

Data Breaches in the African Region

Sophisticated cybercrimes and digital espionage are on the rise due to the financial and economic status of the countries in the African continent.



43%

The past year has seen a 43% increase in the total African population of 1.37 billion connecting to the internet, due to the pandemic and people working remotely.



\$4.1Bn

The cost implications of weak networks and lack of robust cybersecurity policies for Africa are estimated at US\$4.1 billion by Kenyan cybersecurity company Serianu.



AFRIPOL

Business Email compromise is one of the greatest concern for cybercrime on the African continent, according to AFRIPOL.



Source: CIO

Companies in the Middle East and Africa experience the most insider incidents globally



15.4%

Employee or contractor negligence



7.3%

Criminal or malicious insider



4.2%

Credential thief (imposter risk)

Source: Proofpoint



Out of 54 countries, **50%** have enacted data protection legislation

Source: Tamimi



52%

of companies in Africa believed they are unprepared to handle a large scale cyberattack

Source: Weforum



*** \$14.3M

The total average cost of activities to resolve insider threats over a 12-month period

Source: Proofpoint



90%

Businesses in the continent are operating without the necessary cybersecurity protocols in place

Source: Weforum



86%

Nigerian organizations affected by public cloud security incidents

Source: BizCommunity



85%

Financial institutions fallen prey to cyberattack resulting in loss

Source: TheAfricaReport

Identify and Contain a Data Breach in South Africa

177 days

Avg. time to identify a data breach

Source: CSIRT

51 days

Avg. time to contain a data breach once identified

Top 5 Causes for Data Breaches in Africa



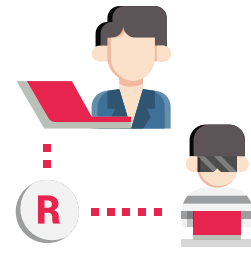
Ransomware



Botnets



Phishing



Digital Extortion



Business Email Compromise

Source: CIO

The Rise of Data Regulations to Solve the Problem

Compliance and Privacy regulations like the Kenya's Data Protection Act (DPA), Ghana Data Protection Act, 2012 (DPA), The Nigeria Data Protection Regulation 2019 (NDPR), and The Data Protection and Privacy Act of Uganda, enacted in 2019 (Act) require organizations to protect critical and sensitive information.



The majority of the data privacy regulations focus on:



Who can **access** consumer data?



Consequences of **sharing** consumer data with vendors



Protecting data at the source to eliminate the **risks associated** with external collaboration, cloud computing and BYOD



Enforcing strict security policies on the **usage and movement of data**

Protect Digital Assets, Curb Insider Threats and Achieve Data Privacy & Compliance with Seclore

- Meet Data Privacy Regulations
- Automate Data Protection
- Protect Incoming Customer Data
- Integrate & Automate with Enterprise System
- Track & Report Data Usage
- Classify digital assets and emails



Learn about the Data Security challenges in the African region and how Seclore helps counter those challenges

[Download Datasheet](#)