Obour Institute Journal
for Engineering and Technology (OI-JET)
Journal homepage: https://oijet.journals.ekb.eg
Volume (2), Issue (1), December 2024

Cyber Insecurity Effect on the Economy of Africa

Open access

Ahmed Gadallah: Dept. of Information Systems, Obour Institutes, Egypt, agadallah@oi.edu.eg
Amany Salah: Dept. of Human and Commercial Studies, Obour Institutes, Egypt, amanis@oi.edu.eg

Received August 10, 2024, Revised September 5, 2024, Accepted September 15, 2024

Abstract

The rapid development of technological progress and the adoption of digital electronic trading portals has had a profound impact on the global economy but is not without security risks. All the human ecosystem is managed through the application of IT and the benefits are evident in the healthcare sector system, economic, educational, political, and corporate sectors globally. Cyberspace has become a focal point for information sharing and management as well as a platform for governments, cooperate with organizations and individuals to harmonize common goals. It is also a platform for Information warfare involves state actors, business leaders and experts in the field. Target of the study aims to study the threats and nature of cybercrime and their impact on the African economy. with particular focus on Nigeria and Ghana. The estimated cost of cybercrime in Africa is estimated at $895 million, a figure that continues to soar in Nigeria lost about $550 million to cybercrime, Kenya ($175 million), Tanzania ($85 million), Ghana ($50 million) million) and Uganda ($35 million) per year. Research recommends more adoption A proactive and defensive approach to cybersecurity resilience through strengthening Cybersecurity policy framework and implementation strategy, rather than a reactive approach This is the case in most developing countries. Need to invest more in training well qualified domain experts as well as providing the infrastructure to support network security cannot is overrated.

***Keywords**: Insecurity, Threats, Cybersecurity, Africa, Economy*

1. Introduction

African economies are growing rapidly, with the region's GDP expected to reach $2.5 trillion by 2025. Digital growth is playing a major role in this growth, with the digital sector contributing to more than 10% of GDP in some African countries. However, digital growth is also accompanied by an increase in cyber threats (WBG 2021a, 3). The global annual cost of cybercrime is estimated to be $6 trillion per year. It cost makes up a value worth 1% of the Global GDP. Institutions and individuals across the continent are increasingly exposed to cyberattacks, leading to significant financial, commercial, and social losses. In addition to cybersecurity has become increasingly important in combating fraud (African Cyberthreat Assessment Report Cyberthreat Trends (2023). With the growing popularity of online shopping and banking, fraudsters have found new opportunities to steal money and personal information. Cybersecurity measures can help protect businesses and consumers from these threats.

As cybersecurity plays a key role in combating fraud in e-commerce transactions, businesses and organizations can protect customer data and financial transactions from cybercriminals by taking strong security measures. Some of the security measures that can be taken to combat fraud in e-commerce include[4]:

- Data encryption: Encryption helps protect data from unauthorized access.
- Two-factor authentication: Two-factor authentication requires users to enter an additional code in addition to their password.
- Monitoring suspicious activity: Businesses can use analytics to monitor suspicious activity on

Correspondence Author Ahmed Gadallah agadallah@oi.edu.eg

Print ISSN, 2974-4539, Online ISSN: 3062-5270

their websites or e-commerce apps.

- Training employees on cybersecurity: Employees should be aware of security risks and how to protect data.

Cyberattacks can cause major financial losses to businesses and organizations of all sizes. In 2021, the average cost of a data breach reached $4.24 million, up from $3.86 million in 2020.

As Cybersecurity in Africa faces several challenges such as Economic constraints: Limited resources hinder investment in cybersecurity infrastructure and personnel. Political disagreements and civil unrest: These factors can create instability and distract attention from cybersecurity issues. Ill-equipped infrastructure: Many African countries lack the necessary infrastructure, such as high- speed internet and reliable electricity, to effectively implement cybersecurity measures. Lack of awareness: Many individuals and organizations in Africa are not aware of the risks of cybercrime or how to protect themselves. These factors combine to make Africa more vulnerable to cyberattacks (African Union Cybersecurity Capacity BuildingProject).

Nigeria is one of the countries most affected by cybercrime in the world. In 2020, it ranked 16th globally. Insider threats: Hackers are increasingly targeting employees of Nigerian organizations, offering them money to divulge sensitive information (NITDA).

- Data breaches: Nigeria experienced a 1616% increase in data breaches in Q3 2022 compared to Q2.
- Government response: The Nigerian government is taking steps to combat cybercrime, with the EFCC convicting over 2800 people since the start of 2022.

As Zambia Facing Growing Cybercrime Challenges.it ranks 58th out of 161 countries on the National Cyber Security Index, indicating moderate preparedness. However, it faces challenges (African Cyberthreat Assessment Report Cyberthreat Trends 2023):

- Limited technology access: Only 50% of Zambians own a personal computer, but 75% own smartphones, making them vulnerable to scams via text
- High cybercrime rate: In 2021, over 10.7 million cybercrimes were reported to the ZM- CIRT.
- Financial losses: The Zambian finance sector lost over 150 million ZMK ($872,000) between 2020 and Q2 2022. SMS fraud cost individuals over 1 million ZMK ($58,000) during the same period.

2. Research problem:

African continent is suffering from a very lack in cyber security, Statistics from the 22 African member countries reveal 399 reported Business Email Compromise (BEC) cases in 2021. However, this limited data paints an incomplete picture of the true scope of the problem, A comprehensive assessment dedicated specifically to BEC within the African region is crucial to uncovering the full extent of this criminal activity (Cyber Threats to the Financial Sector in Africa 2022). This is attributable to several reasons such as economic constraints, political disagreements, civil unrest, inadequate infrastructure, and a general lack of awareness, have limited a similar progression of cybersecurity standards across much of the developing world (FIGI,2022,3), African small and medium-sized enterprises indicated that about 95 percent of those polled were at or below the “security poverty line”— that is, they had few or no resources to invest in security or defensive solutions and were thus unable to plan for or manage cyberattacks effectively (Świątkowska 2020, 20). The cost and lack of immediate return on investment for security activities such as penetration testing or threat intelligence analysis leads many small and medium-sized enterprises to forgo these activities entirely (Kabanda, Tanner, and Kent 2018, 274) The cost of downtime: When cyberattacks disrupt business operations, businesses and organizations can lose revenue and productivity.

3. Research Questions:

The research questions can be summarized in the following points:

- What are the types of cyberattacks targeting African businesses and governments?
- What are the financial, commercial, and social losses caused by cyberattacks in Africa?
- What actions have African governments and businesses taken to improve cybersecurity?
- What are the challenges facing efforts to improve cybersecurity in Africa?
- What is the economic impact of cyber insecurity on the African continent?

4. Research Questions:

Africa's internet penetration rate is booming, reaching an average of 44% according to the 2022 Global Digital Report. This rapid growth, fueled by substantial financial investments in infrastructure and digital access initiatives across the continent, shows no signs of slowing down. Moreover, the rollout of 5G networks in many African nations is further accelerating this impressive expansion (Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018).

Cybersecurity is essential for preserving economic and financial stability. At the macro level, the huge expense of recovering from a Central Bank, Ministry of Finance, or any big commercial bank breach or hack would entail financial loss to stakeholders ranging from national governments to small firms and people. According to a 2019 study of 300 global CEOs, the single greatest danger to the global economy over the next decade is a lack of cybersecurity. According to cybersecurity industry associations, cyber assaults have a significant influence on the worldwide economy. According to one prediction, the worldwide cost of cybercrime would exceed $8 trillion by 2023. This sum is greater than the national economy of all nations except two—the United States and China. As Cybersecurity also plays an important role in combating fraud in electronic commerce operations. By taking strong security measures, companies and institutions can protect customer data and financial transactions from infiltrators.

5. Methodology:

The researcher adopted the descriptive approach to review previous studies, using both the deductive approach and the inductive approach in analyzing the study variables, the independent variables are cybersecurity and its impact on the dependent variable, which is the economies of African countries.

6. Data Sources:

The researcher relied on the following sources to collect data:

- United Nations Office Drugs and Crime reports.
- World Bank reports.
- IBM Security reports.
- African Cyberthreat Assessment report 2023

7. Literature Review:

Because of the importance of cyber security and its role in development and Economic Growth many studies had talked about it mentioned below:

Interpol report (2023) showed that Africa's rapid digitalization has created a double-edged sword. While economic opportunities flourish, it also offers fertile ground for malicious actors, particularly those exploiting Business Email Compromise (BEC). With growing reliance on technology, vulnerable organizations face increased risk due to weak cybersecurity measures in many parts of the continent. This trend poses a significant threat to the global economy, with immeasurable potential costs.

As **IBM report (IBM,2022**) proposed a technique to prevent easy data breaches, as well as effective resistance to make it more difficult for hackers. This method consists of two stages: Preventing unauthorized access to sensitive data. This study focused on preventing network intrusion. The four-cybersecurity attack surface coverage disciplines are as follows: Four cybersecurity disciplines collaborate to cover the whole attack surface. Management of internal security vulnerabilities, data leakage, and vendor risk.

World bank report (2022) about Cyber Threats to the Financial Sector in Africa showed that the financial sector in Africa is the most vulnerable to cybersecurity attacks, and that it needs more awareness of the importance of adopting an effective and safe system to preserve capital and protect the country from any operations that threaten the economic situation.

As **Brett van Niekerk study (2017)** Brett Van Niekerk's study (2017) also aimed to identify the importance of cybersecurity to preserve the economic and social entity of the state of South Africa, as the increase in electronic attacks coincided in 2016. The targets included governmental and non-governmental organizations. Critical infrastructure still requires further investment and strengthening, and some of the most vulnerable organizations, Eskom, are vulnerable and could suffer serious consequences if attacked. Misconfiguration Threats: A worrying trend of security incidents due to human error or system misconfiguration. Potential link to increased awareness and reporting after the 2009 POPI bill. Organizations need to prioritize cybersecurity awareness training and system configuration best practices. Full implementation of the POPI Act may help reduce accidental exposure through accountability measures.

At last, **yadav .H, Shashant.G**(**2014**) study aims to investigate the relationship between Cyber Attacks, and the Economy. In addition to identifying the types of electronic attacks, the effects resulting from those attacks, and recommendations that would reduce those attacks.

8. Types of Cybercrime:

There are a number of different types of cybercrime that have increased during the pandemic. These include18:

- Phishing scams: Phishing scams are emails or text messages that try to trick people into revealing personal information, such as passwords or credit card numbers.
- Malware attacks: Malware is software that is designed to harm computers or steal data.
- Ransomware attacks: Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key.

In addition to these traditional types of cybercrime, there have also been an increase in attacks on critical infrastructure, such as hospitals and power grids. The increase in cybercrime has had a significant impact on businesses and individuals. Businesses have suffered financial losses from data breaches and ransomware attacks. Individuals have had their personal information stolen and their identities used for fraud.

9. Reasons of cybercrime:

Lack of awareness and failure to follow security protection policies are considered among the most important weaknesses that cause cyber-attacks, which cost approximately $300 billion to $1 trillion in the world, which represents 0.4% to 1.4% of the global gross domestic product19.) yadav .H, Shashant.G (2014), P:938). In addition to common reasons for cybercrime:

1. **Financial gain**: This is the most common motivation for cybercrime. Cybercriminals want to steal money or valuable information that they can sell. This can include credit card numbers, bank account numbers, and personal information that can be used for identity theft.

2. **Espionage**: Cybercrime can also be used for espionage purposes. Governments and corporations often use cybercrime to steal trade secrets or other confidential information from their competitors.
3. **Vandalism**: Some cybercriminals simply want to cause damage or disruption. They may launch denial-of-service (DoS) attacks to overwhelm websites or servers, or they may release malware that can damage computers or networks.
4. **Revenge**: Cybercrime can also be motivated by revenge. For example, a disgruntled employee may hack into their employer's computer system to steal data or cause damage.
5. **Activism**: Some cybercriminals see themselves as activists who are fighting for a cause. For example, hacktivists may target websites or computer systems that they believe are unethical or harmful.
6. **Thrill-seeking**: Some cybercriminals are simply thrill-seekers who enjoy the challenge of breaking into computer systems. They may not have any financial or other motives, but they enjoy the feeling of power and accomplishment that comes from successfully hacking into a system.

10. Relationship Between Cyber Security and Development:

The United States Agency for International Development (USAID) defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation." As USAID partner nations continue to digitally change and embrace new digital tools and systems, cyber threats and vulnerabilities multiply. Failures in cybersecurity endanger USAID partner nations and erode partner country government credibility. USAID must safeguard its digital assets by ensuring that its digital programming tackles cyber threats and incorporates cybersecurity mitigation mechanisms *(yadav .H, Shashant.G 2014).*

11. The Impact of Cyber Insecurity on the African Economy:

The COVID-19 pandemic has created a perfect storm for cybercriminals. With more people working from home and using online services, there are more opportunities for attackers to exploit (NIST). In addition, the pandemic has created a sense of fear and uncertainty, which can make people more susceptible to scams. As a result of these factors, cybercrime has increased dramatically since the start of the pandemic. According to a report by the United Nations Office on Drugs and Crime (UNODC), cybercrime has increased by up to 600% in some countries. (NIST) It is estimated that, worldwide, cybercrimes will cost $10.5 trillion annually by 2025. The global annual cost of cybercrime is estimated to be $6 trillion per year. The cost of downtime: When cyberattacks disrupt business operations, businesses and organizations can lose revenue and productivity.

Cybersecurity insecurity is a growing threat to the African economy. It can lead to a variety of problems, including:

- **Financial losses**: Cyberattacks can result in the theft of sensitive financial information, such as credit card numbers and bank account information. This can lead to financial losses for individuals and businesses.
- **Disruption of operations**: Cyberattacks can also disrupt operations, such as by taking down websites or computer systems. This can lead to lost productivity and revenue for businesses.
Damage to reputation: Cyberattacks can damage the reputation of businesses and organizations. This can make it difficult for them to attract customers and partners.

In addition to these direct costs, cybersecurity insecurity can also have a negative impact on the African economy in more indirect ways. For example, it can:

- **Decrease investment**: Foreign investors may be less likely to invest in Africa if they are concerned about the risk of cyberattacks.
- **Reduce innovation**: Businesses may be reluctant to invest in new technologies if they are concerned about the security of those technologies.
- **Slow economic growth**: Cybersecurity insecurity can slow economic growth by making it more difficult for businesses to operate efficiently and effectively.
  Here are some specific examples of how cybersecurity insecurity can affect the African economy:
- In 2022, a cyberattack on a Zambian bank resulted in the theft of personal information for over 1 million customers. This caused financial losses for the bank and damaged its reputation.
- In 2021, a cyberattack on a Nigerian telecommunications company disrupted service for millions of customers. This caused lost productivity and revenue for businesses and individuals.
- In 2020, a cyberattack on a South African government agency resulted in the theft of sensitive data, including personal information for government employees. This damaged the reputation of the government and made it more difficult to attract foreign investment.

By taking steps to improve cybersecurity, African governments and businesses can help to mitigate these threats and protect the African economy.

Cybercrime cost makes up a value worth 1% of the Global GDP. on average, a malware attack costs a company over $2.5 million (including the time needed to resolve the attack. (United Nations Office on Drugs and Crime annual report 2020)

Weak cybersecurity can have a devastating impact on the African economy, as it can lead to:

- **Major financial losses:** Cyberattacks can cause significant financial losses for businesses and governments. For example, Kaspersky Lab estimated that cyberattacks caused losses worth $1.3 billion in Africa in 2022.

- **Business disruptions:** Cyberattacks can disrupt businesses, leading to lost profits and increased costs. For example, a cyberattack on South African Airways caused the cancellation of more than 400 flights in 2022.

Loss of trust in government: Weak cybersecurity can lead to loss of trust in government, making it difficult for governments to address other economic and social issues. For example, cyberattack on the government of South Sudan in 2022 disrupted critical government services.

Cybersecurity costs versus the cost of non- compliance Cybersecurity is an essential investment for businesses and organizations of all sizes. By implementing strong cybersecurity measures, organizations can protect themselves from a variety of cyber threats, including malware attacks, data breaches, and ransomware attacks.

The cost of cybersecurity can vary depending on the size and complexity of an organization's IT infrastructure. However, in general, the cost of cybersecurity is a fraction of the cost of a successful cyberattack.

For example, a 2022 study by the Ponemon Institute found that the average cost of a data breach was $3.86 million. This includes the cost of notifying affected individuals, investigating the breach, and implementing corrective measures.

In contrast, the cost of implementing strong cybersecurity measures is relatively low. For example, the cost of implementing a basic cybersecurity plan can be as little as $5,000. As the cost of cyber threats continues to rise, the cost of cybersecurity is becoming increasingly affordable. By investing in cybersecurity, organizations can protect themselves from significant financial losses. Here are some of the specific benefits of cybersecurity:

- **Protects sensitive data**: Cybersecurity measures can help protect sensitive data, such as customer PII and financial information. This can help organizations avoid regulatory fines and lawsuits.

- **Reduces downtime**: Cybersecurity measures can help prevent cyberattacks that can disrupt operations and lead to lost productivity.
- **Increases customer trust**: Customers are more likely to do business with organizations that they trust to protect their data.
-

12. Cyber insecurity undermines economic growth opportunities in Africa by targeting small and medium-sized enterprises.

the African continent is home to a large and growing population of small and medium-sized enterprises (SMEs). These businesses are the backbone of the African economy, generating jobs and driving economic growth. Unfortunately, SMEs are often vulnerable to cyberattacks. This is because they may have limited resources to invest in cybersecurity, and they may not have the expertise or knowledge to protect themselves from cyber threats. Cyberattacks on SMEs can have a devastating impact on these businesses. They can lead to financial losses, disruption of operations, and damage to reputation. In some cases, cyberattacks can even lead to the closure of businesses.

Smaller Firms are Attractive Targets to cyber insecurity because of:

a. **Lower Security**: Attacks on less well-protected networks require less expertise and investment from the attackers.
b. **Cheap Access**: A large part of the ease of attacking small firms is due to the availability of large quantities of very cheap Remote Desktop Protocol (RDP) credentials.
c. **High Payouts**: Despite being less secure, smaller firms are still often willing to pay significant ransoms to recover their data, making them a lucrative target.
d. **Limited IT Security Awareness**: Small professional service firms often have limited attention to IT security, making them easy prey for ransomware attackers. This lack of awareness and preparedness puts them firmly in the sights of extortionists (ISTR, 21, April 2016).

Cove ware's latest set of statistics from Q3 of 2020 show that more than 70% of ransomware incidents were companies with fewer than 1,000 employees, and 60% had revenues of less than $50 million.

Looking at the breakdown by industry sector, more than a quarter of companies are in the professional services category, by far the largest single vertical and challenged only by health care and the public sector. As noted above, these get perhaps more attention than they should, weighing in at only 11.3% and 11.6% of incidents. No other category tops 10%. With professional services firms making up only 14% of businesses in the US, but making up over 25% of ransomware attacks, this industry sector is absorbing more attacks than it should. Increased Ransomware Vulnerability of Small and Medium-Sized Businesses, over 50% of all cyber-attacks are done on SMB's.

Cyber-attacks cause billions of dollars in losses, as well as loss of company reputation. Cyber- attacks take many forms, including DoS, theft of information, destruction of the database, and many other forms that negatively affect the economy, which increases the company's need to defend itself more and protect its information and its customers. (yadav .H, Shashant.G(2014), P:937) These assaults are not limited to micro, small, and medium-sized organizations (MSMEs). According to one research, businesses with less than 100 employees are three times more likely to be attacked by hackers than bigger businesses. Cyber assaults or cybercrime against micro, small, and medium-sized firms (MSMEs) can destroy individual business owners' and their workers' livelihoods. After a cyber assault, 60% of MSMEs go out of business within 6 months.

13. The financial losses from cyber-Insecurity can *include:*

1. **cost of data breaches**:

The cost of data breaches: When cybercriminals steal data, businesses and organizations must pay to notify affected customers, investigate the breach, and implement new security measures. shows trends in the cost of lost business, ex-post response, notification and detection and escalation over the past six years. The pattern shows consistency in these costs. Notification continues to be the lowest and lost business is the highest cost component. Organizations in the United States had the highest average total cost at $8.64 million, followed by the Middle East at $6.52 million. In contrast, Latin American and Brazilian organizations had the lowest average total cost at $1.68 million and $1.12 million, respectively. The average cost of a data breach in South Africa was $52.14 million in 2020 (Cost of a Data Breach Report, 2020*)* The average cost of a data breach in 2022 was USD 4.35 million[32]

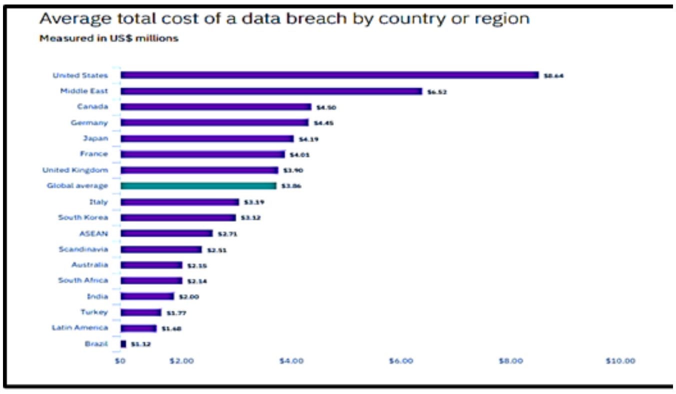

Fig. (1) Average total cost of a data breach by country or region
Source: Cost of a Data Breach Report 2020

Data breach Cyberattacks can lead to data breaches of sensitive data, such as customer or financial data. This can have serious consequences, such as identity theft or fraud.it costs rose from $3.86 million to $4.24 million in 2021, 10% increase in average total cost of a breach from 2020-2021.the highest average total cost in the 17-year history of this report. The average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach. Enterprises experienced 130 security breaches per year, per organization, on average. The annual number of security breaches on enterprise organizations increased by 27.4%. on average enterprises needed 50 days to resolve an insider's attack and 23 days to recover from a ransomware attack. The average cost of a data breach to small business can range from $120,000 to $1.24 million.

2. **The cost of ransomware payments:**

Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. Ransomware attacks have become increasingly common in recent years, and they can have a devastating impact on businesses and organizations. The economics of ransomware attacks are complex, but there are a number of key factors that contribute to the profitability of these attacks. These factors include:

- The increasing value of data: Data is becoming increasingly valuable to businesses and organizations, and they are willing to pay large sums of money to protect it.
- The ease of carrying out ransomware attacks: Ransomware attacks are becoming increasingly easy to carry out, thanks to the availability of cheap and easy-to-use tools.
- The difficulty of tracking down ransomware attackers: Ransomware attackers are often located in countries with weak law enforcement, making it difficult to track them down and prosecute them.

Ransomware attacks are increasingly targeting mid-market enterprises, which are thought to be simpler to corrupt and have a higher potential to pay ransoms than extremely tiny businesses. Due to a lack of specialized IT security staff, flat network topologies, and insufficient access control procedures, professional services organizations, particularly small law firms and financial services firms, are regularly attacked. These businesses frequently misjudge their vulnerability to ransomware attacks and fail to install proper security measures, making them prime targets for attackers." Average Ransom Demand Q4 Ransomware Payment Cost Some cybercriminals encrypt data and demand a ransom payment to decrypt it. Ransomware is 57x more destructive in 2021 than it was in 2015.There are 30 million SMB in the USA and over 66% of all SMB's had at least 1 incident between 2018-2020

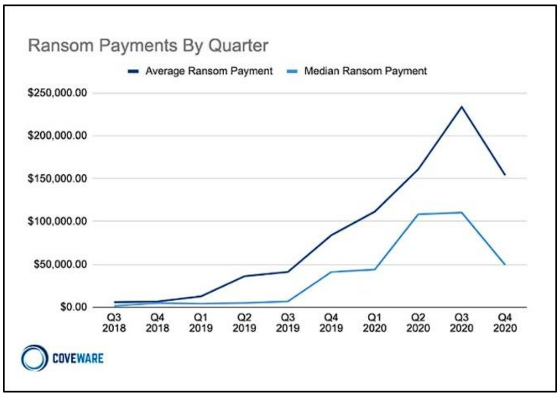

Fig. (2*) Ransom Payments 2*

Source*: https: //www.coveware.com /blog/ranso mware-marketplace-report-q4-2020*

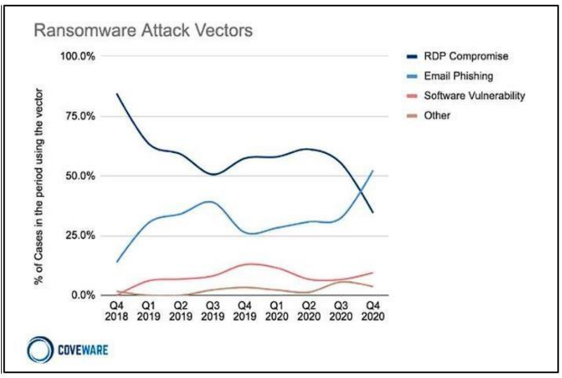

Fig. (3) Ransom Attack

Source: https: //www.coveware.com /blog/ranso mware- marketplace-report-q4-2020

3. In addition to the cost of reputational damage:

Cyberattacks may harm a company's brand, making it difficult to acquire customers and partners. In addition to these direct financial losses, cyberattacks can also lead to indirect financial losses, such as increased insurance premiums, decreased stock prices, and lost legal battles. The financial impact of cyberattacks can be devastating for businesses and organizations of all sizes. It is important to take steps to protect yourself from cyberattacks, such as implementing strong security measures, educating employees about cybersecurity risks, and having a plan for responding to cyberattacks.

14. The Economics of Ransomware Attacks:

Like other forms of financially motivated crime, cyber extortion is driven by the power laws of basic economics. Legitimate goods have a cost to produce, a cost to sell, and an end amount of profit earned from sales. Illegitimate "services" like extortion are no different. A ransomware attack costs money to stage and execute. Just like a legitimate firm, the average attack has a success rate and monetization rate that threat actors can expect as their profit. Rational economic behavior predicts that a financially motivated actor will seek to maximize profits (costs less proceeds). Attacks on larger, better-defended targets are more difficult to pull off. They take more time and expertise to set up, sometimes even involving expensive zero-day exploits which can only reliably be used once. They can also take more time and effort to complete, with negotiations stretching for days or weeks, and throughout there is a higher risk of failure, of an attack being spotted and blocked, of a surprise system change undoing the attacker's hard work, or of a victim simply refusing to pay up. The very high ransoms demanded reflect both the effort and the risk.

As a result of these factors, ransomware attackers have been able to make significant profits from their attacks. In 2021, ransomware attacks are estimated to have cost businesses and organizations over $6 billion. The impact of ransomware attacks can be devastating for businesses and organizations. In addition to the financial costs of paying ransoms, businesses and organizations can also suffer from downtime, lost productivity, and reputational damage. In some cases, ransomware attacks can even have a significant impact on society as a whole. For example, in 2021, a ransomware attack on the Colonial Pipeline, which supplies fuel to much of the US East Coast, caused widespread fuel shortages and price spikes.

There are a number of things that businesses and organizations can do to protect themselves from ransomware attacks. These include:

- Implementing strong security measures: Businesses and organizations should implement strong security measures, such as firewalls, intrusion detection systems, and data encryption.
- Educating employees about cybersecurity risks: Businesses and organizations should educate their employees about cybersecurity risks and how to avoid them.
- Having a plan for responding to cyberattacks: Businesses and organizations should have a plan for responding to cyberattacks, including how to isolate the affected systems, notify law enforcement, and restore data from backups.

Ransomware attacks are a serious threat to businesses and organizations of all sizes. By taking proactive steps to protect themselves, businesses and organizations can reduce their risk of falling victim to these attacks.

15. The Growing Threat of Ransomware in Africa:

The increasing adoption of digital technologies and internet connectivity in Africa has made the continent more vulnerable to ransomware attacks. Cybercriminals recognize the growing reliance on digital infrastructure and the potential for substantial financial gains, making African countries attractive targets.

The African continent has witnessed a notable surge in ransomware attacks in recent years. According to a report by Interpol, Africa accounted for 10% of all detected ransomware attacks globally in 2021. This represents a significant increase from previous years, indicating the growing prevalence of ransomware threats in the region.

16. The Economics of Ransomware Attacks in African *Countries:*

Ransomware attacks have become increasingly prevalent in recent years, posing a significant threat to businesses and organizations worldwide. African countries are not immune to this growing cybersecurity threat, as evidenced by the rising number of attacks reported in the region. The economic impact of ransomware attacks in Africa can be substantial, affecting businesses, organizations, and even governments.

Ransomware attacks can have a devastating economic impact on businesses and organizations in Africa. The forced payment of ransoms can drain financial resources, leading to operational disruptions, productivity losses, and even business closures. The reputational damage caused by ransomware attacks can further hinder growth and business opportunities.

The impact of ransomware attacks extends beyond individual businesses and organizations, affecting the broader economy. Ransomware attacks can disrupt critical infrastructure, such as healthcare systems, transportation networks, and energy grids. These disruptions can have widespread consequences, impacting the lives of citizens and hindering economic development (The latest 2023 cyber crim Statics, 2023).

Cyber Crime in Africa (Cyber Threats to the Financial Sector in Africa, 2022)**:**

Economic constraints, political disagreements, civil unrest, ill-equipped infrastructure, and lack of awareness helped in limiting the progress of cybersecurity standards, making them more vulnerable to cyber threats and attacks (Kshetri, Nir. 2019).

Cybercrime in Nigeria:

In 2020, Nigeria was ranked 16th in the world for countries most affected by cyber-crime. A recent development in Nigeria's cyber threat landscape is hackers tempting employees of Nigerian organizations to act as insider threats. Research has revealed that hackers have started offering money in return for employees to divulge sensitive information on an organization's network. While the report did not say whether any staff had acted as insider threats, it is clear that this is a growing area of concern. In Q3 of 2022, Nigeria experienced a 1616% increase in data breaches, from 35,472 in Q2 to 608,765 in Q3. However, the Nigerian government is continuing to fight against cyber-crime. Since the start of 2022, Nigeria 's Economic and Financial Crimes Commission (EFCC) have convicted 2847 people in connection with cyber-related crimes.

Cybercrime in Zambia

Zambia ranks 58th out of 161 countries on the National Cyber Security Index and 73rd out of 194 countries on the Global Cyber Security Index. As a developing country, access to technology is somewhat restricted – only 50% of Zambians own a personal computer. However, around 75% own smartphones, which makes scams via text a particular issue. In 2021 alone, 10.7 million cybercrimes were reported to the Zambia Computer Incident Response Team (ZM-CIRT), which included mobile money reversal scams and social media hijacking. The GDP per capita of Zambia is
$4000. Between 2020 and Q2 2022, the Zambian finance sector suffered losses of over 150 million ZMK ($872,000). In the same period, SMS fraud cost Zambians over 1 million ZMK ($58,000).

Cybersecurity Challenges in Africa:

Africa faces a number of challenges in developing and implementing effective cybersecurity measures. These challenges include:

- A lack of public awareness about cyber threats and digital hygiene
- A shortage of cybersecurity professionals (Świątkowska 2020).
- Reliance on outdated and poorly secured information technology infrastructure
- High rates of pirated software (Khatri 2019).
- Economic constraints that make it difficult for businesses to invest in cybersecurity
- (Kabanda, Tanner, and Kent, 2018).
- Socioeconomic factors that make cybercrime an attractive option for some individuals (Świątkowska 2020).
- Ineffective law enforcement

These challenges make African cyberspace an attractive target for motivated threat actors. As a result, African countries are increasingly vulnerable to cyberattacks.

Key Points

- Africa's size and diversity make it difficult to establish comprehensively the general state of cybersecurity across all of the continent.

- The following common issues make African cyberspace an attractive target for motivated threat actors:
  - Human factor
  - Lack of capacity
  - Resources
  - Economic constraints
  - Socioeconomic factors
  - Ineffective law enforcement

17. Solutions to Improve Cybersecurity in Africa:

Cybersecurity is essential for the African economy. African governments and businesses need to work together to improve cybersecurity and protect the continent from cyberattacks. African countries need to take proactive measures to combat ransomware attacks and protect their digital infrastructure. This includes strengthening cybersecurity measures, raising awareness among businesses and organizations, and fostering collaboration between governments, law enforcement agencies, and the private sector.

Building resilience against ransomware attacks is crucial for African countries to maintain economic stability and growth. Businesses and organizations should adopt robust cybersecurity practices, including regular backups, data encryption, and employee training. Governments should play a role in promoting cybersecurity awareness, providing support to businesses, and enacting stricter regulations to deter cybercriminals.

There are a number of solutions that can help to improve cybersecurity in Africa, including:

- Legislation and regulations: African governments need to enact strong cybersecurity legislation and regulations. These regulations should require businesses and individuals to take steps to secure their systems and networks.
- Public awareness: Governments and businesses need to raise public awareness of cybersecurity. Individuals need to be taught how to protect themselves from cyberattacks.
- Investment in education and training: Governments and businesses need to invest in cybersecurity education and training. Cybersecurity professionals need to be trained to address the ever-evolving threats.
- Increased investment: Governments and organizations need to invest in cybersecurity infrastructure and personnel.
- Improved awareness: Educational campaigns can help individuals and organizations understand the risks of cybercrime and how to protect themselves.
- Collaboration: African countries need to work together to share information and intelligence about cyber threats.
- International cooperation: Developed countries can assist African nations by providing expertise and resources.

By taking these steps, Africa can become better prepared to combat the growing threat of cybercrime.

18. Recommendations:

- African countries should invest in cybersecurity awareness campaigns and training programs to educate citizens about online threats and protective measures.
- African countries should increase the number of cybersecurity professionals through education and training programs to address the continent's growing cybersecurity workforce shortage.
- African countries should invest in modern and secure IT infrastructure to strengthen their digital defenses against cyberattacks.

- African countries should crack down on software piracy to reduce the availability of unlicensed and potentially vulnerable software that cybercriminals can exploit.
- African countries should provide financial support to businesses for cybersecurity investments to help them implement adequate protective measures.
- African countries should address the socioeconomic factors that contribute to cybercrime by promoting economic growth, education, and employment opportunities.
- African countries should strengthen their law enforcement capabilities to investigate and prosecute cybercrime by establishing specialized cybercrime units and fostering international cooperation.

Security Measures to Prevent Fraud in Internet Commerce:

- Encryption of data: Protects data from unauthorized access by scrambling it into an unreadable format.
- Bilateral certification: Requires users to provide an additional code, such as a one-time password, in addition to their traditional password for enhanced authentication.
- Suspicious activity control: Utilizes analytics to monitor user behavior on websites or e-commerce platforms and identify anomalies that may indicate fraudulent activity.
- Cybersecurity training for employees: Educates employees about cybersecurity risks and best practices to prevent data breaches and human error-related incidents.

Examples of Cybersecurity Applications in Preventing Internet Commerce Fraud:

- Data encryption safeguards credit card information and other sensitive payment details from unauthorized access during transmission.
- Bilateral certification adds an extra layer of security to user accounts, making it more difficult for cybercriminals to gain unauthorized access.
- Analytics can detect suspicious patterns, such as multiple failed logins attempt or unusually large transactions, which may signal fraudulent activity.

19. Conclusion:

Cyber insecurity is a major issue for the entire African continent. The rapid growth of technology and the increasing reliance on digital platforms have made African nations more vulnerable to cyberattacks. These attacks can have a significant financial, commercial, and social impact on individuals, businesses, and governments. The research has identified several key challenges that African countries face in improving their cybersecurity posture: Economic constraints: Many African countries lack the resources to invest in the necessary cybersecurity infrastructure and personnel. Political instability: Political disagreements and civil unrest can distract attention from cybersecurity issues. Inadequate infrastructure: Many African countries lack the high-speed internet and reliable electricity needed to effectively implement cybersecurity measures.

Lack of awareness: Many individuals and organizations in Africa are not aware of the risks of cybercrime or how to protect themselves.

The research has also identified several recommendations for improving cybersecurity in Africa:

Invest in cybersecurity infrastructure and personnel: African countries need to invest in the necessary infrastructure and personnel to effectively combat cybercrime. This includes funding for cyber security awareness programs, training for law enforcement and judicial officials, and the development of national cybersecurity strategies. Promote public- private partnerships: Public- private partnerships can help to leverage the resources and expertise of both the government and the private sector to improve cybersecurity. Raise awareness of cybercrime: There is a need to raise awareness of cybercrime risks and encourage individuals and organizations to take steps to protect themselves. This can be done through public education campaigns, media outreach, and cybersecurity training programs. Strengthen cybersecurity laws and regulations: African countries need to strengthen their cybersecurity framework for effective law enforcement. Increase international cooperation: African countries can benefit from increased international cooperation in the area of cybersecurity. This includes sharing information about cyber threats, collaborating on cyber investigations, and providing technical assistance to developing countries.

References

1. *Nigeria: National Information Technology Development Agency (NITDA): https://nitda.gov.ng/*
2. *"ISTR: Internet Security Threat Report," Symantec, volume 21, April 2016,https://www.symantec.com/content/dam/symntec/docs/ reports/istr-212016en.pdf?aid=elq_&om_sem_kw=elq_14823723&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elq id=2902& elqat=2*
3. *2018.op.cit.p:93.*
4. 2022 Digital Global Report (www.wearesocial.com)
5. *33. Pathways for Prosperity Commission, January 2020, accessed October 2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_ unleash_developing_countries_digital_potential.pdf*
6. *-A Complete Guide to Data Breaches (2022). Cost of a data breach 2022. [online] www.ibm.com. Available at: https://www.ibm.com/reports/data-breach. www.upguard.com*
7. *-African Cyberthreat Assessment Report Cyberthreat Trends (2023), Outlook By The African Cybercrime Operations Desk, ©Interpol Global Complex For Innovation, p:4.* https://www.interpol.int/Crimes/Cybercrime/Cybercrime- operations/AFJOC-African-Joint-Operation-against-Cybercrime
8. -African Cyberthreat Assessment Report Cyberthreat Trends (2023), Outlook By The African Cybercrime Operations Desk, ©Interpol Global Complex For Innovation, pp:1-30.
9. *-African Union: African Union Cybersecurity Capacity BuildingProject:* https://au.int/en/treaties/african-union- convention-cyber-security-and-personal-data-protection
10. *-Cisco Umbrella. (n.d.). 2021 Cybersecurity threat trends: phishing, crypto top the list. [online] Available at: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.*
11. *-Cost of a Data Breach Report 2020, IBM Security © Copyright IBM Corporation 2020 Availableat: https://community.ibm.com/community/user/ security/events/eventdescription?CalendarEventKey=13 8799f1-67eb-475f 9832-a630417397c7*
12. *-Cyber Threats to the Financial Sector in Africa (2022), Financial Inclusion Global Initiative (FIGI) @worldbank.org, P:3.*
13. *-Cyber Threats to the Financial Sector in Africa (2022), Financial Inclusion Global Initiative (FIGI) "@worldbank.org, P:3.*
14. ***-Cyber Threats to the Financial Sector in Africa** An Assessment of the Current Threat and an Analysis of Emerging Trends on the Future Threat Landscape(2022), ©2022 International Bank for Reconstruction and Development, PP:3-4,available at https://documents1.worldbank.org/curated/en/09983040 5172214598/pdf/P16477000601530760af01093740e385*
15. *-Cyber Threats to the Financial Sector in Africa, op.cit. p:4*

16. -Cybersecurity: ECONOMIC GROWTH AND TRADE (EGAT),p:1.available at: c yb ers ec u rity. itr @us a id.gov.
17. cybersecurity_practices_in_developing_countries/links/ 5cd56c2ea6fdccc9dd9d5ae4/Exploring- SMEcybersecurity-
18. fe8.pdfŚwiątkowska, Joanna. 2020. Tackling Cybercrime to Unleash Developing Countries' Digital Potential. Background Paper 33. Pathways for Prosperity Commission, January 2020, accessed October2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/fi les/2020-01/tackling-cybercrime-to-unleash-developing-countries_digital_potential.pdf.
19. -Global Ransomware Damage Costs (https://cybersecurityventures.com/global-ransomware- damage-costs-predicted-to-reach-250-billion-usd-by-2031/13file:///C:/Users/User/Dow n lo ads /2023_03% 20CY BE R _African% 20Cyberthreat% 20Assessment% 20Repo rt% 202022_E N.pdf
20. -https://www.coveware.com/blog/2020/11/30/why-small-professional-service-firms-are-ransomware-targets
21. -https://aag-it.com/the-latest-cyber-crime-statistics/
22. -https://aag-it.com/the-latest-cyber-crime-statistics/
23. -https://purplesec.us/resources/cyber-security- statistics/
24. -https://www.cisa.gov/.
25. -https://www.ponemon.org/
26. -Kabanda, Salah, Maureen Tanner, and Cameron Kent.
27. -Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018. "Exploring SME Cybersecurity Practices in Developing Countries." *Journal of Organizational Computing and Electronic Commerce* 28, no. 3: 269–82, accessed October 2021. https://www. researchgate.net/profile/Salah-Kabanda-2/publication/326385562_Exploring_SME_
28. -Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018. "Exploring SME Cybersecurity Practices in Developing Countries." *Journal of Organizational Computing and Electronic Commerce* 28, no. 3: 269–82, accessed October 2021. https://www.researchgate.net/profile/Salah-Kabanda-2/publication/326385562_Exploring_SME_cybersecurity_practices-in_developing_countries/links/5cd56c2ea6fdccc9dd9d5ae4/Exploring-SMEcybersecurity-practices-in-developing-countries.pdf
29. -Kshetri, Nir. 2019. "Cybercrime and Cybersecurity in Africa." Journal of Global Information Technology Management 22, no. 2: 77–81, accessed October 2021. https://www.tandfonline.com/doi/pdf/10.1080/1097 198X.2019.1603527
30. -National Institute of Standards and Technology (NIST): https://www.nist.gov/cyberframework
31. -National Institute of Standards and Technology (NIST): https://www.nist.gov/cyberframework
32. -practices-in-developing-countries.pdf.
33. PROGRAMME 2020 © United Nations, January 2021. All rights reserved.https://www.unodc.org/documents/ropan/2021/C CP_2020_REPORT.pdf https://purplesec.us/resources/cyber-security-statistics/
34. -Small Business Administration (SBA): https://www.sba.gov/blog/protect-your-small- business-cybersecurity-attacks
35. -Small Business Administration (SBA): https://www.sba.gov/blog/protect-your-small-business-cybersecurity-attacks
36. -Świątkowska, Joanna. 2020. *Tackling Cybercrime to Unleash Developing Countries' Digital Potential*. Background Paper 33. Pathways for Prosperity

Commission, January 2020, accessed October 2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/ files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf

37. *-Świątkowska, Joanna. 2020. Tackling Cybercrime to Unleash Developing Countries' Digital Potential. Background Paper*
38. *-United Nations Office on Drugs and Crime annual report (2020) OF THE UNODC-WCO CONTAINER CONTROL*
39. *-Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication (AJIC),20, 113-132. https://doi.org/10.23962/10539/23573.*
40. *-WBG (World Bank Group). 2021a. Consumer Risks in Fintech: New Manifestations of ConsumerRisks and Emerging Regulatory Approaches. Policy Research Paper. World Bank Group, accessed December* 2023. https://documents1.worldbank.org/curated/en/5157716219 21739154/pdf/Consumer-Risks-in-FinTech-New- Manifestations-ofConsumer-Risks-and-Emerging-RegulatoryApproaches-Policy-Research-Paper.pdf
41. *-yadav .H, Shashant.G(2014), Cyber Attacks: An impact on Economy to an organization, International Journal of Information & Computation Technology. ISSN 0974- 2239 Volume 4, Number 9 (2014), p. 937 © International*
42. *-yadav .H, Shashant.G(2014), Cyber Attacks: An impact on Economy to an organization, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 9 (2014), p. 937 © International Research Publications House http://www. irphouse.com.*
43. *-yadav .H, Shashant.G(2014), OP.CIT.P:938.*
44. *-Zambia: Zambia Computer Incident Response Team (ZM- CIRT): https://www.cirt.zm/about.phpAfrican Cyberthreat Assessment Report Cyberthreat Trends (2023), Op.cit. p:15.*