The State of Data Breaches in the African Cyberspace: A Trend Analysis Using Social Media and Research Literature

Jabu Mtsweni[1&2], Muyowa Mutemwa[1], Mfundo Masango[1], Samson Chishiri[1], and Siwe Moyakhe[1]

[1] Council for Scientific and Industrial Research (CSIR), Information and Cyber Security Centre, Pretoria, South Africa
[2] Stellenbosch University, Military Academy, Stellenbosch, South Africa

[1]mtswenij@gmail.com,
[1]mmutemwa@csir.co.za,
[1]mmasango1@cisr.co.za,
[1]schishiri@csir.co.za, and
[1]smoyakhe@csir.co.za

Abstract. Cybersecurity attacks are classified in the top 10 global risks by the World Economic Forum in 2023. The common cyber-incidents that affect businesses, governments, and individuals across the globe are data breaches. Recent reports indicate that these incidents are on the rise, with an estimation of over 12 billion personal records breached, impacting on individual's privacy and organization's reputation. Comprehensive insight on data breaches in Africa is not readily available as reporting of these incidents by victims is not mandatory in many African countries, and available trends tend to be limited and scattered. This paper aims to provide a contextual understanding of data breach trends in Africa using social media data (current) and research literature (past). The data from social media, including news websites, were collected over a 3-month period tracking data breaches in the African content, whilst the research literature focused on prominent data breaches in African countries between 2020 and 2023. The research results indicate the data breaches trend that is on the rise in Africa with Nigeria showing higher engagements on social media, whilst South Africa being the data breach haven with a large exposure of personal data online. The impact of data breaches on customers and businesses in Africa is determined as being negative and unabated. This paper recommends practical and evidence-based security controls to minimize data breaches.

Keywords: Cybersecurity, Information Security, Data breach, African Cyberspace, Cyber Attacks.

1 Introduction

Data is growing faster and, in more places, than we think [1]. This is fueled mainly because organizations sometimes do not even know their entire data universe. Data breach, leakages, and/or exposure are bound to happen, and this is supported by the 59% of data breaches observed globally in 2022 alone [1]. As such, it is agreed by various experts that data breaches are becoming more common and have been on the rise for several years, and this trend isn't slowing down. As countries take steps to implement data protection laws, it is evident, at least based on [2], that African countries are lagging behind on data protection laws with only a handful of African countries having robust data protection laws [2].

In South Africa, the increasing trend in data breaches is also observed through data breach notifications to the Information Regular. By June 2023, the Information Regulator in South Africa had received over 1,021 data breach notifications, which is double the number that was reported in the previous five months of the same year [3]. In February 2023, the Nigerian Data Protection Bureau (NDPB) announced that it was investigating over 110 companies over allegations of privacy and data breaches [4]. The Communications Authority of Kenya (CAK) reported that the number of cyber threats had more than doubled in the financial year 2021-2022, attributing this to the growth of internet users as well as digital transformation in the country [5].

These events clearly indicate that cyber incidents, particularly data breaches pose a serious threat to the African cyberspace and its users. These incidents are no longer merely a technological issue but have a direct impact on business reputations and personal privacy. Nevertheless, the research-based understanding of data breach trends in Africa is still limited to business reports and newspapers articles.

This study, therefore, seeks to understand the trend of data breaches in Africa using social media analysis as well as research literature reviews. This is done to contextualize the phenomenon from different perspectives using current and historical reports and data, which may provide comprehensive insights and research-based evidence on the scale of this scourge including its impact as well as possible mitigations.

The rest of this paper is structured as follows; Section 2 covers the general global data breach trends to lay the foundation for focusing on the African cyberspace. Section 3 describes the research objectives and approach that underpin the research presented in this paper. In Section 4, we cover the first phase of the analysis focusing on the social media data analysis and complementing this with the research literature analysis of data breaches in Africa in Section 5, which is phase 2 of the research study. Section 6 provides a discussion and implications of data breaches in the African cyberspace taking into consideration the two-phased analyses. The research paper is concluded with recommendations to decision-makers in Section 7.

2 Global Data Breach Trends

On a global scale, cybersecurity attacks, including data attacks are ever increasing, and this is caused in part by the rising number of software and hardware vulnerabili-

ties reported and recorded on the National Vulnerability Database (NVD). Fig. 1 shows that in the last five (5) years the disclosed number of vulnerabilities have been on the increase. The severity of the vulnerabilities that are classified as critical or high, does not always translate to the impact as also being severe. This is because exploiting a vulnerability depends on several factors such as the environment wherein the vulnerability is found, the human factor, availability of an exploit code, and value of the digital asset.

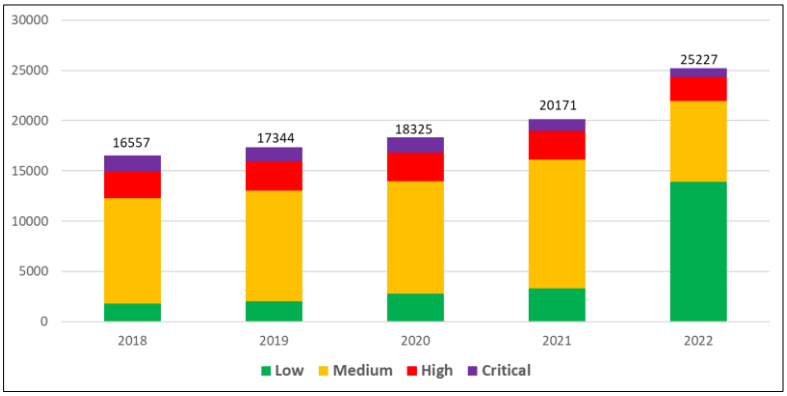

Fig. 1. Vulnerabilities per year since 2018.

According to [6], the increase over the years in the number of vulnerabilities could mean that researchers are discovering more vulnerabilities; or that there is a high number of software or hardware that is released with vulnerabilities. This has a direct impact on the trend of data breaches and other cyber incidents. According to [7], threat actors are becoming successful with data breaches through the exploitation of disclosed vulnerabilities found in different software and hardware, including security tools. As such there seems to be a direct link between the number of disclosed vulnerabilities and the rate of data breaches.

The following two subsections give a high-level look at data breach trends seen on a global scale as discussed in subsection 2.1 and in the African scale as discussed in subsection 2.2 below.

2.1 Cybersecurity Data Breach Trends: Global Perspective

According to the Verizon Data Breach Investigations Report (DBIR) of 2023 [8], Business Email Compromise (BEC) amounted to 50% of social engineering attacks. DBIR also shows the presence of ransomware in 24% of data breaches. One of the major factors seen in the report is that 74% of data breaches was due to a human factor, of which 84% of that human factor element originated from external sources, largely driven by a financial gain. The DBIR lists the three major techniques by which organization were breached, which are: *stolen credentials*, *phishing attacks*, and the *exploitation of both disclosed and zero-day vulnerabilities*.

According to the Sophos Survey [9], over the years cyber-criminals have been developing and sharing tools through ransomware-as-a-service and this has resulted in more organizations across the world being hit with ransomware-related data breaches. The survey states that 66% of organizations across the world had experienced a ransomware breach between 2020 and 2023. The survey report further states that between the years 2020 and 2023, there was a noticeable reduction in the number of breaches related to ransomware as was the case in 2021, however, in general the trend graph has shown an aggregated steady increase of data breaches over that same period. From the Sophos survey report [9] looking at the year 2023, Singapore was the country with the highest rate of ransomware attacks with 84% of organizations in that country experiencing a ransomware breach. In contrast, the United Kingdom had the lowest surveyed rate of 44% ransomware breaches. What was noticeable is that South Africa had the biggest increase in the number ransomware breaches between 2020 and 2023. What the survey also suggest is that 30% of the organizations that had experienced a ransomware breach also had their data stolen and used as extortion, thus contributing to 46% of organizations that were forced to pay ransomware to regain access to their data.

2.2 Cybersecurity Data Breach Trends: African Perspective

According to African Cyberthreat Assessment Report [10], the main driver for the African internet penetration is attributed to mobile devices being connected to the internet. However, this internet penetration also comes with cybersecurity challenges.

According to the Africa Cyber Security Outlook [11], the most common cybersecurity data breaches experienced by African in 2022 were Business Email Compromise (BEC) with 26%, ransomware breaches with 17%, data leakage with 16%, denial of service with13%, insider threat with 11% and supply chain attacks with 5%. Furthermore, according to [11], the top three attacks seen in the Eastern Africa region were ransomware attacks, followed by BEC and lastly data leakages.

In the Western Africa region, the top three attacks that were observed were Denial-of-Service (DoS) and/or Distributed DoS, followed by BEC and data leakage. In Southern Africa, the top three cyber-attacks seen were BEC, followed by data leakages and l ransomware. The following are two examples of data breach techniques used to compromised organizations in the African region. The first is Business Email Compromise (BEC), where threat actors gain access to an enterprise' email servers using social engineering techniques, then send malicious emails to their targets. Such emails contain malicious attachments, links to malware and malicious domains. In addition to sending out malicious emails, threat actors are also able to edit and change payment or banking details thereby resulting in immediate financial damage.

According to [10], majority of the threat actors responsible for carryout BEC scams were found in West Africa. The Interpol's African Cybercrime Operations Desks discovered that Nigeria region was high on the list of hosts for threats actors in the African region. Hosting such BEC threat actors is not the only challenge, the African continent has also experienced BEC attacks, which have results in financial losses. Although in comparison to other regions around the world, the Africa region is the

least targeted region for BEC scams with 0,74%, of which South Africa alone accounts for more than half of the target recipients of BEC scams on the continent. This may, however, be because the formal tracking and monitoring of such attacks in Africa is generally limited. The second example of data breaches in Africa is banking trojans and stealers. Banking trojans and stealers is a type of trojan that is installed on a victim's machine disguised as a game or useful software with the hope of monitoring a victim as they type in sensitive information such as usernames, passwords, credit card details, and other personal information. Examples of such trojans include spyware and rootkits. According to Trend Micro [10], Morocco was the most affected African country with 18,827 detections, followed by South Africa with 6,560 detection and Nigeria with 5,366 detections. The Trend Micro report [10] further reveals that the two most prevalent bank trojans and stealers seen in the Africa region is Zbot with 67.67% of detections, followed by Fareit with 15,39% of detections.

According to [10], one of the biggest challenges in the African region is the lack of reported cases of data breaches. Of the 20 countries surveyed across the African continent, only over two-thousand cases had been reported compared to a much larger number seen by security tools deployed across the continent. In addition to the 42 countries surveyed [10], only half of these countries had a mechanism for organizations and individuals to report cybercrime. However, according to the United Nations Conference on Trade and Development [11], 39 of the 54 countries on the African continent have legislation in place that deals with reporting of cybercrime, but implementation is still a challenge. Out of the 15 remaining Africa countries, 2 countries are still drafting their legislations while 13 have not even started.

This section has shown based on literature review that the world and the African content still has some mileage to cover at legislation and technical levels to reduce the increasing trend of data breaches.

3 Research Objective and Approach

The main research objective for this paper is to understand and contextualize the state of data breaches in the African cyberspace through timely social media engagements and research literature reviews. The research approach adopted to realize this objective was multi-pronged, influenced by the timely manner of data on social media, but also by the research that has been done over time in this domain by other researchers and news reporters.

The primary data collection for this study focused on the scrapping of public social media data and news websites over a 3-month period (May – July 2023) focusing on reports and engagements around data breaches in Africa. The data collection process was aided by a custom data breach tracker focusing on all African countries guided by case-insensitive keywords such as "data breach", "data leak", and "data exposure". The public data collected from social media and other websites were analyzed using

the Topic Analytics feature found in Talkwalker[1] and qualitative analysis with the specific focus on the data collected over the research period, engagements, potential reach, unique authors, distribution of engagements across the different African countries, popular themes on data breaches, grouping of similar stories as well as sentiment of data breaches.

Phase 2 of the data analysis was supported by the research literature review analysis and data collected through a desktop study of the prominent data breaches in Africa that have occurred between 2018 and 2023. The data was then analyzed using a simple matrix to understand the organizations affected, period of the breach, data compromised, number of data records compromised, attack vectors, and breach impact. It is acknowledged that the social media and research data used for the trend analysis in this paper is not exhaustive, mainly because data attacks are forever evolving. However, the analyzed data was found sufficient to provide qualitative and quantitative insights on the trend of data breaches in the African cyberspace.

4 Understanding Data Breaches in Africa: Social Media Trend Analysis

In this section, we present and discuss the analysis of data breach trends in Africa using social media posts and engagements. The analysis is structured into the overview of the results, themes discovered, trend analysis of results over the 3-month period, distribution of data breach posts and engagements per country, sentiment analysis, and future trend forecasting.

Between May – July 2023, over 1,944 tweets related to data breaches were collected and analyzed, authored by 1,207 unique authors resulting into 1,858 engagements on social media and news websites with a potential reach of 45.9 million users, based on views, followers, retweets, and engagements scores. Data breach stories that are similar were grouped together and this resulted in a total of over 178 unique data breaches conversations over the research period across Africa. However, this does not necessarily mean 178 data breaches occurred in Africa in 3 months because some of the data was on data breaches that may have occurred in the past and authorities were either investigating or providing updates on breaches that have occurred before May 2023 when the data collection period started.

[1] https://app.talkwalker.com/

Fig. 2. Top themes on data breach posts and engagements on social media and news websites.

Fig. 2 shows the top themes as per the data collection over 3 months. The common themes associated with data breach are data, breach, ransomware, cybersecurity, privacy, data protection, data security, and phishing. These themes are correlating with the data found in literature (as highlighted in Section 2) on attack types and techniques in various data breaches in African and rest of the world.
On analysis of the themes over the period of the study, it was evident that the data breaches trend was increasing across all different themes supporting claims that data breaches in Africa are on an upward trend (see Fig. 3).

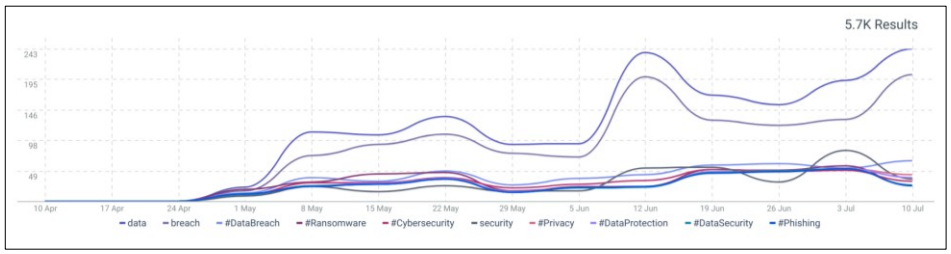

Fig. 3. Data breach theme analysis over time.

Focusing on the total results collected over 3 months, the data breach trend in the African cyberspace indicates an upward trajectory using the stream graph as show in Fig. 4.

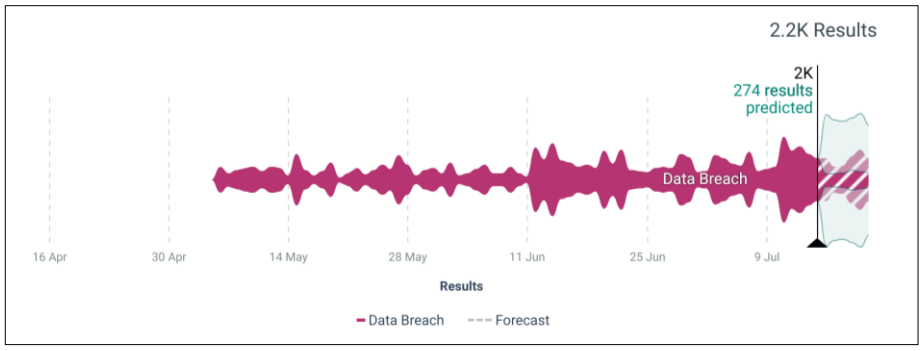

Fig. 4. Data breach trend analysis over 3-months with a forecast

In addition, a prediction of 274 data breach results over a 7-day period suggests a trend in the African cyberspace that is not decreasing. This is done using the Talkwalker forecasting feature [12].

When drilling into the African countries affected by these results Fig. 5 depicts that most of the data breach stories emanate from Nigeria (36%), followed by Kenya (16%) and South Africa (15%). These results are congruent with the observations in literature (see Section 2) as well as global trend reports.

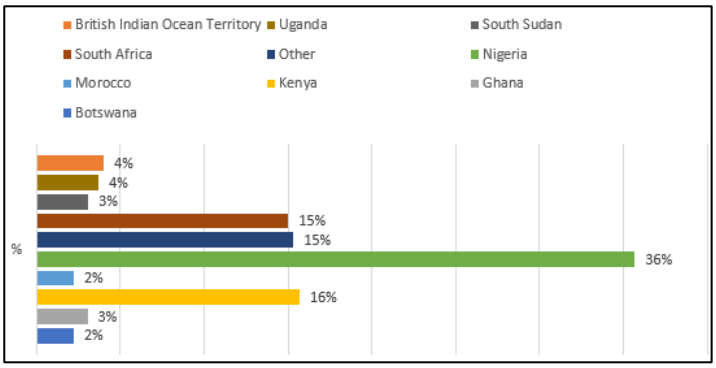

Fig. 5. Data breach posts share across the African continent (over a 3-month period)

Fig. 6 demonstrate the trends of data breach stories over a 3-month period and clearly shows that as more data collection was done, it became evident that data breach stories were more on an increase. The increase over the period of the study was caused by different data breach events such as the news of the Nigerian Data Protection Commission (June 2023) announcing the investigation of financial institutions, universities, and insurance companies for data breaches as well as the South African Department of Justice being fined 5 million rands by the Information Regulator for a data breach that occurred in 2021.

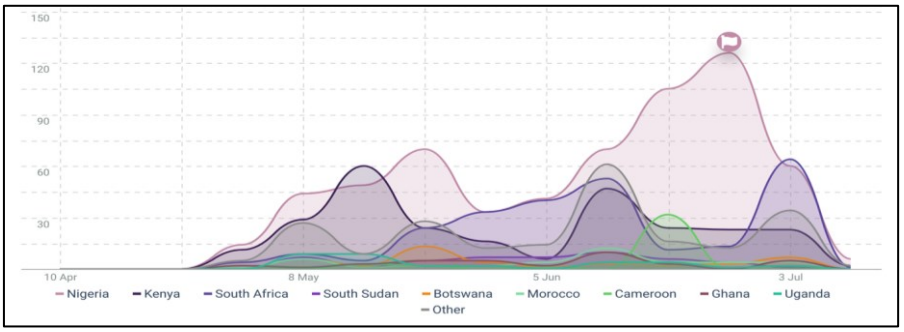

Fig. 6. Data breach peak trends over 3 months in African countries.

In understanding the potential impact of data breaches in the African cyberspace on business and citizens, sentiment analysis of the social media and news website data

was done. Fig. 7 depicts the sentiments through engagements by possible customers, clients, stakeholders, and organizations that have been affected by the data breaches. The sentiments are split up into 3 categories, namely positive, neutral, and negative. From the analysis, it is evident that the data breaches have a negative impact on affected parties with over 62% of the posts attracting negative sentiments. The trend line also suggests that as data breach posts increase so are the negative sentiments, albeit we observed a slight decline in month#3.

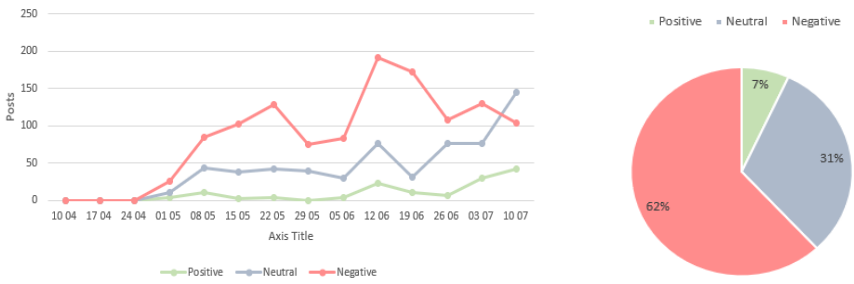

Fig. 7. Sentiment analysis of tweets across different Africa countries

The sentiments key drivers around data breaches during this reporting period were mostly influenced by potential loss of revenue, loss of customers, loss of trust, data theft, financial losses by customers, breach of users' privacy, exposure of users to cyber-crime, reputational harm, data exposure by employees, and regulatory fines. These key drivers indicate, to a large extent, potential impact of data breaches on organizations and individuals and are aligned to what is already reported in literature and other countries outside the African continent. In analyzing the individuals' posts, the extent of data breach impact was also evident in individual stories such as the one cited in Fig. 8.

Fig. 8. Impact of data breaches on individuals

In wrapping up the analysis of phase 1, the data breach events in the top three countries over the reporting period are summarized in the subsections that follow. It should be noted that the subsections only deal with data breach engagements over 3 months, and that the engagements do not only deal with the actual data breaches, but also other stories related to the data breaches in the specific countries as collected from social media and news websites.

4.1 Nigeria

The data breach stories that were observed related to Nigeria during the research period relate to:

The Nigeria Data Protection Commission. The commission announced that it was investigating three deposit money Banks, Babcock University, Leadway Insurance, and other suspects over alleged data breaches, and this was accompanied by a possible loss of revenue by this companies amounting to 2% of their profits. This obviously has direct impact on the cited business and as such expected to generate heightened engagements on social media [13]. This story had a potential reach of over 2.8 million.

Houbi Data Breach Fix. This story was reshared in Nigeria reporting on the fix that a cryptocurrency company based in Seychelles conducted after a leak of contact details of just under 5.000 users.

Strange Ways Employees Expose Data. The awareness story on how users could leak data accidentally was also well shared and engaged on social media. Several tips were shared in this regard.

4.2 Kenya

In Kenya, most of the data breach related stories were influenced by the following events during the reporting period:

New Mega Africa Ltd and Absa data breach case. This data breach story was popular in Kenya during the reporting period where the court barred the Absa bank from auctioning the property of New Mega Africa over unpaid loans. This is due to a pending Sh1.5 billion data breach lawsuit that the firm had initially won where Absa was alleged to have leaked confidential of New Mega Africa to third parties that led to their credit rating diminishing. The bank is currently appealing the order [14].

Equity Bank Kenya Data Breach. The Kenyan Equity Bank was on the spot after a client lost Ksh300,000 in 17 minutes following a major data breach. The bank indicated that they are investigating the matter, even though indications are that the bank has had numerous data fraud and data breach complaints [15].

Dismissal of a Data Breach Complaint: The Court in Kenya dismissed the complaint by Wamae & Allen against the Office of the Data Protection Commissioner (ODPC) that one of their former employees had shared personal and sensitive data with other former employees. The case was dismissed due to the reasons that the data was already in public and that data subjects does not include juristic persons as per the data protection laws in Kenya.

4.3 South Africa

Between May – July 2023, South Africa had over 283 data breach related stories that when analyzed based on similarities resulted into 33 unique data breach stories. The topical data breaches engagements during the period of the study involved the following stories:

Half a Million Customers Data Breach. A data leak of over half a million customers data at Incredible Connection, HiFi Corp, Rochester, Russell's, Sleepmasters, Bradlows and Everyshop made headlines in South Africa during the research period [16]. The group that owns all these companies was compelled by the Protection of Personal Information (POPIA) regulation in South Africa to publicly notify data subjects of the data breach. The impact of the breach was the exposure of personal information of customers on a publicly accessible hacker, but at a cost. It was not clear at the time of the research study how the data breach occurred.

Showmax Subscribers Online Data Breach. The other data breach that created engagement on social media in South Africa during the period of the research study was the leakage of login details of more than 27 000 Showmax subscribers online [17]. In this data breach, customers' emails and passwords were compromised, and Showmax in a statement indicated that this was an external incident and none of their database systems were breached [17].

Department of Justice Data Breach Fine. The other data breach related story that made the most social media engagement headlines was the Department of Justice fine of R5 million by the South African Information Regulator for not taking the necessary measures to correct security gaps after a data breach in 2021 [18].

The qualitative analysis of the social media data provided in this subsection clearly demonstrate that the awareness of data breaches in Africa has increased and data breaches posts are common across different countries, further confirming that data breaches are on the rise in the African continent.

The next section delves into understanding the data breaches in Africa using research literature focusing on the period between 2020 and 2023 to triangulate the data breach global and social media trends with research literature.

5 Understanding Trend of Data Breaches in Africa using Research Literature

This section details data breaches in Africa between January 2018, and July 2023. Table 1 presents the attack type, country, and impact of the data breach. Within the African continent, a trend analysis of cyber-attacks reveals that various types of attacks, including ransomware, DDoS, insider-threats, and others, have been observed

in data breach incidents. It is noted that the information available regarding the identified data breaches was either limited or not disclosed by the organizations, however, it can be noted that one (1) data breach was indicated as a ransomware attack [18], another data breach was indicated to be a DoS/DDoS attack [19], four (4) data breaches were indicated to be hacking incidents [20], [21], [22], [23] and one (1) data breach was classified as a malware attack [24].

The analysis of these data breaches shows some alignment and correlation with the data analyzed in the previous section, particularly with the data breach on Equity Bank that seems to have a wider impact in East Africa.

Each of the analyzed data breach may have resulted in the extraction of different types of data from the affected organization, such as personally identifying information of customers, stakeholders, employees, and even executive board members' personal information.

The financial impact of these data breaches extends beyond the volume of data lost; organizations also suffer reputational damage and face additional penalties imposed by regulators in African countries.

Table 1: Summary of prominent and selected data breaches in Africa (2020-2023)

Country	Organization	Types of attacks	Impact	Year-Month
South Africa	Department of Justice	Ransomware	Financial Reputation damage Regulatory fine	2021-Sep
Senegal	Senegalese Government Websites	DoS/DDoS	Reputation damage	2023-May
Rwanda	Equity bank	Hacking	Financial Reputation damage	2021-Jul
Uganda	MTN Airtel	Hacking	Financial Reputation damage	2020-Oct
South Sudan	Bank of South Sudan	Hacking	Financial Reputation damage	2023-Apr
Morocco	IKEA	Malware	Reputation damage Data Breach	2022-Nov
Kenya	Naivas	Hacking	Reputation damage Data Breach	2023-May

Legend	
	Hacking
	DoS/DDoS
	Ransomware
	Malware

The process of gaining unauthorized access to an organization's network is a timely process and the time to gain access varies based on the type of attack being used by the external actor [25]. Different attack vectors are utilized to identify possible points of entry. Some common attack vectors include ransomware, social engineering with BEC, insider threats, open-source intelligence [25].

The data breaches discussed above could explained as a triangle that identifies 3 main key components that could be used as a root cause analysis (see Fig 9).

The people component can be identified as a possible point of entry to the organization. The people component has access to the data component and is recognized as a resource within the organization by the technology component which will implement less security restrictions as the compared to security restrictions that need to be

implemented for an external actor. According [26], people are viewed as being high risk within cyber-attacks as they become an immediate internal threat actor.

The organizational triangle identifies the people component as employees that have access to internal assets within the organization, the data is all the information that is collected, processed, and stored within the organization and the technology component controls, implements, and manages access to the data component within the organization.

The data breaches discussed in this section all touch on the 3 key components of the organizational triangle. For instance, the analysis of the Department of Justice data breach, the technology component was compromised as licenses for the tools were not renewed within a proper time frame [18], thus access to the data component was not adequately controlled or monitored by the technology component.

The Moroccan data breach, a possible compromise through the human component, thus bypassing the technology component and allowing for access to the data component. [27], discusses different attack vectors that were used during the COVID-19 pandemic. These attack vectors exposed flaws in both the people and technology components of the organizational triangle.

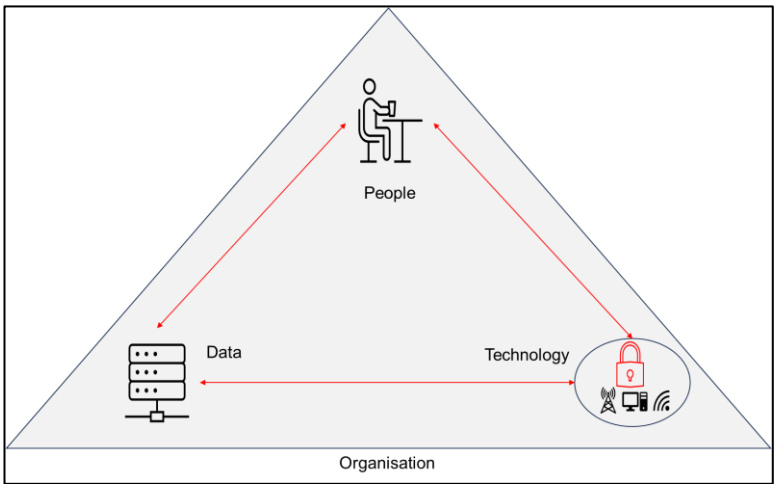

Fig 9: Organizational Triangle

6 Discussion and Implications

This research study demonstrates that data breaches in Africa are topical in government and businesses. From the analysis done based on social media and research data, it is evident that data breaches have also become part of legal disputes as well as law enforcement activities in Africa, where perpetrators are arrested (e.g., Equity Bank data breach) or organizations fined (e.g., Department of Justice in South Africa).

The trend analysis shows that data breaches are on the rise from the incidents and awareness point of view across the different African countries with Nigeria leading from the awareness point of view and South Africa prominent in the number of actual

data breaches. Kenya has demonstrated the real harm of data breaches on users, as well as how data breaches do not only impact one country but could also be impactful across boarder as observed with the Equity Bank breach. Other countries may be having low engagement and data on breaches, but this does not necessarily mean they are not experiencing them or are immune from cyber-attacks. In Africa, it is evident that many data breaches are not reported, possibly due to less robust data protection laws and lack of business and user awareness. Using expert knowledge, we have demonstrated in this paper that data breaches are triggered by the organizational triangle that focus on people, data, and technology. It is clear that people are the weakest link, but when security controls in people or processes are not strong, data breaches will occur through various techniques such as ransomware attacks, business email compromise, phishing, malware attacks and in some instances accidental data leakages and exposure by business and individuals.

It is also evident from the analysis that detailed information about the data breaches in Africa are limited to what is reported on the news websites and social media. Most organizations that fall victim to data breaches do not even share threat intelligence so that other organizations could be aided not to suffer the same data breaches. The lack of reporting and sharing plays into the hands of malicious actors because they can repeat the same data breach attacks without much effort.

The impact of data breaches on customers and businesses in Africa is determined as being negative, and unabated. And based on the data analysis, it is apparent that data breaches can have serious financial, reputational, legal and privacy implications. As such decision makers need to ramp-up the practical implementation of data protection laws as well as data protection awareness campaigns to protect organizations and users from malicious actors, thus promoting national security.

7 Conclusion and Recommendations

This research paper provides a contextual understanding of data breach trends in the African cyberspace using social media and research literature analysis. Close to 2,000 data points were collected on social media and news posts using specially crafted keywords over a 3-month period to understand the trend over time. The results indicate that data breaches are common African countries and data breach incidents are no longer superficial or distant but are real and impacting on businesses and individuals.

The following practical and evidence-based recommendations are made by the authors for African government and organizations to arrest the increasing rate of data breaches in the public and private sector. Robust legislation: we recommend implementation of strong legislative laws that could be used as a hindrance to threat actors. These legislative laws could be used to guide individual citizens, government departments and the private sectors on how to report cybercrime. The laws could also be used by the African governments to penalize negligent organization that fail to implement the minimum-security controls, thus at the very least circumventing a data breach. Specifically related to BEC, multifactor authentication could aid in reducing the high number of data breaches observed. Employee awareness training and phish-

ing simulation can also be used as forms for countermeasures. Phishing simulations allow for organizations to measure users' responsiveness towards identifying phishing emails that are sent to their mailboxes. Based on the organizational triangle, the phishing simulations that are conducted within each organization are also meant for the continuous assessment of the knowledge and operational use of the security controls by the employees. Other common best security practices such as regular patching of software, user awareness training, and deployment of NextGen security tools are encouraged. Consistent period data risk assessments are recommended, including privilege user activity monitoring and activity management. Lastly, it is also no longer sufficient at minimum to install security tools, but these security tools also need to be periodically patched and updated to prevent data breaches caused by the same tools.

References

1. Rubrik Zero Labs, https://www.rubrik.com/content/dam/rubrik/en/resources/report-review/rpt-rubrik-zero-labs-global-report.pdf, last accessed 2023/09/05.
2. DLA Piper, https://www.dlapiperdataprotection.com/, last accessed 2023/09/05.
3. ITWeb Homepage, https://www.itweb.co.za/content/j5alrMQAJOQMpYQk, last accessed 2023/09/18.
4. Niametrics Homepage, https://nairametrics.com/2023/02/14/nigeria-data-protection-bureau-says-110-companies-under-investigation-for-data-breach/, last accessed 2023/09/18
5. TechArena HomePage, https://www.techarena.co.ke/2023/04/13/kenya-airports-authority-suffers-data-breach-from-notorious-hacking-group/, last accessed 2023/07/14.
6. Skybox Security, https://www.skyboxsecurity.com/resources/report/vulnerability-threat-trends-report-2023/, last accessed 2023/09/18.
7. The Record Homepage, https://therecord.media/zyxel-says-a-threat-actor-is-targeting-its-enterprise-firewall-and-vpn-devices, last accessed 2023/07/14.
8. Verizon, https://www.verizon.com/business/resources/reports/dbir/, last accessed 2023/09/18".
9. Sophos, https://www.sophos.com/en-us/whitepaper/state-of-ransomware/, last access 2023/09/13.
10. Interpol, https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf, last accessed 2023/09/13.
11. KMPG, https://kpmg.com/za/en/home/insights/2022/09/africa-cyber-security-outlook-report-2022.html, last accessed 2023/09/13.
12. Talkwalker platform, https://www.talkwalker.com/blog/summer-2022-release, last accessed 2023/07/15.
13. Daily Trust, https://dailytrust.com/banks-telcoms-oil-firms-to-lose-2-revenue-for-data-breach-fg/, last accessed 2023/07/12.
14. Business Daily Africa, https://www.businessdailyafrica.com/bd/corporate/companies/court-bars-absa-from-auctioning-firm-in-sh1-5bn-data-breach--4285810, last accessed 2023/07/15.

15. KDB, https://mambomseto.co.ke/equity-bank-on-the-spot-once-again-after-client-loses-300k-in-17-minutes/, last accessed 2023/07/15.
16. Mybroadband, https://mybroadband.co.za/news/security/494239-half-a-million-customers-hit-by-incredible-hifi-corp-and-everyshop-data-breach.html, last accessed 2023/07/13.
17. Showmax, https://stories.showmax.com/za/important-notice-security-incident-affecting-user-credentials, last accessed 2023/07/13.
18. News24, https://www.news24.com/news24/tech-and-trends/news/department-of-justice-fined-r5m-for-not-beefing-up-cyber-security-after-2021-data-breach-20230705, last accessed 2023/07/13.
19. Reuters, https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/, last accessed 2023/07/10.
20. The East African, https://www.theeastafrican.co.ke/tea/business/rwanda-jails-8-kenyans-equity-bank-hacking-case-3463908, last accessed 2023/07/10.
21. MTN, Stanbic & others in Uganda, https://myjoyonline.com/hackers-break-into-mobile-money-system-to-steal-billions-from-airtel-mtn-stanbic-and-others-in-uganda, last accessed 2023/07/10.
22. The City Review, https://cityreviewss.com/anonymous-takes-down-boss-website-wants-exchange-rate-below-40k/, accessed 2023/07/10.
23. Business Daily, https://www.businessdailyafrica.com/bd/opinion-analysis/columnists/naivas-data-breach-a-wake-up-call-for-firms-to-comply--4223182, last accessed 2023/07/10.
24. SC Magazine, https://www.scmagazine.com/brief/threat-intelligence/ikeas-kuwait-morocco-franchises-hit-by-vice-society-ransomware-gang, last accessed 2023/07/10.
25. Hammouchi H., Cherqi O., Mezzour G., Ghogho M., and El Koutbi M.: Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time, Procedia Computer Science, vol. 151, pp. 1004-1009, (2019).
26. T. Krause, R. Ernst, B. Klaer, I. Hacker and M. Henze, Cybersecurity in Power Grids: Chal-lenges and Opportunities., Sensors 21, no. 18 (2021): 6225.
27. V. Susukailo, I. Opirskyy and S. Vasylyshyn, Analysis of the attack vectors used by threat actors during the pandemic, IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), pp. 261-264, 2020.