Management Analytics and Social Insights

www.masi.reapress.com

Manag. Anal. Soc. Insights. Vol. 1, No. 2 (2024) 260–271.

Paper Type: Original Article

The Outlook of Cyber Security in African Businesses: Issues and Way-Out

Adedayo Ayomide Adeniran[1,*], Adetayo Olaniyi Adeniran[2], Olayemi Babawole Familusi[3], Oluwafemi Adedayo[4]

[1]Department of Geography and Planning, University of Ibadan, Nigeria; dayoddone2@gmail.com.
[2]Department of Transport Planning and Logistics, University of Ilesa, Nigeria; adetayo_adeniran@unilesa.edu.ng
[3] Department of Research and Public Policy, University of Ibadan, Nigeria, Nigeria; yemi80s@hotmail.com.
[4] Project Strategy and Business Management, University of Waterlo, Canada; ooadeday@uwaterloo.ca.

Citation:

Received: 15 April 2024 *Revised: 16 June 2024* *Accepted: 16 August 2024*	Adeniran, A. A,Adeniran, A. O, &Familusi, O. B. &Adedayo, O. (2024). The outlook of cyber security in African businesses: issues and way-out. *Management analytics and social insights, 1* (2), 260-271.

Abstract

This study explores the outlook of cyber security in African businesses. Issues and ways out in a changing environment were highlighted. Cybersecurity measures need to be strengthened because cybercrime is estimated to cost the African continent about $10 billion annually. With just 20,000 certified cyber security specialists in Africa compared to over 1.3 million in the US, the study emphasizes African firms' low awareness and understanding. Based on empirical research and worldwide cyber security indexes, the paper analyzes the main obstacles to successful cyber security measures, such as resource limitations, knowledge gaps, and insufficient legislative frameworks. It also delved into real-world implementation problems, including disjointed infrastructure and linguistic hurdles. The report suggests cyber security awareness, utilizing technology, and encouraging cooperation through public-private partnerships to minimize these issues. The study further highlights the application of Artificial Intelligence (AI), which is revolutionizing cyber security defenses and promoting the adoption of cyber security in Africa. African businesses can negotiate the complicated cyber security landscape, resulting in a more reliable and secure digital environment and enormous potential for economic growth.

Keywords: Cyber security, African businesses, Business, Artificial intelligence.

1 | Introduction

Cybercrime is a prominent and recurring issue worth studying in academia. Cybercrime, which can be called computer crime, is a well-known and recurring issue in recent times. O'Brien[1]revealed that "cybercrimes existed since the invention of the Abacus when people use the device for the wrong purpose". Onodugo and Itodo[2]noted that "cybercrime has been defined in different dimensions and directions by various scholars, and there is no generally acceptable definition of cybercrime; rather, the definition is contextual".

Corresponding Author: dayoddone2@gmail.com

Regretfully, as innovation and technology grow quickly, cybercrime has sadly followed suit, permeating every aspect of our lives. Defense, medical, transportation, aviation, banking, logistics, governance, and others are receiving more attention due to an increasing number of cases on cyber security, which exposes those sectors to loss of private data at the hands of cybercriminals. Indeed, public and private organizations worldwide now work jointly to consider cyber security of utmost importance[3]. The World EconomicForum predicts that by 2025, cybercrime will cost the world economy $10.5 trillion yearly[3],[4].

Sustainable development is the nature of development that meets the needs of the present without compromising the ability of future generations to meet their own needs [4]. Cybercrime is an obstacle to achieving the Sustainable Development Goals (SDGs), most especially Goal 16, which relates to money laundering and combating the financing of terrorism, corruption, and arms trafficking[4]. Cybercrime threatens a nation's social, technological, environmental, educational, political, security, and economic development.

In the cyber security policy review, Donovan et al. [5] call for a plan to raise awareness and include a sufficiently knowledgeable and skilled workforce to be cyber-ready in response to any threats that may arise. Talents in cyber security are desperately needed to protect national and international organizations' infrastructure from increasing cyber threats [3]. Due to varying factors, such as increasing internet penetration and mobile phone usage, Africa's corporate sector is currently experiencing a rapid digital revolution [6]. This offers a substantial employment generation opportunity, economic expansion, and better service accessibility.

The African Union's Digital Transformation Strategy for Africa provides a framework for doing this, focusing on innovation, skills development, and digital infrastructure [4]. Digital technologies, e-commerce, and mobile money are revolutionizing key industries, including banking, agriculture, and education [4]. To guarantee equitable growth, however, issues like cost, lack of digital knowledge, and unequal infrastructure access must be resolved [5]. There are two sides to the expanding digital landscape, which are caused by rising internet usage and pervasive technical innovation. It encourages social advancement and economic expansion. It also brings up new cybersecurity risks. Businesses are particularly susceptible to cyber-attacks as they depend increasingly on digital infrastructure and networked technologies [7].

Effective cyber security measures are essential to safeguard sensitive data, guarantee business continuity, and uphold customer trust in the modern digital age. Likewise, to help African businesses navigate this changing digital landscape, this study explores the issues and ways out of cyber security in African businesses. It provides solutions for creating a more secure digital future.

2|Literature Review

2.1|Cybercrime, Cyber Security and Criminology

Abdulkarim [7] defined cybercrime as the unauthorized use, access, modification and destruction of hardware, software, data, or network resources; unauthorized release of information; unauthorized copying of software; denying an end-user access to his/her hardware, software, data or network resources; using or conspiring to use computer resources to obtain information or tangible property illegally. Adesina[8] further defined cybercrimes as crimes committed using the internet through the medium of networked computers, telephones, and other Information and Communications Technology (ICT) equipment. It encourages all illegal activities perpetrated by one or more people referred to as scammers, hackers, internet fraudsters.

Cybercrimes encompass a range of illegal activities that compromise the confidentiality, integrity, and availability of data and computer systems. These activities include unauthorized access to computer systems, illegal data interception, data interference (destroying, altering, deteriorating, or suppressing data), system interference (obstructing the proper operation of a computer or other device), fraud, identity theft, and forgery.

Additional categories of cybercrimes are content-related and include the creation, offering, distribution, acquisition, and possession of online content that is illegal by national laws. Examples of such content include online child sexual abuse, material supporting terrorist acts, extremist content (material encouraging hate, violence, or acts of terrorism), and cyberbullying (using technology to engage in offensive, menacing, or harassing behavior). To ensure internet safety and security, cybercrime is a component of a larger cybersecurity strategy [6].

Ribadu[10]identified the nature of cybercrime, which are Computer and internet fraud, mail scams, credit card fraud, Bank Verification Number (BVN) scams, Automated Teller Machine (ATM) scams, bankruptcy fraud, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, copycat website, cyber plagiarism, kickbacks, counterfeiting, laundering, embezzlement, as well as economic and copyright/trade secret theft, websites cloning, financial fraud, identity theft, cyber-pornography, cyber-harassment, drug trafficking deals, fraudulent electronic mails, cyber laundering and virus/worms/trojans.

The term cyber security refers to the set of instruments, regulations, rules, risk management strategies, activities, training, best practices, guarantees, and technology that may be employed to safeguard an organization and the environment, as well as the assets of its users.

As a result of cybercrimes, organizational, legal, policy, and technological components are all included in cyber security governance measures[9]. Thousands of cyber-attacks are being made worldwide on internet users. Cyber-attacks are becoming incredibly common and costly for economies, enterprises, organizations, and other infrastructure-related institutions, in addition to individual individuals. 91% of the more than 430 million new malware samples that symantec[10] found in 2016 resulted from phishing attacks.

People are often acknowledged to be the weakest link in cyber security. The prevailing belief among most system security firms is that the human element represents the weakest link in cyber security. In actuality, people are becoming the primary target of cybercriminals rather than equipment. Internet users increased from 2 billion in 2015 to 3.8 billion in 2017 [11]. Cyber Security Ventures [12] projects that by 2022, there will be 6 billion internet users worldwide, and by 2030, there will be over 7.5 billion. With so many more people using the internet, there is cause for worry over the vulnerabilities and new risks that those with ideological motivations may use to damage people and further their political and social objectives.

Nonetheless, a dearth of empirical studies constrains our understanding of the variables influencing cyber-attackers' behavior. According to Sandeep [13], the relationship between humans and computers is characterized by a complex interplay of social, psychological, technological, and environmental elements that operate along an organizational internality and externality continuum rather than a straightforward process. Many theories have developed on the subject of criminology to explain why crimes happen, why some people act in deviant ways while others do not, and how to anticipate the behaviors and practices of future crimes[14]. Some selected theories on cybercrime will be explored in the next section.

3|Theoretical Review

3.1|Routine Activity Theory

This hypothesis, which Jaishankar [15] developed, contends that motivated offenders, appropriate targets, and the lack of qualified guardians are the three main factors that determine the likelihood of victimization, with most victims exhibiting recurrent and predictable behavio. The target is something that the motivated offender values (credit card information, for example), the competent guardian is someone or something that prevents the offender from obtaining the target, and the motivated offender is someone who is prepared to commit a crime if the proper chance arises.

3.2 | Aker's Social Learning Theory

This theory covers four main areas: imitation, definitions, differential reinforcement, and differential association. It is specifically used to explain a wide range of criminal behaviors. The hypothesis supports the notion that those who associate with criminals (deviant peers) get the motivation and abilities to commit crimes. Research suggests that this approach might assist in clarifying the problems associated with software piracy and cybercrime. people who hang out with peers who pirate software pick up on the illegal behavior and eventually adopt it themselves.

The social learning hypothesis explains software piracy and other cybercrimes because it may account for the justifications, abilities, and behaviors that cybercriminals reinforce through their interactions with and observing others[18]. Understanding the motivations of delinquent peers and their roles in the context of various cybercrimes is, thus, the central notion of this theory.

3.3 | Situational Crime Prevention Theory

By altering the environment to raise the risk to the offender while lowering the possible benefit of committing the crime, the situational crime prevention theory aims to prevent certain types of crimes[17]. Unlike other criminology theories, this theory does not speculate why the criminal committed the crime. Instead, it usually focuses more on lowering the opportunity for crime. This idea is implemented by encrypting sensitive data, putting access control measures in place, protecting off-site data, running background checks on personnel, and prohibiting illegal computer installations. Applying Situational Crime Prevention Theory decreases cyberstalking and other online victimization crimes.

A combination of ideas is needed to compensate for the gaps in our understanding of criminal behavior, as no one explanation can fully explain it. However, whereas criminological theory in the physical world has a long history, marked by various contributions, paradigm changes, and progress, studies that explain digital and electronic crime, as well as the success of information security, remain comparatively underdeveloped.

Cybercrime is rising throughout Africa, threatening nations' economic and social development efforts. While vicious cybercriminals like hackers utilize cyber vulnerabilities to enter and damage vital systems for financial gain or to hold people hostage, cybercrime, cyber espionage, cyber terrorism, and cyber warfare are all emerging forms of cybercrime that constitute a threat to African countries[16]. Many have attempted to hide this under various pretenses, such as ordinary system updates or glitches. Only when they begin to involve the legal system will cybercriminals come forward and the public stakeholders be made aware of the enterprise's breach of truth?

This is not unique to African Enterprise; in May 2021, for example, there was a ransomware assault in which an American oil corporation was kidnapped and forced to pay a hefty ransom. It was initially referred to as a "System Outage." Additionally, the the following offenses as cybercrimes as of a year ago:

I. Willful access to any computer system, in whole or in part, without authorization.

II. The deliberate, illegal eavesdropping of private computer data communications.

III. Among other things, purposeful destruction, erasure, degradation, change, or suppression of computer data without authorization.

IV. Willful and substantial interference with a computer system's ability to operate by the entry, transmission, destruction, deletion, deterioration, alteration, or suppression of computer data.

V. The creation, marketing, acquisition for use, importation, or distribution of equipment intended to carry out any of the aforementioned offenses or [i.e., obtaining] passwords or other such information needed to gain access to computer systems to carry out any of the aforementioned offenses.

4 | Cyber Security in Africa

Global cybercrime has increased unprecedentedly in recent years[20],[17]. Africa has not been excluded either, as reports indicate that it has one of the highest rates of cybercrime, which impacts the continent's strategic, economic, and social development[18]. According to reports, expected expenses have increased to $550 million for Nigeria, $175 million for Kenya, and $85 million for Tanzania, among other things[18].

The lack of knowledge among the African people about the hazards involved in utilizing cyberspace is one of the elements contributing to a permissive environment for cybercrime[18]. Furthermore, the security posture of African nations is strongly impacted by the degree of development of their business digital infrastructure. Furthermore, as was previously discussed, cybercriminals take advantage of the general public's extremely lax security practices[19] and encourage corporate and governmental policymakers to launch awareness campaigns[18]because there is compelling evidence that these efforts can effectively reduce the success rate of cybercrime [18].

More particularly, according to some white papers, spending on security awareness and training may alter user behavior and cut hazards associated with cyberspace by 45% to 70% [19]. Raising awareness of cyber security issues is a critical first step in the battle against cybercrime in Africa. Because of this, it is imperative that any African business planning to carry out initiatives in this domain have a comprehensive grasp of the degree of cyber security awareness throughout its workforce and nation.

In this direction, attempts have been made to assess the state of cyber security awareness (knowledge of cyber threats and risk, cyber hygiene, and suitable response options) in Africa [20]. Overall, the results indicate that a lack of awareness campaigns about cyber security and Internet safety leads to a lax corporate environment regarding information security and has harmed public trust on multiple occasions [20], [21]. This report analyzes the potential and problems facing business cyber security in Africa today.

4.1 | Cyber Security Awareness in African Businesses

To identify vulnerabilities and create mitigation methods that work, it is imperative to assess cyber security awareness in African businesses while also knowing the present status of cyber security awareness among African organizations. Many African businesses, especially smaller ones, may be underestimating the cyber hazards they face while being aware of the consequences of cybercrime. Studies indicate a deficiency in knowledge concerning the many types of cyber-attacks, including ransomware assaults, malware invasions, and phishing schemes[20]. This lack of knowledge frequently results in insufficient funding for cyber security and a delusion of security, leaving them vulnerable to security breaches. Determining vulnerabilities and creating efficient mitigation methods need an understanding of the present cyber security knowledge among African organizations. Different awareness levels in Africa are explored in detail below.

Internal vs. external threats

Some businesses may exclusively focus on external dangers such as malware or hackers. On the other hand, insider threats from irate co-workers or unintentional human mistakes might be just as harmful[25]. Evaluating their awareness of internal vulnerabilities and implementing security procedures to fix them is essential.

Customer data and privacy concerns

With the development of web3/crypto exchanges, e-commerce, online transactions, and financial technology. African firms are collecting and storing customer data at an increasing rate. Understanding data privacy laws like the General Data Protection Regulation (GDPR) or comparable local laws is essential to being aware of cyber security. Nonetheless, research indicates that many African businesses may not be as knowledgeable about data privacy laws and compliance procedures as they should be [6], [18].

Limited resources and expertise

In Africa, resource limitations are a major element influencing cyber security awareness. Many companies, especially small and medium-sized organizations (SMEs), lack the specialized funding and staff for thorough cyber security awareness campaigns and training programs [25]. This frequently results in a dependence on free internet resources or rudimentary internal training, which might not be adequate to handle the constantly changing dangerous landscape.

Language and cultural barriers

Materials on cyber security awareness are frequently written in Western languages, which presents a challenge for companies in multilingual areas. Understanding and implementing best practices may be hampered by a lack of translated information or culturally appropriate training opportunities[21]. This emphasizes the necessity of locally relevant awareness campaigns tailored to a certain location.

Shifting threat landscape

Both the frequency and sophistication of cyber-attacks are ever-changing. It could be difficult for many African businesses to stay up to speed with the newest risks and appropriately modify their cyber security procedures[3], [4]. They may be vulnerable to new threats if unaware of new attack vectors, such as supply chain weaknesses or social engineering techniques.

Perceptions and misconceptions

Erroneous beliefs regarding cyber security may also impede consciousness. Some companies may think they are not a target for cyber-attacks because of their size or industry. Some people could consider cyber security the IT department's domain exclusively, undervaluing staff members' role in preserving a safe workplace [28]. It is important to dispel these myths with focused awareness initiatives.

The role of regulatory frameworks

Raising awareness may be greatly aided by the creation and use of strong cyber security policies and laws [19]. Stronger cyber hygiene procedures can be encouraged by educating companies about their legal responsibilities and the possible repercussions of non-compliance. An intricate picture emerges when evaluating African firms' overall cyber security knowledge. While some businesses actively try to strengthen their posture, many encounter difficulties because of a lack of resources, communication difficulties, and a constantly changing threat landscape. A multifaceted strategy, including culturally appropriate training materials, focused awareness efforts, and the creation of extensive national cyber security frameworks, is needed to address these problems.

4 | Empirical Analysis

4.1 | Spatial Analysis of Cyber Security in African Businesses

The CyberSecurity Exposure Index (CEI) identifies the nations least and most impacted by cybercrime. It is a poll conducted regularly across 108 countries on all continents (Europe, America, Asia-Pacific, and Africa). Africa is the continent most vulnerable to cyber security attacks, whilst Europe is the least vulnerable [33]. The nations with the least exposure to cybercrime include Finland, Denmark, Luxembourg, Australia, and Estonia. In contrast, all African nations are extremely vulnerable to cybercrime, as no single nation on the continent is listed among the nations with the lowest cyber security exposure worldwide.

The countries with the greatest cyber security risks include Afghanistan, Palestine, Ethiopia, Burma, and Venezuela. Ethiopia has Africa's greatest cyber security danger, followed by Tanzania, Zimbabwe, Algeria, and Cameroon. Namibia is the country in Africa with the least exposure to cyber security. This, as of late in 2024, is not implausible. A bank in Ethiopia lost $40 million due to a system glitch [22], [23]. Things are only worsening as Tanzanian commercial banks report an 84% rise in cybercrime in Q4 2023. And Nigeria is indeed not left out, as there is a 2024 revelation of diverted ₦40 billion ($29 million) unnoticed for almost 2 years [22], [23].

Mauritius leads the list of African nations most committed to cyber security, followed by South Africa, Egypt, Kenya, Nigeria, Tunisia, and Uganda. *Tables 1-3* presented statistical data on the countries most vulnerable to cybercrime on a regional and global scale and the ranking of African nations. It's important to remember that this ranking was published before Flutterwave, which, as of March 2024, was the most valuable startup in Africa. Patricia, another significant operation in Nigeria, lost $2 million to cybercriminals in Africa's rapidly developing fintech capital [24]. While Flutterwave, with a major operation in Nigeria, lost ₦19 billion (about $24 million) in February 2024 and another ₦11 billion ($7 million) security breach in May 2024 [22], [23]. According to *Table 3*, the United States is rated first in the world, followed by Saudi Arabia and the United Kingdom, which are placed second [25].

In addition, Mauritius came in first in Africa but 17th globally. Ghana came in second in Africa, as *Table 4* shows. Egypt came in second. Even though African enterprises are seeing enormous growth in innovation, technology, and market development, *Table 3* review by Larnyohdemonstrates how less informed the region's enterprises are of changes and security measures needed to safeguard themselves [25]. Many African nations spend too little on cyber security because of a lack of trained labor, high unemployment rates, inequality and poverty, and high crime rates [26]. Businesses usually lack the funds to invest in cyber security protection, even though many emerging nations view it as essential. This restricts their capacity to put policies in place to stop and lessen sophisticated cyber threats [27].

Table 1. The most exposed countries to cybercrime

Country	Rank	Exposure Score
Afghanistan	85	1.000
Myanmar	84	0.910
Ethiopia	83	0.866
Palestine	82	0.855
Venezuela	81	0.807
Libya	80	0.793
Bolivia	79	0.783
Nepal	78	0.762
Bangladesh	77	0.759
Source: Statista [33]		

Table 2. Cybercrime security exposure index ranking of African countries.

Country	Africa Rank	World Rank	Score
Mauritius	1	12	0,200
South Africa	2	34	0,414
Egypt	3	48	0,548
Kenya	4	48	0,548
Nigeria	5	58	0,614
Tunisia	6	58	0,614
Uganda	7	61	0,634
Namibia	8	65	0,679
Cameroon	9	69	0,707
Algeria	10	70	0,721
Zimbabwe	11	71	0,724
Tanzania	12	72	0,731
Ethiopia	13	83	0,910
Source: Statista [33]			

Country	Score	Rank

USA	100	1
UK	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Republic of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada	97.67	8
France	97.6	9
India	97.5	10

Table 3. Top 10 countries in the global

Table 4. Global cyber security index of top 10 countries in the world.

Country	Overall Score	Regional Rank
Mauritius	96.89	1
Tanzania	90.58	2
Ghana	86.69	3
Nigeria	84.76	4
Kenya	81.7	5
Benin	80.06	6
Rwanda	79.95	7
South Africa	78.46	8
Uganda	69.98	9
Zambia	68.88	10

5|Discussion

5.1|Issues Surrounding Cyber Security in African Businesses

The cyber security risks that African businesses must contend with are growing along with the continent's digital ecosystem. Despite the enormous potential for economic growth, several obstacles prevent the adoption of effective cybersecurity solutions. Key issues militating against effective cyber security measures in African businesses are:

Constraints in resources

For African firms, particularly SMEs, budgetary constraints and a shortage of qualified cyber security specialists pose serious obstacles. Many do not have the funds to invest in modern security technologies, qualified staff, or full cyber security strategies [30]. This frequently results in their dependence on antiquated technology and insufficient training, making them open to assault.

Low awareness and knowledge

Many African businesses, especially smaller ones, may be unaware of the cyber threats they face and may not have a basic understanding of cyber security best practices, as seen by the statistics above[20]. They are susceptible to possible breaches due to this information gap, making proactive risk management difficult and fostering a false feeling of security [33].

Insufficient regulatory frameworks

Although certain African nations actively create national cyber security policies, advancements may be hampered by a lack of strong legal frameworks and effective enforcement procedures. Businesses may have a poor cyber security posture because they are ignorant of their legal responsibilities or care little about the repercussions of non-compliance.

Legacy and fragmented infrastructure

A large number of African firms use antiquated or badly maintained IT infrastructure. This can include out-of-date software, unpatched systems, and careless password management procedures, leading to vulnerabilities that hackers can easily exploit. Resource constraints are made worse by the fact that upgrading and safeguarding this infrastructure sometimes calls for a large increase in expenditure.

Barriers related to language, culture, and audience literacy

Training materials and cyber security awareness are frequently created in Western languages, neglecting Africa's varied linguistic terrain. Understanding and implementing best practices may be hampered by a lack of translated information or culturally appropriate training opportunities[21]. Numerous patrons of this establishment, particularly public and governmental entities, may have rendered the acceptance of change less enticing to certain enterprises.

Changing threat landscape

Cyber-attacks are becoming more frequent and sophisticated daily. Companies may struggle to stay up to speed with the most recent security risks, update their procedures, and maintain vigilance against newly developing attack vectors such as supply chain vulnerabilities or social engineering[3],[4].

5.2|Way-Out on Cyber Security in African Businesses

While it's important to recognize the issues facing African businesses in cybersecurity, there are also certainties for development and innovation. Businesses may access a more secure digital environment and enjoy several advantages by removing these issues, and a small number of businesses around the continent are already seizing the certainties.

Cost of cyber-attacks on African businesses: It was estimated in Serianu's[27] report that a whooping sum of $10 billion was incurred in 2022 on cybercrime costs in Africa. In addition to the huge cost incurred, there are 20,000 certified cybersecurity professionals[27], which seems inadequate for the United States, which has over 1.3 million certified cybersecurity professionals[28].

This implies that if educational institutions and government agencies embark on processes to train and graduate cyber security experts, the huge cost incurred on cybercrime cost will be minimal.

Based on the literature, the following are the advantages of having improved cyber security:

I. Improved reputation and consumer trust: vigorous cyber security procedures help to safeguard client information, which fosters loyalty and trust. This enhances a significant competitive edge in the online market.

II. Business financial stability: effective cyber security measures help prevent expensive data breaches and cyber-attacks. This reduces the likelihood of financial loss.

III. Enhanced operational effectiveness: employee knowledge of cyber security and streamlined security procedures can result in fewer interruptions and higher operational effectiveness.

6 | Conclusion and Recommendations

Evidence has shown in this study that cyber security is directly or indirectly eating up the benefits of many technologically driven businesses in African countries. African enterprises and individuals are losing money due to high cyber fraud. The issues and way-outs were explored in this study. Navigating the complex cyber security landscape in Africa requires a multi-pronged approach. Addressing the challenges of resource limitations, knowledge gaps, and outdated infrastructure is also crucial. Collaboration, capacity building, and leveraging affordable technologies like cloud security can empower African enterprises. It is essential to note that cyber security cuts across all sectors that uphold the economy.

The policy will not stop cyber criminals, and introducing cyber security charges will not stop cybercriminals, especially in the face of a serious economic crisis in many African countries with no clear funding plan [29]. Hence, technology development, improving education curriculum, collaboration, and personnel training are vital to address cyber security. An exciting new frontier lies in utilizing Artificial Intelligence (AI) for cyber security. Examples of AI applications to address cyber security challenges and emerging threats are:

I. Automated threat detection and response: this is an AI-powered security solution that can analyze vast amounts of data to identify suspicious activity in real-time, enabling faster and more effective responses to cyber-attacks;

II. Phishing and social engineering protection: the use of AI to detect and filter out malicious emails and social media messages, mitigating the risk of falling victim to phishing attempts.

III. Vulnerability management: the use of AI to automate vulnerability scanning and prioritization, allowing businesses to focus resources on patching the most critical weaknesses.

While large-scale businesses may be able to invest in and maintain AI-powered solutions, a culture of in-house expertise is essential. Medium-scale and large-scale businesses can explore training programs to develop cybersecurity specialists and reduce over-reliance on external resources.

Author Contributions

Adedayo Ayomide Adeniran: Led the study design, conceptualization, and manuscript preparation.

Adetayo Olaniyi Adeniran: Conducted data analysis and contributed to the discussion on legislative frameworks and challenges.

Olayemi Babawole Familusi: Focused on practical implementation issues and provided real-world case studies.

Oluwafemi Adedayo: Researched the role of AI in cyber security and contributed to drafting solutions and recommendations.

All authors approved the final manuscript.

Funding

Not applicable.

Data Availability

Not applicable.

References

[1] O'Brien, J. A. (1997). *Introduction to information systems*. Richsrd DIrwin.https://www.amazon.com/Introduction-Information-Systems-Text-Only/dp/B004HOTCHC

[2] Onodugo, I. C., & Itodo, S. M. (2016). Cyber crime and Nigerian business environment. *National journal of advanced research*, *2*(2), 28–38. https://thestudiesjournal.com/assets/archives/2016/vol2issue2/2-2-24-992.pdf

[3] World Economic Forum. (2023). *Why we need global rules to crack down on cybercrime*. https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

[4] World Economic Forum. (2023). *Global risks report 2023*. https://www.weforum.org/publications/global-risks-report-2023/

[5] Donovan, B. C. S., Daniel, M., & Scott, T. (2016). *Strengthening the federal cybersecurity workforce*. Obama White House. https://obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce

[6] Adeniran, A. O., Oyeniran, G. T., Adeniran, A. A., & Mosunmola, M. J. (2024). Digitization in logistics and its effect on sustainability in Nigeria. *Discovery*, *60*(334), 1–11. DOI:10.54905/disssi.v60i334.e15d1420

[7] Adeniran, A. O., Sidiq, O. B., Oyeniran, G. T., & Adeniran, A. A. (2024). Sustainability impact of digital transformation in e-commerce logistics. *International journal of innovation in marketing elements*, *4*(1). DOI:10.59615/ijime.4.1.1

[8] Abdulkarim, U. S. (2012). *A study of cybercrime in kano metropolis*.

[9] Stella Adesina, O., & Lecturer, S. (2017). Cybercrime and poverty in Nigeria. *Canadian social science*, *13*(4), 19–29. www.cscanada.netwww.cscanada.org

[10] Ribadu, N. (2007). *Cybercrime and commercial fraud: a Nigerian perspective*.Proceedings of the fortieth annual session of UNCITRAL on Modern Law for Global Commerce. UNCITRAL.

[11] Orji, U. J. (2012). *Cybersecurity law and regulation*. Wolf Legal Publishers.https://www.researchgate.net/publication/320624755_Cybersecurity_Law_and_Regulation

[12] Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. *2016 14th annual conference on privacy, security and trust, (PST)* (pp. 223–228). IEEE. DOI: 10.1109/PST.2016.7906931

[13] Reid, G. (2018). How many internet users will the world have in 2022, and in 2030? *Cybersecurity ventures online magazine*. https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

[14] Mittal, S. (2015). Understanding the human dimension of cyber security. *Indian journal of criminology and criminalistics*, *34*(1), 141–152. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975924

[15] Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International journal of cyber criminology*, *1*(2), 7–9. https://core.ac.uk/reader/30447720

[16] Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: examining the importance of a full social learning model in the virtual world. *Journal of crime and justice*, *33*(2), 31–61. DOI:10.1080/0735648X.2010.9721287

[17] Trend Micro. (2017). *Is there a budding West African underground market?* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/west-african-underground

[18] Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: extending the generality of routine activity theory. *Journal of research in crime and delinquency*, *47*(3), 267–296. DOI:10.1177/0022427810365903

[19] Oladipo, T. (2015). *Cyber-crime is Africa's' next big threat', experts warn*. Retrieved July. https://www.bbc.com/news/world-africa-34830724

[20] Peter, A. S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International journal of critical infrastructure protection*, *17*, 49–59. DOI:10.1016/j.ijcip.2017.03.002

[21] Serianu. (2016). *Africa cyber security report 2016*. https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[22] Symantec. (2016). *Cyber crime and cyber security trends in Africa*. https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

[23] Technologies, W. S. (2016). *African union cybersecurity profile: seeking a common continental policy*. https://usafcg.com/african-union-cybersecurity-profile-seeking-a-common-continental-policy/

[24] PwC. (2022). *2022 global digital trust insights*. https://riskproducts.pwc.com/resources/2022-global-digital-trust-insights/

[25] UNCTAD. (2020). *E-commerce and the digital economy in Africa: opportunities and challenges*. https://unctad.org/topic/ecommerce-and-digital-economy/digital-economy-report

[26] Fortinet. (2022). *Global threat landscape report*. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf

[27] TechCabal. (2024). *Exclusive: first bank employee on the run after diverting ₦40 billion; bank begins recovery*. https://techcabal.com/2024/05/31/first-bank-employee-on-the-run-after-40bn-fraud/

[28] TechCabal. (2024). *Exclusive: flutterwave loses ₦11 billion in security breach*. https://techcabal.com/2024/05/16/exclusive-flutterwave-loses-₦11-billion-in-security-breach/

[29] TechCabal. (2023). *Exclusive: Patricia's newly reported hack happened in 2022 and cost the company $2 million*. https://techcabal.com/2023/05/27/patricia-loses-2m-to-hack/

[30] Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. *International journal of research in business and social science (2147- 4478)*, *11*(4), 384–396. DOI:10.20525/ijrbs.v11i4.1714

[31] Mcanyana, W., & Brindley, C. (2020). *Insight into the cyber threat landscape in South Africa*. https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa

[32] Serianu. (2023). *Reimagining the African cybersecurity landscape*. https://www.serianu.com/downloads/KenyaCyberSecurityReport2023.pdf

[33] Statista. (2023). *Size of cyber security workforce worldwide in 2023, by country*. https://www.statista.com/statistics/1172449/worldwide-cyber security-workforce

[34] KPMG Nigeria. (2024). *Wale Ajayi. central bank issues guidance on the collection and remittance of the national cybersecurity levy*. https://kpmg.com/ng/en/home/insights/2024/05/central-bank-issues-guidance-on-the-collection-and-remittance-of-the-national-cybersecurity-levy-by-financial-institutions.html