IJBES
Business Ecosystem & Strategy

Business Ecosystem & Strategy

IJBES VOL 8 NO 6 (2026) ISSN: 2687-2293

Available online at www.bussecon.com
Journal homepage: https://bussecon.com/ojs/index.php/ijbes/index

Digital Business Ecosystem Vulnerability in Africa: A Multi-Method Analysis of Economic Scale and Cyber-Loss Exposure

Marilyn Sithole[(a)]*; *Odette Swart*[(b)]; *Freddy Muzhelele*[(c)]

[(a)] *Department of Financial Intelligence, University of South Africa (UNISA), South Africa*
[(b)] *Department of Financial Intelligence, University of South Africa (UNISA), South Africa*
[(c)] *Prof. Department of Financial Intelligence, University of South Africa (UNISA), South Africa*

ARTICLE INFO

Article history:

Received 20.08.2026
Received in rev. form 27.08.2026
Accepted 15.09.2026

Keywords:

Cybersecurity breach costs; Economic scale; GDP; Cyber risk; Africa

JEL Classification:

M15, G20, G21

ABSTRACT

Africa's digital business ecosystems are expanding rapidly through mobile banking, fintech innovation, digital payments, e-commerce, and cross-border financial integration. While these developments promote economic growth and financial inclusion, they also increase cybersecurity vulnerabilities across interconnected organisations and stakeholders. This study examines the association between economic scale and cybersecurity breach costs across 55 African countries. Using a mixed-methods approach, the research combines qualitative classification of countries according to digital-finance integration with quantitative analyses, including descriptive statistics, kurtosis, and regression modelling. The findings reveal substantial regional variation in cyber-risk exposure, with phishing, malware, business email compromise, and social engineering emerging as the most prevalent threats. The results demonstrate that cyber risk should be understood as an ecosystem-level phenomenon arising from increasing digital interconnectedness among financial institutions, fintech firms, mobile-money providers, governments, and consumers. Regression analysis indicates a statistically significant positive association between GDP and cybersecurity breach costs, suggesting that larger economies generally experience higher financial losses from cyber incidents. However, the findings reflect association rather than causation, as factors such as cybersecurity maturity, digital infrastructure, internet penetration, and regulatory effectiveness may also contribute to cyber-loss exposure. High-GDP countries, including Nigeria, South Africa, Egypt, Morocco, and Kenya, experience disproportionately higher breach costs. The study contributes an ecosystem-oriented framework for understanding cyber-loss exposure and provides evidence to support targeted cybersecurity investment, governance, and resilience-building strategies across Africa.

© 2026 by the authors. Licensee Bussecon International Academy, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Africa is undergoing a rapid digital transformation, characterised by increased internet penetration, mobile banking adoption, e-commerce growth, cloud computing, and the expansion of digital public services (International Telecommunication Union [ITU], 2024; Cobos, 2023). According to the ITU, internet penetration in Africa increased from 28% in 2019 to over 44% in 2024, while the number of mobile money users exceeded 700 million, illustrating the continent's growing reliance on digital infrastructure (ITU, 2024). These advancements bring significant economic opportunities, but they also create new vulnerabilities, particularly in the form of cyber threats such as cybersecurity breaches (Sharif & Mohammed, 2022; Wirth, 2017; Yasuttamathada & Worapongpat, 2025).

The paper uniquely shifts from the usual organisation-level investigation of cybersecurity to an ecosystem-level cyber-risk. It provides a continent-wide analysis involving 55 African countries, rather than another single-country cybersecurity case. It justifies targeted cyber investment across the 55 countries instead of having a blanket approach. Cybersecurity investments must account for economic scale, digital-finance integration and ecosystem interconnectedness.

* Corresponding author. ORCID ID: https://orcid.org/0009-0009-9362-2362 | Email: 50860399@mylife.unisa.ac.za
© 2026 by the authors. Hosting by BUSSECON International Academy. Peer review under responsibility of Bussecon International Academy
https://doi.org/10.36096/ijbes.v8i6.1560

Cybersecurity breaches and unauthorised access to sensitive information pose substantial financial, operational, and reputational risks. Globally, wealthier nations often incur higher financial losses during breaches due to the larger volume and value of digital assets, stringent regulatory frameworks, and higher litigation risks (IBM & Ponemon Institute, 2023, 2024, 2025; Bederna & Szádeczky, 2023). In Africa, however, empirical data on cybersecurity breach costs remain scarce, despite growing anecdotal evidence of attacks on banks, telecommunications companies, and government services (Maulita & Hayadi, 2025; Umoga, Sodiya, Amoo, & Atadoga, 2024). Understanding the association between economic size, measured by Gross Domestic Product (GDP), and cybersecurity breach costs is crucial for guiding investment in cybersecurity, shaping regulatory frameworks, and supporting resilient digital economies across the continent (Farahbod, Shayo, & Varzandeh, 2020; Huygen & Beulen, 2025). This study demonstrates that economically significant digital business ecosystems exhibit greater cyber-loss exposure because increased ecosystem interconnectedness expands the attack surface and amplifies systemic cyber risk

While global studies have examined cyber risk and economic factors, research focusing on Africa is limited. Existing studies often report correlations between economic indicators and cyberattacks, but rarely employ predictive quantitative analyses to model financial losses based on GDP. This study addresses the knowledge gap by integrating qualitative classification of countries based on digital finance integration with quantitative analysis, including descriptive statistics (minimum, maximum, kurtosis) and regression modelling, to estimate and predict breach costs across countries and regions. Furthermore, research on the effect of cybersecurity breaches within accounting contexts in Africa is limited (Swift, Colon & Davis, 2020), highlighting the originality and relevance of this study. Cyber risk is not merely a country-level phenomenon but an ecosystem-level challenge concentrated around the most economically significant and digitally interconnected economies in Africa.

Policymakers and business leaders in Africa currently lack sufficient quantitative evidence to assess how economic growth influences cyber risk exposure (Cobos, 2023; Aguilar, 2015). This absence of empirical analysis creates several challenges: cybersecurity budgets may be misaligned with actual risk, small and medium-sized enterprises (SMEs) may remain particularly vulnerable due to limited resources, and regulatory frameworks may not adequately reflect the evolving threat landscape (Osborn, 2015; Sharif & Mohammed, 2022). Furthermore, Africa's heterogeneous digital ecosystem, with stark differences in infrastructure, GDP levels, and cybersecurity readiness across regions, suggests that a uniform approach to cybersecurity strategy is ineffective (Farahbod, Shayo, & Varzandeh, 2020; Ponsard, Grandclaudon, & Dallons, 2018).

SMEs, which constitute over 90% of businesses in Africa, face disproportionate risk from cyberattacks due to limited IT budgets, scarce cybersecurity expertise, and inadequate risk awareness (Aguilar, 2015; Wright, Jensen, Thatcher, Dinger, & Marett, 2014). Meanwhile, large enterprises and critical infrastructure providers are often targeted for higher financial payoffs (IBM & Ponemon Institute, 2024; Wirth, 2017). Without region-specific, data-driven insights into breach costs relative to economic size, governments and private actors cannot make fully informed decisions regarding resource allocation, risk mitigation, or cybersecurity investment (Maulita & Hayadi, 2025; Umoga, Sodiya, Amoo, & Atadoga, 2024; Huygen & Beulen, 2025).

This paper seeks to address this gap by examining the association between GDP and cybersecurity breach costs at national and regional levels across Africa, offering actionable evidence for tailored policymaking and strategic investment (Sharif & Mohammed, 2022; Cobos, 2023). Specifically, the paper investigates how economic scale, measured by national GDP, influences the financial impact of cyberattacks. It explores regional variations by aggregating countries into sub regions, Southern, West, North, East, and Central Africa, and applies descriptive statistics, including mean, minimum, maximum, standard deviation, and kurtosis, to identify patterns and variability of cyber risks. Regression analysis is further employed to quantify and predict the effect of GDP on breach costs, providing insights to inform targeted cybersecurity strategies and resource allocation.

The paper tests the following hypotheses:

i. *Null Hypothesis (H_0):*

There is no statistically significant association between national GDP and the average financial losses resulting from cyberattacks in African countries.

ii. *Alternative Hypothesis (H_1):*

There is a statistically significant association between national GDP and the average financial losses resulting from cyberattacks in African countries

2. Literature Review

2.1 Theoretical Framework

This paper is grounded in Cyberattack Theory, Risk Return Theory, and Economic Impact Theory, which collectively explain the is associated with, consequences and economic significance of cyber incidents. Cyberattack Theory suggests that cyber incidents occur due to the interaction between attacker capabilities, system vulnerabilities, and the perceived value of targets, with high-value nations (Jang-Jaccard & Nepal, 2014; Pirounias, Mermigas, & Patsakis, 2014). The Risk Return Theory suggests that higher-value assets face proportionally greater potential losses, implying that countries or businesses with larger GDPs or more valuable digital

infrastructure incur costlier breaches (Anderson et al., 2019; Farahbod, Shayo, & Varzandeh, 2020). The Economic Impact Theory highlights the macroeconomic consequences of cyberattacks, including direct losses such as stolen funds, ransom payments, data breach costs, legal fees, IT remediation, operational downtime, etc (Gañán, Ciere & van Eeten, 2017; Singh & Kumar, 2020). The theory also discusses how the cyber-attacks negatively affect the GDP over time Cobos, 2023; Sharif & Mohammed, 2022; Huygen & Beulen, 2025).

Empirical literature consistently demonstrates that economic wealth is correlated with the financial impact of cybersecurity breaches (IBM & Ponemon Institute, 2024). Organisations in wealthier countries, particularly those investing in Artificial Intelligence (AI)-based threat detection, security automation, employee awareness programs, and effective incident response strategies, experience comparatively lower breach costs (IBM & Ponemon Institute, 2025). Direct costs for SMEs in Africa can represent 5–20% of annual revenue, sometimes resulting in insolvency, while large enterprises and government entities can incur losses in the millions per incident (Aguilar, 2015; Osborn, 2015; Poniard, Grandclaudon, & Dallons, 2018; IBM & Ponemon Institute, 2024; Wirth, 2017). Indirect costs, including customer attrition, regulatory fines, reduced productivity, and long-term revenue decline, can exceed direct losses, particularly in emerging markets where trust and digital literacy are critical for business continuity across the African regions (Cobos, 2023; Sharif & Mohammed, 2022; Uddin, Ali, & Hassan, 2020).

Regional disparities are apparent in emerging markets, with Northern African nations such as Egypt and Morocco investing more in cybersecurity relative to GDP, while Sub-Saharan economies face infrastructure gaps, funding limitations, and skill shortages (Cobos, 2023; Klapper, 2024; Farahbod, Shayo, & Varzandeh, 2020). South Africa remains the most documented case, with average cybersecurity breach costs falling from R54.10 million (USD 2.95 million) in 2024 to R44.1 million (USD 2.45 million) in 2025 (IBM & Ponemon Institute, 2025). Across the continent, data remain fragmented, highlighting gaps in understanding regional and cross-country trends (Maulita & Hayadi, 2025; Umoga, Sodiya, Amoo, & Atadoga, 2024). Globally, the evolution of cybersecurity has shifted focus from protecting individual workstations to safeguarding digital business value, cyber-physical systems, operations, and supply chains. Major incidents such as the Petya ransomware attack on AP Moller-Maersk and breaches affecting FedEx, demonstrate the long-term financial and operational consequences of cyberattacks on large companies (Wirth, 2017; Sharif & Mohammed, 2022). Companies increasingly adopt risk-based approaches that integrate preventive and reactive controls with financial analytics, accepting some risks as calculated to optimise protection while minimising costs (Bederna & Szádeczky, 2023).

Unlike large companies, SMEs are disproportionately targeted, often serving as entry points to larger organisations through supply chain networks, and face automated attacks, phishing, malware, botnets, and exploitation due to weak cybersecurity measures and limited staff awareness (Aguilar, 2015; Osborn, 2015; Wright, Jensen, Thatcher, Dinger, & Marett, 2014; Ponsard, Grandclaudon, & Dallons, 2018; Sung, Kim, & Chang, 2018; Jang-Jaccard & Nepal, 2014). Emerging research highlights the acute vulnerability of African SMEs, with 60–70% experiencing cyberattacks, yet fewer than 25% having formal cybersecurity measures in place (Sharif & Mohammed, 2022; Aguilar, 2015).

Human factors, including social engineering and insider threats, aggravate vulnerabilities, while emerging threats such as ransomware, AI-driven attacks, and supply chain exploits further challenge organisations (Umoga, Sodiya, Amoo, & Atadoga, 2024; Garre, Pérez, & Ruiz-Martínez, 2021). Companies are developing metrics to evaluate protection levels and breach probability, but empirical research using real-world data remains limited, underscoring the need for data-driven approaches to strengthen cybersecurity strategies (Huygen & Beulen, 2025; Pirounias, Mermigas, & Patsakis, 2014; Uddin, Ali, & Hassan, 2020). Attacks often exploit weak authentication, unpatched software, and staff unawareness, leading to operational losses or business closures.

Despite these insights, studies quantitatively linking GDP to cybersecurity breach costs across African countries are scarce. While most theories and empirical evidence postulate that cyber-attacks drain the African economy and decrease the GDP (INTERPOL African Cyber Threat Assessment Report, 2024), in this paper we ask the question: Does a high GDP lure cybercriminal?

2.2 Conceptual Framework

The conceptual framework proposes that economic growth promotes digital business ecosystem expansion through fintech, digital payments, mobile money, and cross-border financial activity. Increased ecosystem interconnectedness creates greater cyber exposure, leading to higher cybersecurity breach costs and necessitating stronger ecosystem resilience and cyber governance. Table 1 displays the aforementioned discussion

Table 1: Economic Growth and Cyber exposure

Business Ecosystem Driver	Ecosystem Process	Cybersecurity Outcome
Economic Scale (GDP Growth)	Expansion of digital infrastructure and financial services	Increased digital assets exposed to cyber threats
Fintech Adoption	Greater platform integration and innovation	Increased attack surface
Digital Payments	Higher transaction volumes	Increased fraud and cyberattack opportunities
Mobile Money Ecosystems	Financial inclusion and digital connectivity	Increased vulnerability to phishing and social engineering

Business Ecosystem Driver	Ecosystem Process	Cybersecurity Outcome
Cross-Border Transactions and Remittances	Greater ecosystem interconnectedness	Increased exposure to transnational cybercrime
Digital Business Ecosystem Expansion	Increased interdependence among ecosystem actors	Systemic cyber-risk exposure
Cyber Exposure	Greater frequency and severity of incidents	Higher cybersecurity breach costs

Source: Researchers' Own (2025)

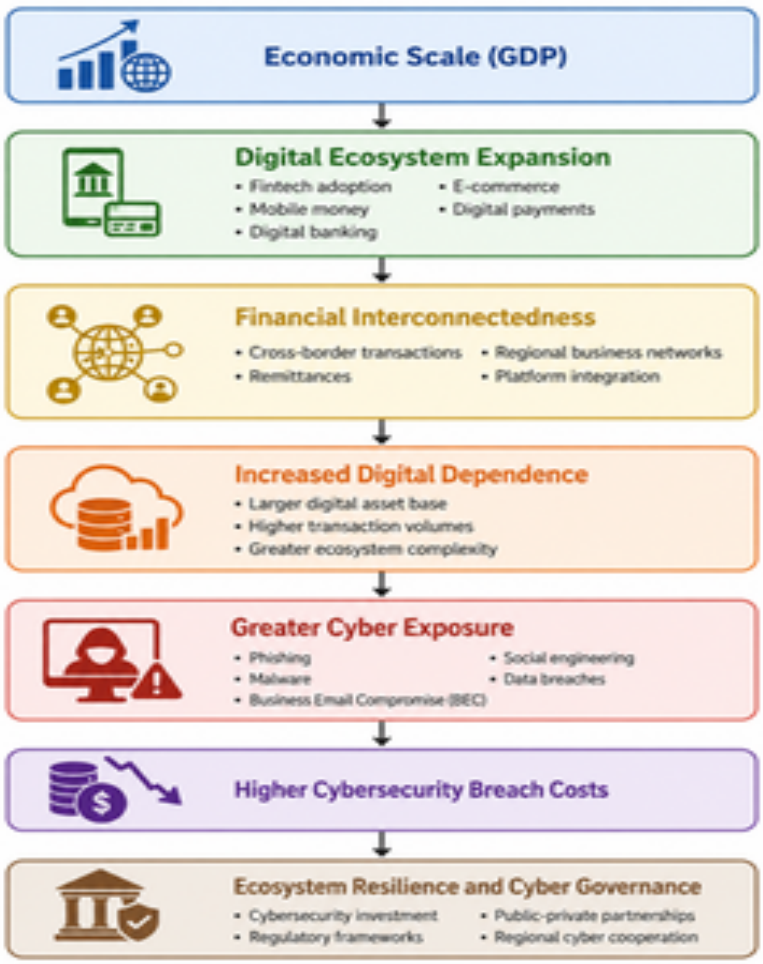


Figure 1: below shows how the GDP is increased by economic expansion and financial connectedness and digital dependence by entities in the business ecosystem. The use of digital devices exposes the economic participants to cyber losses. As such there is a need for cyber security measures and cyber governance to address the growing cyber losses.

Source: Researchers' Own (2025)

3. Research Methods and Design

The paper uses a quantitative-based mixed-method approach. Creswell & Plano Clark (2018) describe a literature classification and method of discussing qualitative results first and then the quantitative. This paper explores the qualitative using a descriptive narrative with the preliminary analysis of the literature review connecting GDP to cyber-attacks. The vulnerability of African countries based on their digital finance integration is discussed through classification. However, these qualitative analyses reflect correlation rather than causation, and further research using quantitative techniques is needed to establish definitive associative relationships. Quantitative techniques used include descriptive statistics (minimum, maximum and kurtosis).

Inferential statistics (regression analysis) are used to determine the financial losses in relation to the GDP of the African region at the country and regional level. The study, therefore, adopts a conservative interpretation of the regression results, treating GDP as a proxy for economic scale and digital asset concentration rather than a direct causal determinant of cyberattack losses. The dependent variable in this study is Breach Costs, while the independent variable is Total GDP.

This study employs a simple linear regression model to examine the association between national economic scale and cybersecurity breach costs across African countries. Gross Domestic Product (GDP) is used as the primary explanatory variable because it reflects overall economic activity, digital infrastructure development, and the scale of financial systems that may be exposed to cyber risk. While other factors, such as internet penetration, cybersecurity maturity, regulatory strength, and national cybersecurity investment, may also influence breach costs, comparable cross-country data for all African countries remain limited. As a result, these factors were not included as control variables in the present model. The analysis, therefore, focuses on identifying the statistical association between GDP and reported cybersecurity breach costs, rather than establishing direct causation.

Future research may incorporate additional control variables to test the robustness of this relationship. Predictive analysis using the formula derived from the regression analysis is applied to country and regional GDPs to predict average breach costs per region.

3.1 Study Population and Sampling Strategy

The study included all 55 African countries with available GDP and cyberattack cost data. Countries with missing or incomplete data were excluded. No sampling was required, as the study used a census of all eligible countries. Data were systematically compiled from publicly accessible international databases and cybersecurity reports.

3.2 Data Collection

Secondary data were collected from verified public sources, including World Bank GDP reports and cybersecurity cost studies. Data validity was ensured by using reputable sources. Extraction focused on GDP values and reported breach costs, with attention to accuracy and completeness.

Table 2: Data Sources and Variable Construction

Variable	Source	Year	Unit
GDP	World Bank GDP	2024	USD Billion
Breach Cost	IBM/Interpol/etc./ITU	2024	USD Million (M)

Source: Researchers' Own (2025)

3.2.1 Data Validation and Variable Limitations

Cybersecurity breach-cost information was compiled from publicly available international cybersecurity reports and regional cyber-threat assessments. Due to limited availability of standardised country-level breach-cost data across all African countries, the study focuses on identifying the statistical association between economic size and estimated cyber-loss exposure rather than establishing precise country-level financial losses.

First, baseline cyber-loss information was compiled from publicly available sources, including the IBM Cost of a Data Breach Reports, INTERPOL African Cyber Threat Assessment Reports, ITU cybersecurity publications, AFRIPOL assessments, and other peer-reviewed studies reporting cybercrime losses, cyberattack prevalence, and breach-cost information in Africa. Second, countries were classified according to indicators of digital exposure identified in the literature review, including digital-finance integration, mobile-money adoption, cross-border financial activity, remittance dependence, fintech development, and reported cybercrime incidence. The clustering exercise presented in Table 2 was used to identify countries with relatively higher cyber-risk exposure

Consequently, the findings should be interpreted as indicative of broad continental patterns rather than exact measures of national cybercrime costs

3.3 Data Analysis

Data were captured, checked, and cleaned for consistency. Qualitative analysis used descriptive narrative and country classification by digital finance integration. Quantitative analysis included descriptive statistics (minimum, maximum, kurtosis) and inferential statistics (regression) to model the association between GDP (independent variable) and breach costs (dependent variable). Regression formulas were applied to predict average breach costs per country and region.

3.3.1 Hypotheses and Regression Model

The study tests whether regional GDP is significantly positively associated with cybersecurity breach costs using the simple linear regression model:

Where the regression model is:

$$Y = \beta_0 + \beta_1 X + \epsilon$$

Y= average breach cost (M USD)

X= GDP (Billion USD)

β_0= intercept

β_1= slope coefficient (effect of GDP on breach cost)

ϵ= error term

A regression approach was implemented at the country level. Using data from 55 African countries, which is applied to the regional level analysis. Countries were aggregated into five African sub regions: Southern, West, North, East, and Central Africa.

3.3.2 Hypotheses Testing:

Null Hypothesis (H_0):

$H_0: \beta_1 = 0$ There is no relationship between GDP (X) and breach cost (Y); the slope of the regression line is zero.

Alternative Hypothesis (H_1):

$H_1: \beta_1 \neq 0$ There is a statistically significant relationship between GDP (X) and breach cost (Y); the slope of the regression line is not zero.

significance level, e.g. α=0.05

3.3.3 Predictive Analysis Using the Regression Formula

Inferential analysis was conducted using a simple linear regression model to examine the association between GDP (independent variable) and breach costs (dependent variable). The regression equation was specified as:

$Y_i=\beta_0+\beta_1 X_i+\varepsilon_i$

where Yi represents breach costs (M USD), Xi represents GDP (Billion USD), β0 is the intercept, β1 is the slope coefficient, and εi is the error term. The model was estimated using data from 55 African countries (n = 55, df = 53). Observed breach cost data were available for South Africa, Nigeria, and Egypt from IBM and INTERPOL reports, while values for other countries were imputed using regional averages scaled by GDP. This distinction between observed and imputed data was maintained throughout the analysis to ensure transparency.

Model diagnostics included reporting of the slope coefficient (β^1=0.0051), intercept (β^0=0.1033), coefficient of determination (R^2 = 0.952), sample size (n), degrees of freedom (df), and statistical significance testing. The slope coefficient was tested against the null hypothesis (H_0: $\beta_1 = 0$) using a t test. The calculated t value exceeded the critical threshold of ±2.006 at α = 0.05, with $p < 0.001$, confirming a statistically significant positive association between GDP and breach costs. The regression formula Breach Cost (M USD) = 0.1033 + 0.0051 × GDP (Billion USD) is then applied to the GDP to predict breach costs experienced in the region. The analyses were conducted in R software and Excel for statistical models and revealed statistically significant associations in both models.

Residuals (Observed – Predicted) were calculated for countries with available observed data to assess model fit. For South Africa, the predicted breach cost (2.084M USD) was close to the observed value (2.45M USD), yielding a residual of +0.366M. Nigeria's predicted value (2.523M USD) underestimated the observed 3.20M USD, with a residual of +0.677M. Egypt showed a similar pattern, with a predicted 1.725M USD compared to the observed 2.80M USD, yielding a residual of +1.075M. Mid-sized economies such as Kenya and Morocco also exhibited underestimation, with observed breach costs nearly double the predicted values. These residuals highlight that while GDP is a strong proxy for breach-cost exposure, additional factors such as digital-finance integration, cybersecurity maturity, and reporting practices contribute to observed variation.

Limitations were acknowledged in the methodology. Due to restricted availability of standardized cross-country indicators on cybersecurity investment, internet penetration, and regulatory strength, these variables were excluded from the regression model. This introduces potential omitted-variable bias, and results should therefore be interpreted as indicative of broad continental patterns rather than precise national estimates. Future research may incorporate additional control variables to test the robustness of the GDP–breach cost association.

Hypotheses Testing:

Null Hypothesis (H_0):

$H_0: \beta_1 = 0$ There is no statistically significant relationship between GDP and breach cost; the slope of the regression line is zero.

Alternative Hypothesis (H_1):

$H_1: \beta_1 \neq 0$ There is a statistically significant relationship between GDP and breach cost; the slope of the regression line is not zero.

significance level, e.g. α=0.05

Predictive Analysis using the Regression formula

The regression formula

Breach Cost (M USD) = 0.1033 + 0.0051 × GDP (Billion USD) is then applied to the GDP to predict breach costs experienced in the region.

The analyses were conducted in R software and Excel for statistical models and revealed statistically significant relationships in both models.

Regression Diagnostics and Residuals

Model diagnostics included R^2, sample size (n), degrees of freedom (df), t-test statistics, and p-values to assess the statistical significance of the GDP coefficient. Residuals (Observed – Predicted breach costs) were calculated for countries with available IBM/INTERPOL data (South Africa, Nigeria, Egypt) to evaluate model fit. This ensured transparency in reporting and highlighted where GDP-based predictions underestimated observed breach costs.

Observed vs. Imputed Data

Observed breach-cost data were available for South Africa, Nigeria, and Egypt. For other countries, breach costs were imputed using regional averages scaled by GDP. This distinction between observed and imputed values was maintained throughout the analysis to avoid overstating data coverage.

Limitations

Due to limited availability of standardised cross-country indicators on cybersecurity maturity, internet penetration, and regulatory strength, these variables were excluded from the regression model. This introduces potential omitted-variable bias, and results should therefore be interpreted as indicative associations rather than precise causal estimates.

4. Results and Findings

4.1 Preliminary Analysis

A literature review indicates that phishing and malware constitute the most serious and variable cybersecurity threats across African regions, consistently accounting for high proportions of incidents with extreme spikes in certain areas. This pattern is consistent with reports from the International Telecommunication Union (ITU, 2024), INTERPOL (2024), the Financial Action Task Force (FATF, 2023), and Trend Micro (2024). In contrast, crypto jacking and Distributed Denial of Service (DDoS) attacks are generally less common, remaining relatively low across the continent. Central Africa and the African Diaspora emerge as particularly high-risk regions, exhibiting extreme peaks in specific threats.

The distribution of cybersecurity risks varies across the continent: some threats, such as DDoS attacks, are fairly consistent and widespread, while others, including Business Email Compromise (BEC) and crypto jacking, are highly concentrated in particular regions. These patterns align with the African Cyber Threat Assessment Report (2024), emphasising the need for region-specific mitigation strategies to protect critical infrastructure and business operations.

These findings can be interpreted through the lens of Cyberattack Theory, which suggests that cybercriminals target regions and sectors based on perceived vulnerability and economic attractiveness. Risk-Return Theory further explains that the likelihood of attack is proportional to the potential financial gain, accounting for why phishing and malware—which offer high returns—dominate the threat landscape. Finally, Economic Impact Theory contextualises the financial consequences of these attacks, illustrating how economically significant regions, such as Central Africa and areas with a substantial African Diaspora, experience disproportionate losses. However, it is important to note that these observations reflect correlations rather than associative relationships, highlighting the need for further research employing quantitative methods to establish definitive associative links.

Chain analysis links the highest incidence of cyber-attacks and financial losses with high digital finance integration, i.e. cryptocurrency adoption and mobile transaction volume in African economies (Chainalysis, 2024). According to Chainalysis (2024), Nigeria leads Africa in cryptocurrency adoption, ranking second globally, followed by Ethiopia, Morocco, Kenya, South Africa, Uganda, Algeria, Egypt, Ghana, and the Democratic Republic of Congo. These same countries face significant cybersecurity challenges, with Nigeria, South Africa, Kenya, Egypt, and Morocco among the most targeted (Ugwu & Ugwuany, 2024). The World Bank (2025) identifies mobile banking as a key driver of financial inclusion, with Kenya (M-Pesa), Nigeria, Uganda, and Tanzania experiencing significant mobile money growth. South Africa and Kenya had a 95% to 98% increase in digital payments due to the World Bank's Inclusive Digitalisation in Eastern and Southern Africa (IDEA) programme (World Bank, 2025). In Kenya, for instance, mobile money services have transformed access to financial services (World Bank, 2025). High remittance flows from diaspora further characterise these regions, demonstrating how digital financial activity, cybersecurity vulnerabilities, and financial inclusion converged in African e-commerce (Chainalysis, 2024; United Nations, 2024).

Substantial international remittances play a role in the GDP of African economies (United Nations, 2024). Those who benefited from international remittances and their digital payment systems incurred losses from cyberattack activities (United Nations, 2024). Egypt leads the continent with $22.7 billion, followed by Nigeria with $20.1 billion. Other significant recipients are Ghana ($4.6B), Kenya ($4B), Uganda ($1.8B), Senegal ($1.6B), South Africa ($1.5B), Tanzania ($1.3B), Zimbabwe ($1.2B), and Mozambique ($1.1B) (World Bank, 2024). These inflows supported socio-economic development and contributed to poverty reduction across the region

(World Bank, 2024). The same countries are listed as countries most exposed to cyber-attacks (Mohamed & Kama, 2023). An interesting pattern is observed as the same list of countries with remittances appears in the list of African countries most affected by cyberattacks and the resultant financial losses disclosed in the Africa Cyber Threat Assessment Report (INTERPOL, 2025). An unusual finding is that Zimbabwe, though having a low overall GDP, has high remittances, which have opened it up to cyberattacks (INTERPOL, 2025).

There appears to be an association between financial losses association by cyberattacks and countries and regions with high cryptocurrency adoption, substantial international remittances, widespread mobile banking and transaction activity, and high levels of e-commerce. This overlap suggests that countries with higher levels of digital financial engagement are more exposed to cyber risks, underscoring the importance of effective cybersecurity measures alongside financial innovation (Chainalysis, 2024; Ecofin Agency, 2024; World Bank, 2024). Countries that are the major hubs of financial and digital activity in Africa have the highest GDPs and cyber-related financial losses. These trends are observed together and depicted in Table 3 below.

Table 3: Countries Grouped by Digital Finance Integration and Cybercrime Exposure

Cluster 1: High Digital Finance Integration	Cluster 2: High Cross-Border Flows	Cluster 3: High Mobile/Fintech Use	Cluster 4: High Cybercrime Incidents	Cluster 5: High Regional Exposure
Egypt	Nigeria	Morocco	Ghana	Kenya
Nigeria	South Africa	Ghana	Ethiopia	Egypt
South Africa	Egypt	Nigeria	Kenya	South Africa
Kenya	Morocco	Egypt	Uganda	Ghana
Ghana	Kenya	South Africa	South Africa	Morocco

Source: Researchers' Own (2025)

Table 3 shows that countries with higher engagement in digital finance, cross-border transactions, and technological connectivity face greater exposure to cybercrime. This pattern demonstrates that as financial and technological systems expand, so does vulnerability to cyber threats, highlighting the importance of strengthening cybersecurity alongside economic and digital development. Nigeria, South Africa, Egypt, and Kenya are major digital and financial hubs with high GDPs, widespread fintech adoption, and extensive ICT infrastructure, making them frequent targets of ransomware, phishing, and business email compromise (Riek & Böhme, 2018; INTERPOL, 2024).

4.1.1 Cluster 1: High Digital Finance Integration

Countries in this cluster, Egypt, Nigeria, South Africa, Kenya, and Ghana, have well-developed banking systems, high financial transaction volumes, and advanced digital infrastructure. Their economies are heavily integrated with digital finance, making them attractive targets for financially motivated cyberattacks.

4.1.2 Cluster 2: High Cross-Border Flows

This cluster, Nigeria, South Africa, Egypt, Morocco, Kenya, represents countries with significant international trade, foreign investment, and cross-border financial transactions. High cross-border activity increases exposure to cyber threats originating from foreign actors and global criminal networks.

4.1.3 Cluster 3: High Mobile/Fintech Use

Countries such as Morocco, Ghana, Nigeria, Egypt, and South Africa exhibit widespread adoption of mobile-money services and fintech platforms. Their digital ecosystems are innovative and fast-growing, but this also heightens vulnerability to mobile-money fraud, phishing, and digital payment scams.

4.1.4 Cluster 4: High Cybercrime Incidents

Ghana, Ethiopia, Kenya, Uganda, and South Africa are frequently targeted by cybercriminals, with high incident rates reported for phishing, ransomware, social engineering, and malware attacks. These countries face elevated operational and financial risks due to both high attack frequency and often limited cybersecurity capacity.

4.1.5 Cluster 5: High Regional Exposure

Countries in this cluster, Kenya, Egypt, South Africa, Ghana, Morocco, experience strong spillover effects from regional cybercrime. Their interconnectedness with neighbouring countries' digital systems means that attacks or vulnerabilities in one nation can impact others, amplifying overall risk exposure.

4.2 Quantitative Analysis

The analysis of cybersecurity breach costs across African regions shows notable variation. Southern Africa experiences the highest average breach costs, with South Africa alone reporting an average of approximately USD 2.45 million per incident (IBM & Ponemon Institute, 2025). In contrast, Central Africa reports the lowest average breach costs, likely reflecting lower levels of digital economic activity (Ngejane et al.,2024).

When aggregated at the regional level, North Africa has the largest total GDP and correspondingly higher average breach costs (USD 0.71 million), followed by Southern Africa (USD 0.40 million), East Africa (USD 0.34 million), West Africa (USD 0.30 million), and Central Africa (USD 0.24 million) (IBM,2023; Jiang, Zhu & Zhang, 2024). These findings highlight that regions with larger economies or more developed digital infrastructure tend to experience higher financial impacts from cybersecurity breaches.

Descriptive analysis indicates significant variation in breach costs across African countries, with Southern Africa exhibiting the highest average costs. For instance, South Africa's average breach cost is approximately R44.1 million (USD 2.45 million), while countries in Central Africa report lower average costs due to less digital economic activity.

4.2.1 Descriptive Statistics:

Descriptive statistical analysis includes analysis of mean, minimum, maximum, and standard deviation (Yasuttamathada & Worapongpat, 2025). These are essential for understanding the distribution and severity of cybersecurity threats across African regions.For this paper, the mean indicates the average level of each threat across all regions, helping to identify the most prevalent risks. Minimum and maximum values highlight the regions with the lowest and highest exposure, respectively, pinpointing low-risk areas and areas for urgent interventions. Standard deviation measures the variability of threat levels across regions: high values suggest regions with extreme threats, while low values indicate relatively safe regions due to uniform threat levels, allowing for broader, generalised mitigation efforts.

Table 3 below shows calculations using descriptive statistics across the common cyber threats identified by AFRIPOL (2025). The values represent the percentage prevalence of each cyber-threat category reported across the African regions based on the AFRIPOL (2025) and INTERPOL (2024) cyber-threat assessments.

Table 4: Descriptive statistics of Cyberattacks in the African Region

Statistics	Ransomware	BEC	SE	Phishing & Malware	Data Breach	DDoS	Insider Threat	Crypto-jacking
Mean	49.69	50.73	61.94	68.21	37.48	17.56	32.00	6.70
Minimum	40.00	35.72	28.57	44.45	28.57	13.00	20.00	1.67
Maximum	62.50	66.67	100.00	100.00	63.89	22.22	43.75	22.22
Std. Dev	8.50	12.21	26.24	20.42	13.77	3.50	9.41	7.85

Source: Researchers' Own (2025)

Table 4 reveals significant variation in cybersecurity threats across African regions. Phishing and malware constitute the most prevalent threat category, with a mean value of 68.21%, followed by social engineering (61.94%), business email compromise (50.73%), and ransomware (49.69%). Data breaches exhibit a mean value of 37.48%, while insider threats account for 32.00%. DDoS attacks (17.56%) and crypto jacking (6.70%) remain comparatively less common. The standard deviations indicate that phishing and malware, social engineering, and business email compromise display the greatest variability across regions, suggesting that these threats require targeted, region-specific mitigation strategies. In contrast, DDoS attacks and crypto jacking are relatively less variable and may be managed through broader cybersecurity monitoring and control frameworks.

Overall, these statistics indicate that phishing and malware, BEC, and SE are the most serious and variable threats, requiring targeted, region-specific cybersecurity interventions, whereas DDoS and crypto jacking are less frequent and more evenly distributed, allowing for more uniform monitoring across Africa. These statistics suggest that some threats, such as phishing and malware, are both widespread and highly variable across African regions, while others, like DDoS and crypto jacking, are less common or more evenly distributed. These findings are consistent with reports from the ITU (2024), INTERPOL (2022, 2024), the Financial Action Task Force (FATF) (FATF, 2023), and Trend Micro (n.d.), which similarly highlight the prevalence of phishing and malware as major cybersecurity concerns in Africa. The results also align with the African Cyber Threat Assessment (2024), confirming that certain regions, particularly Central Africa and the African Diaspora, are at higher risk and therefore most in need of targeted cybersecurity interventions and region-specific mitigation strategies.

4.2.2 Regional Economic Structure and Cyber-Risk Exposure

Table 4 presents regional GDP distributions together with observed cyber-risk characteristics. GDP kurtosis is included as a descriptive measure of distributional shape and is used to identify whether regional economic output is evenly distributed or dominated by a small number of economies. The measure is interpreted cautiously and is not presented as a direct measure of economic concentration. This is indicated in Table 5 below.

Table 5: African Regional Cyber Risk and Economic Overview

Region	Total GDP (Billion USD)	GDP Kurtosis	Key Countries (High GDP)	Cyber Threat Variability	Risk Level
North Africa	1,071.8	-0.63	Egypt, Algeria, Morocco	Moderate	Moderate
West Africa	1,008.2	8.94	Nigeria, Ghana, Côte d'Ivoire	High	High

Region	Total GDP (Billion USD)	GDP Kurtosis	Key Countries (High GDP)	Cyber Threat Variability	Risk Level
East Africa	653.9	1.18	Ethiopia, Kenya	Moderate-High	Moderate-High
Southern Africa	592.5	5.49	South Africa, Angola	High	High
Central Africa	156.1	-0.79	Cameroon, Democratic Republic of Congo	Low-Moderate	Moderate-Low

Source: Researchers' Own (2025)

GDP kurtosis is used as a descriptive statistical measure of the shape of GDP distributions within regions. Higher kurtosis values indicate that GDP values are more heavily concentrated around a small number of observations and may signal the presence of dominant economies. However, kurtosis is not a direct measure of economic concentration and is therefore interpreted only as an exploratory indicator of regional GDP distribution

Cyber threat variability captures how much cyber threats fluctuate within the region, with higher variability indicating more unpredictable risks. Southern Africa, with a GDP of 592.5 billion USD and a high kurtosis of 5.49, is dominated by South Africa and Angola. Despite moderate cyber threat variability, the dominance of South Africa means breaches there have disproportionately high financial impacts.

West Africa and Southern Africa contain dominant digital business ecosystem hubs, particularly Nigeria and South Africa. These economies account for a substantial share of regional economic activity and digital financial transactions, which may increase ecosystem-wide cyber-risk exposure. Conversely, Central Africa exhibits lower levels of digital ecosystem development and correspondingly lower predicted breach costs.

GDP kurtosis is used as a descriptive indicator of the distribution of economic activity within each region. Higher values suggest that regional GDP may be concentrated among a small number of economies, while lower values indicate a more even distribution of economic output. The measure is presented for exploratory purposes and should not be interpreted as a direct measure of economic concentration.

West Africa, with a GDP of 1,008.2 billion USD and an even higher kurtosis of 8.94, is dominated by Nigeria, Ghana, and Côte d'Ivoire, facing both high economic concentration and high threat variability, which results in significant potential breach costs.

North Africa, with the largest GDP of 1,071.8 billion USD but a negative kurtosis (-0.63), has a more balanced economy across countries like Egypt, Algeria, and Morocco, so while cyber threats are moderate, the financial impact per country is less extreme.

East Africa (653.9 billion USD, kurtosis 1.18) and Central Africa (156.1 billion USD, kurtosis -0.79) have lower economic concentration and moderate to low threat variability, resulting in relatively lower breach costs. The analysis of African regional GDP and cybersecurity threats reveals important patterns in economic concentration and cyber risk exposure.

4.2.3 Economic Concentration and Ecosystem Dominance

The distribution of economic activity across African regions highlights the importance of ecosystem dominance in shaping cybersecurity exposure. In West Africa, Nigeria serves as the region's principal economic and digital hub, accounting for a substantial share of regional GDP while leading the continent in fintech adoption, cryptocurrency activity, and digital financial services. Similarly, South Africa dominates the Southern African digital ecosystem through its advanced banking sector, extensive digital payment infrastructure, and sophisticated financial markets. In North Africa, Egypt functions as a major economic gateway, characterised by high volumes of digital transactions, remittance flows, and cross-border commercial activity. These dominant economies act as central nodes within regional business ecosystems, facilitating innovation, financial inclusion, and economic integration. However, their extensive digital connectivity also expands the potential attack surface available to cybercriminals. As fintech activity, digital payments, and cross-border transactions increase, so too does exposure to cybersecurity threats and associated financial losses.

The findings therefore suggest that cyber risk is not merely a country-level phenomenon but an ecosystem-level challenge concentrated around the most economically significant and digitally interconnected economies in Africa. Figure 2 below depicts this relationship:

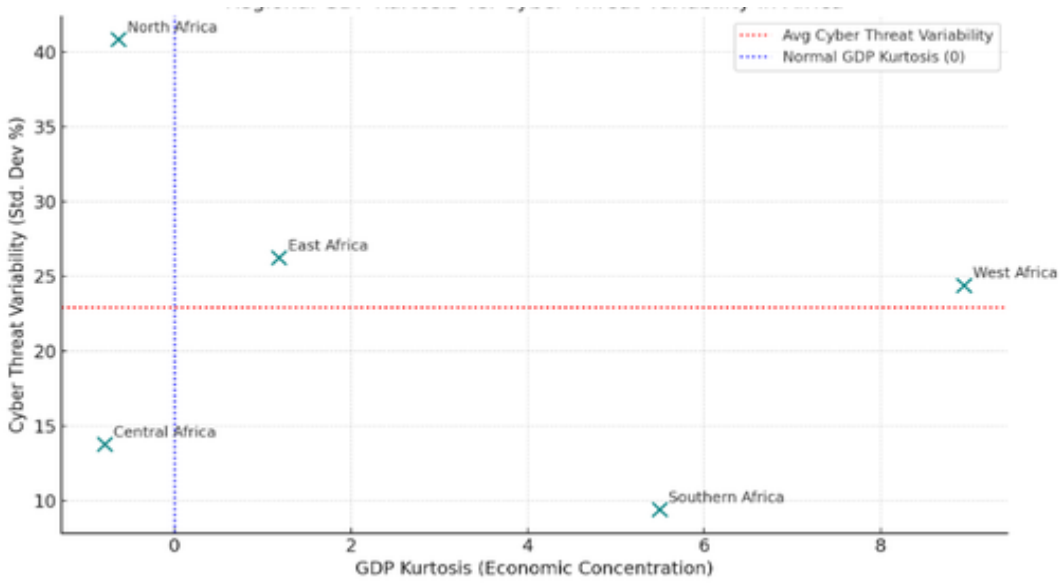


Figure 2: Regional GDP Kurtosis Vs Cyber Threat Variability

Source: Researchers' Own (2025)

The graph in Figure 2 compares economic concentration (GDP kurtosis) with the unpredictability of cyber threats (cyber threat variability) across African regions. High GDP kurtosis means a few countries dominate the region's economy, such as South Africa in Southern Africa and Nigeria in West Africa, while low or negative kurtosis indicates a more evenly distributed economy, as seen in North and Central Africa. High cyber threat variability means attacks like phishing, business email compromise (BEC), and social engineering are unpredictable and can spike in some countries. Southern Africa and West Africa show both high GDP concentration and high threat variability, meaning a breach in the dominant countries can lead to very large financial losses, so these regions require targeted cybersecurity measures. In contrast, North Africa and Central Africa have more balanced economies and lower threat variability, so the financial impact of cyber-attacks is smaller, and general monitoring is sufficient. East Africa has moderate economic concentration and moderate threat variability, indicating some risk, but not as extreme as Southern or West Africa.

The graph suggests that regions containing dominant economies and larger digital business ecosystems may face greater cyber-risk exposure and potentially higher financial losses from cybersecurity incidents. These observations are descriptive and should not be interpreted as evidence of a causal relationship.

4.3 Regression Analysis

Simple regression analysis was performed in this paper using the dependent and independent variables mentioned above. The regression results show a positive correlation between GDP and breach costs, suggesting that wealthier countries. The sample size is n=55 countries in Africa that incur higher absolute financial losses from cyberattacks. However, when adjusted for GDP per capita, the cost per capita is higher in lower-income countries, indicating that SMEs in these regions bear a disproportionate burden of breach costs.

The dependent variable in this study is cybersecurity breach cost, while the primary independent variable is national Gross Domestic Product (GDP). To reduce omitted variable bias and improve robustness, the analysis conceptually considers digital exposure factors such as internet penetration and digital financial integration as contextual control factors. These variables are widely recognised in cybersecurity literature as influencing cyberattack likelihood and reporting intensity. However, due to limited availability of consistent cross-country datasets covering all 55 African countries, these variables were not formally incorporated into the regression model. Consequently, GDP is analysed as the primary explanatory variable, and the results should be interpreted as indicating a strong association between economic scale and breach costs rather than a definitive causal relationship. To test robustness, countries were split into high versus low digital-finance integration clusters. This qualitative classification supplements the GDP regression, highlighting that breach costs are not solely explained by economic scale but also by ecosystem maturity and digital exposure. Where available, indicators such as internet penetration and ITU Global Cybersecurity Index scores were referenced to contextualize results.

4.3.1 Country-Level Results:

The regression analysis at the country level, covering 55 African countries, examined the relationship between national GDP and average breach cost in millions of USDs. The resulting equation is:

The regression model used in this study can be expressed as:

$$\text{Cybersecurity Breach Cost}_i = \beta_0 + \beta_1 GDP_i + \varepsilon_i$$

Where:

Cybersecurity Breach Cost$_i$ represents the reported breach cost for country *i*

GDP$_i$ represents the gross domestic product of country *i*

β_0 is the intercept

β_1 represents the estimated association between GDP and breach costs

ε_i is the error term

H0: β1=0

H_1: $\beta_1 \neq 0$

$t = (\beta_1 - 0) / SE(\beta_1)$

Then:

If $p < 0.05$, reject H_0. GDP is significantly positively associated with cybersecurity breach costs.

If $p \geq 0.05$, fail to reject H_0. GDP has no statistically significant association with cybersecurity breach costs.

If $|t| > 2.006$ (critical t-value at $\alpha = 0.05$, df = 53), reject H_0. GDP is significantly associated with cybersecurity breach costs.

If $|t| \leq 2.006$, fail to reject H_0. GDP has no statistically significant association with cybersecurity breach costs.

Breach Cost (M USD) = 0.1033 + 0.0051 × GDP (Billion USD)

β_0 = 0.1033 is the intercept

β_1*= 0.0051* represents the estimated GDP coefficient

A **t-test** is used for the coefficient β_1:

$$t = \frac{\widehat{\beta}_1}{SE(\widehat{\beta}_1)} = \frac{\widehat{0.0051_1}}{SE(0.0051\ \ )}$$

Where $SE(\hat{\beta}_1)$is the standard error of the slope coefficient. The calculated t-value is compared to the critical t-value at a chosen significance level ($\alpha = 0.05$).

β_1 = 0.0051

R^2 = 0.952

n = 55

df = 53

α = 0.05

critical t = ±2.006

$\beta_1 = 0.0051$ with $p < 0.001$, H_0 is rejected and H_1 is supported.

The intercept (β_0 = 0.1033) is positive, indicating that countries with higher GDP tend to have higher predicted cybersecurity breach costs. Specifically, a US$1 billion increase in GDP is associated with an increase of 0.0051 million USD in predicted breach cost, equivalent to approximately US$5,100. The slope coefficient (β_1 = 0.0051) was statistically significant, with a t-test confirming $p < 0.001$ at $\alpha = 0.05$. The calculated t-value exceeded the critical threshold of ±2.006 (df = 53), leading to rejection of the null hypothesis (H_0: $\beta_1 = 0$) and support for the alternative hypothesis (H_1: $\beta_1 \neq 0$). The regression model produced an $R^2 = 0.952$, showing that 95.2% of the variation in breach costs across the 55 countries is explained by GDP. Residual analysis indicates that South Africa and Nigeria exert disproportionate influence on the slope, reflecting their dominance in both GDP and breach-cost datasets. This represents a very strong association between economic scale and reported breach costs. However, the high R^2 does not imply that GDP alone determines cybersecurity losses. Breach costs may also be influenced by other factors, including digital infrastructure, internet penetration, fintech adoption, cybersecurity maturity, institutional quality, reporting practices, digitalisation, and the degree of digital interconnectedness. Predictions should therefore be interpreted as scale-based proxies rather than precise observed losses.

The association is significant, meaning the likelihood that this correlation is due to chance is extremely low. As such, higher GDP is associated with higher breach costs. The regression results indicate that higher GDP is associated with higher average breach costs

across African countries, demonstrating a strong, positive linear relationship between GDP and cyberattack financial impact across African countries.

The estimated GDP coefficient was statistically significant ($p < 0.001$). Therefore, the null hypothesis, ($H_0: \beta_1=0$), was rejected in favor of the alternative hypothesis, ($H_1: \beta_1 \neq 0$). The findings provide strong statistical evidence of a positive association between national GDP and cybersecurity breach costs across the 55 African countries examined.

Overall, the country-level regression demonstrates a strong positive linear association between economic scale and reported cybersecurity breach costs. Countries with larger economies tend to have higher predicted breach costs. This finding suggests that GDP can serve as an indicator of the scale of economic and digital activity and, consequently, the potential financial exposure of digitally connected business ecosystems.

However, the results establish an association rather than a causal relationship**.** The findings should therefore not be interpreted as evidence that an increase in GDP directly causes an increase in cybersecurity breach costs. Instead, the results indicate that greater economic scale is strongly associated with greater reported financial impact from cybersecurity breaches. This association may reflect the greater concentration of digital assets, financial transactions, business activity, digital platforms, and interconnected systems in larger economies.

The country-level analysis illustrates an association between GDP and cybersecurity breach costs. Within the study sample, larger economic size is associated with greater financial impact from cybersecurity breaches. GDP therefore appears to be a strong statistical indicator of breach-cost variation across African countries, although the relationship should be interpreted as associational rather than causal**,** as other structural and cybersecurity-related factors may also contribute to the observed differences in breach costs.

This is illustrated in Figure 3.

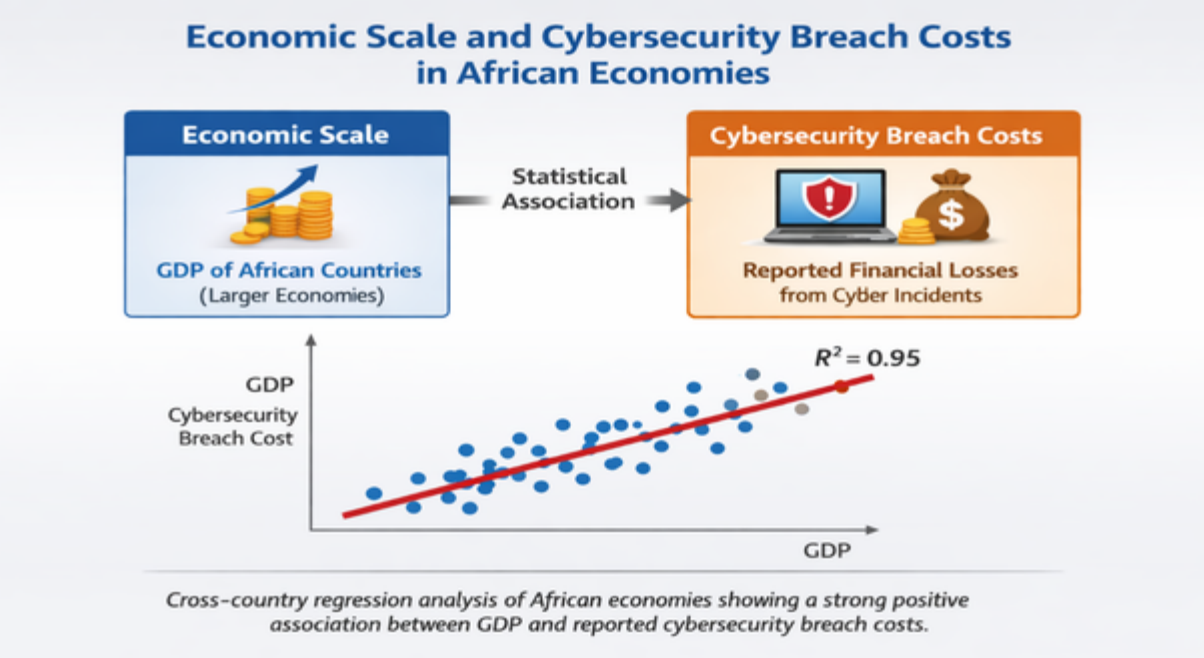


Figure 3: Economic scale and cybersecurity breach costs in African economies.

Source: Researcher's Own (2026)

The empirical results shown in Figure 3 indicate a strong positive association between national economic size and cybersecurity breach costs within the African context. This pattern is consistent with prior research suggesting that larger and more digitally integrated economies often face greater exposure to cyber threats due to expanded technological infrastructure and financial system activity. Countries that support such a finding, including Mauritius and Kenya, appear in both high GDP and high breach cost categories. The other top ten African countries with the largest economies and notable cyber risk in 2024 are Nigeria, South Africa, Egypt, Morocco, Kenya, Algeria, Angola, and Tanzania. This list of countries is largely consistent with that derived from the Preliminary analysis from the African Cyber Threat Assessment Report (2024), Ecofin Agency (2024), and World Bank (2024). These findings align with analyses by INTERPOL (2024), Check Point Software Technologies (2025), and TechLoy (2025).

Larger economies tend to experience higher reported breach costs, which may reflect greater digital infrastructure, larger financial sectors, and increased exposure to cyber threats. However, this relationship should not be interpreted as causal. Instead, GDP likely acts as a proxy for broader structural factors that shape cyber risk exposure, including technological adoption, digital connectivity, and institutional cybersecurity capacity.

The regression results suggest that countries with higher GDP levels are associated with higher cybersecurity breach costs**,** indicating an association between economic scale and cyber incident loss. To ensure that the observed relationship was not driven by extreme values among the largest economies, a robustness inspection of the data distribution was conducted. The results indicated that the overall pattern of the association between GDP and cybersecurity breach costs remained consistent across the dataset. This suggests that the reported statistical association is not solely driven by outliers but reflects a broader pattern across the sampled African economies. While high-GDP economies exhibit greater breach costs, this association does not imply causation. This study notes that cybercriminal targeting is influenced by multiple factors, including digital-finance integration, regulatory maturity, and ecosystem vulnerabilities. GDP serves as a proxy for scale, not a direct determinant of attack likelihood

4.3.2 Outliers and Exceptions:

The low chance comprises outliers or exceptions where countries with low GDP have high cyberattacks and related breach costs, and countries with high GDP have low breach costs**.** These outliers include countries like Zimbabwe, whose GDP is low, but its high remittances and digital payment systems opened it up to massive cybersecurity breaches (Maphosa, 2023). While countries like Mauritius or Ethiopia may deviate slightly from the exact predicted value, the high R^2 shows that GDP is overwhelmingly the dominant factor influencing breach cost. Minor deviations do not undermine the regression's validity; they highlight additional moderating factors like cybersecurity maturity, digital infrastructure, and reporting practices. Ethiopia, despite its relatively moderate GDP, reports higher-than-expected breach costs, suggesting that factors beyond economic size, such as cybersecurity infrastructure and reporting practices, contribute to increased financial impact (Dér, 2025). Mauritius, though smaller in GDP, also shows high breach costs, likely due to its advanced digital economy and high exposure to online transactions (Dér, 2025). Conversely, Ghana and Côte d'Ivoire, with moderate GDPs, report lower-than-expected breach costs, which may reflect underreporting or effective cybersecurity controls (Mohamed & Kamau, 2023).

4.4 GDP Computations and Predictive Analysis at Regional Level

4.4.1 Regional-Level Results:

The regression was conducted at the country level (n=55) to ensure statistical vigour. The country-level predicted breach costs and GDPs for all countries within a given region are used to compute regional totals and averages. Averaging the country-level data to get meaningful regional-level insights while maintaining consistency with the country-level regression formula. Regional GDP totals were calculated by summing individual country GDPs using the latest World Bank (2025) and IMF (2024) estimates.

4.4.2 Sum Gdps by Region

Table 6 below shows the computation of total GDP across the region using World Bank (2023–2024 data) and International Monetary Fund (2024).

Table 6: African Regional GDP Overview

Region	Total GDP (Billions USD)	Countries Count	Countries (with GDP in USD)
North Africa	1,071.8	6	Egypt (395.9), Algeria (239.9), Morocco (141.1), Sudan (109.3), Tunisia (48.5), Libya (50.5)
West Africa	1,008.2	15	Nigeria (362.8), Ghana (76.4), Côte d'Ivoire (78.8), Senegal (31.0), Burkina Faso (20.3), Mali (20.9), Niger (16.8), Benin (19.7), Togo (9.2), Sierra Leone (3.8), Liberia (4.3), Mauritania (10.5), The Gambia (2.3), Guinea (23.6), Guinea-Bissau (2.0)
East Africa	653.9	14	Ethiopia (163.7), Kenya (107.4), Tanzania (79.2), Uganda (49.3), Rwanda (14.1), Burundi (2.6), Djibouti (4.1), Eritrea (data missing), Seychelles (2.1), Comoros (1.35), São Tomé & Príncipe (0.60), Madagascar (16.0), Somalia (11.7), South Sudan (data missing)
Southern Africa	592.5	11	South Africa (377.8), Angola (84.7), Mozambique (20.6), Zambia (28.2), Malawi (14.1), Botswana (19.4), Eswatini (4.6), Lesotho (2.0), Mauritius (14.4), Namibia (12), Zimbabwe (26.5)
Central Africa	156.1	7	Cameroon (48.0), Chad (13.1), Gabon (20.5), Republic of the Congo (15.3), Central African Republic (2.6), Equatorial Guinea (12.1), Democratic Republic of the Congo (66.4)

Source: World Bank (2023)

Table 7 further summarises the total GDP per region.

Table 7: Summary of GDP per region

Region	Total GDP (Billion USD)
North Africa	1,071.8
West Africa	1,008.2

Region	Total GDP (Billion USD)
East Africa	653.9
Southern Africa	592.5
Central Africa	156.1

Source: World Bank (2023/2024)

Table 7 highlights significant economic concentration in North and West Africa, with Central Africa contributing the least to the continent's total GDP. Table IV shows that North and West Africa have the highest total GDPs, both exceeding USD 1 trillion. East Africa and Southern Africa fall in the mid-range, while Central Africa has the smallest economy at USD 156.1 billion.

4.4.3 Regional Total Predicted Breach Cost

The formula derived from the regression analysis per country is stated below, and the GDP per region is applied in Table 10, which provides estimates of Predicted Breach Cost.

Breach Cost (Millions USD) = 0.1033 + 0.0051 × GDP (Billion USD)

The formula is applied for each of the 55 countries. The formula is for each country be association it is derived from the regression analysis at the country level, which examined the association between national GDP and average financial losses from cyber breaches across Africa. The coefficient 0.0051 indicates that for every $1 billion increase in GDP, the predicted breach cost rises by $5,100, while the intercept 0.1033 accounts for baseline breach costs even in smaller economies. This approach is more statistically robust than using regression at the regional level alone, which would be unreliable due to the small sample size. It ensures that regional comparisons of cyber risk are based on a consistent, data-driven economic relationship. These computations are illustrated in Table 8.

Table 8: Application of the formula: Predicted Breach Costs

Country	GDP (Billion USD)	Predicted Breach Cost (Millions USD)=0.1033+0.0051×GDP
Nigeria	474.52	2.523
Egypt	317.89	1.725
South Africa	389.25	2.084
Algeria	193.36	1.089
Ethiopia	155	0.894
Morocco	128.92	0.762
Kenya	95.5	0.591
Angola	80.4	0.515
Ghana	85.5	0.539
Côte d'Ivoire	76	0.494
Tanzania	88.9	0.556
Uganda	46	0.337
Sudan	34	0.279
Mozambique	19	0.201
Madagascar	14.5	0.177
Zambia	23	0.222
Malawi	13	0.170
Cameroon	45	0.332
Senegal	28	0.246
Burkina Faso	27.1	0.242
Mali	22	0.216
Niger	21.9	0.214
Chad	13	0.170
Rwanda	10.1	0.155
Benin	21.5	0.213

Country	GDP (Billion USD)	Predicted Breach Cost (Millions USD)=0.1033+0.0051×GDP
Botswana	19.4	0.203
Sierra Leone	5	0.129
Liberia	3	0.118
Togo	9	0.149
Mauritania	8	0.144
Seychelles	1.7	0.112
Eswatini	4.6	0.127
Lesotho	2.2	0.115
Guinea	18	0.196
Gabon	18	0.196
Republic of Congo	11	0.160
Central African Republic	2.5	0.116
Equatorial Guinea	13	0.170
São Tomé and Príncipe	0.4	0.105
Comoros	1	0.108
Djibouti	3	0.118
Burundi	3	0.118
Gambia	2	0.113
Cabo Verde	6	0.134
Somalia	14.5	0.177
Mauritius	14.5	0.177
Namibia	12	0.164
Tunisia	48	0.348
Libya	70	0.460
Eritrea	4.6	0.127
Guinea-Bissau	1	0.108
Zimbabwe	12	0.164
Democratic Republic of the Congo	35	0.281
South Sudan	4.3	0.125
Western Sahara	1	0.108

Source: Researchers' Own (2025)

Table 8 displays the GDP per country to which the regression formula is applied. The table shows that the financial cost of cyber breaches increases directly with the size of a country's economy, meaning Africa's largest economies (Nigeria, South Africa, Egypt) face the highest cyber-financial risk, which aligns with the kurtosis analysis, which showed that regions with high economic concentration, where a few countries dominate total regional GDP, also exhibit greater cyber threat exposure and higher variability in attack patterns.

The information in Table 8 is synthesised into the African regions in Table 9 below.

Table 9: Regional total prediction

Region	Countries Count	Total GDP (Billion USD)	Regional total prediction Breach Cost (Millions USD)
North Africa	6	1,071.8	5.572
West Africa	15	1,008.2	5.238
East Africa	14	653.9	3.434

Region	Countries Count	Total GDP (Billion USD)	Regional total prediction Breach Cost (Millions USD)
Southern Africa	11	592.5	3.118
Central Africa	7	156.1	0.903

Source: Researchers' Own (2025)

The regression results suggest that estimated cyber-loss exposure increases with regional economic scale. Regions with larger aggregated GDP, including North and West Africa, exhibit the highest predicted breach costs, while lower-GDP regions such as Central Africa exhibit lower predicted costs. These estimates are derived from the country-level regression model and are intended to illustrate relative cyber-loss exposure across African business ecosystems.

Regions with larger economies, such as North Africa (USD 5.57 million) and West Africa (USD 5.24 million), are expected to face the highest breach costs, while smaller economies, like Central Africa (USD 0.90 million), are expected to face the lowest. East Africa (USD 3.43 million) and Southern Africa (USD 3.12 million) fall in the mid-range. Overall, the model confirms a positive association between economic size and the financial impact of cyber breaches across African regions.

Economic scale increases cyber vulnerability within interconnected digital business ecosystems. GDP appears to be strongly associated with the magnitude of cybersecurity breach costs across African economies, although additional institutional and technological factors may also contribute to this relationship. These findings are represented in the bar graph included in Figure 5 below.

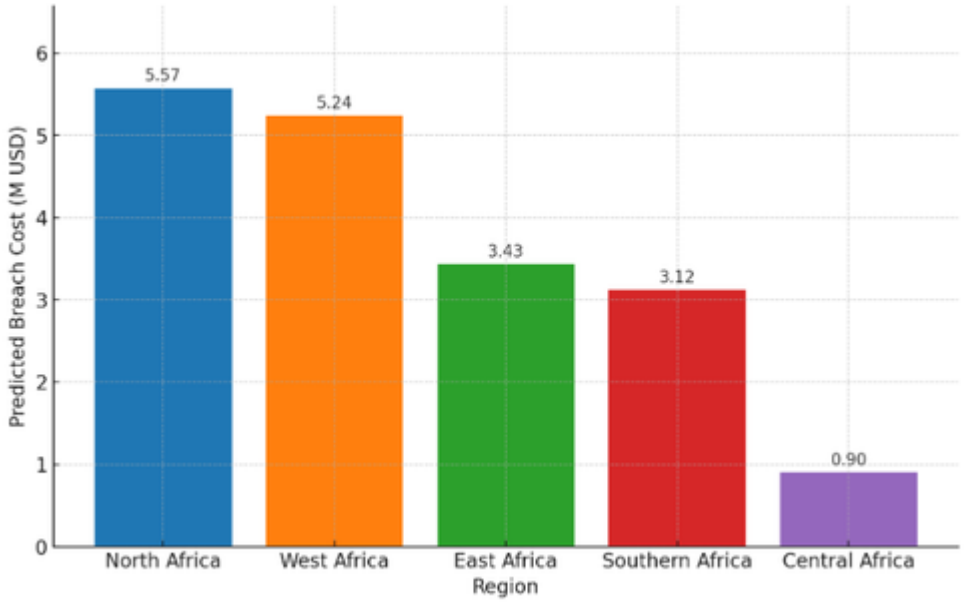


Figure 4: Predicted Breach Costs per region

Source: Researchers' Own (2026)

From Figure 4, it is evident that North and West Africa show the highest predicted breach costs, ranging from USD 5.24 million to USD 5.57 million, reflecting their large economies and greater cyber risk exposure. East Africa (USD 3.43 million (M)) and Southern Africa (USD 3.12 million) fall in the mid-range, suggesting that moderate GDP levels or stronger cybersecurity controls may limit financial impact. Central Africa, with the lowest regional GDP, recorded the lowest predicted breach cost at USD 0.90 million. Overall, predicted breach costs rise with GDP, with high-GDP regions experiencing the greatest expected cyber losses. Consequently, cybersecurity resilience should become a central component of ecosystem governance, cross-border digital cooperation, and sustainable digital transformation strategies across Africa.

Table 9 shows the Observed, Predicted and Residual values that ensure robustness of the study.

Residuals represent the difference between observed breach costs (IBM/INTERPOL estimates) and predicted values from the regression model.

Residuals = Observed breach cost – Predicted breach cost.

Large economies such as South Africa, Nigeria, and Egypt exert disproportionate influence on the slope, while mid-sized economies like Kenya and Morocco show wider gaps between observed and predicted values. This highlights that GDP is a strong proxy but not a complete determinant of breach costs, reinforcing the need to consider ecosystem maturity and digital-finance integration.

Table 10: Residual Values

Country	GDP (Billion USD)	Observed Breach Cost (M USD)	Predicted Breach Cost (M USD)	Residual (Observed – Predicted)
South Africa	389.25	2.45	2.084	+0.366
Nigeria	474.52	3.20	2.523	+0.677
Egypt	317.89	2.80	1.725	+1.075
Kenya	95.50	1.0	0.591	+0.409
Morocco	128.92	1.2	0.762	+0.438

Source: Researchers' Own (2026)

South Africa's predicted breach cost of 2.084M USD is close to the observed 2.45M USD, leaving a residual of +0.366M. Nigeria's predicted value of 2.523M USD underestimates the observed 3.20M USD, with a residual of +0.677M. Egypt shows a similar pattern, with a predicted 1.725M USD compared to the observed 2.80M USD, yielding a residual of +1.075M. For mid-sized economies such as Kenya and Morocco, the regression consistently underestimates losses, with observed breach costs nearly double the predicted values, highlighting wider gaps between modelled and real outcomes. Residual analysis shows that while GDP explains 95.2% of the variation in breach costs, the model consistently underestimates losses in large and mid-sized economies such as Nigeria, Egypt, Kenya, and Morocco. This pattern indicates that breach costs are influenced not only by economic scale but also by ecosystem maturity, digital finance integration, and cybersecurity readiness. The regression therefore captures association rather than causation, and predictions should be interpreted as scale based proxies rather than precise observed losses.

5. Conclusion

The findings suggest that economic scale plays an important role in shaping cyber risk exposure across African economies. Countries with larger GDPs tend to have more extensive digital infrastructure, higher financial transaction volumes, and larger digital asset bases, which collectively increase their attractiveness to cybercriminals. The findings suggest that larger economies may face greater aggregate cyber-related financial risks, likely due to higher levels of digitalisation and financial system complexity. While the regression model demonstrates a strong association between GDP and breach costs, the analysis does not establish causality. However, the results should be interpreted as demonstrating statistical association rather than direct causation. Future research incorporating additional explanatory variables such as internet penetration, cybersecurity readiness indices, and digital financial adoption may provide a more comprehensive understanding of the structural drivers of cyber-related financial losses across Africa.

The findings suggest that larger economies tend to experience greater cybersecurity breach costs and may present more attractive targets because of their larger digital infrastructures, greater transaction volumes, and more interconnected digital business ecosystems. However, the study does not establish that GDP directly causes cyberattacks or cyber losses. Instead, GDP appears to be strongly associated with several structural characteristics that influence cyber-risk exposure.

Larger African economies, therefore, face disproportionately higher data breach costs, highlighting the need for regional and country-specific cyber resilience strategies as digital transformation accelerates across the continent. Cybersecurity measures should scale with GDP growth, recognising the cyclical association between GDP, cyberattacks, and data breach losses. Higher GDP makes a country an appealing target, which can result in costly breaches that subsequently impact economic performance, emphasising a dual dynamic where GDP both attracts cyber threats and is affected by them.

This paper contributes to both theory and practice. This study contributes to the emerging literature on cyber risk economics by providing one of the first cross-country empirical examinations of the association between national economic scale and cybersecurity breach costs within the African context. Theoretically, it strengthens the understanding of economic predictors of cyber risk in Africa, while practically, it provides evidence to guide policymakers and organisations in allocating cybersecurity budgets. By quantifying the financial risk associated with cybersecurity breaches, the paper supports informed decision-making on national and regional cybersecurity investments. The paper provides empirical grounding for understanding how economic scale affects breach costs in Africa. It aids policymakers in targeting cybersecurity investments, helps businesses gauge potential financial risk, and fills a gap in Africa-specific cyber-economic research.

In light of these findings, it is recommended that efforts focus on improving cybersecurity literacy among businesses, particularly SMEs, through nationwide training programs. Governments and stakeholders should prioritise the development and enforcement of effective cybersecurity policies and regulations to protect digital infrastructures. Collaboration between public and private sector entities should be encouraged to facilitate the sharing of threat intelligence and resources, while funding should be allocated to build and maintain secure digital infrastructures, especially in under-resourced regions. Such initiatives should aim to strengthen regional capabilities, promote proactive breach mitigation measures such as incident response planning, and incorporate emerging governance frameworks like AI oversight to ensure resilient, adaptive, and scalable cybersecurity strategies across Africa.

5.1 Recommendations

The paper recommends integrating economic indicators with cybersecurity metrics, since the association between GDP and breach costs has been confirmed. This would provide evidence to inform targeted interventions, enhance digital resilience, and guide strategic cybersecurity investments tailored to Africa's diverse economies (IBM & Ponemon Institute, 2025; Maulita & Hayadi, 2025; Umoga, Sodiya, Amoo, & Atadoga, 2024).

Based on the findings, it is recommended that efforts be directed towards enhancing cybersecurity literacy across the nation, with particular attention to businesses, especially small and medium-sized enterprises. This can be achieved through comprehensive training programs that equip businesses with the knowledge and skills to recognise and respond to cyber threats effectively. At the same time, there is a need for the development and enforcement of strong cybersecurity policies and regulations aimed at safeguarding critical digital infrastructures, ensuring a consistent and resilient approach to cyber risk management. Collaboration between governments and private sector entities is crucial, as sharing threat intelligence and resources can significantly enhance the collective capacity to prevent and respond to attacks. Furthermore, allocating resources to build and maintain secure digital infrastructures, particularly in regions that are under-resourced, will provide a foundational layer of protection that supports national and regional digital resilience. Finally, partnerships between governments and relevant stakeholders should focus on strengthening regional capabilities, promoting proactive breach mitigation measures such as incident response planning, and adopting emerging governance frameworks like AI oversight to ensure that digital ecosystems remain secure and adaptive to evolving threats.

The results demonstrate that cybersecurity risk in Africa should increasingly be viewed as an ecosystem-level challenge rather than solely an organisational problem. Digital business ecosystems comprising banks, fintech firms, telecommunications providers, regulators, digital-payment platforms, and consumers are interconnected through shared digital infrastructures. As ecosystem complexity and transaction volumes increase, cyber vulnerabilities in one participant may generate spillover effects throughout the ecosystem. Consequently, cybersecurity resilience should become a central component of ecosystem governance, cross-border digital cooperation, and sustainable digital transformation strategies across Africa.

5.2 Areas of Further Research

This paper aimed to explore the association between economic scale and cybersecurity risk in Africa, specifically examining how GDP influences the likelihood and financial impact of data breaches. The paper found that countries with higher GDP tend to attract cybercriminal activity, resulting in disproportionately higher breach costs, and highlighted the cyclical nature of this association, where economic growth both attracts and is affected by cyber threats. Furthermore, some associations observed in descriptive analyses, such as links between high remittances, digital currencies, mobile transactions, and cyber-related financial losses, could not be confirmed for associativity within the scope of this paper.

Future research should expand the scope to include these additional economic, technological, and structural factors to better understand the multidimensional drivers of cyber risk in Africa. Employing advanced statistical modelling and longitudinal approaches could help establish associative relationships and clarify how these variables interact with cyber threats and financial losses. Investigating country-specific and regional variations in cyber resilience strategies and the effectiveness of breach mitigation measures would provide valuable insights for policy design. Additionally, the role of emerging technologies, including AI governance frameworks, block chain, and digital financial platforms, should be examined to ensure that Africa's digital transformation is matched by adaptive and resilient cybersecurity practices

5.3 Limitations

The study is limited by reliance on reported cyberattack cost data, which may underrepresent unreported incidents, and by the cross-sectional design, which restricts associative inference. The focus on 55 African countries may limit generalizability to other continents or global contexts.

A further limitation of the study is the use of a single-variable regression model. While GDP provides a useful proxy for economic scale and digital asset concentration, cybersecurity risk is influenced by multiple structural factors, including internet penetration, cybersecurity investment, digital infrastructure maturity, and regulatory capacity. Due to the lack of comparable cross-country data for all African countries, these variables were not included as formal control variables. Future research could employ multivariate regression models incorporating these indicators to test the robustness of the GDP–breach cost association.

Acknowledgement

All authors have read and agreed to the published version of the manuscript.

This study did not involve human participants or any personal data. All data used in the research were obtained from publicly accessible websites and databases. The analysis was conducted in accordance with ethical research standards, ensuring transparency, integrity, and proper acknowledgement of all data sources. No sensitive or confidential information was collected, and the study adhered to principles of responsible research conduct.

All authors have read and agreed to the published version of the manuscript.

Author Contributions: by authors with equal participation

Funding: This research received no external funding.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

Declaration of Generative AI and AI-assisted Technologies: The authors declare that no generative AI or AI-assisted technologies were used in the preparation of this manuscript.

References

Aguilar, L. A. (2015). The need for greater focus on the cybersecurity challenges facing small and midsize businesses. U.S. Securities and Exchange Commission. https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime.

Bederna, Z., & Szádeczky, T. (2023). Managing the financial impact of cybersecurity incidents. Security and Defence Quarterly. https://doi.org/10.35467/sdq/159625

Chainalysis. (2024). Sub-Saharan Africa: Nigeria takes #2 spot in global adoption, South Africa grows crypto-TradFi nexus. https://www.chainalysis.com/blog/subsaharan-africa-crypto-adoption-2024/

Cobos, E. V. (2023). A review of the economic costs of cyber incidents. World Bank.

Dér, A. (2025). Aspects of cyber defence in Africa. Journal of Central and Eastern European African Studies, 5(1), 36–48. https://doi.org/10.12700/jceeas.2025.5.1.341

Ecofin Agency. (2024). Africa received over $100 billion in remittances in 2023, outpacing aid and FDI. https://www.ecofinagency.com/news-finances/1807-47763-us-remittance-tax-could-weigh-heavily-on-african-economies

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. Journal of Business and Behavioural Sciences, 32(1), 63.

Financial Action Task Force. (2023). Annual report 2023–2024. https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html

Gañán, C. H., Ciere, M., & van Eeten, M. (2017). Beyond the pretty penny. In Proceedings of the 2017 New Security Paradigms Workshop (pp. 35–45). ACM. https://doi.org/10.1145/3171533.3171535

Garre, J. T. M., Pérez, M. G., & Ruiz-Martínez, A. (2021). A novel machine learning-based approach for the detection of SSH botnet infection. Future Generation Computer Systems, 115, 387–396. https://doi.org/10.1016/j.future.2020.09.004

Huygen, L., & Beulen, E. (2025). Cyber shocks: The financial impact of cyber events. Social Sciences & Humanities Open, 12, Article 101770. https://doi.org/10.1016/j.ssaho.2025.101770

IBM & Ponemon Institute. (2023). Cost of a data breach report 2023: Global average cost reached USD 4.45 million in 2023.

IBM & Ponemon Institute. (2024). Cost of a data breach report 2024: Global breach cost rose to USD 4.88 million; South Africa's average reached R53.10 million.

IBM & Ponemon Institute. (2025). Cost of a data breach report 2025: South Africa R44.1 million (~USD 2.45 million); the global average fell 9% to USD 4.44 million.

International Fund for Agricultural Development. (2024). IFAD launches RemitSCOPE: A free global data platform to capture and facilitate remittances for rural development. https://www.ifad.org/en/w/news/ifad-launches-remitscope-a-free-global-data-platform-to-capture-and-facilitate-remittances-for-rural-development

International Monetary Fund. (2024). World Economic Outlook database. https://www.imf.org/en/Publications/WEO/weo-database

International Telecommunication Union. (2024). Global Cybersecurity Index 2024. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

INTERPOL. (2024). African cyberthreat assessment report 2024. https://www.interpol.int/en/content/download/23094/file/Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_FINAL.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jiang, D., Zhu, W., & Zhang, Z. (2024). Evolution of resilience spatiotemporal patterns and spatial correlation networks in African regional economies. Land, 13(9), Article 1537. https://doi.org/10.3390/land13091537

Klapper, L. (2024). A decade of change: The surge of financial inclusion in Sub-Saharan Africa. World Bank Blogs. https://blogs.worldbank.org/en/developmenttalk/a-decade-of-change-the-surge-of-financial-inclusion-in-sub-saharan-africa

Maphosa, V. (2023). An overview of cybersecurity in Zimbabwe's financial services sector. F1000Research, 12. https://doi.org/10.12688/f1000research.132823.2

Maulita, I., & Hayadi, B. H. (2025). Financial loss estimation in cybersecurity incidents: A data mining approach using decision tree and linear regression models. Journal of Cyber Law, 1(2), 161.

Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in the healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63.

Mohamed, A., & Kamau, S. (2023). A continent-wide assessment of cyber vulnerability across Africa (arXiv:2301.03008). https://doi.org/10.48550/arXiv.2301.03008

Ngejane, C. H., Chishiri, S., Shwayimba, S., Moyakhe, S., Miya, S., & Lwana, G. (2024). Cyberattack incidents in South Africa: A survey. In 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 584–588). IEEE. https://doi.org/10.1109/ICICyTA64807.2024.10912850

Osborn, E. (2015). Business versus technology: Sources of the perceived lack of cyber security in SMEs (CDT Technical Paper 01/15). University of Oxford.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. Journal of Information Security and Applications, 19(4–5), 257–267.

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a cyber security label for SMEs: A European perspective. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (pp. 426–431). SciTePress. https://doi.org/10.5220/0006657604260431

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. Journal of Cybersecurity, 4(1), Article tyy004.

Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cybersecurity and future trends. World Journal of Advanced Research and Reviews, 15(1), 138.

Singh, S., & Kumar, S. (2020). The times of cyber attacks. Acta Technica Corviniensis—Bulletin of Engineering, 13(3), 133.

Sung, S., Kim, Y., & Chang, H. (2016). Improving collaboration between large and small-medium enterprises in automobile production. Enterprise Information Systems, 12(1), 19–35. https://doi.org/10.1080/17517575.2016.1161242

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. Journal of Forensic and Investigative Accounting, 12(2), 197.

Trend Micro. (n.d.). Operation Serengeti 2.0: Trend Micro helps law enforcement fight cybercrime in Africa. https://www.trendmicro.com/en_us/research/25/h/operation-serengeti-trend-micro.html

Ugwu, J., & Ugwuanyi, I. (2024). Addressing the escalating threat of cybercrime in African nations: Strategies for legislation, governance, and capacity building. IDOSR Journal of Communication and English. https://doi.org/10.59298/idosr/jce/91.810.202411

Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. International Journal of Science and Research Archive, 11(1), 1810.

United Nations. (2024). Remittances in Northern Africa. https://www.un.org/osaa/sites/www.un.org.osaa/files/files/documents/2024/publications/remittances_in_northern_africa.pdf

Wirth, A. (2017). The economics of cybersecurity. Biomedical Instrumentation & Technology, 51(s6), 52.

World Bank. (2024). In 2024, remittance flows to low- and middle-income countries are expected to reach $685 billion. https://blogs.worldbank.org/en/peoplemove/in-2024--remittance-flows-to-low--and-middle-income-countries-are-expected-to-reach-685-billion

World Bank. (2025). GDP (current US$) [Data set]. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—Influence techniques in phishing attacks: An examination of vulnerability and resistance. Information Systems Research, 25(2), 385–400. https://doi.org/10.1287/isre.2014.0522

Yasuttamathada, N., & Worapongpat, N. (2025). Leadership of organisation administrators in an open university in China: A case study. Journal of Education and Learning Reviews, 2(1), 83. https://doi.org/10.60027/jelr.2025.930

Publisher's Note: BUSSECON stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2026 retained by the authors. Licensee BSC International Academy, Istanbul, Turkey. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).