SERIANU

Africa Cybersecurity Report

Kenya, 2023

Reimagining the African Cybersecurity Landscape

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

SERIANU

Africa Cybersecurity Report

Kenya, 2023

Reimagining the African Cybersecurity Landscape

United States International University-Africa

ISACA Kenya Chapter

Africa Cyber Immersion Centre
Engage | Educate | Empower

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 specific industry ranking, cost of cybercrime and priority focus areas for organisations. The report pulls intelligence from numerous threat sensors, industry experts, regulators and professional associations and spans over 10 African countries.

Table of Contents

> 90% of CEOs believe the digital economy will impact their industry, but less than 15% are executing on a digital strategy.

MIT Sloan and Capgemini

1. Acknowledgements

In developing the Africa Cybersecurity Report - Kenya 2023, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;

The USIU-A's Centre for Informatics Research and Innovation (CIRI) at the School of Science and Technology has been our key research partner. They provided the necessary facilities, research analysts and technical resources to carry out the extensive work that made this report possible.

The ISACA-Kenya Chapter provided immense support through its network of members spread across the country. Key statistics, survey responses, local intelligence on top issues and trends highlighted in the report were as a result of our interaction with ISACA-Kenya chapter members.

We would like to single out individuals who worked tirelessly and put in long hours to deliver the document.

Co-Authors

→ Carol Muchai - Editor

→ Matthew Wanjohi - Researcher

→ Nabihah Rishad - Researcher, Cyber Insurance

→ Barbara Munyendo - Researcher

→ Brian Nyali - Researcher

→ Brenda Kamangara - Researcher

→ Agnes Chege - Data Analyst

→ Joy Victoria - Data Analyst

→ John Kuria - Data Analyst

→ Lorraine Malinda - Data Analyst

→ Natasha Muthusi - Data Analyst

Commentaries

→ **Shikoli Makatiani**

COO, Turnkey Limited

→ **Ann Gekaara**

SOC Professional

→ **Dr. Laibuta Mugambi**

Certified Information Privacy Manager

→ **Nabihah Rishad**

Product and Research Lead, Serianu Ltd

Building Data Partnerships

In an effort to enrich the data we are collecting, Serianu continues to build corporate relationships with like-minded institutions. We partnered with The Honeynet Project ™ and other global Cyber intelligence organisations that share our vision to strengthen the continental resilience to cyber threats and attacks. As a result, Serianu has a regular pulse on malicious activity into and across the continent. Through these collaborative efforts and using our Intelligent Analysis Engine, we are able to anticipate, detect and identify new and emerging threats. The analysis engine enables us identify new patterns and trends in the Cyber threat sphere that are unique to Africa.

Our Serianu CyberThreat Command Centre (SC^3) Initiative serves as an excellent platform in our mission to improve the state of Cybersecurity in Africa. It opens up collaborative opportunities for Cybersecurity projects in academia, industrial, commercial and government institutions.

For details on how to become a partner and how your organisation or institution can benefit from this initiative, email us at info@serianu.com

Design, Layout and Production: Tonn Kriation

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

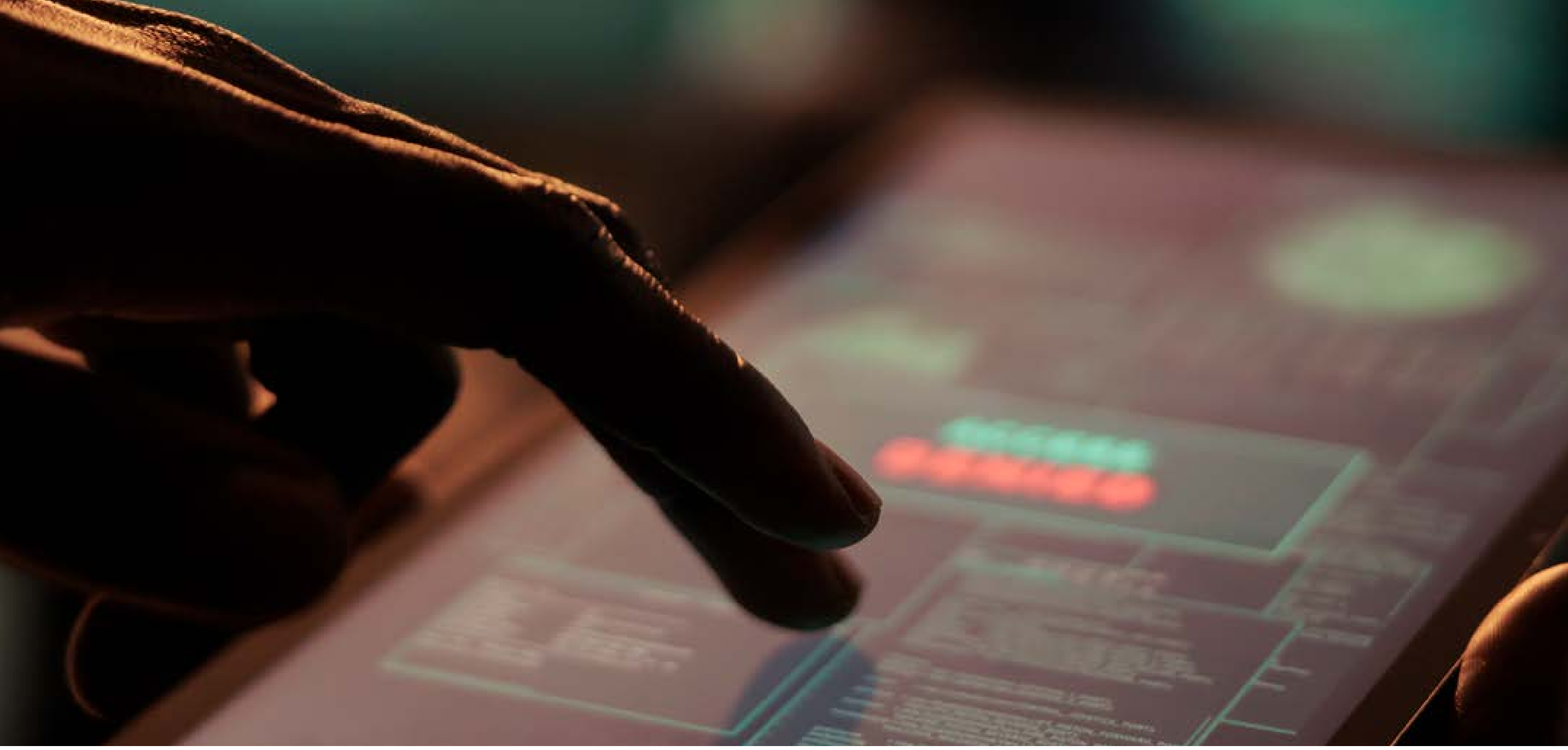
2. Introduction

In an era dominated by digital innovation and interconnectedness, the African cyber landscape stands at the crossroads of challenges and opportunities. As we unveil this year's annual cyber security report, we embark on a journey of reimagining the very fabric of cyber resilience across the continent, with a spotlight on Small and Medium Enterprises (SMEs).

The theme, "Reimagining the African Cyber Security Landscape," underscores the imperative to fortify our digital foundations, with a keen focus on the often-overlooked SME sector. This report delves into the intricate interplay of artificial intelligence, data privacy, and the burgeoning costs of cybercrime, offering insights that are not only timely but crucial for navigating the evolving cyber terrain.

Join us as we explore the transformative potential of proactive cyber strategies and pave the way for a secure and resilient future in the face of ever-evolving cyber threats.

> It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change.
>
> Charles Darwin



3. Editor's Note

Carolyne Muchai

Risk and Compliance Lead
Serianu Ltd

Aptly themed 'Reimagining the African Cyber Security Landscape', this latest report on the state of cyber security across the continent covers the key issues, threats and much more that everyone in information security and ICT should take note of.

The first section covers top cyber security threats, with ransomware, social engineering and phishing, advanced persistent threats and supply chain attacks coming as the initial four threats. The supply chain breaches have especially raised eyebrows as 9 out of 10 CEOs show their concern for third party organizations' vulnerability.

We have also outlined the top threat indicators of compromise that provide insights into the tools and employed by cyber criminals, essentially to help security practitioners recognize patterns. This includes details on the way attackers nest their malware in certain file types and shortcuts, with the latter experiencing a strong surge in 2023.

Financial services and loss of funds have maintained the lead as the most affected while insiders have also remained the biggest source of cybercrime. Mobile devices, despite facilitating higher digital penetration, emerged as the largest platform for financial fraud.

> The cyber intelligence section computes the number of vulnerabilities and exploits, with remote code execution emerging as the most preferred method that threat actors utilize to gain access to systems and infiltrate networks.

In addition to listing website attacks by country, we also provide an outline of the degree of exposure for devices in selected countries, where Morocco has surprisingly topped with 21 percent even though South Africa registered the highest number of devices connected online.

We have also outlined the IP addresses that originated the most attacks, including 41.212.30.91 that counted at least 43,750 attacks.

The report includes perspectives from industry players such as Mugambi Laibuta and Nabiha Rashid. The former discusses briefly the importance of compliance with the data protection law while the latter covers cyber insurance and what it entails for information security practitioners.

Furthermore, the document details two key initiatives that are run and involve Serianu. These are the highly successful Cyber Shujaa training program for students and working information security practitioners, as well as the proprietary Cybercare service.

Information theft is the most **expensive** and **fastest rising** **consequence** of **cybercrime.**

At the tail end, the report covers priorities for cyber security industry players in the new year and which include adopting risk-based threat exposure management frameworks to guide cybersecurity investment prioritization as well as simplifying cybersecurity management by adopting unified, single view and consolidated platforms among others.

Overall, this year's cyber security report is more detailed, pointing technical professionals to specific data and capturing the essence of the landscape in a way that shows the extent to which it needs to be reimagined if African organizations, particularly SMEs are going to make any significant headway in the drive to secure their cyber spaces.

4. Foreword

Joseph Mathenge
COO,
Serianu Ltd

Small and Medium Enterprises (SMEs) are a crucial part of contributing to Africa's socio-economic growth. These businesses anchor the economies of countries globally and in Africa play a key role in contributing to inclusive socio-economic growth.

In addition to employing people, they also supply products and services and act as an important link in the manufacturing value chain, generating economic activity along the way. Many manufactured products reach consumers through SMEs, usually through a network of small independent retail stores such as ***dukas*** and ***kiosks*** in Kenya, ***ojas*** in Nigeria, ***hanouts*** in Morocco or ***spaza shops*** in South Africa.

In this report, our survey focused on SMEs because the majority of African businesses fall in that category. Countries like Kenya, Ghana, South Africa and Nigeria have SMEs, which as we know are of various sizes and scale although it is critical to note that they are fast catching on digitalization and embracing digital business tools in line with evolving market dynamics.

For instance, in manufacturing, operations, finance and HR, institutions have adopted modern technology- based systems in order to stay or become more competitive. The use of ICT systems at various levels includes connecting to the Internet, thus necessitating inclusion of information and system security.

As the Africa Cyber Security Report shows, organizations are increasing their use of ICT tools in their operations. This is illustrated by the rise in use of mobile devices and various operating systems. On the application front, payment systems in Africa that are increasingly mobile led and with it we see, have led to marked increase in mobile fraud across the continent.

> We have listed the top eight (8) cyber security threats in our report. While the list is not exhaustive, it outlines the most prevalent attacks that include ransomware, social engineering, phishing, advanced persistent threats and notably, supply chain attacks.

The latter has interestingly seen a remarkable rise in the number of attacks with our survey showing that criminals are now targeting third party institutions and pointing to an even stronger need for more sophisticated cyber intelligence, threat detection and remediation program.

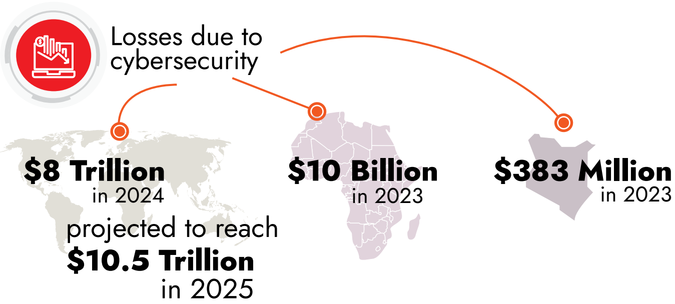
Over the past five (5) years, ransomware, social engineering and phishing attacks have sustained their veracity and increased intensity, registering at 76% and 88% respectively in the past 12 months.

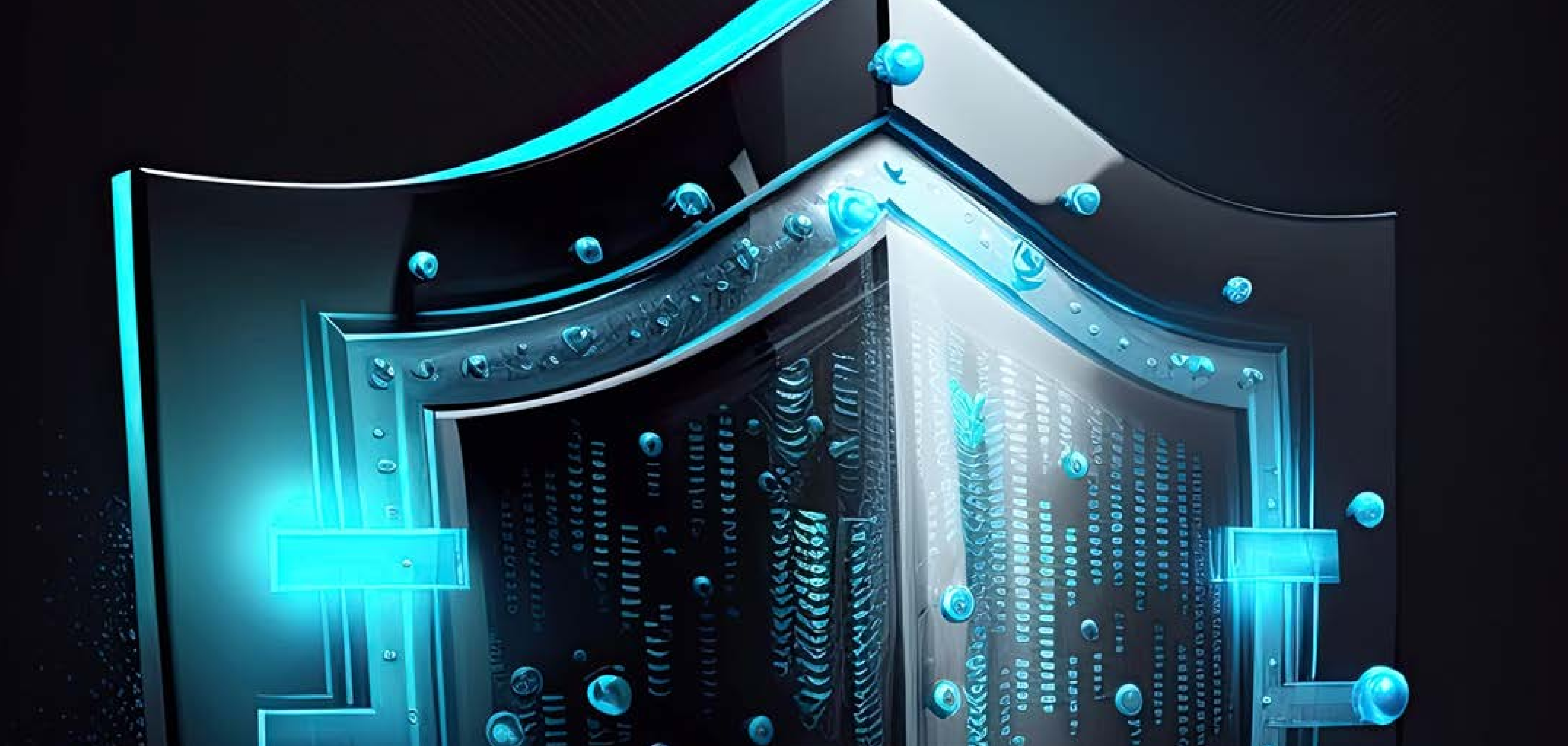
The report includes a review of the global financial cost of cyber security. Losses continued to mount an upward trajectory, rising to an estimated USD 8 trillion in 2024 and projected to reach USD 10.5 trillion in 2025. Africa's losses are estimated to be USD 10 billion in 2023 while Kenya's costs may gross USD 383 million.

While demand for better cyber professionals is apparently outstripping supply, threat actors are becoming bolder and using advanced ICT tools for malicious work. On the positive side, regulation, through data protection laws for instance, is gaining prominence. As we live in borderless IT world the reality is that there is no turning back on the need for digitalization in organizations.

It is incumbent upon SMEs to proactively seek guidance on cyber security in order to build the necessary capacity to mitigate against their potential attackers. No organization is immune to cyber risk.

The good news is that the cyber security industry in Africa has also evolved to develop locally suitable solutions and programs. Help, is thus at hand.





5. Threat Indicators and Emerging Areas

Highlight of Top Cyber Security Threats of 2023

This list is not exhaustive as the threat landscape is constantly evolving, and new threats can emerge at any time.

Ransomware Attacks

In 2022 **76%** of organizations were targeted by ransomware attack.

out of these 64% were actually infected.

Social Engineering and Phishing

Approx **88%** of organizations encounter spear phishing attacks within a year

Advanced Persistent Threats (APTs)

In **2024** APTs may continue to evolve and target critical infrastructure, government agencies, or high-value corporate networks.

Supply Chain Attacks

out of **1,325 CEOs,**

76% believe protecting their partner ecosystem and supply chain is just as essential as building their own security infrastructure.

- KPMG survey

Cloud Security Risks

migration to cloud environments continues to grow

Internet of Things (IoT) Vulnerabilities

IoT malware cases skyrocketed by **87%** to **112.3 million cases**

Artificial Intelligence (AI) / Machine Learning (ML) - based Attacks

Increase discussion on AI

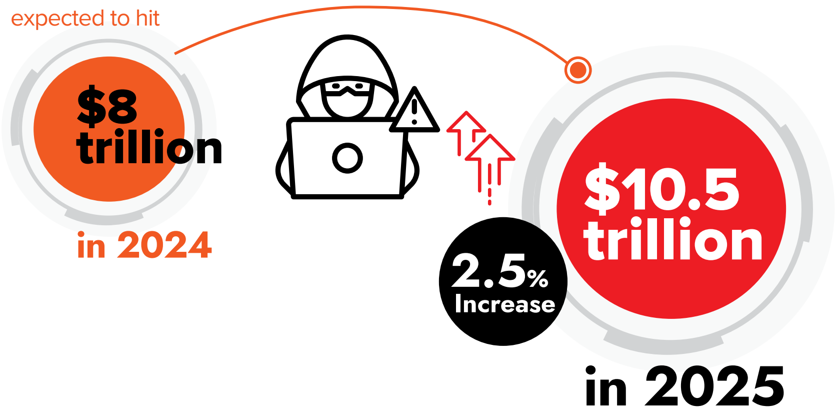
organizations with fully deployed security AI and automation technologies experienced damages of **$3.05M** cheaper compared to organizations without such deployments.

Mobile Device Vulnerabilities

the severity and probability of these threats can change over time, and different organizations or industries may have varying levels of exposure.

5.1. Top 8 Cyber Security Threats of 2023

Cost of Cybercrime



expected to hit

$8 trillion

in 2024

2.5% Increase

$10.5 trillion

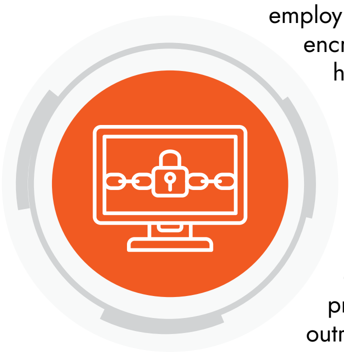
in 2025

This list below is not exhaustive as the threat landscape is constantly evolving, and new threats can emerge at any time. However, based on historical trends and potential future developments, here are some prominent cyber security threats for organizations to consider :

a. Ransomware Attacks

High Impact: High Probability

As a top global attack vector by FBI, ransomware continues to be a significant threat. In 2023, we noted ransomware attacks becoming more sophisticated, targeting critical infrastructure, state corporations, healthcare systems, and cloud service providers. Ransomware attackers employ advanced techniques such as zero-day exploits and encryption techniques to maximize their impact and extort higher ransom payments.



In 2022, 76 percent of organizations were targeted by ransomware attack, out of these 64% were actually infected. 50% of these organizations were able to retrieve their data after paying the ransom. According to a recent survey, 72% of respondents claim they have a ransom policy in place, and the procedure for 49% of them is to pay the ransom outright.

Due to the severity of the attack, organizations may obtain cyber insurance to safeguard against financial losses. This coverage protects against liability for breaches involving sensitive customer information, such as personal identification number credit (PIN), credit card details, information about minors, health records etc. As a key part of a comprehensive cybersecurity strategy, cyber insurance helps mitigate risks and offers peace of mind.

b. Social Engineering and Phishing

High Impact: High Probability

Social engineering gain unauthorized access to sensitive information or systems.

Cybercriminals mostly abuse Microsoft's brand in phishing attacks, with 30 million messages using Microsoft products like Office or Outlook. Other companies frequently used by cybercriminals include Google (mentioned in 2.6 million attacks); DHL (2 million attacks) and Adobe (1.5 million attacks). Approximately 88% of organizations encounter spear phishing attacks within a year, this indicates that businesses and organizations are targeted almost daily.

c. Advanced Persistent Threats (APTs)

High Impact: Low Probability

APTs are well-funded and highly skilled threat actors that aim to gain unauthorized access to targeted networks and maintain a long-term presence. In 2024, APTs may continue to evolve and target critical infrastructure, government agencies, or high-value corporate networks, aiming to steal sensitive information or disrupt operations.

d. Supply Chain Attacks

Medium Impact: Medium Probability

Supply chain attacks involve compromising the software or hardware of trusted vendors and suppliers to gain unauthorized access to targeted organizations. In 2023, supply chain attacks became more prevalent and sophisticated, with attackers targeting software update mechanisms, hardware components, or third-party service providers to gain widespread access to multiple organizations.

Research claims that over a third of organizations have become "collateral damage" because of a third-party cyber incident. 9 out of 10 IT leaders are concerned about the cyber resilience of such third parties. In a recent survey conducted by KPMG, out of 1,325 CEOs, 76 percent of the CEOs believe protecting their partner ecosystem and supply chain is just as essential as building their own security infrastructure.

e. Cloud Security Risks

Medium Impact: Medium Probability

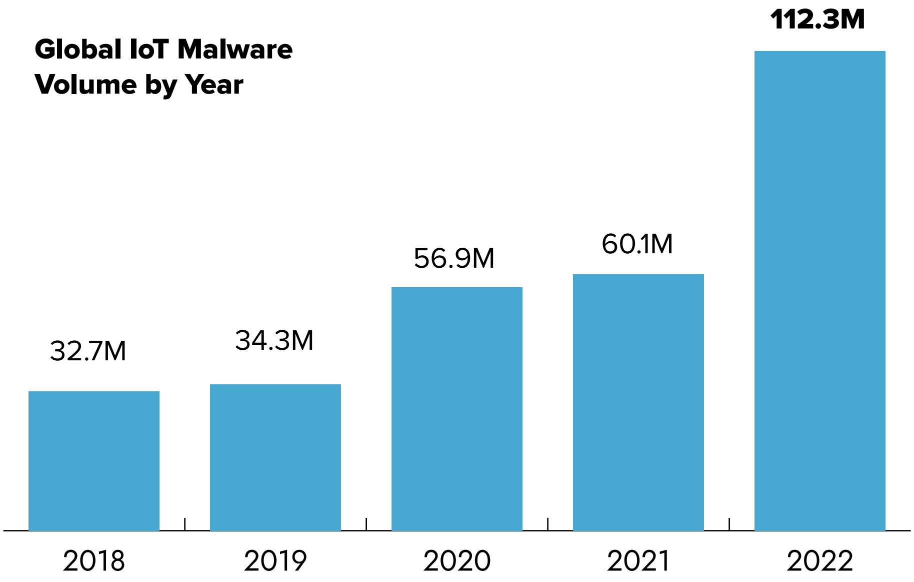
The migration to cloud environments continues to grow, and so do the associated security risks. Organizations are likely to continue facing challenges such as misconfigurations, insecure APIs, and data breaches in cloud platforms. Attackers may target cloud infrastructure, exploit weak access controls, or abuse shared resources to gain unauthorized access to sensitive data.

f. Internet of Things (IoT) Vulnerabilities

Medium to High Impact: Medium Probability

As the number of connected devices continues to increase, so does the potential attack surface for cyber criminals. IoT devices may be targeted more frequently due to their often-inadequate security measures. Attacks on IoT devices can lead to data breaches, disruption of critical services, or even physical harm.

Cases resulting to IoT malware has skyrocketed by 87% compared to previous years, resulting to an all-time high of 112.3 million cases.



g. Artificial Intelligence (AI)/ Machine Learning (ML) - based Attacks

Medium to High Impact: Low Probability

The adoption of AI in various domains brings new security challenges. In 2023, there have been increased discussions around the use of AI, similarly, we expect an increase in AI-based attacks, where malicious actors leverage AI techniques to automate and enhance their attacks. This include the use of AI-generated deepfakes, AI-powered phishing attacks, or AI algorithms exploiting vulnerabilities in systems. It is possible for attackers - even the very non-technical ones — to ramp up their development of exploits and zero-day discovery utilizing large language models (LLMs) such as ChatGPT.

However, organizations with fully deployed security AI and automation technologies experienced damages of $3.05 million cheaper compared to organizations without such deployments. This also resulted to an average 74-day reduction in breach identification and containment compared to those without such implementations.

h. Mobile Device Vulnerabilities

Medium to High Impact: Medium Probability

With the widespread use of smartphones and mobile devices, they become attractive targets for cyber criminals. We may witness an increase in mobile malware, banking trojans, and attacks targeting vulnerabilities in mobile operating systems and applications.

It is important to note that the severity and probability of these threats can change over time, and different organizations or industries may have varying levels of exposure. It's essential to conduct a comprehensive risk assessment specific to your environment to determine the severity and probability of these threats accurately.

5.2. Top 6 Indicators of Compromise of 2023

In the ever-evolving landscape of cybersecurity, understanding the tactics, techniques, and procedures (TTPs) employed by malicious actors is crucial for effective threat detection and response.

Key to improving detection capabilities is uncovering Indicators of Compromise (IOCs) left behind by attackers during their intrusions.

These IOCs serve as invaluable breadcrumbs, providing insights into the tools and methods used throughout the attack lifecycle. By categorizing IOCs based on their respective attack phases, security teams can gain a comprehensive understanding of the adversary's actions, identify vulnerable assets, and enhance their incident response strategies.

The following table presents an overview of IOCs identified from attacks (ransomware and targeted attacks) that have occurred in Kenya and across the globe, classified into distinct categories: Tools, Asset Discovery, Persistence, Credential Access, Lateral Movement, and Exfiltration.

This classification enables security practitioners to recognize patterns and tactics commonly employed by threat actors during each stage of an attack, empowering them to bolster their defenses and safeguard critical assets.

Category	**Description**
Tools	Malicious tools and software leveraged by attackers.
Asset Discovery	Techniques used to identify and enumerate target assets.
Persistence	Methods to maintain unauthorized access over time.
Credential Access	Acquisition of login credentials for unauthorized entry.
Lateral Movement	Techniques to expand influence within the network.
Exfiltration	Unauthorized extraction and theft of sensitive data.

5.3. Actual Indicators of Compromise IOC's

Tools	Asset Discovery	Persistence	Credential Access	Lateral Movement	Exfiltration
Impacket Powershell ADfind Bloodhound Psexec Advanced IP scanner Angry IP scanner NetScan Anydesk DW agent Mesh Agent NGROC Mimikatz Keyloggers SQLdeveloper HeidiSQL Custom scripts*	ADfind Advanced IP Scanner Angry IP Scanner Net Commands Whoami Bloodhound NetScan	Remote Tools (Anydesk, DWagent, MeshAgent) NGROC Scheduled Tasks NSSM Custom scripts*	Mimikatz SecretsDump Keyloggers	RDP SMB WMI IPC shares Psexec Smbexec Wmiexec AtExec SchtasksExec WinRM DCOM	Cloud instances (AWS, Azure) MegaNZ

Files / Malicious files

In 2022, Microsoft started blocking VBA macros by default across their product suite. Following this, adversaries changed their techniques. They shifted away from malicious macros in their phishing emails and began leveraging container files (Optical Disk Image (ISO) files and Virtual Hard Drive (VHD)) and compressed files (RAR and ZIP files) to deliver their malware, often nesting these file types within each other in an attempt to bypass security controls.

Windows shortcut files, known as LNK files, have seen increased malicious use in 2022. LNK files provide adversaries a way to execute binaries, scripts, and other arguments. Based on the specific arguments configured when a LNK file is created, it can point to and execute files or include scripts configured to download additional malware. Additionally, MSI files are also being abused by malicious actors. MSI files are used to install and update legitimate software on Windows systems. They are also used by adversaries to install malicious binaries, run scripts, and elevate system privileges.

Tools/malicious tools

Certain tools and components, such as Impacket, Mimikatz, BloodHound, Rundll32, Powershell, and PStools, have been heavily utilized in attacks that have occurred across the continent, almost appearing in each and every incident investigated in the past few years. While these tools are not inherently bad and often serve legitimate purposes, adversaries have found ways to misuse them, exploiting their functionalities for malicious intent and causing significant security concerns.

These tools and components are not intrinsically malicious, and their primary purpose is to streamline legitimate IT tasks and empower system administrators. However, the darker side of cyberspace has seen adversaries exploit the versatility and power of these tools for their nefarious purposes. To mitigate the risk of such abuse, organizations must remain vigilant, employ strong cybersecurity practices, and implement proactive measures to detect and prevent unauthorized access and malicious activities within their networks. Regular security awareness training, network monitoring, and implementing the principle of least privilege are essential steps in securing the ever-evolving digital landscape against potential threats.

Detection

Traditional signature-based detection, while effective against known and established malware threats, faces significant challenges when dealing with the tools mentioned earlier (Impacket, Mimikatz, BloodHound, Rundll32, Powershell, and PStools) due to their specific characteristics and the ways they are abused by adversaries.

To effectively defend against these advanced threats and the abuse of legitimate tools, organizations need to complement traditional signature-based detection with more sophisticated security solutions. Behavior-based detection, anomaly detection, heuristics, machine learning, and artificial intelligence (AI) are some of the advanced techniques that can help identify suspicious activities and novel attack patterns. Implementing a multi-layered security approach that includes these advanced detection mechanisms and continuous monitoring is essential to staying ahead of modern cyber threats and protecting sensitive data and systems from exploitation.

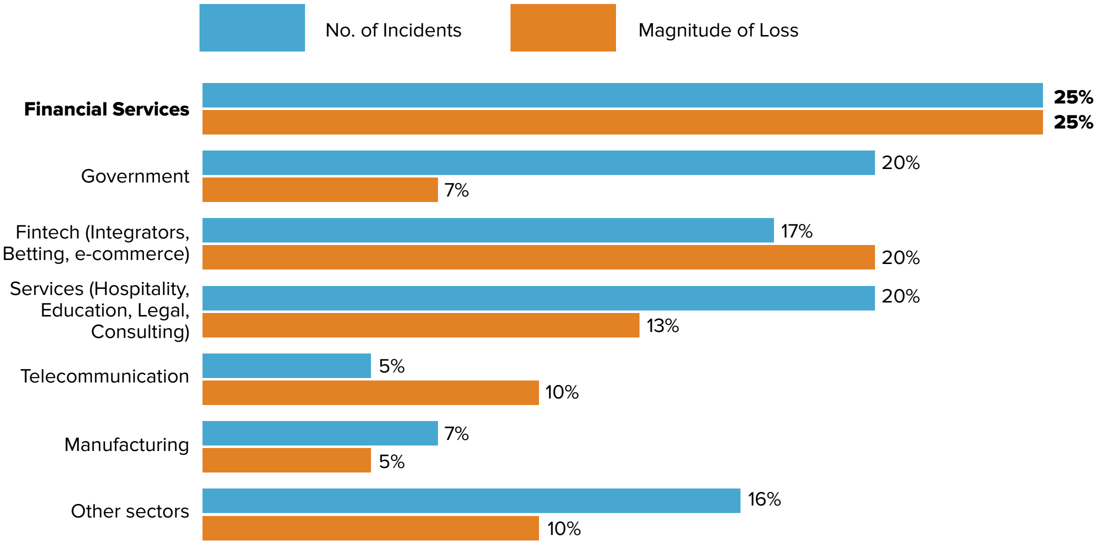
5.4. Cost of Cybercrime in Africa (estimate)

Breakdown of key statistics for In-Scope countries:

	Population (2022 Est.)	Nominal GDP (2022)	Internet users & subscribers (2022)	Estimated Cost of cyber-crime (2022)	Estimated No. of Certified Professionals
Africa	1,468,612,526	**$2,988B**	545,790,000	**$10B**	20,000
Nigeria	223,804,632	**$477B**	144,949,194	**$1.2B**	5,000
Kenya	55,100,587	**$89.591B**	46,877,042	**$383M**	4,000
Uganda	48,582,334	**$46B**	18,502,166	**$67M**	700
Botswana	2,604,172	**$20B**	1,247,000	**$39M**	300
Lesotho	2,330,318	**$2.6B**	682,990	**$2.3M**	120

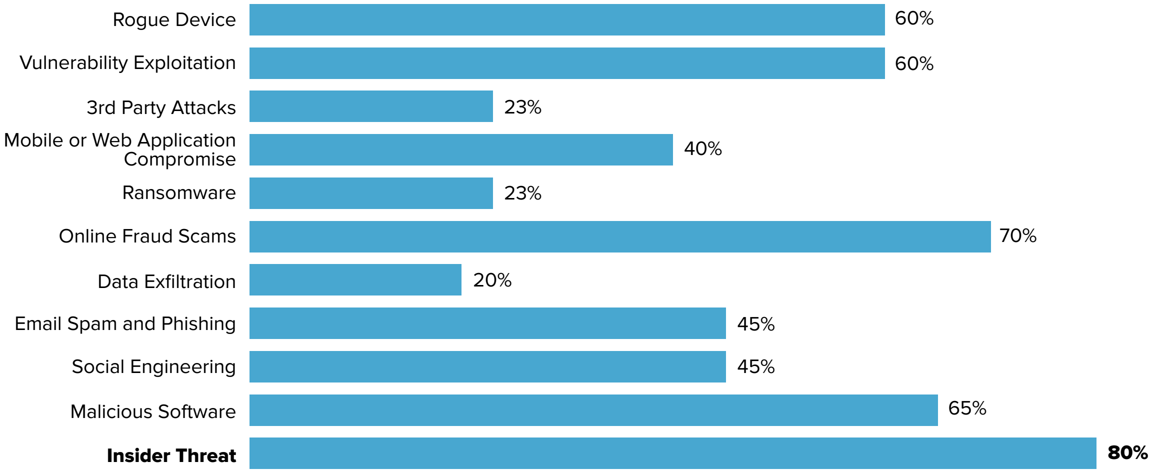
*Certified Professionals is limited to the following certifications: CISA, CISM, GIAC, SANS, CISSP, CEH, ISO 27001 and PCI DSS QA
*Economic and internet usage data extracted from respective country Internet regulator reports and World Bank site.

Most Affected Industries By Number of Incidents and Loss Magnitude



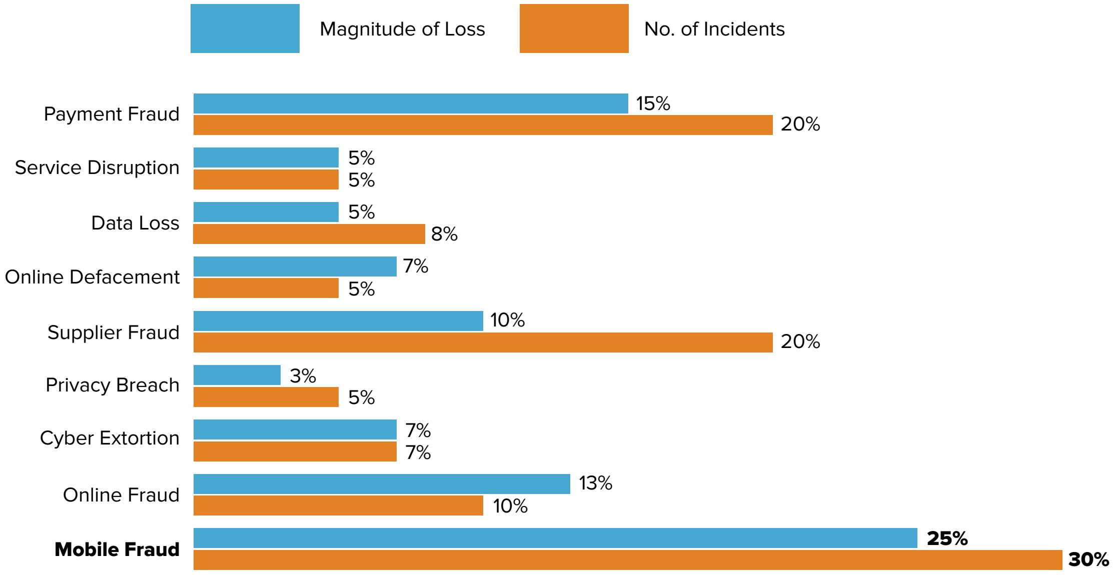
The Financial Services Industry remains the most affected by magnitude of loss and number of incidents

Most Popular Threat Scenario Analysis



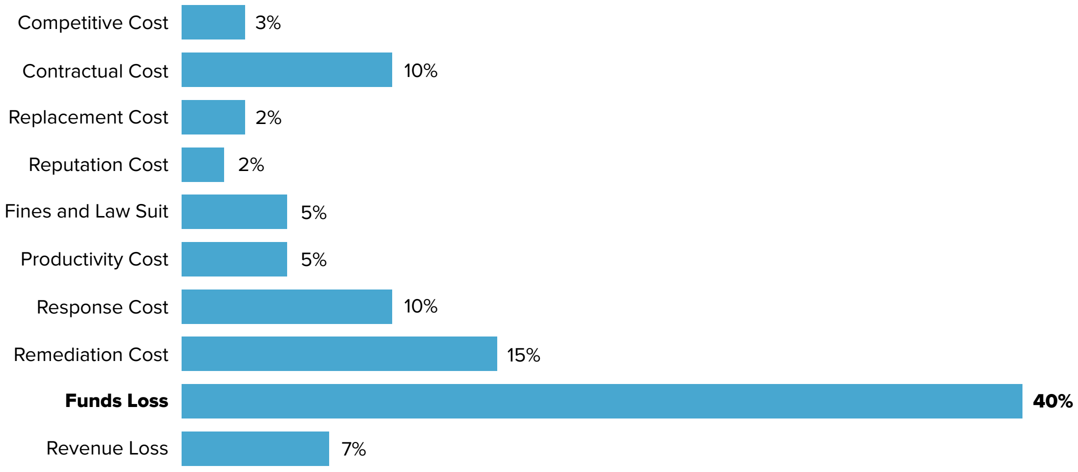
Insider threats remain a great threat across board at 80% followed closely by online fraud scams at 70%. We estimate a significant increase in ransomware attacks in the year 2024.

Most Popular Risk Exposures

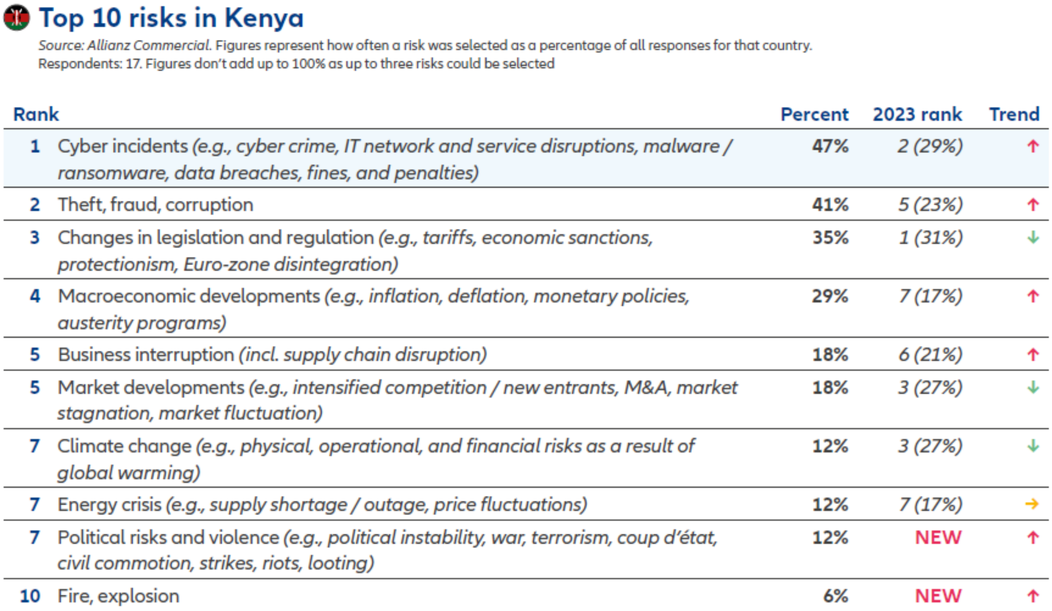


In 2023, we noted that mobile fraud carries the highest loss magnitude (financial loss) compared to the other risk exposures.

Most Popular Loss Scenarios



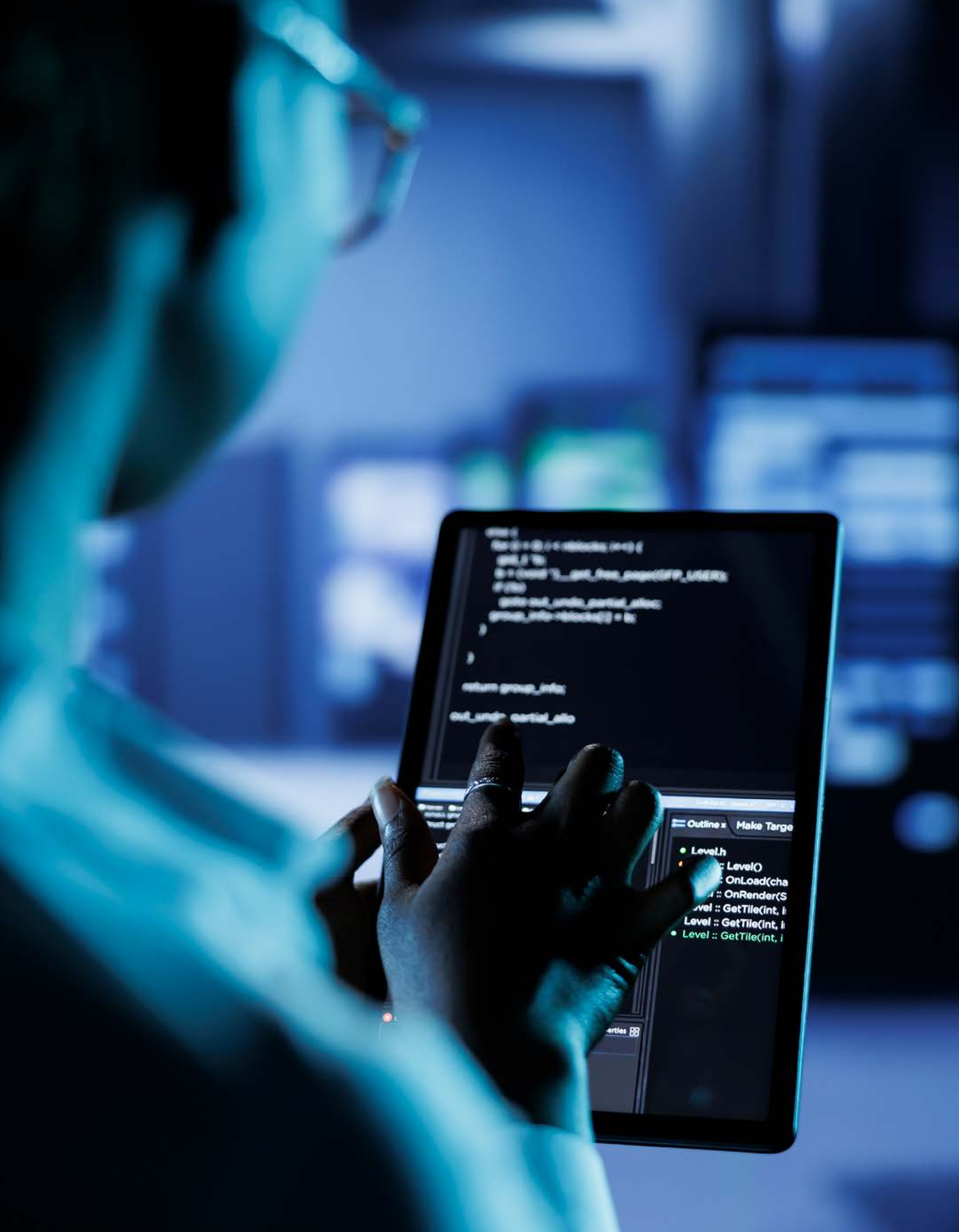
Loss scenarios look at the potential aggregate financial losses that an organization faces as a result of various successful cyberrisk breaches or attacks. Funds loss remain the highest loss scenario at 40% in 2023 with remediation costs coming a close second.



Top 10 risks in Kenya

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country. Respondents: 17. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2023 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	**47%**	*2 (29%)*	↑
2	Theft, fraud, corruption	**41%**	*5 (23%)*	↑
3	Changes in legislation and regulation *(e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	**35%**	*1 (31%)*	↓
4	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	**29%**	*7 (17%)*	↑
5	Business interruption *(incl. supply chain disruption)*	**18%**	*6 (21%)*	↑
5	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	**18%**	*3 (27%)*	↓
7	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	**12%**	*3 (27%)*	↓
7	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	**12%**	*7 (17%)*	→
7	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)*	**12%**	NEW	↑
10	Fire, explosion	**6%**	NEW	↑


return group_info;
out_undo partial_allo
Outline x
Make Targe
Level.h
Level()
OnLoad(cha
OnRender(S
Level :: GetTile(int, i
Level :: GetTile(int, i
Level :: GetTile(int, i

Industry Player Perspective

Enhancing Cybersecurity with a Data-Driven AI Approach

By Shikoli Makatiani

COO,
Turnkey Africa Ltd

In the current landscape, organizations are increasingly combining their operations with digital technologies, making cybersecurity an integral aspect of business strategy. This digital adoption requires a significant shift from traditional, siloed risk management to a comprehensive framework that encompasses all facets of an organization.

Risk management has evolved from a standalone function to an integrated process, where potential risks, whether operational, financial, compliance, or reputational, must be identified and assessed across departments. The data gathered through standardized risk assessments is manually entered into platforms for further analysis, a process loaded with inefficiencies and human error.

The traditional tools for risk management, such as Excel sheets and Governance Risk and Compliance (GRC) systems like RSA Archers, are manual and cumbersome. The implementation of an automated risk management software should be key investment for all organizations, where risks across the entire organization are not only identified and assessed automatically but also monitored across the organization.

An automated risk management environment requires a strategy that integrates technology, organizational culture, and processes. The aim is to create a holistic digital ecosystem where business strategies are fully aligned with security measures. In this ecosystem, risks are seen as part of a larger picture, similar to the understanding of a human body rather than its isolated parts.

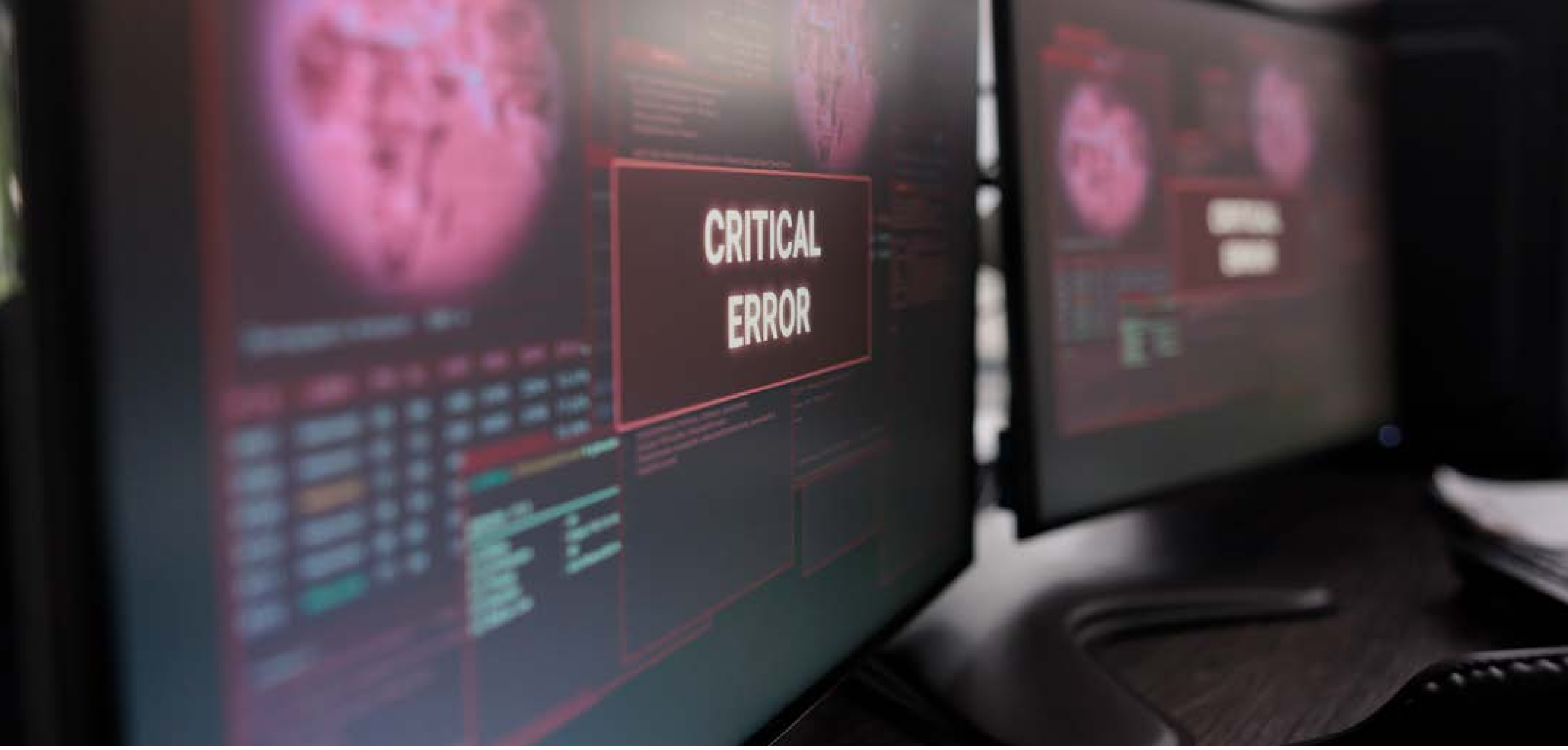
In order to achieve an interconnected digital risk management ecosystem, organizations need to embrace concepts such as Artificial Intelligence, API-driven architectures and large language models (LLMs). APIs allow for seamless communication between different systems, applications and databases, essential for the real-time data flow necessary for AI and LLMs to effectively predict and analyze risks.

These technologies enable the automation of complex assessments, drawing from vast datasets to uncover subtle patterns but also present challenges centered around transparency and accountability due to the opaque nature of AI decision-making. This requires an assessment of the ethical and regulatory implications of AI in decision-making especially in sensitive sectors such as finance and healthcare.

To address these challenges, organizations need to adopt a framework that assess risks within an organization as a whole and implement robust data privacy and compliance measures. The CVEQ framework is an innovative risk modeling and quantification approach that assesses and quantifies cyber security risks across all aspects of an organization. It focuses on assessing It is based on the globally accepted Credit Scoring Methodology which enables organizations to model and measure cyber risk.

Cybota is an automation of the CVEQ framework that automates the data collection processes and quantifies cyber security risks across an organization. The process utilizes the CVEQ Digital Resilience Bow-Tie model which focuses on an assessment of risks within business data creation, digital assurance, digital risks and business value creation enabling decision-making.

In conclusion, a data-driven AI approach to cybersecurity offers the potential to transform risk management into a dynamic, proactive, and integrated part of business strategy. However, this transformation requires careful planning, cultural alignment, and a commitment to ethical practices and regulatory compliance. By doing so, organizations can harness the full potential of AI to secure their digital frontiers while remaining accountable and transparent to stakeholders.



6. Cyber Intelligence

Our Cyber Threat Intelligence aggregates, correlates and analyzes information from a vast network of sensors deployed across Africa. This section provides deep insights into the cyber threat landscape, and amplifies the preparedness of organisations by providing relevant, predictive, and prioritized cyber threat visibility and intelligence.

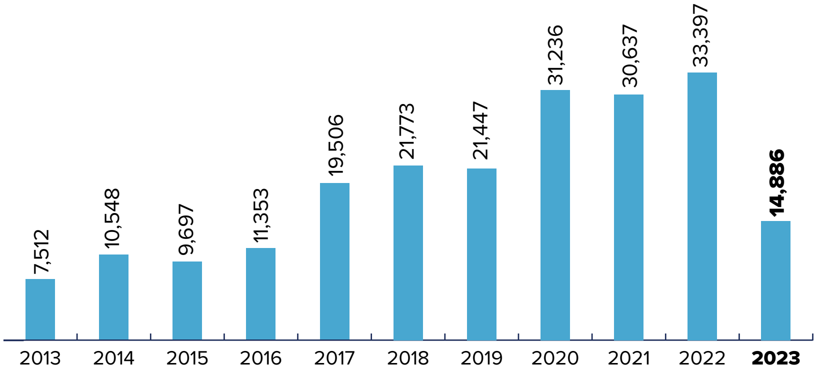
6.1. Africa

a. Vulnerabilities

14,866 vulnerabilities were published in 2023.

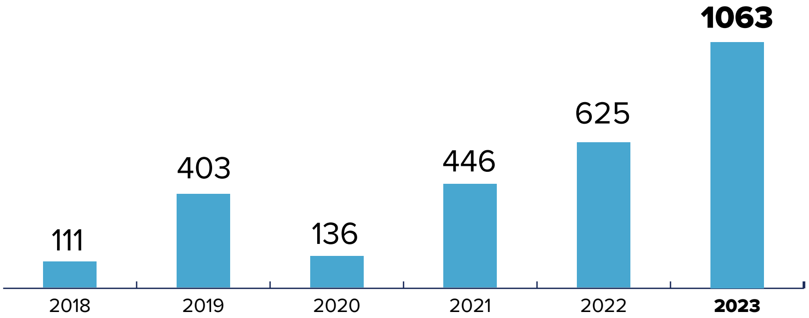
CVE published 14,866 vulnerabilities published in 2023, a higher number than in previous years (33,397 in 2022, 21,447 in 2021, and 31,236 in 2020).

Graph 1. Vulnerabilities Published by Year



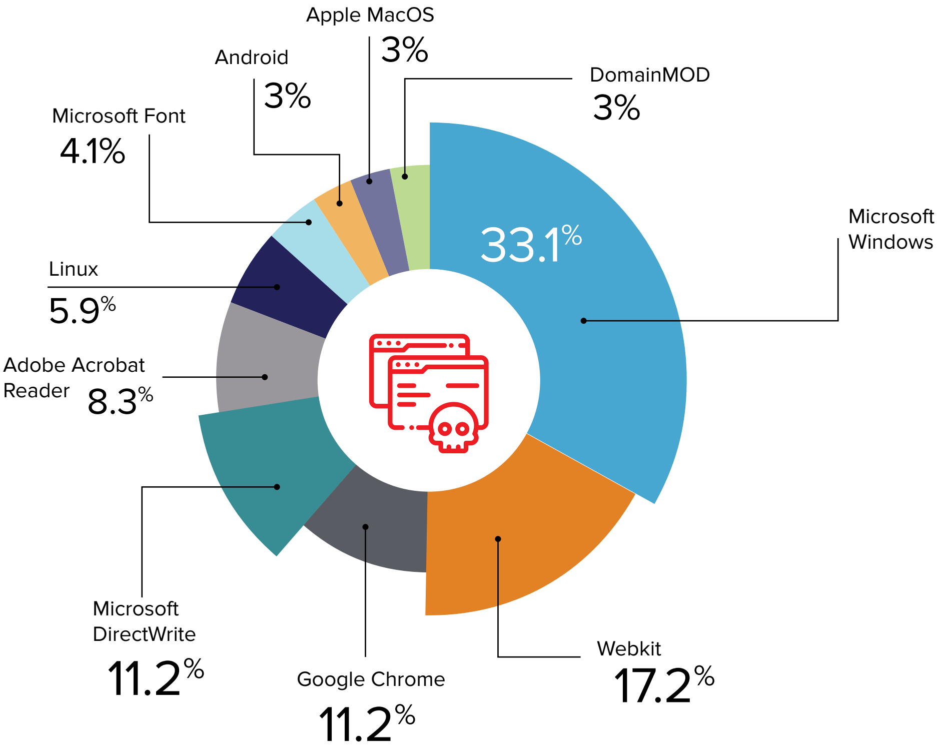
b. Exploits

Graph 2. ExploitDB published 1068 vulnerabilities in 2023, a higher number than in 2022 (625 exploits) and 2021 (446 exploits).



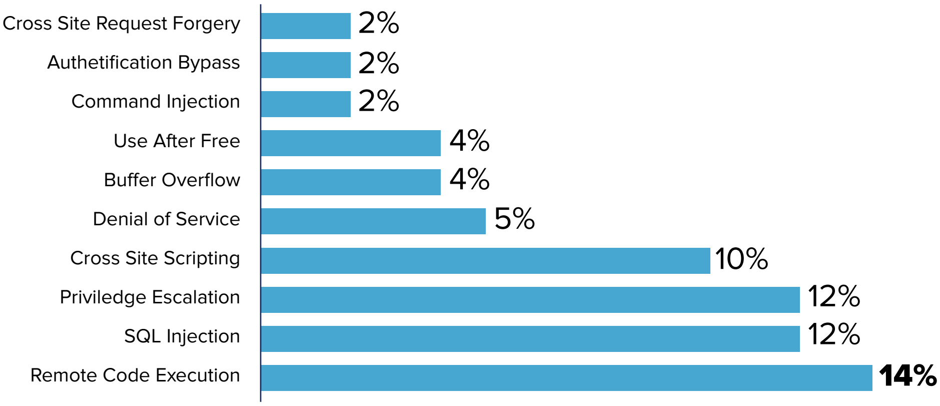
A large number of the exploits targeted systems as illustrated below.

Chart 1. Exploits Released by Application



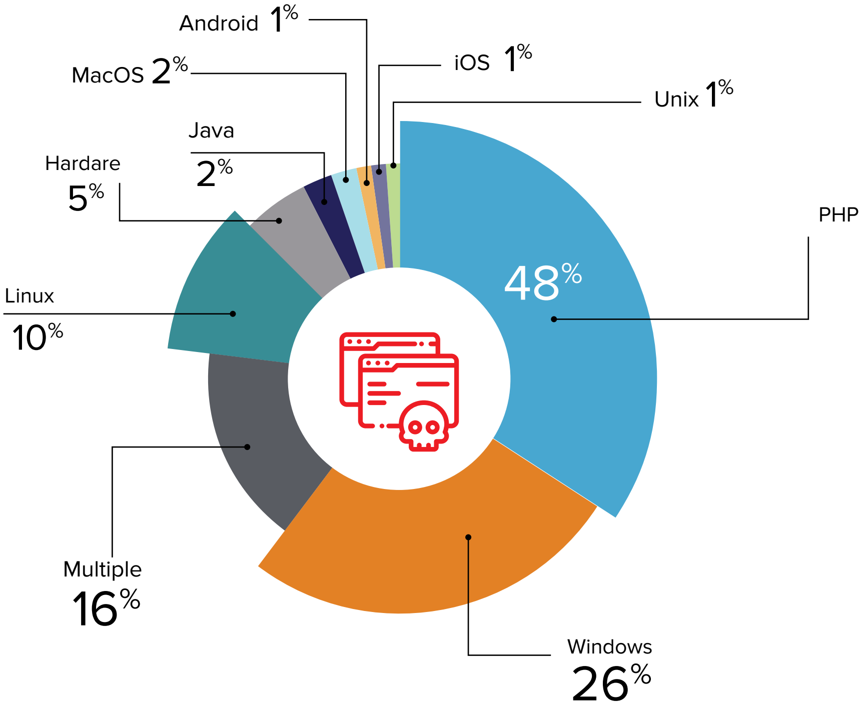
The top 10 exploits allowed malicious actors to gain access to systems and exfiltrate data.

Graph 3. Exploits Released by Attack Type



The top affected operating systems.

Chart 2. Exploits Released by Platform



c. Hacking Articles

Graph 4. Cyber Attack Articles by Year

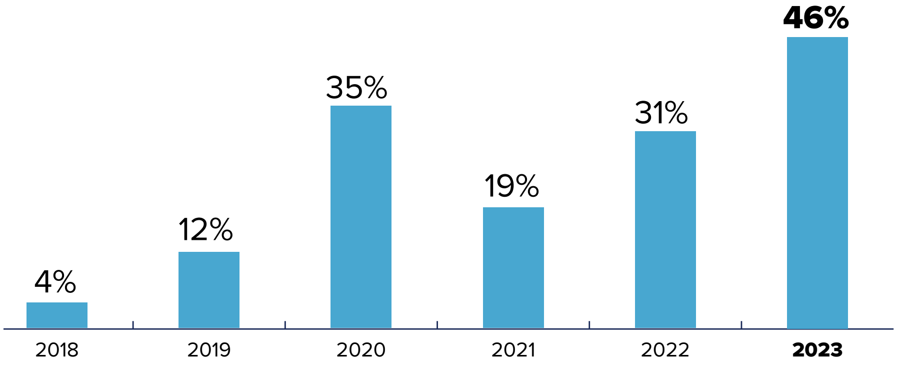
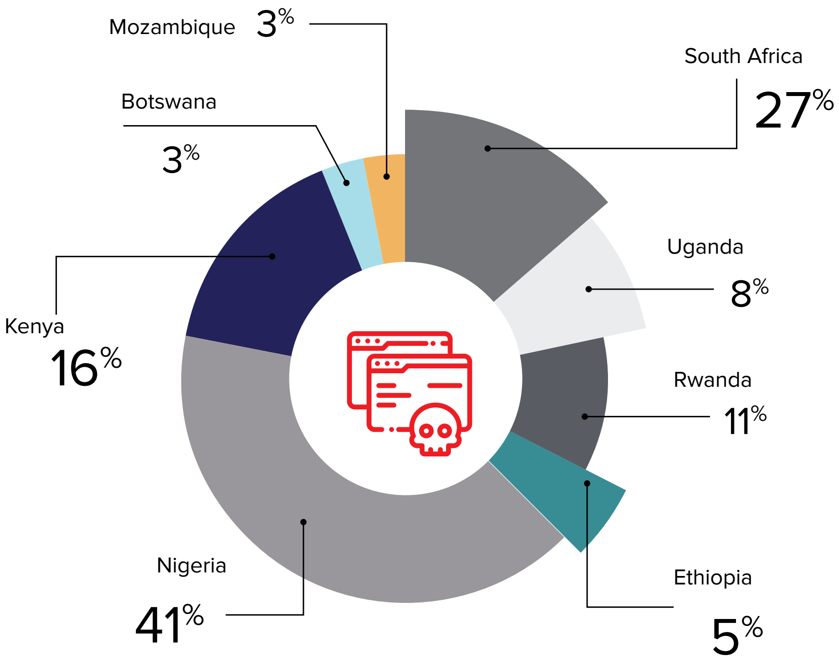
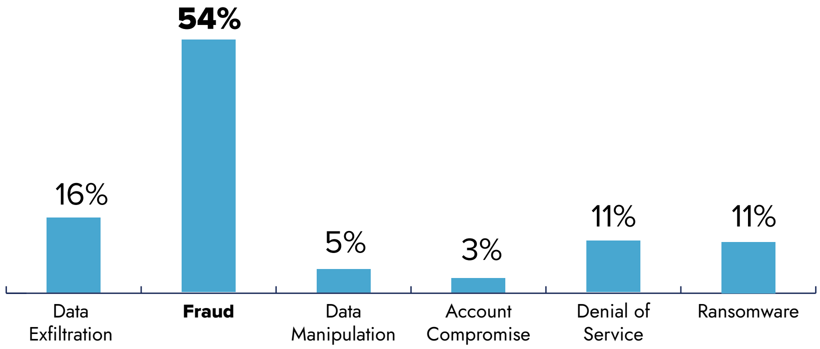


Chart 3. NIgeria had the highest number of articles published with 41%.

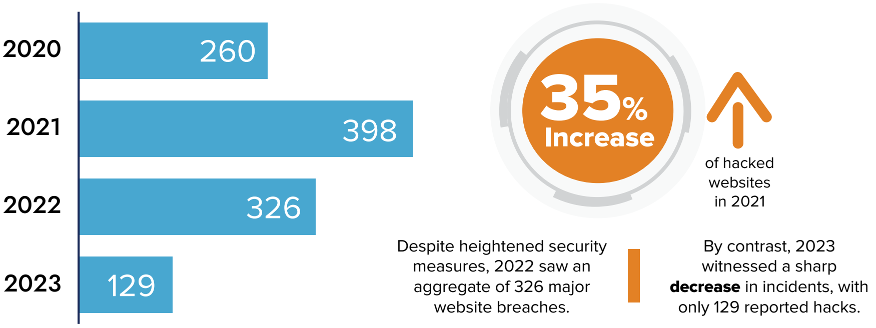


Graph 5. Cyber Attack Articles by Attack Type.



d. Hacking Websites

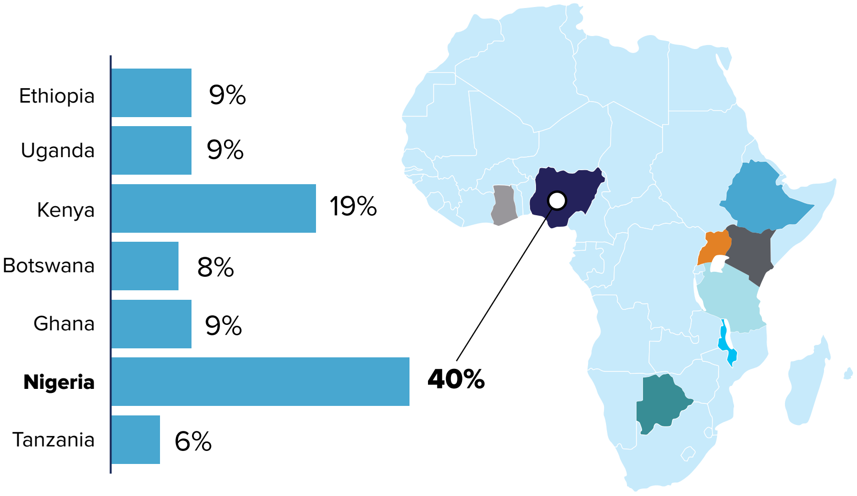
Graph 6. Hacked Websites by Year



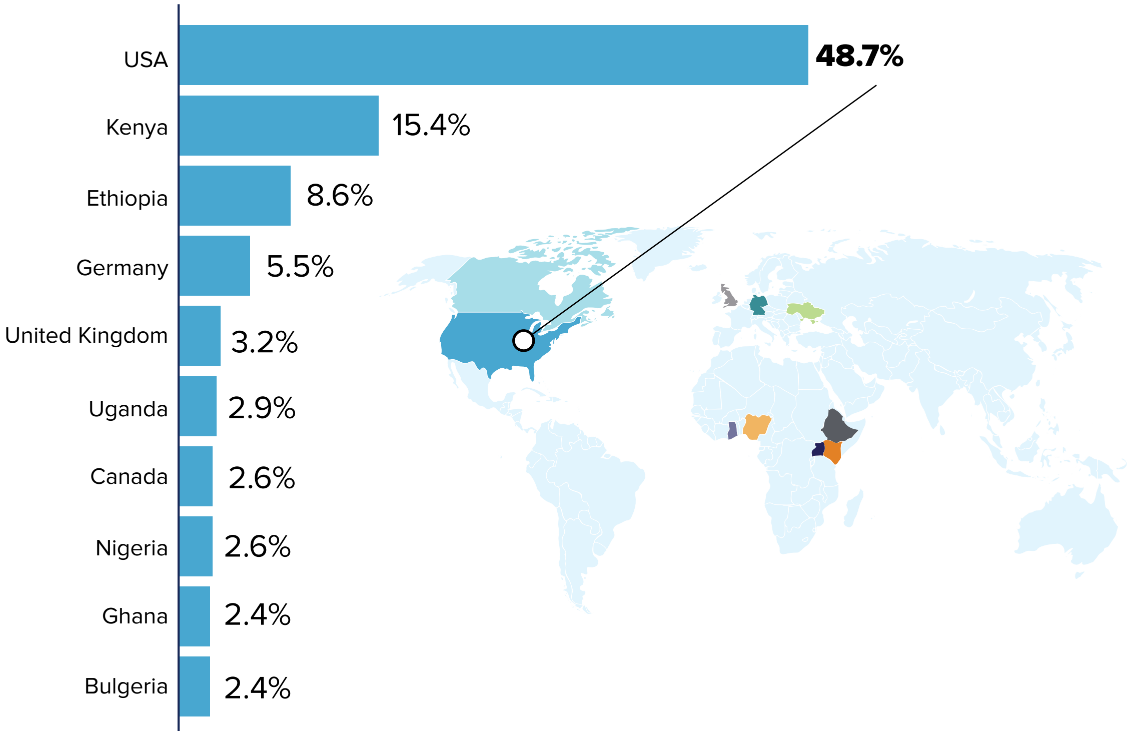
Despite heightened security measures, 2022 saw an aggregate of 326 major website breaches.

By contrast, 2023 witnessed a sharp **decrease** in incidents, with only 129 reported hacks.

Graph 7. Hacked Websites by Owner Country

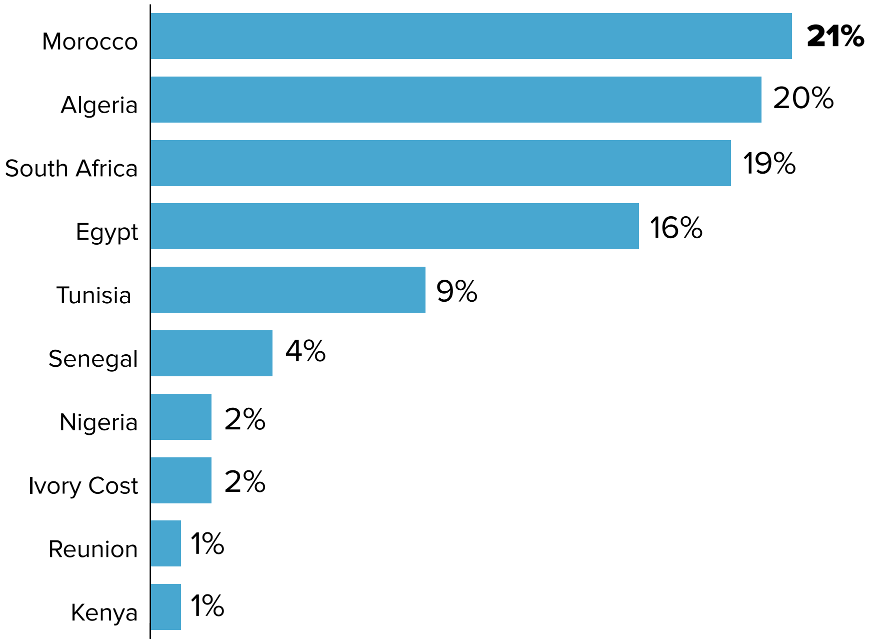


Graph 8. A high number of websites that were hacked were hosted as illustrated below.



e. Exposed Devices

Graph 9. Top 10 Countries with the Most Exposed Devices:



Industry Player Perspective

Automating Security Operation Center Processes Using Artificial Intelligence

By Anne Gikaara

SOC Professional

The Serianu Security Operations Center (SOC) receives an average of four thousand nine hundred and forty-six (4,946) events per seconds every 24 hours. For a Managed Security Service Provider (MSSP) to manage and analyze the generated data an MSSP has to invest in tools to support its SOC processes such as a log analytics platform, an issue management system and a threat detection and response platform.

The traditional approach to threat analytics relies on the SOC analyst's expertise to analyze generated incidents. SOC analysts have to sift through a large number of events as a means of correlating incidents. Platforms such as FortiSIEM have adopted rule-based analytics to define correlation rules to detect complex events reducing the SOC analyst's workload. However, this approach has its limitations, particularly in detecting complex cyber threats, as it confines analysts to predefined rules and patterns.

In 2022, Devo Technology released the ***2022 Devo SOC Performance Report*** which highlighted several challenges faced by Security Operations Centers (SOC). The results focused on security operations center across the U.S., Canada, UK, France, Germany, Italy, and Australia/New Zealand which highlighted 9 key challenges which include:

1. **Dependance on too many tools to manage the collection and analysis of data.**
2. **Integration issues with log generation and analytics platforms.**
3. **Limited SOC investment and resources.**
4. **Complexity and chaos of managing a SOC.**
5. **Inability to capture actionable intelligence.**
6. **Lack of visibility into the attack surfaces.**
7. **Struggle to keep up with attack tactics and strategies.**

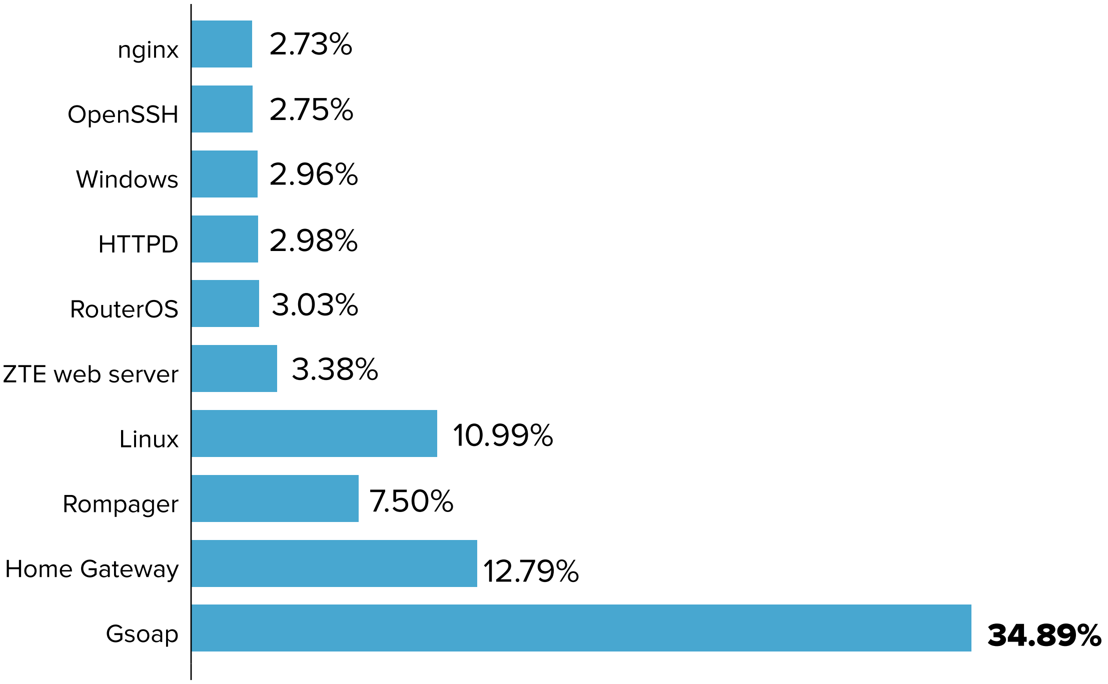
The African market encounters similar challenges, including limited resources, a shortage of skilled expertise, and budget constraints. In response to the rising number of attacks, organizations are need to invest in tools for detection and response, as well as to employ security analysts to ensure that risks are identified and mitigated. Additionally, increased investment in technologies like cloud computing, remote working, and artificial intelligence introduce new attack vectors.

The modern approach to security monitoring is centered on process automation through eliminating manual analysis, automating evidence gathering and correlation as a means of offering timely and accurate detection and response capabilities. Key concepts such as agents can assume roles such as a security analyst that analyzes alerts or an incident handler that responds to threats while models can be utilized in reducing noise generated by the large number of events and identifying attack patterns.

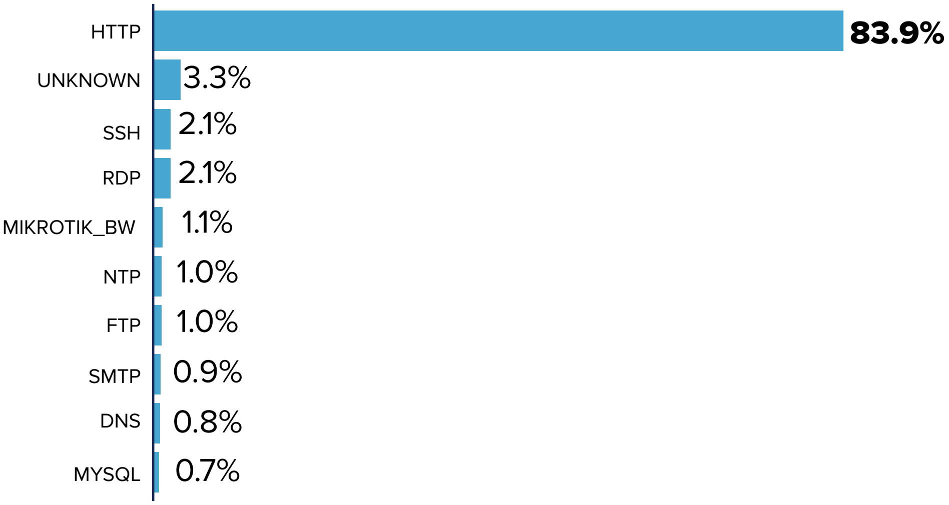
In the era of AI dominance, both employees and stakeholders are exploring ways to leverage AI for automating processes, while also considering the implications for the workforce. It's crucial to note that AI doesn't operate in isolation; it requires human assistance to develop ideas and solve problems. This is evident in the design of many AI platforms, which require human input through interactive chat interfaces. AI's primary role is to aid in the analysis of large data sets therefore reducing the cognitive load.

In the context of the Security Operations Centers (SOC), It empowers SOC analysts in developing intelligent workflows that analyze and correlate data from multiple data sources. This streamlines their processes, enabling them to focus on generating actionable insights and quickly responding to cyber threats. AI introduces the 10x concept by increasing effectiveness, solving problems, and reducing the cost and speed of operations therefore making it one of the most powerful assistants.

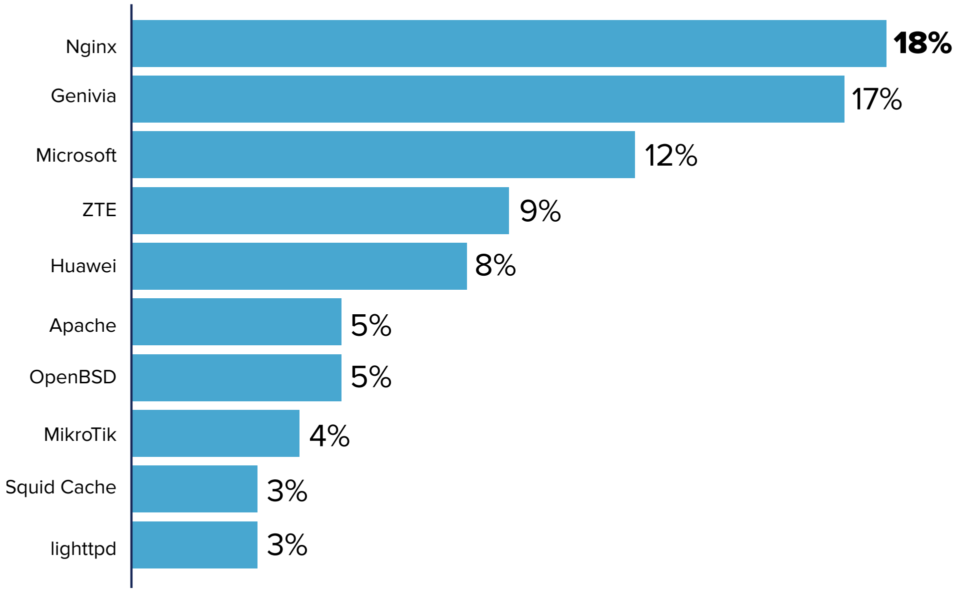
Graph 10. The graph lists software products by their exposure rates, with gSOAP leading at 34.89%, followed closely by HomeGateway and Linux.



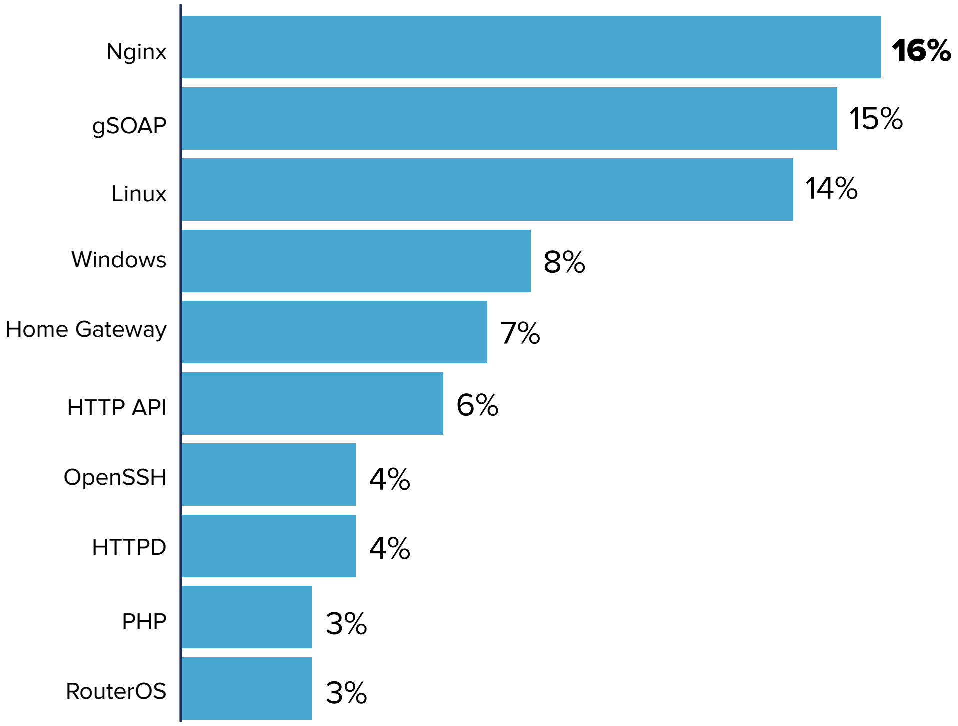
Graph 11. Web applications were the top supported services.



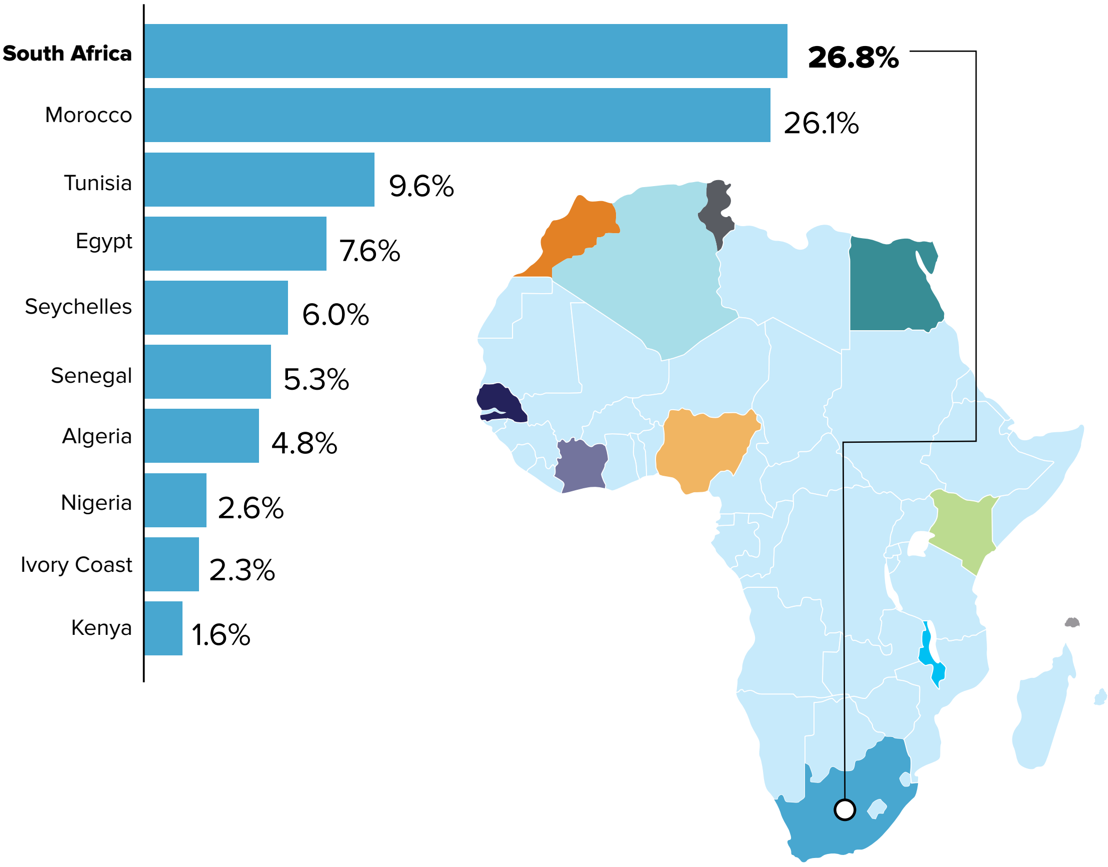
Graph 12. The web server software Nginx is the top supported software vendor with 18%.



Graph 13. The top software product is Nginx with 16%.



Graph 14. South Africa had the most devices online with 26.8%.



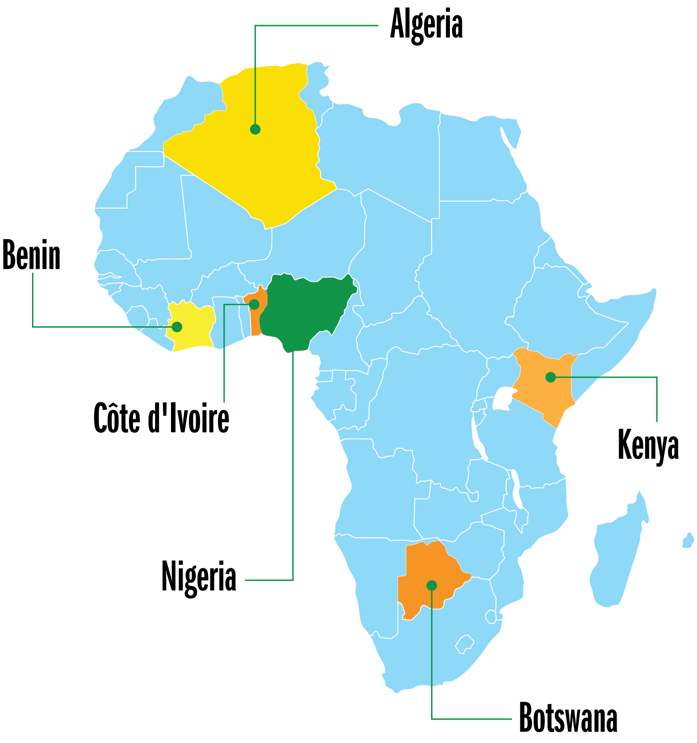
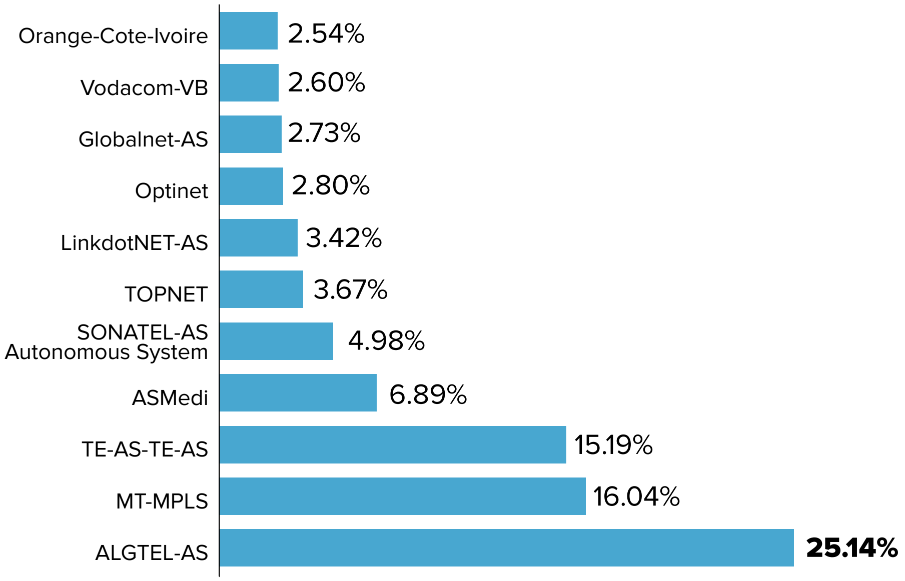


Table 1. Top 10 Malicious IP Addresses

IP Address	Country	Total
41.212.30.91	Kenya	43,750
193.194.92.242	Algeria	6,232
41.222.193.24	Benin	6,112
168.167.87.85	Botswana	3,038
41.201.24.6	Algeria	2,530
213.136.113.233	Côte d'Ivoire	2,162
41.223.142.96	Botswana	1,888
168.167.94.12	Botswana	1,800
168.167.87.1	Botswana	1,563
41.219.132.170	Nigeria	1,303

Graph 15: Top 10 ISPs in Africa:

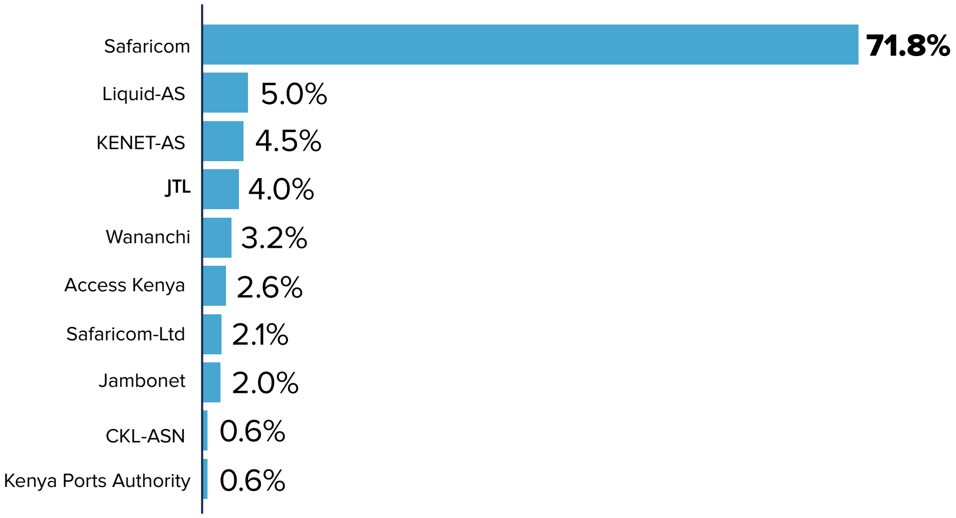
This information highlights the ISPs that are managing the networks where these exposed devices are located.



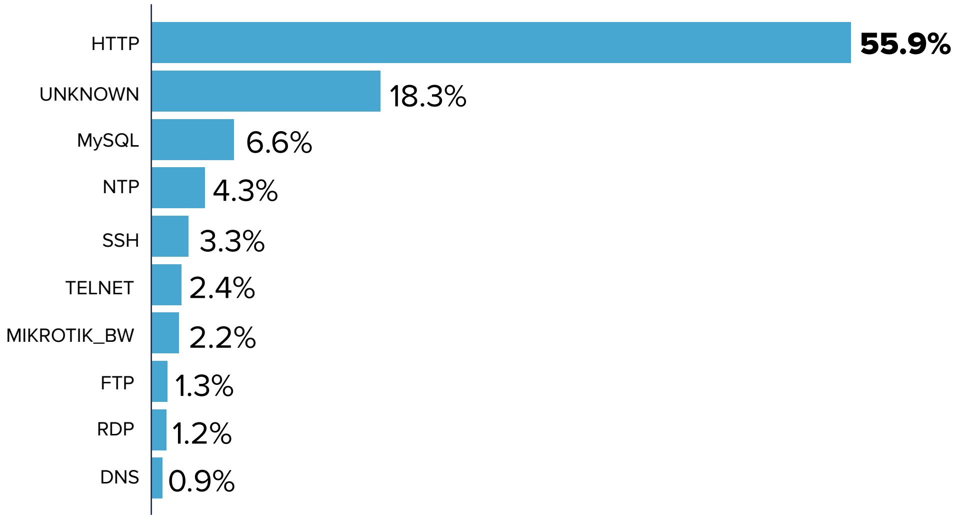
6.2. Kenya

a. Exposed Devices

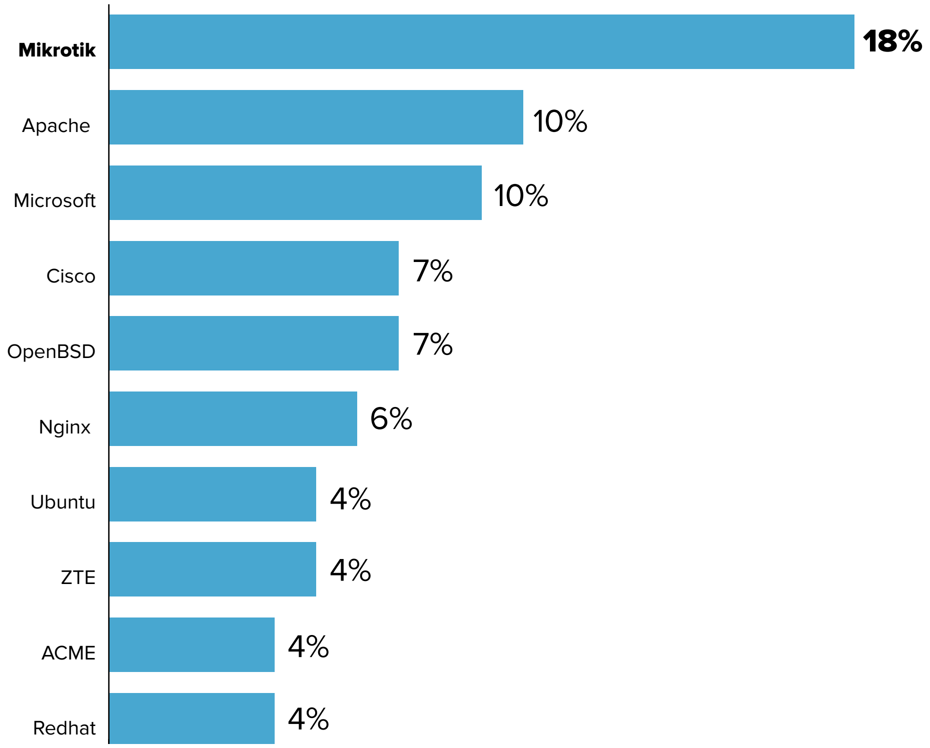
Graph 16: Safaricom has 71.8% assets exposed online.



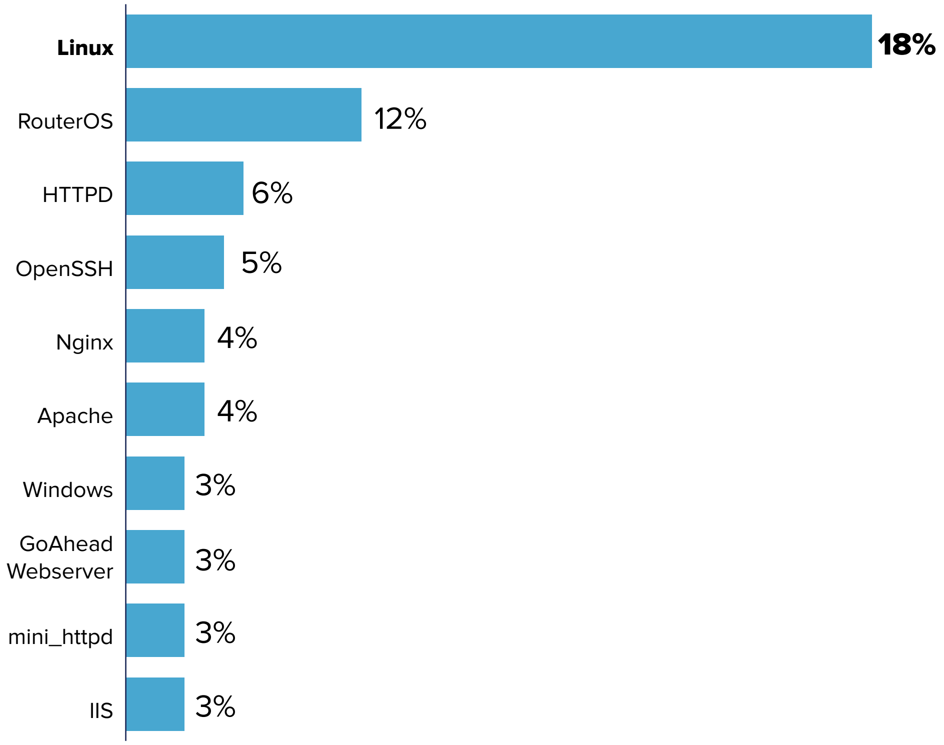
Graph 17: HTTP is the top supported service with 55.9%.



Graph 18: Devices running Mikrotik software form the top number of software vendors in Kenya with 18%.



Graph 19: Top 10 Software Products in Kenya



Top 10 Malicious IP Addresses in Kenya

The table serves as a highlighting of the top 10 most frequently reported malicious IP addresses detected by the Project Honeypot. These IP addressess have been involved in data harvesting, dictionary, comments and spamming attacks.

Table 2.

Malicious IP	Total
41.212.30.91	43,750
41.206.37.141	518
41.212.53.163	500
212.49.92.25	436
41.206.43.218	249
41.215.133.175	184
196.201.229.182	164
196.207.18.182	137
41.215.76.82	137
41.212.99.42	134

Industry Player Perspective

Impact of Regulatory Developments to SMEs

By Mugambi Laibuta

Certified Information Privacy Manager

This year's cybersecurity report focuses on data protection and cyber insurance. In the recent past in my work with clients in data protection compliance, the issue of data protection insurance has come up. The insurance companies that were approached with the possibility of offering data protection insurance were not sure how to handle the matter.

Some of the insurance companies, firstly, had not established comprehensive privacy programmes and secondly, they had no structures or policies related to data protection insurance cover. One of my clients finally found an expensive cybersecurity insurance cover that had data protection elements from an insurance company in the United States.

What the example demonstrates is that data controllers and data processors are potentially fully exposed to liability arising out of non-compliance with the Data Protection Act, 2019. To mitigate such exposure, it is instructive that at first instance, data controllers and data processors establish comprehensive privacy programmes that cover all compliance aspects in the Data Protection Act and Regulations.

In her speech at the International Data Privacy Day celebrations, Commissioner Immaculate Kassait, Kenya's Data Protection Commissioner reported that slightly over 1400 data controllers and data processors had successfully registered with her office.

This is a far cry from the 100s of thousands of data controllers and data processors operating in the country. The interesting bit about registration with the Data Commissioner is that seemingly, it is an easy process. However, registration is just one of the steps to comply with the Data Protection Act, 2019, but many are not complying.

In the last few months, the Data Commissioner has issued a penal notice of Ksh. 5 million to OPPO Kenya. The Commissioner has also been investigating 40 digital lenders and has issued an enforcement notice against Agha Khan hospital. Ideally, the possibility of an enforcement or a penal notice should motivate data controllers and data processors to establish comprehensive privacy programmes. This has not been the case as we have not witnessed significant activities towards data protection compliance.

One of the factors contributing towards low data protection compliance levels is the cost of compliance. When data controllers and data processors consider the financial constraints they are facing, data protection compliance does not rank among their top priorities. Many are downsizing their workforce or down scaling their operations. The effect is that the data controllers and data processors are left exposed to the possibility of enforcement and penal notices being issued against them. Secondly, they are vulnerable as they have no access to cybersecurity or data protection insurance.

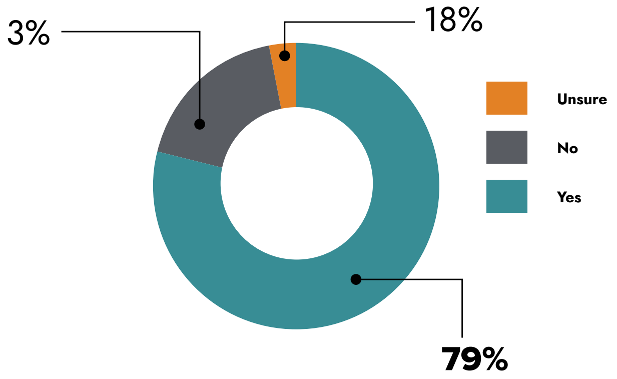
It could be argued that many of these entities have adopted a high-risk appetite mode of operation notwithstanding that they do not have sufficient risk capacity. What would remedy the situation is data controllers and data processors creating their privacy programmes step by step; allocating available resources to a few aspects of compliance at a time. This would work towards reducing exposure to risk. Secondly, sectors could organise and leverage on numbers to collectively train their members on data protection compliance. Thirdly, sectors could provide simplified sector specific data protection compliance guidelines for their members to adopt.

All in all the goal is to ensure there is movement towards data protection compliance and reduction of vulnerabilities and risks.

7. Survey Analysis

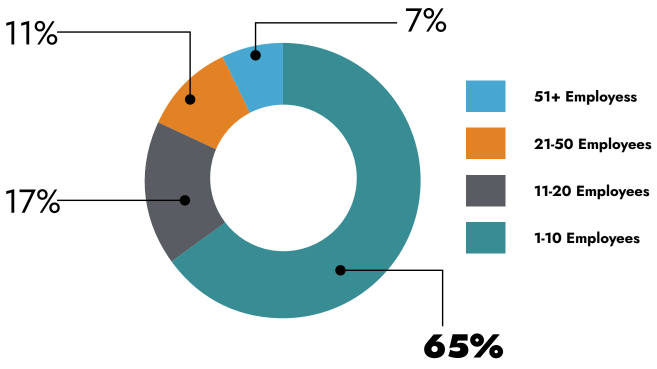
The 2022/2023 Cybersecurity Survey provides insight into what Kenyan organizations, both public and private, are doing to protect their information and assets considering the increasing number of cyber-attacks and successful data breach or funds loss . Based on feedback from over 200 IT and security professionals, the analysis of the findings yielded a few notable themes, which are explored in greater detail in this report.

1. We asked **Does your organisation have a dedicated information security team?**



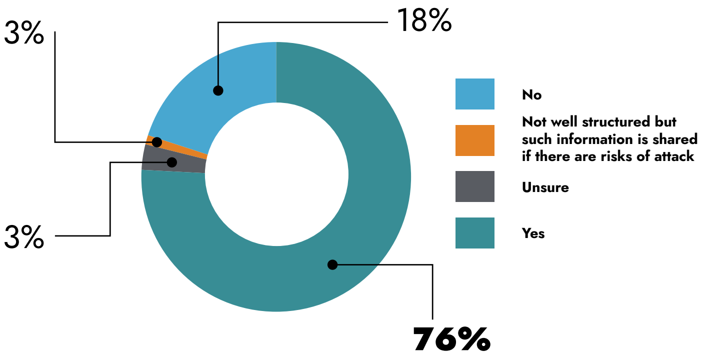
Our assessment revealed that **79%** of the analyzed institutions have dedicated information security teams. This can be attributed to the increasing need to mitigate cyber risks and comply with regulatory requirements.

2. We asked How large is your information security team?



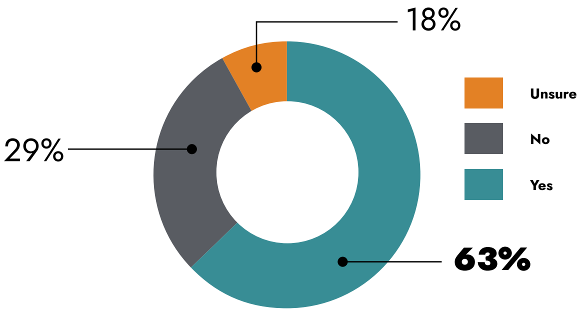
It is possible that certain organizations have encountered challenges in securing candidates with the appropriate skills for information security positions. The size of the security team should be congruent with the size of the organization.

3. We asked Do you have in-house personnel that review and advise your organisation on data protection matters?



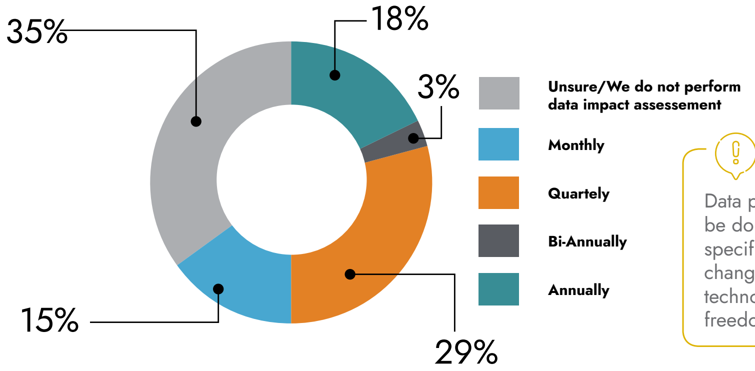
Some organizations engage in intricate data processing operations that demand continuous supervision and specialized knowledge and some organizations handle more sensitive data than others hence needing personnel that review and advise the organization on data protection matters.

4. We asked Does your organization conduct data impact assessments to evaluate its level of compliance against the relevant data protection regulations?



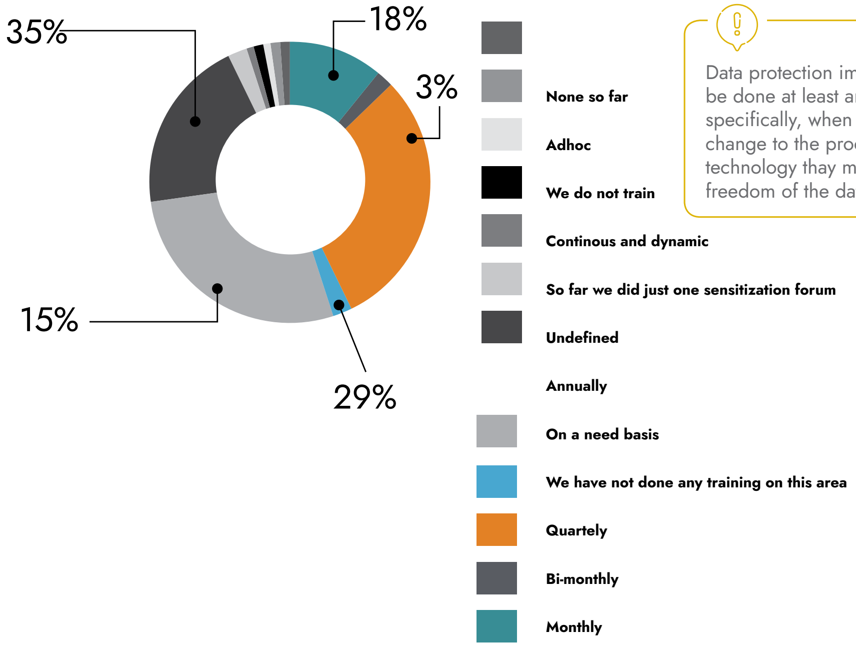
63% of the organizations conduct data impact assessment to evaluate their level of compliance against relevant data protection regulations such as the Data Protection Act (2019). This is also key in determing the nature of processing activities and the risks they may have to their data subjects.

5. We asked How often do these assessments take place?



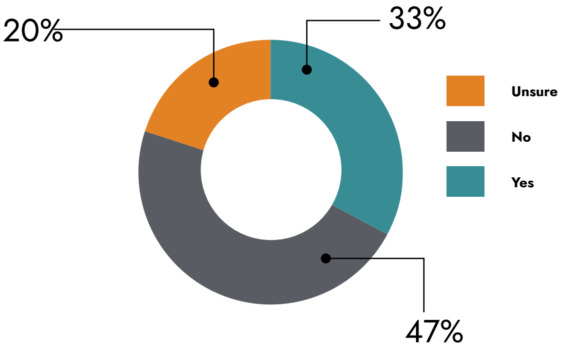
Data protection impact assessments should be done at least annually and more specifically, when there is a significant change to the processing activities and or technology thay may affect the rights and freedom of the data subjects.

6. We asked How often do you train your staff on cybersecurity and cybersecurity risks?



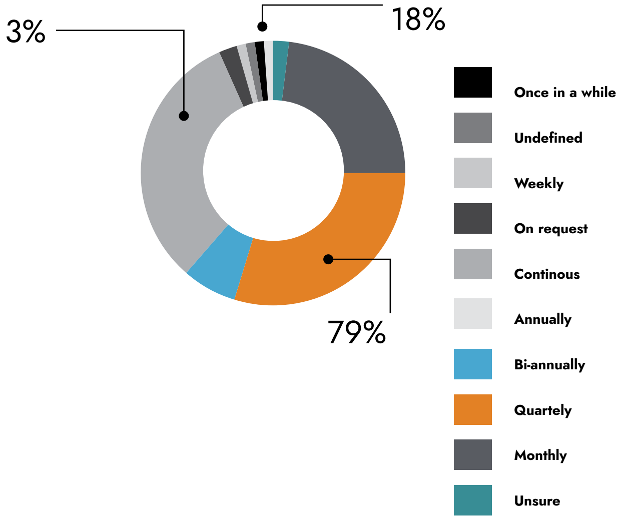
Data protection impact assessments should be done at least annually and more specifically, when there is a significant change to the processing activities and or technology thay may affect the rights and freedom of the data subjects.

7. We asked Does your organization have an insurance policy against cybersecurity incidents (cyber insurance)?



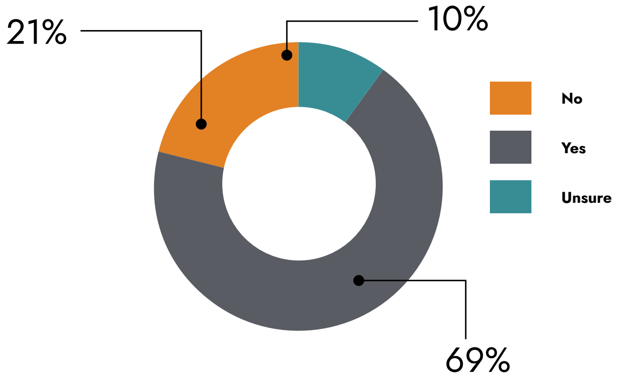
47% of the organizations do not have a cyber insurance. Having cyber insurance is important for an organization to protect it against the risk of cyber events. Some organizations have it to protect their reputation and build trust with their clients.

8. We asked How often does your organization perform cyber security breach testing?



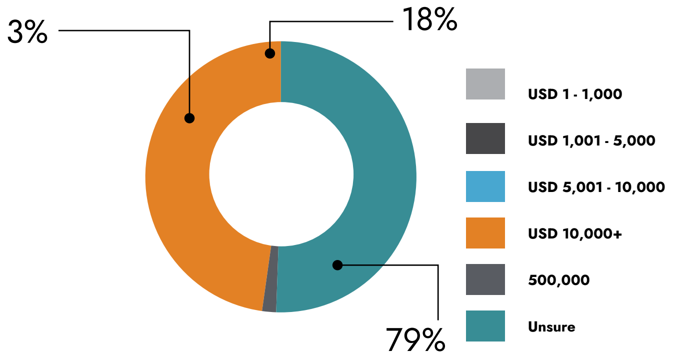
It is important to perform cyber security breach tests to highlight clear flaws and root out subtle vulnerabilities from a hacker's perspective. Penetration testing identifies and highlights possible weaknesses in a system. Penetration testing recognizes the strengths within a system, curbs risk management by assessing practical consequences and probabilities associated with different cybersecurity risks and mitigates the risk of non-compliance. Vulnerability assessment addresses potential weaknesses proactively to prevent exploitation by malicious entities, enhances both security measures and the allocation of resources and strengthens trustworthiness with stakeholders

9. We asked Does your organisation regularly collect and review cyber threat intelligence?



69% of the organizations regularly collect & review their cyber threat intelligence meaning that they are better placed to foresee and prepare for imminent threats.

10. We asked Approximately how much does your organization spend on cyber security annually?



Organizations that set aside an appropriate amount on cyber security related matters (people, processes and technology) are better prepared for any cyber risks.

Industry Player Perspective

Uptake of Cyber Insurance

By Nabihah Rishad

Product and Research Lead
Serianu Ltd

Cyber risks constitute a defining challenge as they are becoming more widespread, high profile and have high financial impact. It has now emerged as one of the top risks that concern Chief Risk Officers and enterprise insurance buyers. Looking at the current trends, the market for cyber insurance is growing however demand is still outstripping supply. It is prudent for business leaders to consider where to invest towards cyber insurance and contingency planning to respond to a breach.

The nature of the current insurance solutions available contain strict monetary limits, well below potential economic exposure as well as carve-outs and exceptions for certain types of loss. One of the key barriers to the industry is accurate risk assessments to expand coverage at appropriate pricing.

As per the fundamental law of insurance that bad risk brings higher premiums, cyber insurance has been made unaffordable for many firms. Small and Medium Sized Enterprises (SMEs) have been affected in particular. Mitigating risks provides a way of reducing premiums and in the case of cyber, best practice guidelines are relatively easy to achieve.

> **Looking at the challenges being faced by the insurance market; poor cybersecurity hygiene, aggregation of risk and capital scarcity are the most significant. As the cyber risk levels continue to rise, demand for cyber insurance is increasing significantly which is reflected in market projections. However, many insurers are struggling with rising losses, technology change and an uncertain regulatory environment.**

As cyber threats increase, defending against them becomes more challenging, cyber insurers are required to ensure that they protect themselves from costly payouts through ensuring the security posture of their applicants.

The Insurance Market

The primary levers that insurers have that will be able to create a functional and sustainable cyber market include:

- Mitigating individual risks through enhanced cybersecurity
- Rightsized exposure, especially for cyber catastrophes
- Access to capital for cyber underwriters

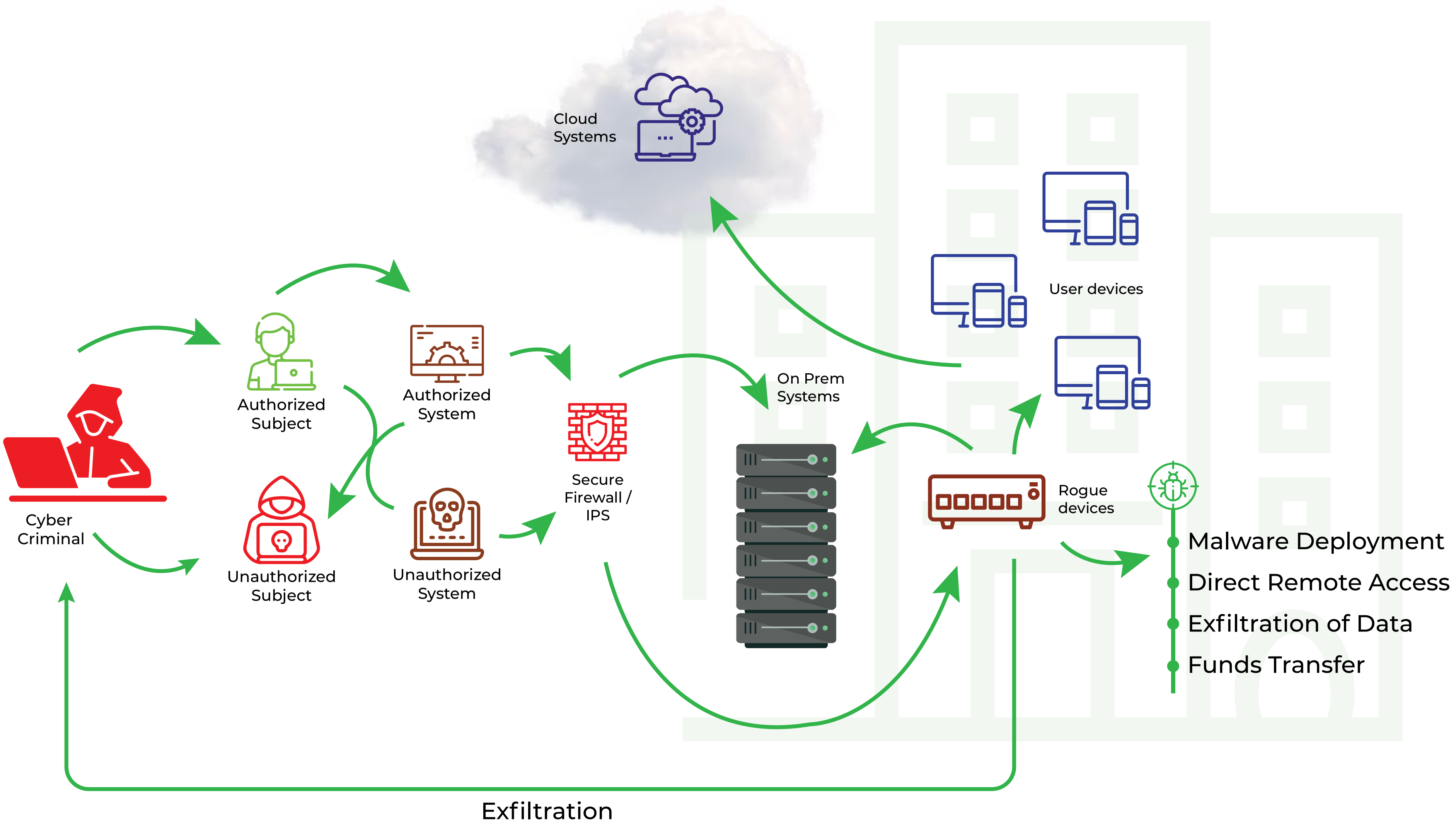
Market Need

- Accurate policy and portfolio pricing while reducing overall risk exposure
- Clear underwriting process
- Cyber analytics technology
- Technology consensus
- Partnership with cyber security experts and with insurers, reinsurers and investors

Conclusion

While insurance policies may help organizations recover some costs they do not necessarily reduce risks. This is due to the fact that these risks are constantly evolving, along with technology, security vulnerabilities, and the motivations of cybercriminals. Cyber insurers are now partnering with technology firms to provide cyber risk management and transfer as a collaborative product. This ensures that the underwriting process is more holistic and informed.

8. Anatomy of Attack



9. 2024 Priorities

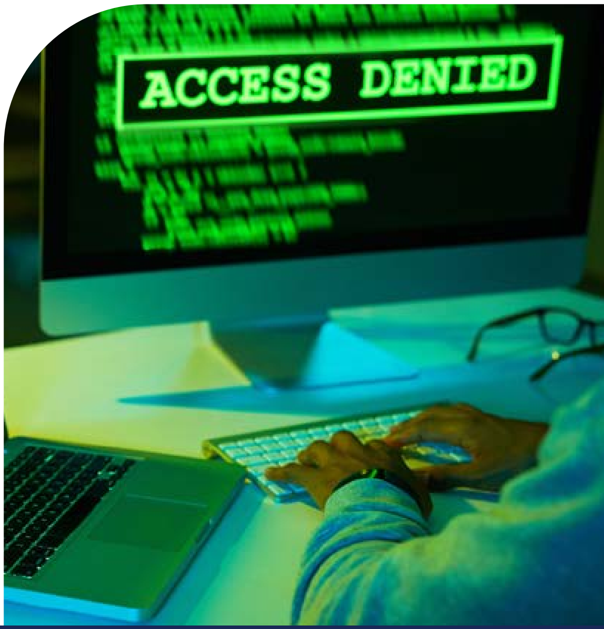
Reducing the cost of cybersecurity at micro level

- **Adopt risk based threat exposure management frameworks to guide cybersecurity investment prioritization.**
- **Simplify cybersecurity management by adopting unified, single view and consolidated platforms.**
- **Build and enhance identity threat detection and response capabilities.**
- **Consider xaas/opex based product offerings to reduce overall cost of technology acquisition and maintenance.**
- **Implement continuous and real-time cybersecurity controls validation and visibility.**
- **Position cybersecurity as a business value creation driver for internal teams.**
- **Adopt human centric cybersecurity design to address distributed working considerations.**
- **Enhance board level cybersecurity competencies and oversight capabilities.**
- **Decentralize cybersecurity management and involve non-technical business departments.**
- **Implement capabilities that automate and improve incident detection and response efficacy.**
- **Embrace and support the design and deployment of secure architectures using composable security approaches.**

Africa's 1st SME-Focused Cybersecurity-as-a-Service

Traditional approaches to cybersecurity are **COMPLEX, INEFFECTIVE** and **EXPENSIVE.**

Serianu Cybercare makes cybersecurity **SIMPLE, EFFECTIVE and AFFORDABLE** for SMEs.



SERIANU
Cybercare
Simple • Effective • Affordable

Serianu's Cybercare for SME leverages best in-class technologies, global frameworks and a dedicated team of certified cyberrisk management professionals to deliver cost effective world class managed cybersecurity risk management services to SMEs across Africa.

Benefits

Cybercare customers gain the advantage of having a single vendor, unified contract, and dedicated customer success team.

Simple
One vendor, easy deployment, practical, automation and realistic outcomes.

Effective
Metrics to track and measure business-relevant cybersecurity outcomes.

Affordable
Predictable, per-user/device, opex-based and subscription pricing.

Flexible
Multiple service offerings giving customers the choice to meet customer needs.

For more information CONTACT US

SERIANU

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
Seriangu Limited

https://www.serianu.com

10.Cyber Shujaa Program

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

Over the last 6 years Serianu has been 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 above challenges. We are focused on continuously analyzing 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.

Through our consortium, Kenya Bankers Association provides the market intelligence that informs the curriculum development, USIU Africa designs the curriculum and ensures the youth are at the heart of the program while Serianu Limited provides the technical training and immersion.

3-year Goal for the Program

Upskill

2000 **youth in cybersecurity skills**

50% **female**

Improve the job decency of

1000 **youth in cybersecurity skills**

Support

30 **Cybersecurity entrepreneurs (youth)**

A harmonized cybersecurity employment framework linking the supply (academia) and demand (industry).

Accessible opportunities for youth (more qualified youth employment in the cyber security industry).

More gender sensitive female mainstreaming in the cybersecurity industry.

Youth access to better paying and stable jobs

Our Success Thus Far

official launch
March 2022

- **2500+** Total Applications
- **1623** Total Recruitments into the program
- **750+** Total Participants trained
- **550** Placed in Organisations
- **75+** Organisations where our graduates are placed
- **75+** Universities and colleges where our graduates are from

Our trainings are for:

- Data Protection for Professionals
- Cloud & Network Security
- Security Analyst
- Entrepreneurship and Business Development for youth seeking to invest in the IT Industry

Let's connect & bridge the gap together

☎ +254 735 919 662

jndegwa@cybershujaa.co.ke

cybershujaa.co.ke

cybershujaa

11. Digital Empowerment Program for Primary School Students

Digital Empowerment Program

This program supports digital learning by giving computer access to children in under-served communities as well as enhancing digital teaching methods. We have built one digital lab in Kibaoni that is serving more than 800 students to improve their digital literacy and are working on building an accredited curriculum for Grade 1 - Grade 6.

Program	**Statistics**	
Serianu Cyber Immersion Program (SCIP)	**19** students Recently graduated	14 — Kenya 5 — Botswana
ACIC for High School	**20** students	Worked with Nairobi Academy in 2023
Digital Empowerment Program	**2** labs built in Kibaoni and Shisasari Primary School Kibaoni — Grade 7 (20) , Grade 6 (150) Shisasari — Approx. 50	
Public Sector Awareness Training	REPUBLIC OF KENYA The National Treasury & Economic Planning The National Treasury	**300+** Members Trained 3 days a week | 7 Topics
Enhancing University Curriculums and Student Projects	UNIVERSITY OF NAIROBI	* students
Cyber Shujaa	Cyber Shujaa	**790** Total trained | **514** Placed

12. References

- ICT Authority: Public Key Infrastructure. ICT Authority - Projects. Kemp, S. (15 February,2022).
- Digital 2022: Kenya. Digital 2022: Kenya — DataReport — Global Digital Insight
- Tanui, C. (11 May, 2022). Cyber threats in Kenya up 142pc despite increased issuance of advisories. Cyber threats in Kenya up 142pc despite increased issuance of advisories - Capital Business (capitalfm.co.ke)
- Eight Cybersecurity Trends to Watch for in 2023 (isaca.org)
- The Web's Largest Community Tracking Online Fraud & Abuse | Project Honey Pot
- Allianz Commercial. (January 2024). Top 10 Risks in Kenya. In Allianz Risk Barometer Results: Appendix 2024. page 27
- Fortinet. (2023). CISOs Need to Take a Holistic Approach to Risk Management. https://www.fortinet.com/blog/ciso-collective/cisos-need-to-take-a-holistic-approach-to-risk-management
- Enisa (2023) ENISA Threat Landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023?v2=1
- Kaspersky, 2023, Top Ten Cybersecurity Trends, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends