injection, and Denial of Service). Vulnerabilities in web servers can lead to data breaches, defacements, or total service outages.
- **Variance:**
- **Likelihood: High** – Due to the large number of exposed HTTP servers and DNS services, attackers can easily identify and exploit vulnerabilities.
- **Consequence:** Web services can expose sensitive customer data or disrupt business operations if compromised.
- **Risk Mitigation:** Regular patching, web application firewalls (WAF), and secure configurations like HTTPS (SSL/TLS).

2. Remote Access Services - SSH (19,077), RDP (1,574), Telnet (5,993), FTP (5,517), OPENVPN (1,308), L2TP (2,969), PPTP (1,748), DCERPC (1,184)

- **Impact:** Remote access services are critical entry points for brute-force attacks, ransomware, and unauthorized access. Services like Telnet and FTP are especially risky due to their lack of encryption.
- **Likelihood: Critical** – Exposed services can be easily targeted by attackers looking to gain control over systems. Telnet and FTP are particularly vulnerable.



➤ **Consequence:** Unauthorized access to servers via these services can lead to full system compromise, data exfiltration, and malware deployment.

➤ **Risk Mitigation:** Disable Telnet/FTP in favor of SSH/SFTP, enable multi-factor authentication (MFA), and implement strong password policies.

3. Network Management and Monitoring Services - SNMP (43,944), NTP (11,295), MIKROTIK_BW (12,152), MIKROTIK_WINBOX (11,056), IKE (6,067), CWMP (1,010)

➤ **Impact:** Network management services (e.g., SNMP, MIKROTIK_BW, NTP) can be used to gather intelligence about the network and facilitate lateral movement within compromised networks. Attackers can misuse these services to disrupt network traffic or redirect it to malicious servers.

➤ **Likelihood: High** – Many devices use default or weak configurations for services like SNMP and NTP, making them attractive targets.

➤ **Consequence:** Compromise of these services can lead to network outages, rerouting traffic, or allowing attackers to gather sensitive information about the network.

➤ **Risk Mitigation:** Disable unused network services, use secure configurations, and segregate these services into isolated network segments.

4. Email and Messaging Services - SMTP (3,436), IMAP (1,195)

➤ **Impact:** Email services (SMTP, IMAP) are prime targets for phishing attacks, email spoofing, and unauthorized access. SIP services can be used for eavesdropping

or VoIP-related attacks.

➤ **Likelihood: Moderate** – While these services are commonly exposed, the direct exploitation of these protocols typically requires more advanced techniques.

➤ **Consequence:** A successful attack on email services can lead to email account compromise, allowing attackers to impersonate legitimate users and steal sensitive information.

➤ **Risk Mitigation:** Implement SPF, DKIM, and DMARC for email security, encrypt communications using TLS, and regularly audit SIP/VoIP systems.

5. Unknown Services - UNKNOWN (23,761)

➤ **Impact:** Unknown services can be highly unpredictable in terms of risk because they could represent custom applications or misconfigurations. These could range from low-risk, unused services to high-risk, vulnerable applications.

➤ **Likelihood: Moderate** – Unknown services are a wildcard, and their risk is harder to assess without further investigation.

➤ **Consequence:** The unknown nature makes it difficult to predict impact, but if these services are critical or vulnerable, they could be an entry point for attackers.

➤ **Risk Mitigation:** Conduct a detailed audit of unknown services and disable or secure them as necessary.

Mitigation Strategies

- Disable unnecessary services.
- Apply strict access controls to remote access and network management services.



- Regularly patch and update exposed services.
- Use encryption and secure protocols for communication and data exchange.
- Audit and monitor all open ports and services regularly.

Open Devices

Statistics

Software Vendor	Count
amazon	19,960
microsoft	11,145
f5	9,052
openbsd	8,390
apache	7,903
akamai	5,360
php	2,015
oracle	1,743
openresty	1,734
dropbear_ssh_project	1,544
lighttpd	1,425
mikrotik	1,415
dovecot	1,296
embedthis	1,222
cisco	1,192
acme	979
allegro_software	930
postfix	918
prometheus	909
3cx	825

Analysis

A large number of systems expose open ports tied to major software vendors. These exposures increase the probability of remote exploitation and service compromise. The most prevalent vendors identified are:

1. **Amazon (19,960):** Cloud-hosted services dominate the exposure landscape. Misconfigured public endpoints present

critical risk.

2. **Microsoft (11,145):** Enterprise services and remote access protocols remain highly exposed. Attack surface is substantial.
3. **F5 (9,052) and OpenBSD (8,390):** Load balancers and security-focused OS deployments still leak entry points when exposed without controls.
4. **Apache (7,903) and Akamai (5,360):** Web and edge infrastructure are frequent targets for web-layer attacks and exploitation attempts.
5. **Other vendors:** PHP (2,015), Oracle (1,743), OpenResty (1,734), Dropbear SSH (1,544), Lighttpd (1,425), MikroTik (1,415), Dovecot (1,296), EmbedThis (1,222), Cisco (1,192), ACME (979), Allegro Software (930), Postfix (918), Prometheus (909), 3CX (825). These represent diverse services such as SSH, databases, routers, mail servers, and VoIP. Each category expands the accessible attack surface.

Distribution pattern shows heavy exposure across hosting providers, enterprise platforms, and critical network infrastructure. Any unpatched system or default configuration increases exploitation likelihood.

Mitigation Strategies

The presence of open ports across critical services provided by these vendors raises concerns about potential exploitation, unauthorized access, and service disruption. To mitigate these risks:

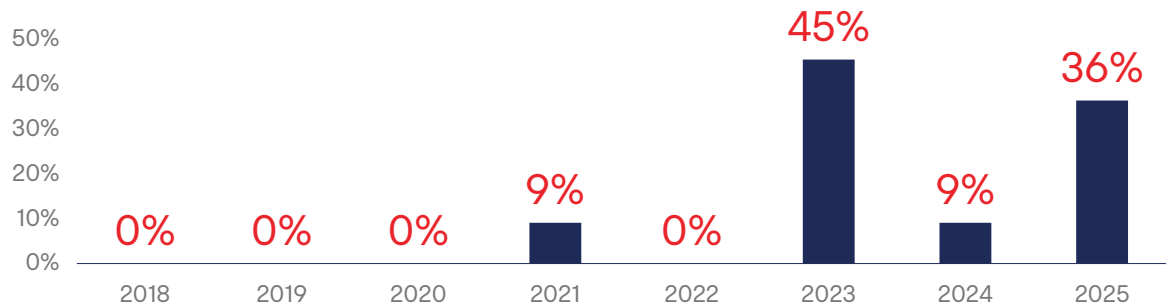
- Enforce firewall policies that default to deny.
- Patch software on a fixed schedule.
- Remove or restrict public access to unnecessary services.
- Prioritize remediation for Amazon, Microsoft, F5, OpenBSD, and Apache systems due to volume.



Public Cyber Attack News

Statistics

Cyber Attack Articles by Year



Analysis

In 2025, the following cyber-attack news were made public:

- **Financial industry:** A digital payments portal was hacked and approximately KSh 49 million was stolen. Attackers accessed the client portal, disabled OTP notifications and transferred funds into mobile wallets, bank accounts and till numbers.
- **Media industry:** A digital media platform was illegally accessed and used to distribute articles.
- **Public-Sector:** A statutory social security fund reported an attempted intrusion on its image-storage system. The core data and financial systems were stated to be unaffected.
- **Banking industry:** A banking fraud case involved a syndicate that defrauded over KSh 6 million from a commercial bank.

Mitigation Strategies

- **Least-privilege access:** Assign users only the permissions required for their role. Review access rights on a fixed schedule.

This lowers the blast radius if any one account is compromised.

- **Strong authentication:** Enforce multi-factor authentication for all remote access and administrative accounts. Prioritize phishing-resistant methods. This blocks most credential-based intrusions.
- **Continuous monitoring:** Use logging and automated alerts to identify abnormal system or user behaviour. Monitor for failed logins, privilege escalation, and unusual data movement. Early detection reduces breach dwell time.
- **Timely patching:** Apply security updates to operating systems, applications, and network devices as soon as possible. Track and remediate vulnerabilities based on severity and exposure.
- **Network segmentation:** Isolate critical servers and data from general networks. Restrict communication paths between segments. This slows down attackers and protects sensitive assets.
- **Security testing:** Run recurring vulnerability scans and scheduled penetration tests. Validate that controls work and confirm that previous weaknesses stay fixed.

- **Configuration hardening:** Remove default credentials, close unused ports, disable unnecessary services, and enforce encryption. Reduce the number of exploitable entry points.
- **Incident response readiness:** Maintain a written and tested plan with clear roles. Have containment, eradication, and recovery steps prepared. Measure response performance to improve over time.

Honeypot Data Analysis

Statistics

IP Address	Attack Type	Count	First	Last
41.212.55.14	Spamming and Defacement	162	01/02/2011	25/07/2025
41.212.91.128	Spamming and Defacement	137	03/08/2010	28/01/2025
41.215.28.30	Spamming and Defacement	87	23/11/2010	22/01/2025
41.212.75.87	Spamming and Defacement	86	30/09/2010	08/05/2025
41.203.218.186	Spamming and Defacement	64	07/06/2010	01/04/2025
41.212.75.89	Spamming and Defacement	45	18/01/2011	23/09/2025
41.212.108.38	Spamming and Defacement	42	16/08/2011	18/04/2025
41.207.97.82	Spamming and Defacement	36	29/08/2009	30/07/2025
41.215.120.22	Spamming and Defacement	30	25/08/2010	29/09/2025
41.212.11.141	Spamming and Defacement	28	02/09/2010	27/04/2025
41.215.97.65	Spamming and Defacement	26	25/05/2011	16/05/2025
41.212.54.211	Spamming and Defacement	23	03/09/2010	23/05/2025
41.215.84.22	Spamming and Defacement	22	11/08/2011	16/01/2025
41.212.55.203	Defacement	15	20/09/2012	12/10/2025
41.215.9.250	Spamming and Defacement	15	23/12/2010	05/09/2025
41.215.140.142	Spamming and Defacement	8	03/10/2012	23/04/2025
41.212.96.11	Spamming	8	07/12/2010	16/02/2024
41.212.99.204	Spamming	7	20/11/2010	24/07/2025
41.212.113.64	Spamming	6	26/07/2011	22/06/2025
41.206.35.70	Spamming	5	20/01/2011	26/09/2025
196.200.31.206	Spamming	4	14/11/2008	12/09/2025
41.222.12.168	Spamming	3	06/08/2010	12/06/2025
41.215.105.168	Spamming	3	27/07/2010	05/05/2025
41.212.55.187	Spamming	2	13/09/2011	30/07/2025
41.212.69.34	Spamming	2	18/11/2015	19/06/2025
41.215.89.136	Spamming	2	01/06/2011	02/05/2025
41.215.14.46	Spamming	2	26/07/2010	20/01/2025
41.215.127.206	Spamming	2	13/03/2013	16/01/2025
41.212.118.159	Spamming	1	21/07/2025	21/07/2025
41.212.58.113	Spamming	1	12/06/2025	12/06/2025
41.212.8.209	Spamming	1	08/05/2025	08/05/2025



Analysis

The data on malicious IP addresses in Kenya from the Project Honeypot reveals a recurring pattern of bad events over an extended period (from as early as 2008 up to mid-2025).

Below is a summary of key observations:

- **Long-Term Threat Actors:** Some IP addresses have been involved in malicious activity for over 14 years. For example, IP 41.212.55.14 first recorded a bad event in 2011 and continues to be active in 2025, highlighting that the devices are still actively used by certain threat actors.
- **High Frequency of Events:** Six (6) of the top ten (10) IP addresses have been involved in hundreds of bad events over the years showcasing persistent threats in an attempt to infiltrate systems.
- **Recent Events:** Ongoing activities in 2025 signals ongoing cyber threats targeting infrastructure and possibly taking advantage of vulnerabilities on online devices.
- **Geo-location in Kenya:** These IP addresses are localized to Kenya, which could indicate either domestic threat actors or compromised systems within the country being leveraged for broader global cyberattacks.

Mitigation Strategies

- **IP Blocking and Blacklisting:** Regularly update firewall rules to block access from known malicious IP addresses, particularly those with a history of repeated bad events.

- **Threat Intelligence Sharing:** Collaborative intelligence sharing among ISPs, organizations, and cybersecurity authorities in Kenya can help mitigate attacks by quickly identifying and neutralizing threats.
- **Traffic Analysis and Anomaly Detection:** Deploy advanced network monitoring tools capable of detecting unusual traffic patterns and promptly alerting cybersecurity teams to potential threats.
- **Incident Response:** Set up rapid response mechanisms to contain and mitigate any successful breaches from these known malicious sources.
- **Regular Updates and Patching:** Ensure all systems are up-to-date with security patches to close vulnerabilities that may be exploited by these IP addresses.

Conclusion

Cyber threats targeting Kenyan infrastructure and businesses are on the rise. The increased frequency of attacks on open ports, exposed devices, and critical vulnerabilities in widely used software poses a clear and present danger. The Kenyan government, businesses, and individuals must take proactive steps to mitigate these risks through enhanced security measures, patch management, and user education.

By mitigating the above risks, Kenya can reduce its exposure to cyber threats and maintain a safer digital environment.





Industry Player Perspective

Public Policy

By Mugambi Laibuta, PhD., CIPM
Chairperson, Data Privacy and Governance Society of
Kenya (DPGSK)



Data Protection, AI and the Future of Cyber Risk Management

Artificial Intelligence is reshaping how organisations manage cybersecurity and data protection. It enhances predictive capability and speeds up threat detection, yet it also introduces new vulnerabilities in the way personal information is collected, processed, shared, analysed and stored. In Kenya's expanding digital economy, this link between AI and data protection has become central to national cyber resilience.

AI models depend on extensive datasets that often contain sensitive personal information. This dependence creates risks such as misuse, bias, re identification and unlawful disclosure. Some generative tools may unintentionally reveal training data, while automated threat hunting systems can process personal records without sufficient safeguards. Kenya's Data Protection Act requires privacy by design, lawful processing and accountability in automated decisions, making it essential to responsible AI use.

In 2024, local institutions experienced increased cases of AI generated impersonation, deepfakes and unauthorised profiling, showing how weak data governance magnifies cyber risk. As AI systems become more autonomous, incidents will carry ethical and legal consequences in addition to technical ones.

Resilience depends on a governance culture built on data protection principles. Organisations must treat personal information as a strategic asset and manage it through clear rules on legitimate use, minimisation, retention, access control, security and disposal. Strong safeguards allow AI systems to operate transparently and support the objectives of privacy, fairness and accountability.

Tools such as Data Protection Impact Assessments and AI Impact Assessments are now essential for identifying risks before deploying AI systems, particularly in sensitive areas like biometrics, surveillance and automated credit scoring.



AI risk management must go beyond technical controls to include ethical and legal oversight. Governance frameworks should clarify the responsibilities of data stewards, cybersecurity teams and Data Protection Officers. The Office of the Data Protection Commissioner can strengthen the ecosystem by issuing guidance on AI compliance, cross border data handling and algorithmic accountability.

AI can reinforce data protection when used responsibly. Machine learning can uncover anomalies, prevent leakage of personal information and support

compliance monitoring. Even so, human judgement remains critical. A governance approach rooted in digital ethics, skills development and public trust is vital to national resilience.

Kenya has a strong regulatory foundation. Its impact now depends on how organisations apply privacy principles within AI systems and cybersecurity practices. With the right legal, technical and ethical safeguards, Kenya can show that responsible AI is both possible and essential for a safe and inclusive digital future.



04

SECTION 4



SURVEY ANALYSIS - KENYA

Section 4: Survey Analysis - Kenya

Executive Summary







The 2024/2025 Cybersecurity Survey gathered 280 responses from organizations across Kenya's critical sectors - financial services, ICT and telecom, government, education, healthcare, and manufacturing.

The survey assessed governance practices, incident experience, investment patterns, data-protection readiness, and resilience maturity.

Key Findings

- **Framework Adoption:** Over 75 % of organizations align with recognized cybersecurity frameworks, mainly ISO 27001 and NIST CSF.
- **Policy Governance:** 71 % have formal cybersecurity policies, but only half review them annually.
- **Incident Exposure:** About 37 % experienced a cyber incident in the past year, primarily through phishing and ransomware.
- **Budget Momentum:** 42 % report budget growth, yet investment still leans toward technology over human capacity.
- **Data-Protection Awareness:** 93.6 % are familiar with the Kenya Data Protection Act (KDPA); 56 % have appointed Data Protection Officers.
- **Resilience Readiness:** Only one-third of organizations test incident-response plans regularly; 35 % rate their resilience as low.

Sectoral Participation

Sector		Share of Respondents	Distinct Trends
	Financial Services	32 %	Highest framework adoption and AI-driven fraud monitoring
	ICT & Telecommunications	21 %	Rapid AI adoption, strong technical controls
	Government	17 %	Improving policy coverage but budget and testing constraints
	Education	12 %	High phishing exposure, limited governance capacity
	Healthcare	9 %	Rising data-protection awareness, weak incident readiness
	Manufacturing & Other	9 %	Mixed maturity, ad-hoc framework use



A. Cyber Governance and Awareness

i. Familiarity with Cybersecurity Frameworks



Survey Question:

Which framework does your organization use to guide its security program?

Framework Adoption

ISO 27001



NIST CSF



CBK Guidelines



Other



Kenyan organizations continue to embrace international frameworks as a foundation for governance. ISO 27001 remains the primary reference standard, with NIST CSF gaining traction among technology firms. Smaller entities depend on internal policies, highlighting a need for simplified sectoral models.

ii. Existence of Cybersecurity Policies



Survey Question:

Does your organization have a formal cybersecurity policy?

Policy Existence

Yes



No



Policy adoption is improving, especially in regulated industries. However, nearly a third operate without formal policies, limiting accountability and risk governance.

iii. Policy Review Frequency



Survey Question:

How often are cybersecurity policies reviewed?

Policy Review Frequency

Annually



Quarterly



Rarely



Regular review cycles indicate growing governance discipline. Public institutions lag due to resource and staffing constraints.

iv. Use of Performance Metrics and Benchmarks



Survey Question:

Has your organization established KPIs or benchmarks to track cyber posture?

Performance Measurement

Yes



No



Organizations using metrics demonstrate better response discipline and control visibility. Lack of quantitative tracking continues to impede strategic reporting to boards.



v. AI Adoption in Cybersecurity



Survey Question:

Is AI utilized within your cybersecurity operations?

AI Use in Cybersecurity

Yes



No



AI integration is growing in fraud detection and anomaly analysis but remains nascent. Challenges include limited skills and the absence of AI governance policies.

B. Cyber Incidents and Threat Landscape

i. Experience of Cyber Incidents



Survey Question:

Has your organization experienced a cyber incident in the past 12 months?

Incident Occurrence

Yes



No



More than one in three organizations suffered an incident, with finance and telecom reporting the highest exposure levels.

ii. Common Attack Vectors



Survey Question:

What types of incidents have you encountered?

Attack Vectors

Phishing



Malware



Ransomware



Phishing remains Kenya's dominant threat vector. Ransomware continues to target financial and data-driven institutions.



iii. Post-Incident Response



Survey Question:

What actions did your organization take following a cyber incident?

Post-Incident Actions

Reviewed Controls



Reported Internally



Regulator



No Action



Post-incident reviews are increasing but external reporting remains low due to reputation concerns and regulatory ambiguity.

C. Cyber Investment and Budget Priorities

i. Budget Changes



Survey Question:

Has your organization's cybersecurity budget changed over the past year?

Budget Change Trend

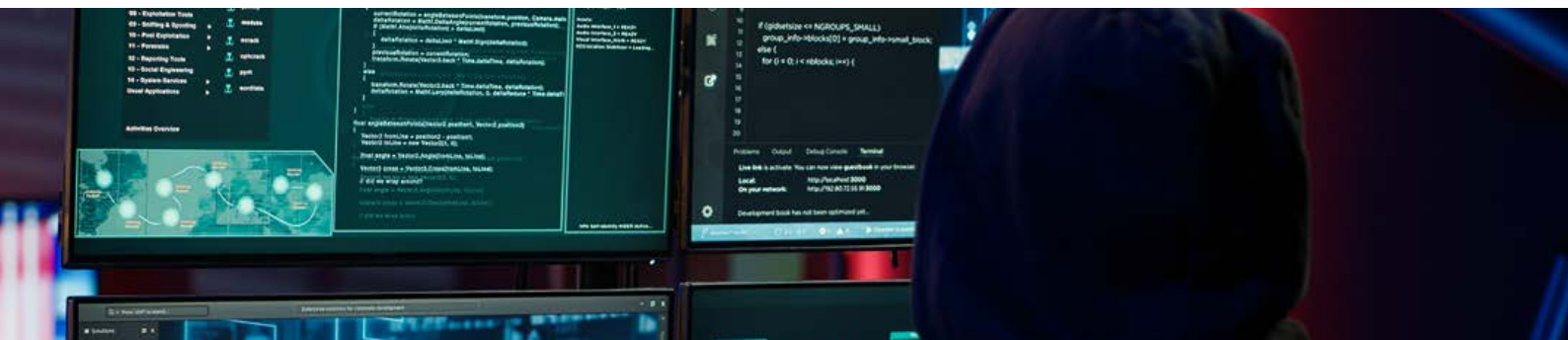
Increased



Unchanged or Reduced



Budget growth has stagnated despite rising risk exposure. Financial institutions lead spending; public agencies trail due to funding constraints.





ii. Primary Investment Areas



Survey Question:

What areas received the largest cybersecurity investment?

Investment Focus

Threat Monitoring



Endpoint Protection



Cloud Security



Awareness



Data Protection



Investment remains technology-heavy. Human-centric controls and data governance receive limited attention.

iii. Skill and Resource Availability



Survey Question:

Does your organization have sufficient qualified cybersecurity personnel?

Cyber Skills Availability

Adequate



Inadequate



Skill gaps persist in incident response and threat analysis. Local training initiatives are helping but scale is still limited.



D. Data Protection and Privacy Compliance

i. Awareness of the Kenya Data Protection Act



Survey Question:

Are you aware of the Kenya Data Protection Act (2019)?

KDPA Awareness

Yes



No



Awareness of the KDPA is almost universal, reflecting strong regulatory sensitization since 2021.

ii. Appointment of Data Protection Officer (DPO)



Survey Question:

Has your organization appointed a Data Protection Officer?

DPO Appointment Status

Yes



No



While DPO appointments are increasing, most serve dual roles without dedicated mandates or resources.

iii. Implementation of Privacy Impact Assessments and Data Mapping



Survey Question:

Has your organization conducted privacy impact assessments (PIAs) or data-mapping exercises?

PIA and Data Mapping Implementation

Yes



No



PIAs and data-mapping remain nascent activities. Lack of expertise and automation tools are the main barriers to compliance.



E. Overall Readiness and Resilience Posture

i. Existence of Incident-Response Plans



Survey Question:

Does your organization have an incident-response plan?

Response Plan Existence

Yes



No



Most organizations now document response plans but testing remains sporadic. This paper-readiness gap reduces practical resilience.

ii. Testing and Simulation Frequency



Survey Question:

How often are incident-response plans tested or simulated?

Testing Frequency

Quarterly



Annually



Never



Organizations that conduct regular exercises recover faster and experience lower loss impacts. Testing culture remains weak outside regulated sectors.



Conclusion and Recommendations

Kenya's cybersecurity landscape is moving from **compliance awareness to resilience measurement**. Governance structures and

data-protection compliance are improving, but practical testing, resource capacity, and human behavioral controls remain undeveloped.

Priority Actions



Institutionalize Metrics: Adopt standard KPIs to track security performance and benchmark resilience levels.



Integrate Continuity and Cyber Response: Unify incident management with business-continuity plans.



Invest in Skills: Scale national programs like Cyber Shujaa to build mid-level analyst capacity.



Operationalize AI Governance: Define responsible AI frameworks for threat detection and decision oversight.



Deepen Privacy Compliance: Make DPO roles fully independent and embed PIAs in every data-processing initiative.



Encourage Information Sharing: Create sector-level threat-intelligence collaboration forums.

Kenya's 2024/25 data indicates a transition to structured maturity under the CVEQ model with strong governance foundations but moderate measurement and testing discipline. With sustained regulatory pressure and board-level engagement, the country can progress toward a proactive, quantifiable resilience culture in the next two years.





Industry Player Perspective

Academia

By Dr. Paula Musuva,
Assistant Professor, School of Science and
Technology United States International University -
Africa (USIU-Africa)



AI Collaboration in Cyber Risk Management

We often say that nothing is new under the sun, but the rise of Artificial Intelligence challenges that belief. AI has begun to reshape how organisations operate and how they defend themselves, bringing both opportunity and disruption.

For many years, the aim of cyber risk management has been to help organisations take informed risks. Sun Tzu's guidance to know yourself and know your enemy has shaped this work. We examine our weaknesses, study the threat landscape and reduce exposure through continuous assessment and improvement. Cybersecurity has always depended on vigilance and adaptation rather than a final state of completion.

AI changes how this practice unfolds. It is a tool, an exceptionally powerful one and its value depends entirely on responsible use. It strengthens detection by analysing immense datasets and identifying patterns that would be impossible for

humans to process at the same speed. It enhances prediction, helping security teams anticipate malicious activity rather than only react to it. Automated response has become more effective through platforms like SIEM and SOAR, which reduce the impact of active incidents when used correctly.

Routine security work is increasingly automated, allowing teams to focus on complex issues that require experience and judgement. In the SOC, analysts are moving from manual review to guiding AI systems through carefully structured prompts so that responses reflect the organisation's specific environment.

However, AI also expands the threat landscape. Attackers are now using AI generated phishing, deepfake content for impersonation and rapidly changing malware designed to avoid detection. AI systems can also be targeted through adversarial manipulation and poisoned training data, which undermine their reliability.

Another concern is the limited explainability of advanced models. Their internal reasoning can be difficult to interpret, which creates risks of bias, inaccurate outputs and challenges in regulated environments. Data privacy concerns are equally significant because AI systems rely on large datasets that may expose sensitive information if not protected.

The shortage of professionals with expertise in both AI and cybersecurity further complicates integration, especially where organisations depend on older systems that require careful alignment with newer tools.

Looking ahead, the most effective approach to cyber threat management will rely on collaboration between human expertise and AI capability. AI should handle routine activity, identify emerging threats and support rapid response, while human specialists provide context, strategic thinking, ethical guidance and regulatory understanding. This partnership allows cybersecurity teams to focus on the high impact decisions that shape long term resilience.



05

SECTION 5

ARTIFICIAL INTELLIGENCE LANDSCAPE IN KENYA



Section 5: Artificial Intelligence Landscape in Kenya

From AI Curiosity to AI Utility



By Shikoli Makatiani

Director & Board Member,
Serianu Limited

Kenya's financial services ecosystem has moved from AI curiosity to AI utility. A Central Bank of Kenya (CBK) survey published in July 2025 found roughly 50% of lenders have adopted AI-led by credit scoring and fraud risk use cases. In parallel, adversaries are leveraging the same techniques to automate phishing, scale malware, and supercharge social engineering, with national telemetry flagging surges in phishing, DDoS, and system attacks. The question is no longer whether to adopt AI, but how to govern it and defend against its misuse without slowing innovation.

A Pragmatic Playbook for Kenyan Institutions

1. **Treat AI as a model portfolio, not a monolith.** Maintain an AI register for each use case (credit scoring, transaction monitoring, chatbots, insider fraud analytics) with purpose, data lineage, owners, risks (bias, drift, adversarial exposure), and controls. Require a one page Model Factsheet before launch-objective, explainability method, fairness tests, cybersecurity posture, and Human-in-the-Loop triggers-aligned to the NIST AI Risk Management Framework functions: Govern, Map, Measure, Manage.



2. **Make cybersecurity Alnative.** Attackers iterate at machine speed; defenders must, too. Deploy anomaly detection and behavioral analytics across identity, endpoints, payments, and core banking. Pair phishing resistant MFA with continuous session risk scoring; auto isolate high risk accounts or halt suspect transactions for human release. Harden models against poisoning, prompt injection, and adversarial examples with input validation, rate limiting, and red team exercises-consistent with NIST's "secure and resilient" attributes.
3. **Close the deepfake & syntheticID gap.** AI Generated voices, faces, and documents now bypass traditional checks. Kenya has already seen high profile impersonation incidents targeting public figures to push financial scams, underscoring sector exposure. Augment remote onboarding with liveness and challenge response (blink/turn prompts, randomized phrases) plus cross source verification (device reputation, SIM history, IP risk). For highvalue approvals, use multimodal verification (voiceprint + behavior + cryptographic device binding) and out of band confirmations. Maintain a Deepfake Response Playbook (takedowns, comms templates, legal paths).
4. **Build fairness and explainability into credit AI.** Widen access without encoding historical bias. CBK has flagged risks around bias, transparency, and accountability in AI deployments. Run bias audits across approvals, pricing, and limits; report summary metrics to the board. Use explainable AI (XAI) so customers and regulators can understand adverse decisions, with clear human recourse; prefer interpretable features and local surrogate

explanations.

5. **Leverage Kenya's collective defense.** The Banking Sector Cybersecurity Operations Centre (BSSOC)-established by CBK on September 22, 2025 provides coordinated threat intelligence, incident response, forensics, and investigations across the sector. Wire your SOC to both consume and contribute: share indicators within hours, not weeks, and align on AI fraud taxonomies (deepfake types, synthetic ID patterns) so signals translate across banks, fintechs, and SACCOS.
6. **Anchor to national strategy and global standards.** Kenya's National AI Strategy 2025–2030 outlines an ethical, secure, inclusive approach to AI, including data governance and regulatory modernization. Align internal policies and industry codes to its pillars and operationalize controls with the NIST AI RMF and emerging ISO/IEC AI governance standards.

What "Good" Looks Like by 2026

- **80%+** of material AI use cases registered with fact sheets, owners, and XAI paths.
- **90%+** of digital onboarding sessions protected by liveness + device binding.
- **<15 minutes** median time from suspected AI enabled fraud to containment.
- **Board dashboards** showing fairness and drift alongside financial KPIs.
- **24hour** cross institution intel loops: one bank's hit becomes everyone's patch.

Kenya can lead not just in fintech adoption, but in trustcentric AI where inclusion, security, and fairness advance together. The winners will pair bold deployment with equally bold governance and collective defense.





Building Cyber Resilience Using AI



By Joseph Mathenge

**Chief Operating Officer,
Serianu Limited**

Here is what this article is NOT about; what is Artificial Intelligence (AI) nor how to use AI. The article too is not about where and how to learn using AI or espousing the benefits of using IT. Read further ahead and you will not see it excoriate AI arguing that it will take over the universe. Those topics and discussions are now available all around and I encourage you to take time and continue reading, researching and forming your own opinion on AI and how it will continue to impact your daily life.

It's been often said that no individual nor organization is immune from a Cyber Security successful attack. There exist simply two types of people/organization when discussing Cyber risks; those that have been hacked and those that don't yet know that they have been hacked. We have all interacted and been impacted by a Cyber Risk. In this article, I focus specifically on how AI can be used to strengthen an organization's resilience against cybersecurity incidents.

As Information Security partitioners, charged with responsibility to protect an organization information asset, we can and should use AI to:

1. reduce attack surface and prevent breaches,
2. detect threats earlier and with higher fidelity,
3. automate safe parts of response so humans focus on judgement, and
4. accelerate recovery and lessons learned.



Achieving all these capabilities doesn't need to follow a linear path. Attacks will often randomly exploit vulnerability via an unpredictable approach hence achieving resilience should be a continuous evolving activity. Some of the key areas that I would put focus on are as follows:

Adaptive Authentication and Access Control

Implement AI-driven behavioral analytics for continuous authentication. Rather than relying solely on passwords or periodic MFA challenges, the system would continuously assess risks based on user behavior, device posture, location patterns, and access anomalies.

Vulnerability Management at Scale

Use AI to prioritize vulnerabilities based on actual exploitability, business context, and threat intelligence not just CVSS scores. AI can correlate which systems are internet-facing, contain sensitive data, and are actively being targeted.

Code and Configuration Security

AI can automatically review code for security vulnerabilities, misconfigurations, and compliance violations before deployment. This embeds security into development (DevSecOps) rather than creating bottlenecks.

Threat Detection and Response

Deploy AI-powered security operations to dramatically reduce detection and response times. This isn't about replacing the security team, it's about giving them superhuman pattern recognition capabilities. AI can detect subtle indicators of compromise, like unusual login patterns or data exfiltration attempts, often catching threats in minutes.

Automated Incident Investigation

When alerts trigger, AI can immediately begin forensic analysis, pulling relevant logs, correlating events across systems, and building attack timelines. This gives my incident response team a head start, with preliminary analysis complete before they even begin their investigation. What used to take hours of manual log correlation now happens in seconds.

Security Awareness and Phishing Defense

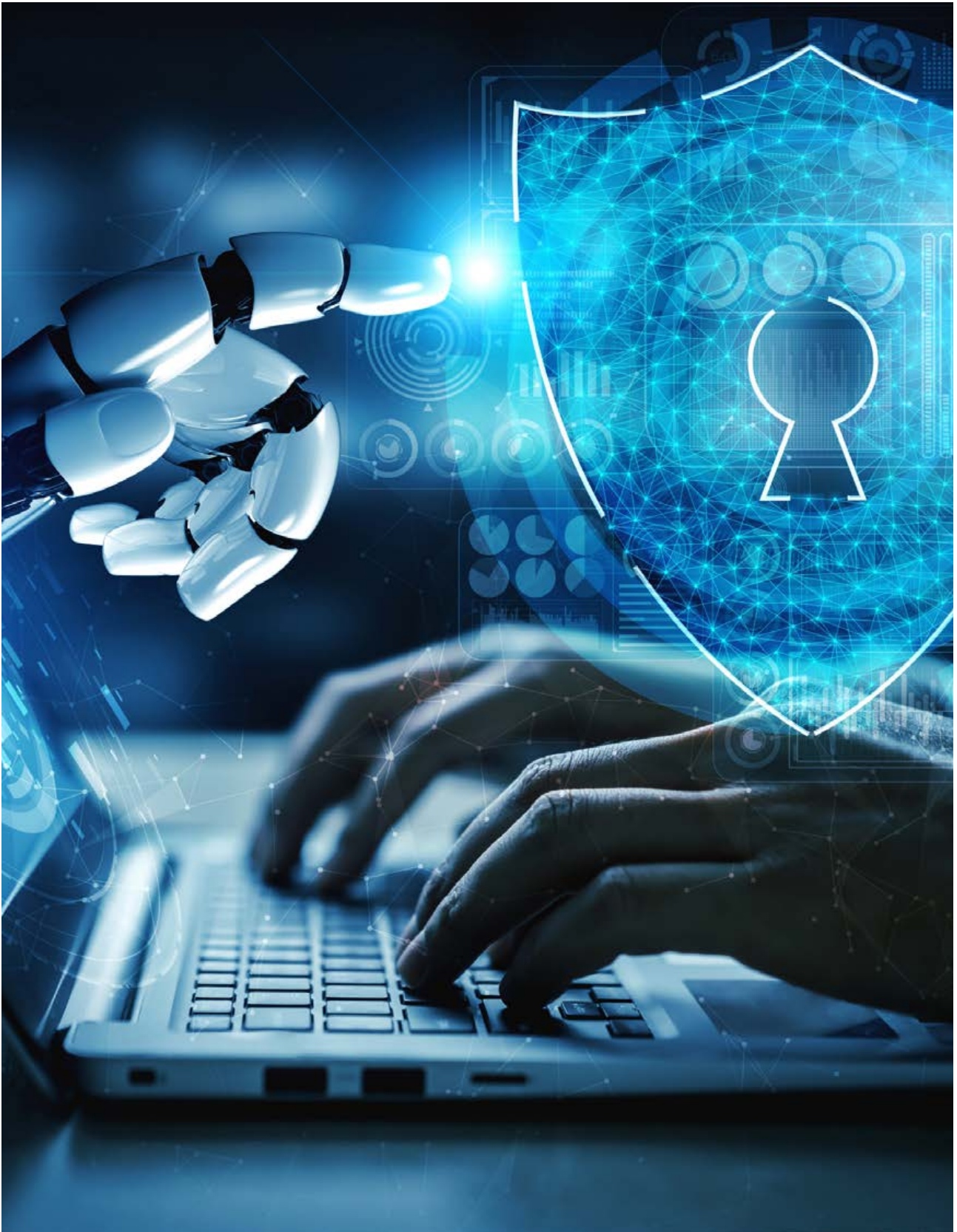
AI-powered email security can analyze not just content and attachments, but contextual factors like sender behavior patterns and communication norms. Consider using AI, in training employees, to generate personalized phishing simulations that adapt to each employee's role and previous performance, making training effective rather than a checkbox exercise.

The Human Element Remains Critical

Crucially, maintain strong human oversight. AI provides recommendations, not final decisions on incident response or policy changes. The security analysts validate findings, provide business context AI lacks, and handle sophisticated adversaries who specifically target AI defenses.

The goal isn't an "AI-powered security team", it's a human security team with AI augmentation that lets them work at the speed and scale modern threats demand. This approach recognizes that cyber resilience requires both technological sophistication and human judgment, particularly when facing determined adversaries who are themselves leveraging AI.

All AI interventions must sit inside a strong governance, data and model management framework to avoid new risks (bias, data leakage, adversarial attacks, compliance gaps).





The Age of Generative AI in Cybersecurity



By John Kuria

**Cyber Threat Management Analyst
Deloitte Kenya**

Demystifying AI, Machine Learning algorithms and Large Language Models

AI is now deeply embedded in everyday business operations, and organisations are increasingly looking to integrate it across departments to improve efficiency and outcomes. This growing interest often comes with fears about job loss, but an even more pressing challenge is clarity. In many cases, when organisations speak about adopting AI, they are actually referring to automation or advanced analytics. These are useful capabilities, but they do not always require AI.

The terms AI, Machine Learning (ML), and Large Language Models (LLMs) are often treated as if they mean the same thing, yet they describe different layers of technology. AI is the overarching concept of giving machines human-like intelligence so they can perform tasks that normally require human reasoning. It includes techniques ranging from robotics and Natural Language Processing (NLP) to ML and LLMs. These approaches teach machines how to learn patterns, interpret language, or mimic human actions.

Machine Learning is a specific branch of AI that allows systems to detect patterns in data and make decisions without being explicitly programmed. It is widely used in fraud detection, anomaly analysis, and behavioural monitoring.



Large Language Models are a specialised form of ML trained to understand and generate human language. Models such as GPT learn from vast text datasets using deep learning transformers. They power applications like chat assistants, translation tools, and generative content platforms.

For any organisation exploring AI adoption, clarity of intention is essential. The business objective must come first. Only then can one determine whether the right solution is an LLM, an ML model, or simply automated workflows.

How AI Is Transforming Cybersecurity

1. Advanced Threat Detection and Prevention

AI reshapes the analyst's role by recognising anomalies, threat patterns, and the presence of Advanced Persistent Threats (APTs) in real time. ML models learn normal user and network behaviour over weeks or months, then highlight deviations that would otherwise be overlooked. This reduces false positives and gives analysts more time to focus on high-value investigations. Tools such as Chronicle Backstory and CrowdStrike Falcon are already applying these capabilities to strengthen detection and response.

2. Changing Initial Access Techniques

Attackers are increasingly using AI to refine and scale their intrusion methods. These include AI-generated phishing campaigns, polymorphic malware, voice impersonation, and social engineering through remote access tools such as Quick Assist, AnyDesk, ScreenConnect, and Cobalt Strike. Malvertising is being used to deliver payloads through online advertisements.

Threat actors also apply LLMs to stolen datasets to identify high-value individuals and locate weaknesses in source code, accelerating the creation of sophisticated exploits.

3. Adversarial AI and Offensive Capabilities

Generative Adversarial Networks (GANs) create synthetic data that mirrors real information. While helpful for training defensive systems such as fraud detectors, they also give attackers a way to craft more refined techniques. GANs can be used to simulate fraudulent transactions, bypass anomaly detectors, or design harder-to-spot phishing and insider attacks. Security teams must now anticipate threats that evolve with each new generation of ML tools.

4. Ethical AI Challenges

One of the most difficult aspects of AI is its "black box" nature. Many models cannot fully explain how they arrive at their conclusions, raising concerns around transparency, fairness, and potential bias. These challenges are especially sensitive in areas like healthcare, loan approvals, or recruitment. This is why some institutions are cautious about deploying AI in high-impact settings. Regulations such as the EU AI Act emphasise transparency, user awareness, and clear communication when people interact with AI systems. Watermarking AI-generated media is one of the measures being explored to limit the spread of deepfakes and misinformation.



5. AI and Election Security

Deepfakes pose a serious and growing risk to democratic processes. Modern recommender systems no longer simply present personalised content. They can now amplify AI generated videos, voices, and images that influence public opinion at scale. Recent global elections have shown how such content can distort political narratives or reduce voter turnout.

In response, the cybersecurity community is working on detection tools, watermarking standards, public education initiatives, and regulatory measures. Even with these efforts, the speed at which AI generated media improves makes the protection of electoral integrity an ongoing and complex challenge.





Industry Player Perspective

Insurance

By Bernard Dulo,
Assistant General Manager-Liability and Specialty
Lines-GA Insurance



Cyber Insurance Trends and Gaps in Kenya

Kenya's insurance market has seen a rise in cyber-related incidents in recent years. Claims have become substantial, often involving loss or theft of funds, ransomware, double extortion, data breaches, and regulatory penalties. The banking sector remains the most affected, with many incidents linked to electronic fraud carried out by employees or through collusion with external actors.

Despite this growing exposure, the insurance industry still has limited appetite and capacity for cyber risks. Local underwriting expertise for these specialised risks is scarce, which has led to most placements being transferred offshore, mainly to the London market.

Cyber insurance is currently dominated by financial institutions such as commercial banks, investment firms, fund managers, Saccos, and insurance companies. Demand from online betting firms and casinos has increased due to licensing requirements, but many insurers both locally and internationally avoid covering this segment.

Sectors that hold large volumes of sensitive third-party information, including hotels, hospitals, laboratories, and pharmacies, have shown very low uptake despite high exposure. Claims data continues to show significant losses among financial institutions, while SMEs struggle to access cover due to weak control environments, inadequate IT security, and premiums that remain out of reach.

Challenges and Way Forward

- The ever-evolving Cyber Security landscape e.g. advent of AI which introduces new Cyber threats and regulatory bottlenecks. How prepared are Insurers?



- The industry is dependent on the global market, mainly in London. Are we not ready to write these risks internally? There is a need for a local solution backed by local Reinsurers in partnerships with the local first responders (Legal firms and IT security firms, Audit firms and PR/ Crisis management firms).
- A huge chunk of the market remains uninsured because they are perceived bad risks. Insurers need to partner with credible IT security firms to help assess the risks at the onboarding stage. This will not only ensure risk quality and resultant premium discounts but will also help clients take a proactive risk management approach by implementing risk mitigation measures proposed, following IT Security audits.
- The Insurance Industry should develop underwriting expertise for Cyber Security Insurance Risks E.g. Commercial Crime insurance, Bankers Blanket Bond and Cyber Liability Insurance.
- The industry should create awareness campaigns to educate the market on existence of Cyber Insurance offerings and its importance in mitigating the risk.



06

SECTION 6

DECISION ASSURANCE - AI FOR BUSINESS LEADERS



Section 6: Decision Assurance - AI for Business Leaders

Across Kenya's corporate landscape, a profound transformation is underway. Artificial Intelligence (AI), automation and data-driven systems now shape and in many cases, make the decisions that define enterprise success.

From loan approvals and credit scoring to compliance reviews and cyber risk detection, machines are now part of the decision chain, often without full board visibility or governance.

This marks the dawn of decision oversight a new era where leadership must not only oversee financial and operational outcomes but also govern the integrity of machine-influenced decisions.

Traditional governance frameworks were designed for the information age but today's environment, the intelligence age, demands a higher level of accountability. Boards, executives, and regulators must evolve from static oversight to Decision Assurance: the discipline that ensures every automated decision is explainable, ethical, and aligned with strategic intent.

A. From Oversight to Decision Assurance

Decision Assurance bridges the gap between what machines decide and what leadership understands. It shifts governance focus from controlling systems to assuring the quality of decisions themselves.

Serianu's Decision Oversight in the Age of AI introduces the BRAID Framework (Business Readiness for AI and Decisioning), a practical governance model that helps institutions:

- Identify where AI and automation already influence decisions.

- Establish clear ownership, accountability, and escalation mechanisms.
- Ensure that decision-making aligns with ethics, fairness, and compliance.
- Build readiness across Process, Data, People, Technology, and Decision dimensions.

The framework provides a structured foundation for Decision Assurance Assessments, helping organizations evaluate maturity, readiness, and risk exposure across all layers of AI-enabled decisioning.



Decision Assurance Framework Assessment – The Five Key Steps

Every organization can begin building its Decision Oversight capabilities through a structured assessment process guided by the BRAID Methodology:

- **Locate:** Identify where AI and analytics are already making or influencing decisions both approved and shadow systems.
- **Map:** Document decision flows to clarify ownership, approval paths, and escalation thresholds.
- **Secure:** Safeguard data, models, and system integrity to ensure decision trustworthiness.
- **Empower:** Build internal literacy and accountability, ensuring teams understand, question, and manage AI outputs responsibly.
- **Monitor:** Continuously measure decision quality, fairness, and impact using oversight dashboards and assurance metrics.

This assessment forms the foundation of a Decision Assurance Framework, a governance structure that protects the integrity of decisions themselves, not just the data or systems behind them.

The Role of the Board

Boards play a pivotal role in shaping how AI and automation are governed across the enterprise. Under the Decision Assurance Framework, the Board's responsibilities include:

- **Championing Governance:** Establish Decision Oversight as a formal governance domain alongside risk, audit, and compliance.

- **Demanding Accountability:** Require management to maintain an **AI Decision Register** detailing where automation influences business outcomes.
- **Integrating Oversight:** Embed Decision Assurance metrics in annual assurance reports and board committee charters.
- **Driving Transparency:** Ensure that decision models, data sources, and algorithmic outputs are explainable and defensible.
- **Setting Tone from the Top:** Make ethical decision-making and AI governance part of the institution's leadership culture.

In the words of the European Central Bank (2025):

“A decision delegated to an algorithm remains a board-approved decision in the eyes of the law and the public.”

How Organizations Can Kick-Start the Process

Many institutions hesitate to begin because AI oversight appears complex. The truth is, the process can start today with three foundational actions:

- Conduct a Rapid Decision Visibility Review - identify all AI, analytics, and automation tools influencing strategic or operational decisions.
- Establish a Decision Oversight Committee or assign accountability to an existing governance body - ensuring that decision integrity is reviewed periodically.
- Undertake a Decision Assurance Readiness Assessment - using Serianu's BRAID Framework to measure governance maturity, readiness, and risk exposure.



- These early actions lay the foundation for full-scale Decision Assurance, turning oversight from a reactive audit exercise into a proactive leadership discipline.

A Call to Leadership

Kenya's digital transformation is accelerating. AI adoption is growing across financial services, manufacturing, telecommunications and the public sector, often faster than governance frameworks can adapt.

For boards and regulators, the defining question is no longer whether AI should be used but how it should be governed.

The institutions that act now, embedding Decision Oversight and Assurance into their governance DNA will define the standards for ethical, resilient and trustworthy leadership in the AI era.

Decision Oversight is not about controlling technology, it is about preserving human judgment, integrity, and accountability in the decisions that shape our collective future.



07

SECTION 7

THE BOARDROOM CYBER RISK LANGUAGE DIVIDE



Section 7: The Boardroom Cyber Risk Language Divide

Why Boards, Regulators, and Executives Must Learn to Speak the Same Language of Resilience;

In today's digital economy, Africa's businesses and public institutions are rapidly adopting technology, cloud computing, AI, data platforms and mobile services are transforming how organizations operate.

While digital adoption accelerates, cyber resilience the ability to anticipate, absorb and recover from cyber disruption continues to lag behind.

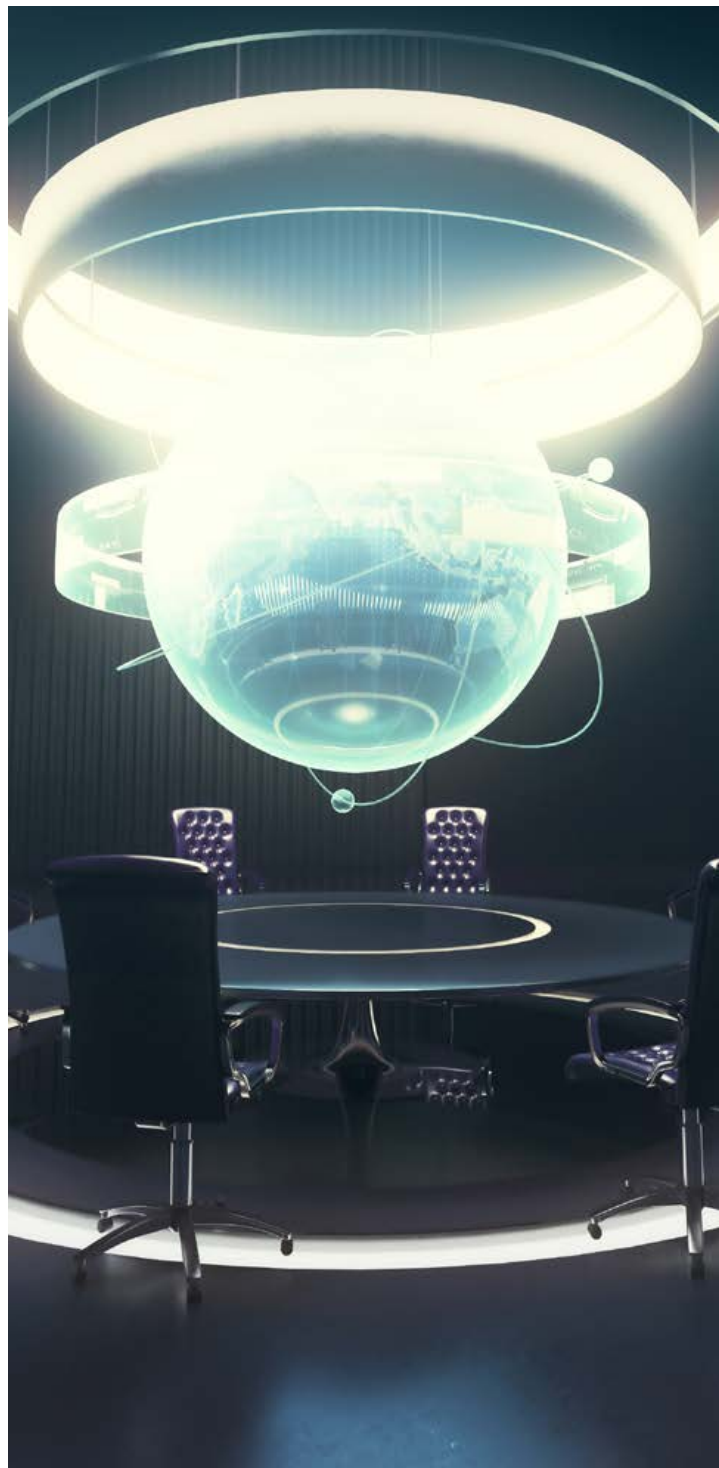
At the heart of this problem lies an often-overlooked challenge: The language divide in cyber risk management.

A Silent Disconnect in the Boardroom

Across industries, those tasked with governing cyber risk, boards, executives, and regulators speak the language of strategy, risk appetite, and accountability. Meanwhile, those charged with managing it, CIOs, CISOs, auditors, and operational teams speak the language of controls, systems, and vulnerabilities.

Both groups are deeply committed to protecting the organization, yet they operate in parallel universes. The result is a widening communication gap where important decisions are made without shared understanding.

- Boards hear about firewalls and patches, but not business exposure.





- CISOs report incident counts, not resilience metrics.
- Regulators receive compliance updates, not quantifiable confidence levels.

And so, cyber discussions often become technical monologues rather than strategic dialogues. This divide is not just semantic, it's structural. It's the reason why billions are spent on cybersecurity while confidence in resilience remains low.

The Cost of Misunderstanding

When business leaders and technologists don't speak the same language, risk becomes distorted:

- Budgets are driven by fear, not evidence.
- Reports focus on activity, not outcomes.
- Assurance becomes anecdotal, not measurable.
- Regulatory oversight becomes reactive, not preventive.

The result is what experts at Serianu describe as "cyber risk management through noise." Organizations invest in the loudest tool or the most alarming threat, rather than the control that delivers the greatest measurable impact. This communication gap is not unique to Africa but its consequences are far more serious here.

In economies where every shilling must count, inefficient cyber investment becomes a development issue, not just a technical one.

The Role of Boards and Regulators

The Cyber Resilience Board Oversight Toolkit emphasizes that cyber resilience is a leadership outcome, not a technical one. Boards now carry a fiduciary duty of care that extends beyond

financial risk to digital resilience.

As the World Economic Forum advises:

Boards must treat cyber resilience as an enterprise-wide issue requiring the same attention as financial resilience."

And according to the National Association of Corporate Directors (NACD):

Boards are not expected to manage cyber risk but they must ensure that it is being managed, measured and reported in a form they can govern."

These two statements summarize the challenge perfectly: boards are not asking for more technical data they're asking for translation. They want cyber information expressed in a form they can use to make decisions: business impact, readiness, accountability and measurable outcomes.



Why the Language Divide Persists

The Cyber Resilience Board Oversight Toolkit reveals that many organizations still treat cybersecurity as a subset of IT rather than a strategic pillar of enterprise risk.

This creates a hierarchical and linguistic divide:

Oversight Domain	Typical Language Used	Common Gap
Board & Executives	Strategy, risk appetite, capital allocation, governance	Can't interpret technical controls in financial terms
Risk & Audit	Frameworks, assurance, compliance	Metrics not linked to resilience or outcomes
ICT & Security Teams	Firewalls, patches, logs, vulnerabilities	Technical detail without strategic context

Without a translator between these groups, data is lost in translation not because it's missing but because it's miscommunicated.





From Confusion to Coordination: The Cybercare Solution

To bridge this divide, Serianu developed Cybercare, powered by the CVEQ Framework (Cyber-risk Visibility & Exposure Quantification), a system designed to harmonize how organizations measure, discuss, and report on cyber resilience.

into the language of business risk and resilience. It aligns oversight (board), management (executives), and operations (CISO/IT) under one quantifiable model turning technical performance data into measurable indicators that boards and regulators can govern.

Cybercare translates complex cyber metrics

At its core, the CVEQ Framework divides the cyber resilience journey into four leadership phases:

Phase	Leadership Role	Focus	Outcome for the Board
 Prepare	Chief Risk Officer	Identify and map digital and data risk.	Visibility of critical assets and exposures.
 Reduce	Chief Information Officer	Implement controls and compliance programs.	Evidence that exposures are being reduced.
 Detect	Chief Information Security Officer	Monitor and respond to threats.	Confidence that detection and response mechanisms work.
 Quantify	Board of Directors	Measure, report, and oversee resilience outcomes.	Strategic insight to guide investment and accountability.



This framework ensures that every operational activity from patching and awareness training to vendor risk management generates measurable indicators that roll up to the board's quantified resilience dashboard.

In essence, Cybercare turns cybersecurity data into board-ready evidence.

Creating a Common Language for Resilience

The Cyber Resilience Board Oversight Toolkit outlines ten CVEQ Indicators that form the foundation of this common language including Profile, Maturity, Visibility, Compliance, Vulnerability, Threat, Continuity, Third-Party, User Literacy, and Resilience indicators.

These indicators allow directors to see how cyber programs perform, how mature they are and whether they're truly reducing exposure. For example:

- **Profile Indicators** define what matters most: data, assets, and business processes.
- **Visibility Indicators** ensure the board can "see" where vulnerabilities exist.
- **Resilience Indicators** answer the question every director asks: "If this happens again, will we survive?"

When used together, these metrics translate technical performance into strategic assurance. They give the board a single, coherent view of cyber resilience in the same way financial dashboards summarize performance.

Closing the Divide: A Call to Action for Leaders

Bridging the language divide is not about learning technical jargon, it's about aligning expectations.

Boards should:

- Demand quantified reporting - not technical slides but risk-based metrics tied to business impact.
- Embed cyber resilience into enterprise risk management, treating it like financial governance.
- Encourage a culture of measurable assurance, where every executive can explain not just what controls exist, but how well they perform.

Executives should:

- Translate operational data into confidence indicators not activity reports.
- Connect technology investments directly to risk reduction outcomes.
- Foster collaboration between Risk, ICT, and Audit to eliminate siloed reporting.

Regulators should:

- Encourage organizations to adopt standardized frameworks like CVEQ for resilience measurement.
- Focus supervision on resilience performance, not just compliance checklists.
- Promote data-driven collaboration between supervised institutions and insurers.



The Bottom Line

Cyber resilience is no longer a technical function; it's a language of leadership. It's how boards demonstrate accountability, how regulators build trust and how organizations secure their digital future.

The Cyber Resilience Board Oversight Toolkit and the Cybercare Platform provide the bridge, turning

confusion into coordination, data into decisions and oversight into confidence.

When leaders and technologists finally speak the same language, resilience becomes measurable, confidence becomes visible and cybersecurity becomes governance not guesswork.





Industry Player Perspective

Telecommunications

By Joan G Mburu,
Chief Information Security Officer, Airtel Kenya



Kenya's Expanding Threat Landscape

Cybercrime continues to grow, with Cyber Crime Magazine estimating its global cost at 10.5 trillion US dollars in 2025, making it the world's third-largest economy after the USA and China. Checkpoint's Global Threat Intelligence Report places Kenya as the second most targeted country in Africa after Angola.

Kenya's leadership in digital financial services contributes to this exposure. The Communications Authority (CA) reports a 91% mobile-based financial services penetration rate and an internet penetration rate of 40.8%, driven mainly by mobile access. This growth has expanded the threat surface. According to KE-CIRT/CC, 4.5 billion cyber threat events were recorded between April and June 2025, an increase of over 80% in three months.

Key attack types include ransomware, Distributed Denial of Service, financial fraud, identity theft, cyberbullying, data breaches, and the spread of false information. Successful attacks result in financial losses, lawsuits, regulatory penalties, operational downtime, and significant reputational damage.

91%

mobile-based financial
services penetration rate

40.8%

internet penetration rate



4.5 B

cyber threat events were
recorded between **April
and June 2025**

over 80%

increase in three months



AI is now used by both defenders and attackers. Organizations are applying AI to automate routine work, enhance threat detection, and improve incident response. Meanwhile, cybercriminals use AI to scale attacks. The dark web hosts ready-made attack tools, including ransomware kits, phishing-as-a-service, and DDoS-as-a-service. Accessible AI platforms are also being used to create deepfakes that fuel false information across social media.

Awareness is essential. Employees and the public must learn how to recognize AI-driven threats. At the same time, organizations need to integrate AI responsibly into their cybersecurity strategies, ensuring human oversight remains central.

Cyber risk is inherent and requires continuous monitoring and leadership commitment. Regular review, enhancement, and reporting of security controls strengthens an organization's ability to protect its critical assets and remain resilient through detection, response, and recovery.

Insights from the Africa Cyber Defense Forum 2025 in Kigali highlight the need for stronger pan-African collaboration, building digital sovereignty, aligning legal and policy frameworks, investing in skills, promoting local solutions, deepening public-private partnerships, and reinforcing digital trust and rights.





Industry Player Perspective

Logistics and Supply Chain

By Dennis Musyoka Katusya
Manager - Technology Service Delivery,
Mitchell Cotts Group



Harnessing AI for security resilience

Artificial intelligence is revolutionizing the world we live in, and one area where its impact is particularly significant is cybersecurity.

Both AI and cybersecurity are crucial for the modern logistics industry, driving efficiency and safeguarding operations against evolving threats across the global supply chain. Efficient and effective operations is utmost importance in the modern competitive world.

These operations are all connected, and technology plays a critical role. With technology and data, comes cybersecurity. The era of AI has just enhanced on how to deal with cyber-attacks and breaches.

With the rapid advancements in technological, and the sophistication of cyber-attacks, technology indeed has

made AI an invaluable tool in combating cyber breaches. AI's future in cyber security is exciting, with room for growth and new ideas.

The adoption of logistics and supply chain management best practices and technology emerges as a strategic move to deliver significant value to businesses. Automation in logistics encompasses everything from automated warehouses to self-driving delivery vehicles. This is taken further through integration of ERP, WMS and TMS system to offer greater visibility on how orders are processed, managed and delivered.



For above to take place, we need secure systems within the supply chain process thus the need of advancements like AI to enable smooth flow of goods and services. Some of the key impacts of AI on cybersecurity in logistics sector include.

1. Including AI in your cyber security strategy will be crucial in its journey to become more digitally resilient.
2. Early threat detection – AI can be used to find threats and possible attacks and prevent the occurrence thus preventing disruptions to supply chain.
3. Vulnerability management – AI can make it easier to find bugs in software by automating trouble shooting processes. This will allow teams to fix issues before causing more harm.
4. User authentication – Use of AI can strengthen user authentication process by monitoring and analysing user behaviour and pattern.



08

SECTION 8



ANATOMY OF AN AI-POWERED
CYBER ATTACK



Section 8: Anatomy of an AI-Powered Cyber Attack

Introduction

Cyber attacks follow a predictable sequence of steps. Attackers begin from outside the organisation, study the target, find a weakness, break in, quietly move through internal systems and eventually carry out actions that cause financial loss, data exposure, or operational disruption. Today, these steps are increasingly strengthened by AI-powered social engineering, which makes attacks more personalised, more convincing and harder to detect.

1. Attacker Initial Approach

The attacker begins by gathering information and probing systems. They scan public-facing infrastructure, probe for vulnerabilities and collect data on employees and vendors. This phase often includes phishing, vishing and other social engineering attempts now enhanced through AI-generated emails, cloned voices, and synthetic messages that closely mimic internal communication styles. AI enables attackers to craft highly tailored lures that dramatically increase the likelihood of a successful initial compromise.

2. Compromise and Network Entry

Using insights from reconnaissance, the attacker attempts to gain access. This may happen through stolen passwords, phishing emails, exploiting unpatched systems or collaboration with a malicious insider. Here again, attackers employ deepfake voice calls, AI-generated executive instructions and realistic fake documents to trick employees into approving access or divulging credentials. These AI-supported techniques significantly raise the success rate of entry into internal systems.

3. Internal Movement and Persistence

Once inside, attackers move laterally between systems, escalate privileges, harvest credentials and identify high-value targets such as Active Directory, databases, core banking or endpoints. While this stage is primarily technical, AI assists attackers by automating reconnaissance, generating scripts and mimicking normal user behaviour to avoid detection. This reduces the chances that traditional monitoring tools will identify unusual activity.

4. Command and Control (C2)

The attacker establishes a secure communication channel to their remote infrastructure. Through this C2 path, they exfiltrate data, receive commands and maintain persistence using cloud-hosted servers, proxies, and tunnelling tools. AI plays a supporting role here by creating adaptive, self-modifying malware and synthetic traffic patterns, making malicious communications appear legitimate.

5. Impact and Monetization

Finally, the attacker executes actions that cause business harm: fraud, data theft, ransomware, extortion, system disruption, or manipulation of ERP and financial systems. Increasingly, attackers leverage AI-fabricated evidence, deepfake video or voice extortion attempts and AI-generated data samples to pressure organisations into paying ransoms or approving unauthorized transactions. These techniques make the impact phase more damaging and more deceptive than ever before.

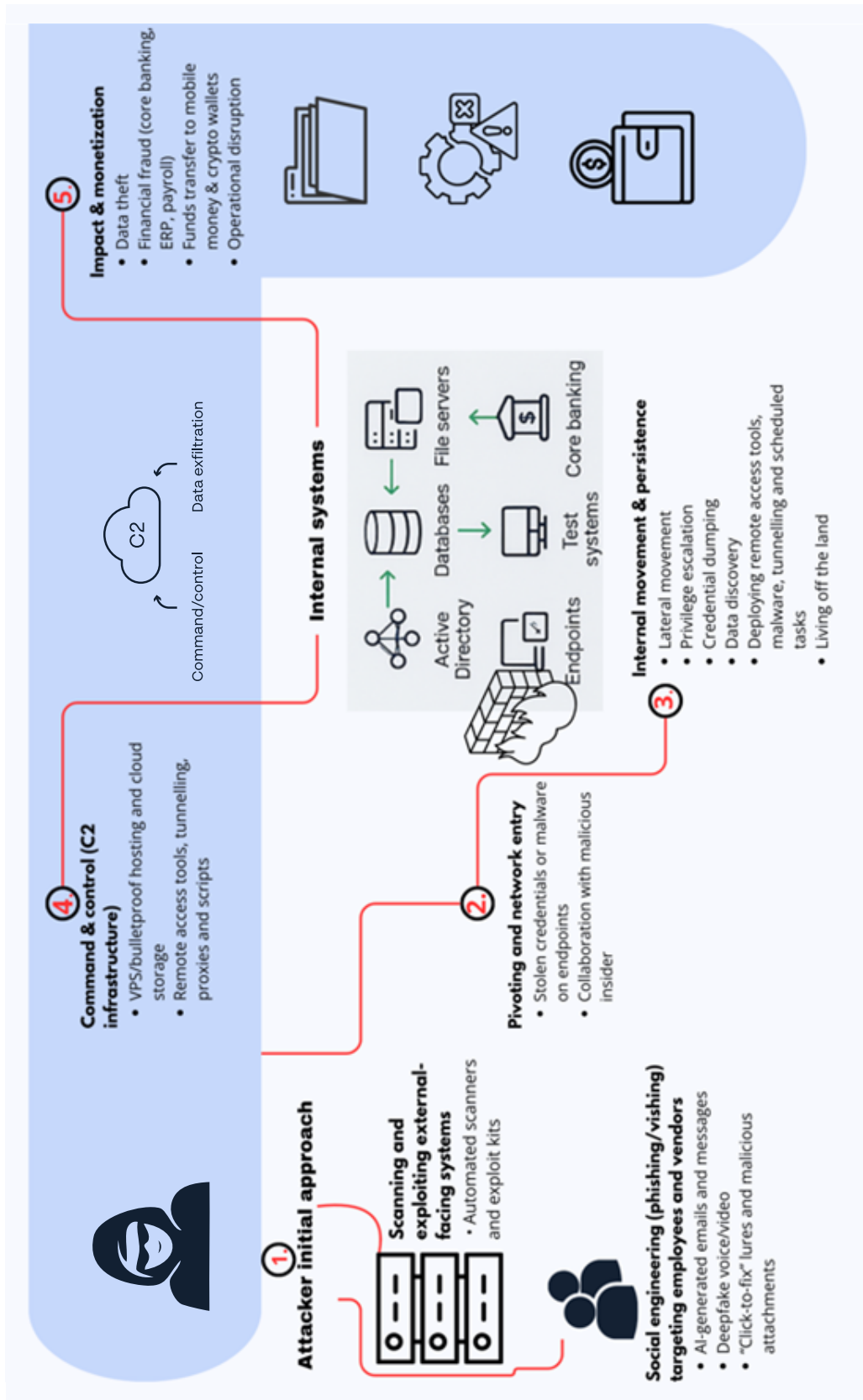
Conclusion

The five stages show how a cyber attack progresses from reconnaissance to impact and how AI-powered social engineering now amplifies every step, particularly the early phases of deception and the final stages of fraud and extortion.

Understanding both the traditional attack path and the new AI-enabled enhancements is essential for building strong defences and improving organisational resilience.



Anatomy of an AI-Powered Cyber Attack



Industry Player Perspective

Hospitality

By Deborah Mutungi
Group IT Manager, Sarova Hotels and Resorts



The more things (technologies, economies) change, the more things remain the same!

Human readiness and moving with, as well as integrating technological advancements, have always been how we manage cyber threats.

The theme "From Risk to Resilience: AI and the Future of Cyber Risk Management " is both timely and vital for the hospitality industry. As we adopt AI to enhance guest experiences through dynamic pricing, predictive analytics, and hyper-personalized services, we are also introducing new layers of cyber exposure.

AI-powered chatbots, smart room technologies, and digital concierge systems rely on continuous data collection, much of it personal and sensitive. These tools improve convenience and efficiency but also expand the potential attack surface for cyber threats. In a sector built on trust, even a minor data breach can have long-lasting reputational and financial consequences.

Moving forward, the focus must shift from reactive risk management to proactive resilience. In practice, most hospitality operators leverage vendor-supplied AI tools rather than building their own machine learning models. These systems can detect anomalies or suspicious activity when properly integrated, but their effectiveness depends heavily on data quality, system tuning, and ongoing governance.

Human factors remain central to effective cyber risk management. Regular staff training, clear processes, and strong collaboration between IT, operations, and security leaders are essential to ensure that technology enhances, rather than compromises, the guest experience.



True resilience, therefore, combines smart tooling with human readiness. By prioritizing both technological and human readiness, hospitality establishments can build trust, protect their reputation, and ensure that innovation delivers sustainable value.

All these remain a vicious cycle that we must navigate every single second, every day of the year!



Industry Player Perspective

Media

By Mercy Kimani
Head of IT, Nation Media Group



AI and the Shifting Cyber Threat Environment

Artificial Intelligence (AI) is transforming every layer of cyber risk management. Organizations that fail to integrate AI into their security and response strategies risk falling behind as threats grow more advanced. AI now strengthens defense capabilities while simultaneously enabling more adaptive and targeted attacks creating a dual challenge for security teams.

The Evolving Threat Landscape

AI and machine learning have pushed cyber threats into highly sophisticated, scalable operations. Social engineering attacks are increasingly convincing, polymorphic malware continues to bypass traditional detection, and the misuse of large language models (LLMs) for exploit creation is rising worldwide.

In the media sector, these challenges are especially sensitive. The industry's role in informing the public means that any compromise affects not only systems but credibility and trust. AI-generated false information and deepfake content are being used to manipulate audiences and undermine brand integrity. Automated bots distort narratives, while AI-enabled phishing and impersonation attacks increasingly target journalists, creators, and public personalities. Even AI-driven tools used inside media organizations such as recommendation engines, analytics platforms, and content production systems are being manipulated to skew engagement or corrupt data.



AI and the Future

Cyber risk strategies must now assume that every organization will be targeted. This requires AI-enabled controls that prevent, detect, and contain threats before they succeed. Priority actions include:

- Utilisation of AI-driven Security Operation Centres (SOCs) to automate triage, correlate threat intelligence thus reducing the detection-response time (MTTD & MTTR).
- Adopt 'Zero-trust' architecture for content workflows
- implement AI watermarking to counter deepfakes and manipulated content.
- Improve awareness through the use of AI-generated phishing simulations and tabletop exercises to train staff on how to identify these unique and near-real tactics.

- Adoption of Passwordless authentication and enforcement of Multifactor Authentication (MFA) to reduce credential compromise. Systems that cannot support MFA should be replaced or supplemented with additional controls.

From Risk to Resilience

Traditional risk management focuses on prevention and mitigation. Resilience goes further, requiring anticipation, rapid response, and fast recovery. The question is no longer if an attack will happen, but how quickly an organization can respond and restore operations.

Strong resilience depends on automated, predictive defenses supported by alignment across content, IT, and security teams. The goal is to protect content integrity, maintain operational continuity, and recover swiftly when disruption occurs.



Resilience is about bouncing back...
fast and efficiently!

Industry Player Perspective

Risk Management

By Catherine Nyaga-Mbithi

Co-Chair, Institute of Risk Management, East Africa Group and
Internal Audit Manager, ABSA Life Assurance, Kenya



From Risk to Resilience: Safeguarding Kenya's Digital Future

On a quiet morning in Kirinyaga, 70-year-old Alex tried to register for Kenya's new Social Health Authority (SHA), the replacement for the National Hospital Insurance Fund (NHIF). The process was supposed to be simple dial *147#. After repeated failures, he abandoned the attempt. Later, three strangers posing as SHA officials arrived at his home. Trusting them, he paid a small registration fee and shared his bank details. By evening, his savings had vanished and loans from digital lending apps had been taken in his name.

His experience is now common across the country, reflecting how Kenya's rapid digital growth has created new openings for cybercriminals. The Communications Authority of Kenya (CAK) recorded a sharp rise in cyber threats in Q3 2025, including ransomware, Distributed Denial of Service (DDoS) attacks, social engineering, Advanced Persistent Threats (APTs), supply chain breaches, zero-day exploitation and Artificial Intelligence (AI)-assisted threats such as deepfakes.

AI continues to accelerate digital innovation, yet the same technology introduces risks due to the scale of data it depends on and the complexity of its algorithms. Manipulation, system compromise and bias now form part of the modern threat landscape. For institutions, resilience requires broadening cyber risk management beyond traditional networks to include ethical, transparent and accountable deployment of AI systems.



Strong governance is the first layer of defense. Boards must set clear policies, reinforce accountability and ensure cybersecurity aligns with business objectives. Having members with Information Technology (IT) and cybersecurity expertise enhances oversight and decision-making.

Organizations should adopt risk-based frameworks built on thorough assessments. Automated detection and response systems are essential for real-time visibility, helping teams act quickly when threats emerge. Cybersecurity must also be treated as a driver of business confidence, not a compliance formality. Regular awareness programmes ensure that every staff member not only IT personnel contributes to responsible digital behaviour.

Continuous improvement remains key: monitoring controls, conducting vulnerability assessments, performing penetration tests and maintaining a strong incident response plan. Strengthening security across third-party partners is equally critical, as supply chain weaknesses often open the door to attacks. Cyber insurance can help absorb residual financial losses.

Managing AI risks calls for organizational maturity and preparedness. AI maturity starts with awareness understanding new threats and investing in national education. In Kenya, closer cooperation between government and the private sector will be essential for prevention and early intervention.

Technology readiness requires adopting AI-supported defenses and building leadership capacity to interpret and apply these tools responsibly. Human judgement must remain at the center to ensure AI strengthens rather than weakens security.

Ultimately, AI mirrors the values of the people deploying it. Kenya's digital future depends not just on how quickly new systems are adopted, but on how carefully citizens, businesses and government protect those using them. If innovation is paired with trust and accountability, future users like Alex will engage with digital services confidently rather than fearfully.

09

SECTION 9



2026 PRIORITY AND FOCUS AREAS



Section 9: 2026 Priority and Focus Areas

Top Priorities and Focus Areas for 2026

Introduction

As African organizations shift from traditional cybersecurity to enterprise-wide cyber resilience, one fact has become clear: technology teams can't secure the business alone. Cyber resilience requires shared responsibility across risk, IT, security, audit and governance functions. The ACSR (Africa Cybersecurity Report) Priority Model translates the emerging 2026 cyber threat landscape, including AI risks, cloud expansion, third-party dependencies and evolving regulatory expectations into practical, role-specific action areas for:

- Chief Risk Officer (Risk Operations)
- Chief Information Officer (IT Operations)
- Chief Information Security Officer (Security Operations)
- Board & Executive Leadership
- Chief Audit Executive (Internal Audit)

These priorities ensure that every leader contributes to reducing exposure, strengthening controls, improving detection, enabling resilience and providing independent assurance. The goal is simple: clarity of responsibility, clarity of action and clarity of accountability.





1. RISK MANAGEMENT (CRO & Risk Operations)

The CRO is responsible for ensuring the organization understands its digital, operational, data, third-party, and emerging AI-related risks before these risks cause harm. Risk Operations must translate technical threats into business-level exposures, ensure regulatory compliance and provide clear reporting to executive leadership and the Board.

PRIORITY 1: Establish Strong AI Governance

Why This Priority Matters

AI tools, especially public tools like ChatGPT, DeepSeek, Gemini and others are being used everywhere in organizations often without approval. Staff unknowingly upload private or confidential information into these systems. Uncontrolled AI use leads to:

- Serious data leakage
- Incorrect or biased decisions being made without review
- Regulatory violations
- Loss of intellectual property

The CRO must ensure that AI is safe, controlled and used responsibly.

3 Steps to Get Started

1. Identify all AI tools used in the business - both approved and unapproved.
2. Create a simple, organization-wide AI policy explaining safe and unsafe use.
3. Establish a small AI oversight group to review new AI use cases.

PRIORITY 2: Strengthen Data Protection & Privacy Risk Management

Why This Priority Matters

Data protection laws across Africa are expanding and enforcement is increasing. Organizations now handle massive amounts of personal, financial, biometric and transactional data. Privacy failures lead to:

- Regulatory fines
- Loss of customer trust
- Brand damage
- Financial losses

The CRO must ensure privacy is not a compliance tick-box but a core risk area.

3 Steps to Get Started

1. Map what personal data is collected, where it lives and who has access.
2. Remove unnecessary data, reducing exposure significantly.
3. Ensure sensitive data is encrypted and protected in key systems.



PRIORITY 3: Understand Third-Party and Ecosystem Risk

Why This Priority Matters

Most African organizations rely heavily on external partners: fintech systems, cloud providers, payment processors, CRM vendors, telco APIs, etc. A breach in any partner can expose your entire organization. Third-party breakdowns now cause more breaches than internal failures.

3 Steps to Get Started

1. List all vendors and classify them into high, medium and low risk.
2. Request basic security evidence from high-risk partners (audit report, certificate, policy).
3. Add mandatory security requirements into new and existing contracts.

PRIORITY 4: Use Realistic Cyber Risk Scenarios

Why This Priority Matters

Leaders must understand “what could go wrong” in simple business terms. Scenarios such as ransomware, business email compromise, payment fraud, insider theft and misuse of AI tools help the business plan effectively instead of reacting blindly during a crisis.

3 Steps to Get Started

1. Select 3 - 5 realistic cyber scenarios relevant to your sector.
2. Estimate financial and operational impact for each scenario.
3. Discuss these with executive teams to align mitigation priorities.

PRIORITY 5: Monitor Cyber Risks Continuously

Why This Priority Matters

Cyber risk changes daily. Traditional annual risk reviews are no longer sufficient. Leaders need continuous visibility into key indicators such as access anomalies, system changes, expired certificates, cloud misconfigurations and third-party outages.

3 Steps to Get Started

1. Define a small set of cyber risk indicators.
2. Set thresholds that trigger alerts or escalation.
3. Review these indicators regularly in risk committee meetings.



2. CONTROL MANAGEMENT (CIO & IT Operations)

The CIO is responsible for the organization's technology foundation, ensuring systems, data, applications, cloud platforms, and infrastructure are secure, reliable and designed with resilience. The CIO directly influences exposure through the quality of technical controls.

PRIORITY 1: Modernize Identity & Access Controls

Why This Priority Matters

In Africa, the most common type of breach involves stolen or weak passwords. Identity is the new "front door" to the organization. Without strong access controls, attackers can quickly enter systems and move freely.

3 Steps to Get Started

1. Enforce multi-factor authentication across all important systems.
2. Remove unused or old accounts, especially admin accounts.
3. Conduct quarterly user access reviews.

PRIORITY 2: Strengthen Cloud, Application & Data Security

Why This Priority Matters

Cloud misconfigurations remain the leading cause of data exposure. Applications and APIs are being built faster than they are being secured. Sensitive data is often stored incorrectly.

3 Steps to Get Started

1. Review cloud setups to ensure nothing sensitive is publicly exposed.
2. Classify data to identify what is sensitive and needs extra protection.
3. Secure APIs by safeguarding keys, tokens, and system credentials.

PRIORITY 3: Automate Patch & Vulnerability Management

Why This Priority Matters

Most cyberattacks exploit known weaknesses for which patches already exist. Manual patching is too slow and inconsistent. Automation drastically reduces exposure.

3 Steps to Get Started

1. Identify systems without automated update processes.
2. Create a patching calendar starting with the most critical systems.
3. Track patch progress and identify systems that always fall behind.

PRIORITY 4: Measure Control Performance Continuously

Why This Priority Matters

Security controls fail quietly. Many breaches occur because an important control silently stopped working. Continuous monitoring gives early warning.

3 Steps to Get Started

1. Choose 5 - 7 key security metrics (e.g., encryption rate, update rate).
2. Assign ownership for each metric.
3. Track and report these metrics monthly.



PRIORITY 5: Strengthen Vendor & Technology Integration Security

Why This Priority Matters

Integrations with vendors, APIs and third-party systems are now the weakest link. A breach at a small partner can compromise a large organization.

3 Steps to Get Started

1. Review all supplier access paths and integrations.
2. Request security documentation from critical vendors.
3. Add security terms to procurement and vendor contracts.





3. THREAT MANAGEMENT (CISO & Security Operations)

The CISO leads the teams responsible for detecting, investigating, and responding to threats. The goal is simple: spot attacks early, contain them quickly, and prevent business disruption.

PRIORITY 1: Build a Modern SOC with Better Threat Visibility

Why This Priority Matters

Attacks move at machine speed, while many organizations detect incidents too late. A modern SOC improves visibility, reduces noise, and highlights real threats.

3 Steps to Get Started

1. Consolidate alerts into one monitoring tool.
2. Enable behavioral monitoring for unusual activity.
3. Use dashboards to track high-risk events.

PRIORITY 2: Document Processes Before Automation

Why This Priority Matters

Automation only works when processes are consistent. If playbooks are unclear or undocumented, automation fails and often magnifies the problem.

3 Steps to Get Started

1. Write down the step-by-step processes for common incidents.
2. Train security staff to ensure consistent execution.
3. Identify parts that could later be automated.

PRIORITY 3: Monitor External Exposure & Threat Intelligence

Why This Priority Matters

Attackers often exploit public-facing weaknesses: exposed databases, forgotten domains, weak APIs, or leaked passwords. Understanding exposure reduces surprise attacks.

3 Steps to Get Started

1. Conduct routine external scans.
2. Subscribe to simple threat intelligence sources.
3. Review high-risk exposures monthly.

PRIORITY 4: Control Shadow AI & Shadow IT

Why This Priority Matters

Staff frequently use unapproved apps and AI tools. This can cause data leakage and compliance violations.

3 Steps to Get Started

1. Monitor for unapproved AI or software use.
2. Offer approved tools or safer alternatives.
3. Block high-risk tools and sites.



PRIORITY 5: Contain Attacks Quickly Using Zero-Trust Principles

Why This Priority Matters

When attackers get in, they move horizontally to other systems. Zero-trust reduces the blast radius and prevents widespread damage.

3 Steps to Get Started

1. Separate networks by department or sensitivity.
2. Limit movement between systems.
3. Isolate suspicious devices immediately.





4. RESILIENCE MANAGEMENT (Board & Executive Leadership)

Cyber resilience is ultimately a governance-level responsibility. Boards must ensure that strategy, funding, oversight and accountability support the organization's ability to withstand, recover from and continue operating during cyber incidents.

PRIORITY 1: Provide Oversight for Cyber Resilience Strategy

Why This Priority Matters

Cyber resilience is no longer a technical discussion. It is a business survival issue. Boards must ensure the organization has a clear plan and the required resources.

3 Steps to Get Started

1. Request a documented resilience strategy.
2. Include cyber resilience as a standing Board agenda item.
3. Approve required funding for critical resilience capabilities.

PRIORITY 2: Demand Proof of Backup & Recovery Capability

Why This Priority Matters

Most organizations assume they can recover from an attack but have never tested it. Boards must verify recovery capability, not accept verbal assurances.

3 Steps to Get Started

1. Require quarterly recovery demonstrations.
2. Ensure backups cannot be tampered with (immutability).
3. Request evidence showing recovery time performance.

PRIORITY 3: Participate in Cyber Crisis Simulations

Why This Priority Matters

Cyber crises require fast, coordinated decision-making. Executives and Boards must practice together to avoid confusion during real incidents.

3 Steps to Get Started

1. Schedule one cyber crisis simulation each year.
2. Involve business, IT, security and major vendors.
3. Review lessons learned and enforce follow-up actions.

PRIORITY 4: Strengthen Third-Party Resilience

Why This Priority Matters

Organizations depend on ecosystems. If key vendors fail, your business fails even if your systems are secure.

3 Steps to Get Started

1. Request a list of critical vendors and their resilience status.
2. Require joint recovery simulations with key partners.
3. Ask to see vendor recovery evidence and SLAs.



PRIORITY 5: Receive Simple, Non-Technical Resilience Reporting

Why This Priority Matters

Boards cannot govern what they do not understand. Reports must be business-friendly, simple, and focused on impact.

3 Steps to Get Started

1. Define 5 - 7 resilience metrics (e.g., time to recover).
2. Require quarterly reporting using these metrics.
3. Ensure reports avoid technical jargon and use business language.





5. ASSURANCE MANAGEMENT (CAE & Internal Audit)

Internal Audit provides independent oversight, validating whether management's controls are functioning and whether the organization is genuinely resilient not just confident.

PRIORITY 1: Provide Independent Oversight of AI Governance

Why This Priority Matters

AI introduces risks that are often invisible to management. Internal Audit must validate that AI is controlled, safe, explainable, and compliant.

3 Steps to Get Started

1. Audit existing AI tools and usage patterns.
2. Verify controls to prevent data leakage.
3. Ensure AI decisions can be traced, explained and justified.

PRIORITY 2: Audit Data Protection & Privacy Implementation

Why This Priority Matters

Many organizations have privacy policies but do not implement them effectively. Audit must test whether privacy controls work in practice.

3 Steps to Get Started

1. Test whether sensitive data is properly minimized or encrypted.
2. Verify data retention and deletion processes.
3. Review high-risk data processes for compliance gaps.

PRIORITY 3: Test Cyber Resilience & Business Continuity Realistically

Why This Priority Matters

Management often overestimates recovery capability. Internal Audit must verify resilience through real testing, not assumptions.

3 Steps to Get Started

1. Conduct an independent restore test.
2. Review crisis logs and past incident responses.
3. Validate reliability of DR simulations.

PRIORITY 4: Validate Continuous Monitoring Data

Why This Priority Matters

Continuous monitoring is only valuable if the data is accurate. Audit must confirm that automated checks are complete and reliable.

3 Steps to Get Started

1. Test samples of automated monitoring results.
2. Verify completeness and accuracy of dashboard data.
3. Escalate inconsistencies to management for remediation.



PRIORITY 5: Assess Third-Party Cyber Risk Controls

Why This Priority Matters

Third-party risks are now the biggest source of cyber incidents. Audit must provide assurance that vendor controls are adequate.

3 Steps to Get Started

1. Review contracts for strong security clauses.
2. Test vendor access paths (APIs, remote access).
3. Audit high-risk vendors annually.



Industry Player Perspective

Sacco Industry

By Robert Kariuki Mogoi,
Chairman, Sacco IT Professionals Association (SITPA)



The SACCO industry in Kenya continues to experience rapid digital transformation, driven by member expectations for instant services, mobile access, and integrated financial solutions. This evolution has simultaneously expanded the industry's threat landscape, exposing SACCOs to increasingly sophisticated cyberattacks. Key risks include social engineering, malware targeting core banking systems, fraud in mobile lending channels, and vulnerabilities in third-party integrations.

As an industry that serves millions of members, many of whom rely on SACCOs as their primary access point to financial services, disruptions have far-reaching socio-economic consequences. Cyber incidents not only jeopardize financial stability but erode trust, which is the core currency of cooperative societies.

However, the emergence of AI offers a powerful opportunity to shift from reactive risk management to proactive resilience. SACCOs are strategically positioned to benefit from AI-driven capabilities such as:

- Real-time anomaly detection to flag unusual account behaviour
- Enhanced fraud analytics that learn from transaction patterns
- AI-powered member authentication, reducing reliance on static credentials
- Automated incident response that accelerates containment and mitigation

While AI introduces new complexities including ethical concerns, model transparency, and data governance, it also marks a turning point in Kenya's cyber preparedness journey. For SACCOs, the imperative is clear: adopt a resilience posture that integrates AI responsibly, strengthens risk culture across all levels, and invests in continuous capacity-building for staff.

To truly benefit from AI, SACCOs must foster cross-industry collaboration, harmonize standards, and encourage real-time threat intelligence sharing. When combined with regulatory alignment and member education, these efforts will help transform SACCO cybersecurity from a siloed defence into a collective shield.



Industry Player Perspective

Development Cooperation

By Amrit Singh Labharam,
Kenyan-German Digital Dialogue Advisor at the GIZ
Digital Transformation Centre Kenya.



As Kenya accelerates its digital transformation, Artificial Intelligence (AI) is redefining both opportunity and risk. For the GIZ Digital Transformation Centre (DTC) Kenya, AI represents a powerful tool to strengthen national cyber resilience, while also demanding renewed focus on ethics, accountability, and inclusion.

AI-driven analytics and automation offer a leap forward in detecting and responding to cyber threats, particularly for nations expanding their digital public infrastructure. Yet, as AI becomes integral to governance and service delivery, it also amplifies vulnerabilities, ranging from algorithmic bias to sophisticated automated attacks.

Addressing these challenges requires a human-centered and collaborative approach to cybersecurity. DTC Kenya works with the Ministry of Information, Communications and the Digital Economy (MICDE) and other partners to embed responsible AI use, align with global standards such as the EU AI Act, and adapt them to Kenya's local realities.

Building cyber resilience is ultimately a shared responsibility. It demands strong institutions, skilled talent, and trusted partnerships across government, private sector, and civil society. As development cooperation partners, we remain committed to advancing AI-enabled, inclusive, and secure digital ecosystems, by fostering innovation and ensuring protection evolve hand in hand.

Industry Player Perspective

Fintech

By George Kisaka
CEO & Co-Founder, hlola.io



The intersection of artificial intelligence (AI) and cybersecurity has become a defining moment for Africa's fintech sector. Digital financial services have expanded access across the continent, but they have also widened the attack surface. As FinTechs scale across borders, they must safeguard customer trust while navigating more complex, AI-enabled threats.

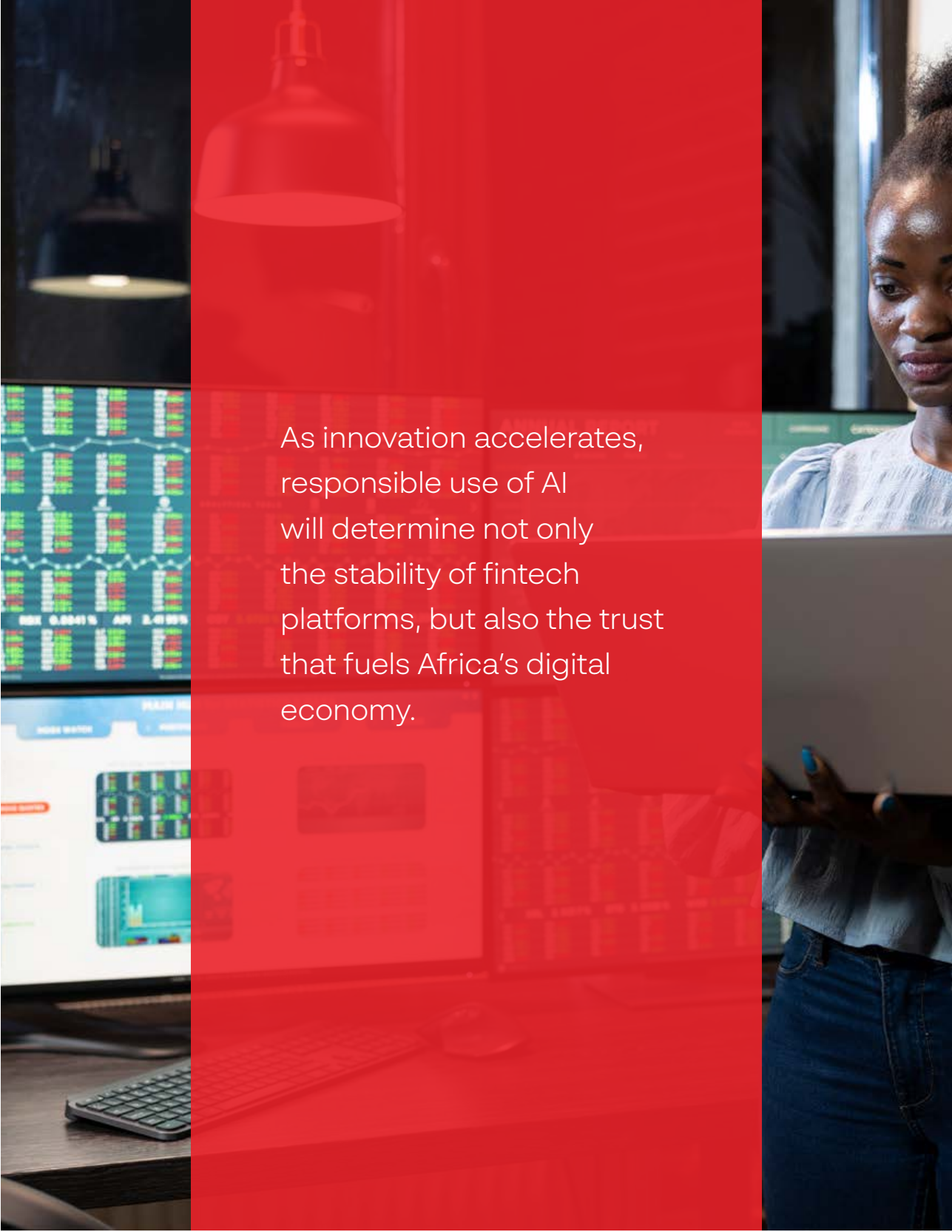
AI is shifting cyber risk management from reactive monitoring to predictive action. Machine learning models can detect anomalies in real time, automate response processes, and anticipate attacks through behavioural analysis. For FinTechs, this presents an opportunity to embed AI into risk frameworks as a driver of compliance, fraud prevention, and operational strength.

Yet the same technologies strengthening defences are being weaponised by attackers. Deepfakes, automated phishing, and AI-driven exploits require organisations to adopt a governance-first approach that balances innovation with ethical responsibility, transparency, and accountability.

At hlola.io, we view RegTech as the connector between compliance and innovation enabling organizations to implement, monitor, and demonstrate adherence to cybersecurity and data protection standards across jurisdictions. As AI continues to reshape the threat environment, the priority is not only preventing incidents but building resilient systems that support sustainable growth for FinTechs.

We believe the future of resilience in fintech aligns around three imperatives:

- 1. AI Governance:** Aligning cybersecurity programs with ethical AI principles, data protection, and model transparency.
- 2. Collaborative Intelligence:** Strengthening cooperation among regulators, financial institutions, and technology providers to share threat insights and harmonize expectations.
- 3. Human-Centric Design:** Developing skills, awareness, and leadership to ensure people remain central to secure, adaptable systems.



As innovation accelerates, responsible use of AI will determine not only the stability of fintech platforms, but also the trust that fuels Africa's digital economy.

10

SECTION 10



ABOUT CYBER SHUJAA



Section 10: Cyber Shujaa Program

Building Africa's Next Generation of Cybersecurity Professionals



Who We Are

Cyber Shujaa project is a youth focused program that is spearheaded Serianu Limited, Kenya Bankers Association (KBA), United States International University -Africa (USIU-A) and funded by Challenge Fund for Youth Employment (CFYE) based out of Netherlands.

Over the last 6 years we have engaged in a series of research activities to understand the gaps within ICT and Cybersecurity sector in Africa. The Cyber Shujaa program seeks to address the skills- gap challenge and is focused on continuously analysing the market and industry for ICT talent needs, designing practical curriculums for these needs, conducting vigorous training for the participants and market placement of these youth.

Since 2022, the program has equipped thousands of young Kenyans with industry-ready digital security skills, bridging the talent gap and strengthening the region's cyber resilience.

What We Do

Cyber Shujaa provides practical, market-driven training designed to prepare youth for employment in the cybersecurity and data protection sectors.

Our career-bridging model includes



hands-on training



mentorship



soft skills development



industry certification pathways



internship and job placements



entrepreneurship support for aspiring cyber innovators.



Our Training Tracks



Security Analyst
Program



Cloud & Network
Security



Data Protection



Data & AI



Ethical Hacking



Cybersecurity
Essentials



Soft Skills
Masterclass



Entrepreneurship
& Business
Development



Women-in-Cyber
Bootcamps

Our Success Thus Far



official launch
March 2022



5,349

individuals accepted into
the program



2,330

successful job
placements across
banking, tech,
government & consulting



3546

graduates with
certification (including
3358 youth)



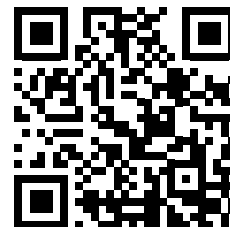
42

youth-led ventures

Join the 2026 Cohort

Applications for the 2026 intake are now open! Gain hands-on skills, access mentorship, and kick-start your cybersecurity career:

<https://bit.ly/cybershujaa-c1-2026>



**Let's connect &
bridge the gap
together**



info@cybershujaa.co.ke



@CyberShujaa

www.cybershujaa.co.ke



Appendix

Africa Data Protection Association. (2024, December). Africa Data Protection Report 2024. Africa Data Protection Association. <https://www.africadata.org/africa-data-protection-report-2024>

Allianz Global Corporate & Specialty. (2025). Allianz Risk Barometer 2025 – Appendix. AGCS SE. <https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer-2025.html>

African Union. (2020, February 9). The Digital Transformation Strategy for Africa (2020-2030). African Union. <https://au.int/en/documents/digital-transformation-strategy-africa-2020-2030>

Allianz Global Corporate & Specialty. (2025). Allianz Risk Barometer 2025 – Appendix. Allianz. <https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2025-cyber-incidents>

BoCERT. (2025). Cybersecurity Bulletins and Awareness Reports 2025. Botswana CERT. <https://www.bocert.bw>

Business Daily. (2025, September 21). How Raila deepfake exposes digital weak spot, sparks AI alarm. Business Daily. <https://www.businessdailyafrica.com/railadeepfake-ai>

CBK. (2025, September 22). Press Release: Establishment of Banking Sector Cyber Security Operations Centre (BS SOC). CBK. <https://www.centralbank.go.ke/cybersecurity-operations-centre>

Censys. (2025). Vulnerable Devices. Retrieved November 3, 2025, from <https://search.censys.io>

Central Bank of Kenya. (2025, July 3). Survey on Artificial Intelligence in the Banking Sector. Central Bank of Kenya. <https://www.centralbank.go.ke/ai-survey-banking-sector>

Check Point Research. (2025). Cyber Security Report 2025 – Global and Regional Threat Trends. Check Point Software Technologies Ltd. <https://research.checkpoint.com/2025/cyber-security-report-2025/>

CIO Africa. (2025, September 22). CBK Launches Banking Sector Cybersecurity Centre. CIO Africa. <https://www.cio.co.ke/cbk-launches-cybersecurity-centre>

Communications Authority of Kenya. (2024). Cyber Security Report Q1 2024/25 and Q1 2025/26. Communications Authority of Kenya. <https://www.ca.go.ke/cybersecurity-report-2024-25>

Cyber Attack Articles. (2025). Cyber Attack Articles. Retrieved November 3, 2025, from <https://google.com>

DataReportal. (2025). Digital 2025 Global Overview Reports. DataReportal. <https://datareportal.com/reports/digital-2025-global-overview>

Deloitte Nigeria. (2025). Cybersecurity Outlook 2025 – Nigeria. Deloitte Nigeria. <https://www2.deloitte.com/ng/en/insights/cybersecurity-outlook-2025.html>



Deloitte Nigeria. (2025). Cybersecurity Outlook 2025 – Nigeria. Deloitte & Touche, Risk Advisory Practice. <https://www2.deloitte.com/ng/en/pages/risk/articles/cybersecurity-outlook.html>

Check Point Research. (2025). Cyber Security Report 2025 – Global and Regional Threat Trends. Check Point. <https://www.checkpoint.com/cybersecurity-report-2025>

INTERPOL. (2025). Africa Cyberthreat Assessment Report 2025. INTERPOL. <https://www.interpol.int/en/How-we-work/Criminal-Intelligence/Africa-cyberthreat-report-2025>

INTERPOL. (2025). Africa Cyberthreat Assessment Report 2025. INTERPOL Africa Cybercrime Operations Desk. <https://www.interpol.int/en/Crimes/Cybercrime/Africa-Cyber-Threat-Assessment-Report>

International Telecommunication Union. (2025). ICT Facts and Figures 2025. ITU. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>

International Monetary Fund (IMF). (2025). World Economic Outlook – October 2025. IMF. <https://www.imf.org/en/Publications/WEO/Issues/2025/10/14/world-economic-outlook-october-2025>

International Telecommunication Union. (2025). *ICT Facts and Figures 2025*. ITU. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>

ISACA. (2024). Understanding the EU AI Act. ISACA. <https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act>

Kenyan Wall Street. (2025, September 22). Deepfake scam exploiting Raila Odinga's X account. Kenyan Wall Street. <https://www.kenyanwallstreet.com/deepfake-scam-railas-x>

KE-CIRT/CC. (2025). Quarterly and Annual Cybersecurity Reports (2024–2025). KE-CIRT/CC. <https://ke-cirt.go.ke/reports>

KE-CIRT/CC. (2025). Quarterly and Annual Cybersecurity Reports (2024–2025). Communications Authority of Kenya. <https://www.ke-cirt.go.ke/quarterly-reports>

Kaspersky. (2025). Africa Cyberthreat Landscape Report 2025. Kaspersky. <https://www.kaspersky.com/africa-cyberthreat-landscape-report-2025>

LCA. (2025). Cybersecurity and CERT Unit Updates 2025. LCA. <https://www.lca.org.cy/cybersecurity-updates>

Lesotho Communications Authority. (2025). Cybersecurity and CERT Unit Updates 2025. LCA. <https://www.lca.org.ls>

Ministry of ICT. (2025, April & September). Kenya AI Strategy 2025–2030; Strathmore CIPIT analysis. Ministry of ICT. <https://www.ict.go.ke/kenya-ai-strategy>

National Institute of Standards and Technology (NIST). (2025). AI Risk Management Framework (AI RMF 1.0) and Generative AI Profile. NIST. <https://www.nist.gov/ai-risk-management>

ngCERT. (2025). National Advisories and Incident Summaries 2025. ngCERT. <https://www.ngcert.gov.ng/reports>



ngCERT. (2025). *National Advisories and Incident Summaries 2025*. Office of the National Security Adviser – Nigeria. <https://www.cert.gov.ng>

NITA-U / CERT-UG. (2025). *National Cybersecurity Reports and Advisories*. National Information Technology Authority – Uganda. <https://www.nita.go.ug/nita/national-cert>

Project Honeypot. (2025). *Honeypot Data*. Retrieved November 3, 2025, from <https://www.projecthoneypot.org/statistics.php>

ResearchGate. (2025). *Generative Adversarial Networks (GAN) for Cyber Security Challenges and Opportunities*. <https://www.researchgate.net/publication/366962736>

Security Scorecard. (2025). *2025 Supply Chain Cybersecurity Trends*. Security Scorecard. <https://www.securityscorecard.com/supply-chain-cybersecurity-2025>

World Bank. (2025). *World Development Indicators 2025*. World Bank Group. <https://databank.worldbank.org/source/world-development-indicators>

Yellowcard. (2024, March). *2025 Report on Data Protection in Africa*. Yellowcard. <https://yellowcard.io/data-protection-report-africa-2025>

Zone-H. (2025). *Hacked Websites*. Retrieved November 3, 2025, from <https://zone-h.org>



[illegible]



W
F
C
Z

Kenya Office

14 Chalbi Drive, Lavington
P. O. Box 56966 - 00200, Nairobi



+254 (0) 20 200 6600

Botswana Office

Plot 54349, Office Block B
3rd Floor, CBD Gaborone

+267 77 820 039



info@serianu.com



[@serianultd](https://twitter.com/serianultd)



[Serianu Limited](https://www.linkedin.com/company/serianu-limited)