From Policy to Practice: Evaluation of Telecom Cybersecurity Regulation and Capacity in Southern Africa.

Njodzi Ranganai
Department of Information and Marketing Science,
Midlands State University,
Gweru, Zimbabwe,
ranganai1981@gmail.com,
https://orcid.org/0000-0003-0451-1417

Mercy Nyasha Magoso
Department of Mathematics and Computer Sciences, Great Zimbabwe University,
Masvingo, Zimbabwe.
mmagoso@gzu.ac.zw
https://orcid.org/0009-0007-9461-5098

Clainos Chidoko
Department of Economics and Finance, Great Zimbabwe University, Masvingo, Zimbabwe
cchidoko@gzu.ac.zw
https://orcid.org/0000-0003-4530-7500

Paul Sambo
Department of Mathematics and Computer Sciences, Great Zimbabwe University,
Masvingo, Zimbabwe.
pasambo@gzu.ac.zw
https://orcid.org/0000-0001-8299-152X

Zvishamiso Mushamainza
Department of Mathematics and Computer Sciences, Great Zimbabwe University,
Masvingo, Zimbabwe.
mmushamainza@gzu.ac.zw
https://orcid.org/0009-0004-6490-0339

Lemias Zivanai,
Department of Information and Marketing Science
Midlands State University, Gweru, Zimbabwe,
zivanail@staff.msu.ac.zw
https://orcid.org/0000-0001-9145-3272

Abstract- **The authors inquired on the effectiveness of cybersecurity controls and regulations within the telecommunications industry in Southern Africa and expounded the strengths and weaknesses of the effective governance frameworks. Complex cyber threats are much targeted to digital technology infrastructure and resilience is important to provide economic stability, consumer protection as well as national security. The investigation used a mixed-method design that includes the surveys of telecom operators, policy documents study, and interviews with regulators and industry actors, the research also determines some crucial tendencies. The findings of the research show the inconsistency of policy implementation in a country, disordered compliance with regulations by telecom operator and lack of enforcement frameworks on a state level. Moreover, the absence of cross-border cooperation, resource insufficiency, and the dissimilarity of the institution capabilities prevent the mutuality of cybersecurity activities. The absence of user consciousness that persists also reduces the strength of resilience as the users are still under the threat of phishing, mobile money attacks and SIM-swap fraud. The positive advances in this study also include the emergence of national Computer emergency response teams (CERT), the adoption and congruency of policies with global standards and the increasing political intent to prevent the cyber threat. To sum up, it is important to note that despite the significant improvement, the telecom industry in the region is at the lowest level of cybersecurity. The paper takes into account standardization of cybersecurity at regional level, increased regulatory controls, capacity-building and sensitization efforts through skills and awareness gimmicks, and regional integration to produce a healthier, more sensitive and secure telecom environment in Southern Africa.**

Keywords: Cybersecurity, Telecommunications, Policy Effectiveness, Southern Africa, Data Protection

I. INTRODUCTION

The telecommunication sphere is also the epicenter of information flow and socio-economic revolution in the modern digital world of Southern Africa. With the mobile networking, internet break- through, and online financial service as the industry experiences a swift growth, it experiences an immeasurable increase in cybersecurity threats [1]. Telecom infrastructure cyberattacks undermine considerably service reliability, customer information, as well as vulnerabilities on the national security [2]. The importance of tough cybersecurity governance measures in the industry cannot be overstated, having been complementary to the digital transformation and regional cooperation. The past school of thoughts has emphasized the achievements and the obstacles in African cybersecurity management. Institutional capacity gaps, or in other words, the lack of technical expertise, and inadequate consciousness were also mentioned as obstacles to the effectiveness of policies and their implementation [3]. Furthermore, observed user- awareness and industry compliance as the areas of weakness in cybersecurity sustenance [4]. However, a limited power of investigations has been performed to consolidate the use of policy to the telecommunication industry of Southern Africa. This is a grey area created by this gulf when it comes to understanding whether the recent regulations have placed telecom operators in a position to stage against the emerging cyber security threats.

A. Problem Statement

The formulated cybersecurity plans and structures by Southern African countries, is not implemented into reality in the telecommunications sector. The regulatory implementation processes of telecom operators are uneven, ineffective in checking compliance, and invest in human and technical capacity. Further, weak region-wide consistent enforcement compounds the weak areas which leave major telecom gadgets vulnerable to increased sophisticated cyber assaults [5]. This research fill the gap by examining the efficiency of latest cybersecurity models or systems and the capability of telecommunications operators to implement them, thereby resolving policy to practice in an industry, spawning regional cyber resiliency.

B. Objectives of the Study

This program will help to assess the performance of current policies on cybersecurity in the telecommunications sector in five South African countries, South Africa, Zimbabwe, Botswana, Zambia, and Namibia, in terms of the compliance rate of licensed telecommunications operators and the regulators. Another critical gap and restriction identified and segmented in the paper includes regulatory inconsistency, capacity deficiency, and different user awareness level that is affecting telecom service providers, consumer groups, and regulators across the region. To evaluate technical and institutional capacity of telecom operators such as infrastructure, workforce competencies and training programs. Lastly, the study provides evidence-based suggestions on how to improve cybersecurity efforts, promote homogenization of policies, integration across regions and development of skills, which are confirmed with the help of numerous consultations with experts, policymakers, and telecom leaders.

C. Research Questions

- To what extent are already existing cybersecurity policies applicable in countering the vulnerabilities of the telecom sector in the Southern African region?
- Which are the most encountered issues of telecom operators and regulators when implementing these cyber security policies?
- What is the relationship between institutional and technical capability of telecom organizations and adoption of cybersecurity policies?
- What are the practical intervention strategies that can be used to close the policy and implementation gap within the telecom industry of Southern Africa?

D. Significance of the Study

These questions will add to the scholarly, as well as, policy discussion relating to cybersecurity governance because it goes beyond policy formulation to consider implementation and practice. The study marks the structural bottlenecks undermining resilience by concentrating on the telecom industry which lies at the core of the digital economy in Southern Africa. Telecom companies, regulators, and policymakers, and regional units including SADC will also be subject to the research findings that will contribute practically to the aligning structures, improving organizational capacities, and creating a culture of cybersecurity awareness and practice. Finally, the investigation aims at informing the creation of the sustainable and reliable telecommunications interdependencies that may prevent the exposure of the important gadgets and consumer information to the emerging cyber threats [6].

II. Literature Review

This question is validated by the set of theoretical approaches that may be applied to inform the investigation of the cybersecurity governance in Telecommunications industry. The concept of Risk Management Framework (RMF) suggests that the cyber security threats have to be identified, assessed, and mitigated using a systematic approach [7]. This is more so considering the Telecom industries, which are involved in carrying the huge amount of delicate information and critical infrastructural set-ups. The RMF has been linked with the Defense-in-Depth model ensuring that the protection of the multilayered administrative, technical, and physical controls is ensured whenever the failure takes place in one of the defense lines, others do not [8]. Furthermore, the Compliance and Regulatory Theory focuses on the dependency of the legal and the organizational practice. It also highlights the fact that the telecommunications companies should modify the operations, according to industry -specific and national regulations. Finally, Stakeholder Theory claims that telecom operators or regulators cannot achieve cybersecurity, but a diversity of actors, which encompasses government, service providers, civil society, and consumers among others, is required [9]. Together, these theories can provide a theoretical stand on a legitimate analysis of how effective the cybersecurity regulations, the pitfalls of the policy enactment, the influence of the publics, and the consciousness of the users are in the case in Southern Africa.

According to [10], good governance means that cybersecurity should be included in the corporate strategy and designing accountability mechanisms that may enhance the level of compliance and resilience. The policies and laws, most significant standards in the world are the General Data Protection Regulation' (GDPR) of the European Union and the standards of ISO/IEC 27001 because they clarify how straightforward and enforceable rules facilitate the adherence to the actions and additionally avert the instances of cyber threat. On the other hand, South Africa form of government is not equitable. They also remain in other nations with partial frameworks, which are undermined by the absence of resources and divided authority, as other countries implement gimmicks of national cybersecurity. The Telecommunications industry is emerging as an issue when it comes to cybersecurity laws. The Southern African encounters are not doing well in this respect. There are discrepancies in the implementation of the policy, whereas [11] suggests the low level of technical and financial capabilities as the forces that hinder compliance. The other notable downside is the awareness of the user in which focus on the lack of knowledge to decompensate such basic operations as password safety or phishing prevention and reduce the overall resilience [12]. The case study evidence is two-sided to be more exact, Cybercrimes Act in South Africa has resulted in more cooperation and reporting practices, but the first bottleneck is still the issue of enforcement and capacity on the regional scope [13].

Regulatory measures have also been gathered separately in the literature. The prescriptive strategies can be used to fuel the compliance baseline, but they can mainly be criticized due to the lack of innovation compared to the adaptive strategies, which makes them more customized at the cost of inconsistency [14]. Through such collaborations, the information flow is activated and regulation concentrates on the practice. Southern Africa is yet to catch up on multi-stakeholder involvement at the same time, which leaves the majority of the policies in bits and pieces and not even consistently treated [15]. The other theme that is reproduced in literature is the growing role of user education and awareness. Among the weakest elements in cybersecurity relationships, the human activity is always mentioned [16] Phishing attack is often committed against end users whose weak passwords or neglect of security patches are normally

exploited. The article by [17] take a step further in this respect stating that it is noticeable that recurring or repeated, targeted awareness campaigns are more noticeable than a campaign that is performed once. Nevertheless, Southern African studies show that the awareness programs lack sufficient funding, are not planned, and are rarely assessed based on their impact [18][19]. This is in a way that the potential effect of even the most mighty policy actions is compromised because the technical interventions will not be put into practice effectively unless they are put into practice by the users and are put under their control.

Fragmentation of regulations and overlapping of mandates to be major challenges, whereas [20] has financial constraints as the primary discouraged factors towards smaller telecom operators. The skills shortage remains a critical issue, [21] observe that the shortage of specialists in the cybersecurity field in the area has not been able to keep abreast of the demand. The policy implementation is also prohibited by organizational inertia because the staff and management are more inclined to resist change efforts and weak cultures which are present in the organization [22]. Even increased body of knowledge on the topic still has major gaps. There are few research studies that have focused fully on Southern Africa which mentions that actions in the Telecommunication Sector for example, data exchange across borders, are grey areas [23]. In Southern Africa the implementation constraints are not often examined thoroughly, rather often the cultural and behavioral criteria or aspects that hinder the compliance are not considered at all [24]. To address these gaps, the region- and sector specialized inquiries should be elaborated by the analyses of the translation of the policies into practice in the environment of the specific socio-economic situation in Southern Africa [25].

The literature also presents a lot of proposals to improve the available frameworks. In addition, the policies across the region should be similar to minimize the disparity [26], whereas [27] explain that the mutual stakeholder knowledge between the governments and telecommunication providers, as well as between the governments and civil society should be improved [28]. The studies stress the long-term and context-specific user-awareness campaigns, the local industries to follow and use the international standards, including ISO/IEC 27001 [29]. The adaptive governance criterion, which focus on customer-oriented approaches and feedback mechanisms is the best in policy to practice [30]. Overall, the literature reveals that the international frameworks indicate the importance of precise governance, enforceable measures and intense enforcement, but the Southern Africa has still resource shortages, chaotic policy and insufficient user awareness rates [31]. Such theoretical models as the RMF, Defense-in-Depth, Compliance Theory, and Stakeholder Theory can be of helpful insight in overcoming these shortcomings [32]. In general, resilience in the telecommunications industry in Southern Africa can be enhanced greatly due to the fine-tuning of governance structures, capacity development, and consumer involvement [33]. The research aims at supporting the literature in place by offering empirical, sector specific conceptualizations that follow the line of policy design to the implementation process in the telecom industry of Southern Africa [34].

III. METHODOLOGY

In this research, the mixed-method research design was selected, which combined both approaches of qualitative and quantitative methods to the actual challenge of cybersecurity governance in the telecommunications sector. The power of this design is in the fact that it will be able to determine different points of view that cannot be exhaustively put into perspective only with the help of a single methodological perspective. The quantitative model helped in measurement of awareness, compliance, and perception levels in a large group of 200 telecommunications stakeholders. On the contrary, qualitative approaches were used to explore lived experiences, shortcomings of policy implementation, and organizational change in greater detail. The triangulation of data increased the validity and reliability of the results, rendering them to be applicable and relevant in practical application to the telecommunications industry in Sub-Saharan African setting [35].

A. Research Design

The research design and methodology employed is qualitative as it includes a literature review to examine the topic. In this case, the research design and approach is qualitative because it involves literature review to discuss the issue. The explanatory sequential design was used where in the first stage of the study, a quantitative data collection method was performed using surveys then the qualitative inquiry given by means of interviews and case studies. This design can be used to make general measurements of cybersecurity awareness and perceptions, which is the basis of finding trends that can be further investigated using qualitative methods. Contextual interpretations and qualitative narratives are important in cybersecurity research the mixed-model approach supplements quantitative data with more substantial information on larger empirical patterns.

B. Population and sampling

The population of the research was telecommunications stakeholders in Southern Africa telecom service providers, cybersecurity professionals, regulatory agencies, and telecom end users. There were three target groups, including: Telecommunications Specialists, Cybersecurity Characteristics of large telecommunications companies in the region. The officials of National Regulatory Bodies that oversee the ICT and cybersecurity challenges. Telecom End Users (Consumers), the awareness, perceptions, and practices of whom are the basis of cybersecurity status in total. Stratified sampling strategy was implemented to facilitate total representation of the different segments of this population, which would increase the applicability of information gathered in the various groups. In the case of qualitative interviews and case studies, purposive sampling approach was used, which made it possible to select respondents with special knowledge, experience, or background in the area of cybersecurity policy implementation. This strategy provided an all-round picture of the opportunities and threats in the industry.

C. Data Collection

Questionnaire was placed online and a sample of 200 telecom consumers and telecom professionals in the Southern part of Africa were asked to fill out a structured questionnaire. The survey collected important information on cybersecurity awareness, policy effectiveness perceptions,

compliance practices, and risk to cyber threat. There were both closed-ended questions (to be analyzed statistically) and several open-ended ones (to provide qualitative information). Interviews and Case Studies, due to the constraints of group-based research, the researcher utilize qualitative data collected through interviews and case studies to gain a clear understanding of the matter at hand. Qualitative Data (Interviews and Case Studies), since group-based research presents limitations, the authors employ qualitative data (interviews and case studies) to develop a clear picture regarding the issue under discussion. The semi-structured interviews with 30 key stakeholders were carried out, comprising of 10 cybersecurity officers, 10 regulatory officials, and 10 selected end users. These interviews were very insightful as they gave insights into policy gaps, implementation issues and ways in which the policy can be made better. Also, two case studies of sampled telecom service providers were constructed to investigate actual practices of cybersecurity, its strategy, success and constraints. Interview and internal reports, and policy documents were used as data sources.

D. Integration of Results

Triangulation of quantitative and qualitative segments findings is the final analysis step. This allowed the research to determine whether statistical trends spell well with stakeholder accounts, and whether change, introduce new findings in connection to cybersecurity governance. As an example, the results of the survey of low levels of user consciousness were used in interview texts that did not provide sensitization gimmicks of the populace. Based on this combination, the enquiry offered a wider scope of the manner in which cybersecurity policies are developed between policy formulation and the implementation to Telecommunication industry in Southern Africa.

E. Ethical Considerations

Only ethical clearance was obtained to obtain data. The study participants signed informed consent, and their confidentiality and anonymity were guaranteed. All data were stored safely and were only used in academic purposes by audio-taping interviews conducted with the subjects only with their direct consent.

IV. RESULTS

The research findings are organized alongside the research goals, as they aimed to synthesize on the research topic regarding the effectiveness of cybersecurity policies, identify any gaps and limitations, and prescribe interventions to address to improve them and gauge the awareness of the Telecom stakeholders in Southern Africa. On the whole, the research observes that cybersecurity policies exist in telecom industry in Southern Africa and they are fairly effective on paper, yet, their implementation and enforcement are poorly managed. The main weaknesses are inadequate financing, a weakness in technical skills and country inconsistent regulations. The lack of uniformity in user awareness, and human skills training is more effective, outreach is limited. These results mean that better integration, standardized structures, and better awareness tactics are needed to implement better cybersecurity governance in Sub Saharan Africa. The current policies on cybersecurity have been tested and found not to be effective, as shown in 4.1. Out of the 200 survey results, the results showed a median perception of effectiveness of cybersecurity policy.

TABLE I. CYBERSECURITY POLICIES PERCEIVED EFFECTIVENESS

Rating (1-5)	Percentage of Respondents (N=200)
1-2 (Low effectiveness)	20% (40 respondents)
3 (Moderate)	50% (100 respondents)
4-5 (High effectiveness)	30% (60 respondents)

The mean score was 3.2 which showed moderately effective policies. This finding indicates that even with the existence of policies, there is a major disparity in the implementation process as indicated by the answers.

TABLE II. KEY INSIGHT ON GAPS AND LIMITATIONS IN IMPLEMENTATION AND ENFORCEMENT

Stakeholder Group	Key Insights
Cybersecurity Officers	Identified significant gaps in public awareness initiatives limiting effective policy implementation. Emphasized the need for ongoing training for employees and end users to enhance cybersecurity knowledge.
Regulatory Officials	Reported challenges in enforcing compliance due to inadequate resources and training within organizations. Mentioned difficulties in coordinating efforts across multiple stakeholders, leading to fragmented compliance efforts.
End Users	Expressed concerns that existing policies do not sufficiently address their specific cybersecurity needs. Highlighted a strong demand for educational resources, including workshops and materials on personal cybersecurity practices.

Case Study Findings	Best Practices	Challenges
Provider A	Implemented regular training sessions, resulting in improved compliance and a knowledgeable workforce.	Faced challenges due to outdated technology affecting compliance enforcement.
Provider B	Demonstrated successful implementation of cybersecurity measures through tailored training programs.	Experienced resistance to policy changes at management levels affecting strategy execution.

The 30 interviewed stakeholders reveal the most significant problems to appropriate cybersecurity implementation in the telecommunications industry. Cybersecurity officers noted that the awareness of the general population has significant gaps and that the continuous process of training the employees as well as the end users should be in view. According to the regulatory directors, there was a problem with the enforcement of compliance due to the inadequacy of the resources and the poor coordination of the stakeholders of these regulatory bodies. End users complained that the existing policies are not user friendly and they must be provided with educational materials. Two case studies of provider's revealed successful training programs but also a number of challenges such as the absence of modern technology in Provider A and the resistance to policy changes in Provider B which can be taken to indicate the complexity of the barriers to successful governance.

TABLE III. THE IMPLEMENTATION CHALLENGES THAT STAKEHOLDERS RAISED.

Barrier	Percent of Respondents (N=30) Identifying.
Lack of Funding	45% (13 respondents)
Inadequate Technical Expertise	30% (9 respondents)
Lack of readiness to change	25% (8 respondents).
Ambiguity in regulations	20% (6 respondents)

The qualitative results indicate that there are a number of important obstacles to effective cybersecurity governance amongst 30 respondents. The most urgent one is the insufficient funding, which 45% of participants reported, which suggests that insufficient funding is a problem that blocks the process of implementing effective cybersecurity. Also, the lack of technical expertise (30%) is an indicator of the insufficiency of skilled staff, and it may cause inappropriate policy implementation, and increased susceptibility to threats. Moreover, 25% of the respondents mentioned the absence of readiness to make a change, which also indicates the culture as the barrier to the implementation of new technologies and practices. Finally, 20 per cent found ambiguity in regulations, which renders compliance activities difficult and generates misunderstanding among the stakeholders. Collectively, these obstacles should highlight the importance of specific interventions to increase cybersecurity resiliency within the telecommunication industry.

TABLE IV. PERCEIVED EFFECTIVENESS OF EDUCATIONAL PROGRAMS.

Type of Program	Effectiveness Rating (1-5)	% of Respondents Rating 4-5 (N=30)
Online Training Modules	4	60% (18 respondents)
Face-to-face Workshops	4.5	70% (21 respondents)
Awareness Campaigns	3.5	50% (15 respondents)

According to the reaction of 30 leading telecom managers, on the table 3 there is the need to have regional collaboration to formulate coherent cybersecurity policies. Face-to-face workshops turned out to be the most effective, as they received a rating of 4.5 and 70% of the respondents perceived them to be useful. This implies that face-to-face interaction improves interaction and experience. Online training modules ranked a little behind at 4 which is deemed as effective by 60% which means that the online training modules are valuable but they might need additional features of interaction to increase engagement. On the contrary, the rating of awareness campaigns is 3.5, and its approval was 50 percent, which means that they understand the necessity of such training but, at the same time, it makes them less effective than other training methods. The obtained results underscore the necessity of implementing various and more entertaining educational programs to enhance cybersecurity awareness within the telecommunication industry to support the political agenda of inter-agency cooperation.

TABLE V. CYBERSECURITY POLICIES AWARENESS AMONG THE USERS

Level of awareness	Percentage of respondents (N=200)
Highly Aware	25% (50 respondents)
Moderately Aware	40% (80 respondents)
Slightly Aware	20% (40 respondents)
Not Aware	15% (30 respondents)

The results of the survey conducted on 200 users about the awareness of cybersecurity policy show that people understand the issue in a mixed manner. The highest level of awareness was only 25% with the majority, 40, being moderately aware of the current policies in use. In addition, 20% admitted that they were slightly aware of such policies and 15% said that they were not aware of such policies at all. Such statistics point to a critical lack of awareness, as a large percentage of the users is not aware enough of the most important cybersecurity measures. These results underline the necessity of more targeted outreach to various demographics to enhance the level of user awareness and interest in cybersecurity behavior.

V. DISCUSSION

The investigation revealed that there were significant gaps in cybersecurity awareness, the efficiency of the policies, and the way they are applied to the telecommunications industry of Southern Africa. The perceived difference in knowledge is very high since only 25% of the respondents were conversant or well-informed about the existence of cybersecurity policies. This result is promising as the previous studies have been developing the idea that human behavior is still a critical vulnerability factor in cybersecurity, and that specific awareness interventions are a priority to enhance cybersecurity practice [36]. Contingency modern policies were rated by their effectiveness modestly, and it was found to be 3.2, indicating the issues of policy implementation. This is consistent with research findings fact that regulatory misconception and lack of technical assistance tend to hamper execution of cybersecurity programs [37]. This research identified and described the key implementation obstacles, including, among others, poor finances and technical incompetence as observed in the literature that indicated that resource limitations are a significant barrier to cybersecurity improvements.

One of the areas of deep concerns turned out to be education. It was suggested that the face-to-face workshops be employed, since enquiry showed that interactive learning are more effective in creating awareness, retention and engagement. The conclusions show that the knowledge gaps and the compliance with the cybersecurity efforts would be addressed with inclusion and interactive programs of the human development adapted to the telecommunications industry. The regulatory frameworks and stricter relationship between the stakeholders are emphasized as important in the study. The policymakers should come up with sector-oriented directives to assist in reducing ambiguity, and conversely, the parties should be prompted to share their resources, analyze threats, and the best practices. The implementation of monitoring and reviewing the policies and educational programs are pertinent to the adjustment to the changing cybersecurity threats. To conclude, these findings suggest that the key factors of enhancement in cybersecurity resiliency in the telecom industry are strategic investment in regulatory clarity, education, infrastructure, and the coordination of various stakeholders. Response to such weaknesses is not only a deterrent to confidential information but also a source of information to more extensive regional cybersecurity tricks, increasing the relevance of user awareness, appropriate policy development, and backup facilities.

A. Implications

The research has numerous implications on cyber security in the telecommunication sector in Southern Africa. To begin with, the adherence to the cybersecurity policy can also be enhanced and will lead to the creation of a safer internet environment among the consumers. The latter plays a crucial role in the growth of digital economies within the region because clients will be more inclined towards the use of services, which will be more proximate to their safety [38]. Secondly, the identification of gaps and limitations will facilitate the stakeholders such as telecom providers and regulators to take certain measures that will address some aspects of vulnerabilities, and this will strengthen the resilience of the system. Better yet, the technical and institutional readiness of the telecom operators will not only empower individual companies, but also result in a more robust cybersecurity framework on a regional basis [39]. The evidence based suggestions could be utilized to construct a blueprint of harmonisation of policies among the countries in an attempt to fight cyber threats regionally. With time these may lead to an integrated telecommunications space, less fragmentation, and increased sharing of knowledge among the operators. The region will therefore become more attractive to foreign investment which will enhance growth and innovation in the economy. The findings can also be transferred to the future, where the policy-making can be motivated, carrying out additional reforms that will transform as the cybersecurity environment shifts at a rapid rate.

B. Limitations of the Study

The study has indicated significant gaps in the effectiveness of cybersecurity policies frameworks and deficit of user knowledge in the telecommunications industry in the Southern African region. The study, though, was limited by its cross-sectional nature and the fact that it only covered one industry only, the telecom industry and this could have serious implications on extrapolation of the research results to other industries within the region. Moreover, the lack of resources and the reliance on self-generated data could have affected the credibility of the findings, too.

VI. Conclusions and Recommendations

This investigation observed the level of user awareness**,** effectiveness of policies, and lack of implementation in the environment of telecommunications sector in Southern Africa. The results were characterized by the lack of awareness among people, relatively weak policies, and serious implementation drawbacks, including, the lack of funds, technical skills, and regulatory inflexibilities. These conclusions support the importance of enhancing the cybersecurity resilience through sealing the knowledge gaps, building up the policy-based efforts, and fostering the cooperation of industry participants. Telecommunications service providers should request all-inclusive and interactive skills development programs that facilitate interaction with consumers in a natural manner, especially interactive workshops to improve the knowledge and memorability [40]. It is the recommendation of policymakers to formulate clear, industry-focused regulatory policies that minimize complexities and enhance compliance, though governments and industry stakeholders invest in cybersecurity framework, employee training, and technological innovation. The collaboration between the private and the public needs to be mutual to share valuable insights and best practices, threat identifications, and resource constraints to establish a healthy cybersecurity environment. Constant checks and balances, policy review and educational programs come in handy in regard to responsiveness to risks that may occur. The investigation of psychological variables impacting consumer behavior and examining the possibility for uprising inventions, like, machine learning and artificial intelligence, can provide deeper insights for enhancing cybersecurity initiatives. All in all, by addressing flaws in consciousness levels, resource allocation and policy implementation, stakeholders can greatly enhance telecommunications sector's cybersecurity and engender a safer and more resilient digital climate within the Southern African context, with insights that span across industries within the region.

References

[1] George AS, Baskar T, Srikaanth PB. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal. 2024 Feb 25; 2(1):51-75.

[2] Lehto M. Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[3] Domorenok E, Graziano P, Polverari L. Introduction: Policy integration and institutional capacity: Theoretical, conceptual and empirical challenges. Policy and Society. 2021 Mar; 40(1):1-8.

[4] Manns G. The Adoption of Cybersecurity in Small-To Medium-Sized Businesses: A Correlation Study. Capella University; 2021.

[5] Inakefe GI, Bassey VU, Amadi JO. Evaluation of the Policy and Institutional Implications of Digital Tools in E-Governance Reforms Implementation for Service Delivery in Cross River State Civil Service, Nigeria. Sage Open. 2024 Nov; 14(4):21582440241297047.

[6] Al Hamli SS, Sobaih AE. Factors influencing consumer behavior towards online shopping in Saudi Arabia amid covid-19: Implications for E-businesses post pandemic. Journal of Risk and Financial Management. 2023 Jan 5; 16(1):36.

[7] Zaydi M, Maleh Y, Khourdifi Y. A new framework for agile cybersecurity risk management: Integrating continuous adaptation and real-time threat intelligence (ACSRM-ICTI). InAgile Security in the Digital Era 2024 Dec 30 (pp. 19-47). CRC Press.

[8] Mukherjee A. The Complete Guide to Defense in Depth: Learn to identify, mitigate, and prevent cyber threats with a dynamic, layered defense approach. Packt Publishing Ltd; 2024 Jul 31.

[9] Osimen GU, Wonosikou MH, Odeigah TN. National cybersecurity policy and citizens' rights in Nigeria. The International Journal of Human Rights. 2026 Jan 24:1-26.

[10] Ali MG. Cybersecurity Governance and Policy Development in Higher Education Institutions: A Strategic Framework for Resilience and Compliance. Online Submission. 2025 Sep 5.

[11] Regal B, FitzGerald C. The relational edge: arbitrage as a key capability in platform organizations. Public Management Review. 2025 Nov 12:1-28.

[12] Singh T. Cyber Security and Human Factors: Keeping Information Safe. Tarnveer Singh; 2023 May 24.

[13] Hadebe S. Digital Sovereignty and Tight Regulation in the EU: Analysing the motivation behind the Digital Markets Act. Available at SSRN 4785054. 2022 Apr 30.

[14] Xi W. Regulatory Changes and Compliance Challenges. InStrategic Financial Management: A Managerial Approach 2024 Oct 25 (pp. 119-134). Emerald Publishing Limited.

[15] Jansen LJ, Kalas PP. Improving governance of tenure in policy and practice: A conceptual basis to analyze multi-stakeholder partnerships for multi-stakeholder transformative governance illustrated with an example from South Africa. Sustainability. 2020 Nov 26; 12(23):9901.

[16] Ewoh P, Vartiainen T, Mantere T. Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review. Journal of Medical Internet Research. 2025 Oct 15; 27:e75584.

[17] Rathee S. Queering Indian Celluloid: Towards a Genealogy of Non-Heteronormative Female Desire in Hindi Cinema and Bollywood, 1998–2018 (Doctoral dissertation, Murdoch University).

[18] Emard KA, Edgeley CM, Hazard CA, Sarna-Wojcicki D, Cannon W, Cameron OZ, Hillman L, McCovey K, Lombardozzi D, Pearse S, Newman AJ. Connecting local ecological knowledge and Earth system models: comparing three participatory approaches. Ecology and Society. 2024 Dec 31; 29(4).

[19] Mukherjee A, Dave K, Park BJ, Pomelnikova A. Evaluating the Extent to Which China's Development Projects Abroad Classify as. Available at SSRN 5545860. 2025 Sep 28.

[20] Grijalva-Salazar RV, Caicedo-Mendoza JA, Zúñiga-Castillo AJ, Olivas-Valencia E, Fernández-Bedoya VH. Bridging Regulation and Innovation: A Systematic Review of Cryptocurrency Taxation and Fiscal Policy (2020–2025). Journal of Risk and Financial Management. 2025 Dec 16; 18(12):720.

[21] Perwej Y, Abbas SQ, Dixit JP, Akhtar N, Jaiswal AK. A systematic literature review on the cyber security. International Journal of scientific research and management. 2021 Dec 6; 9(12):669-710.

[22] Ashok M, Al Badi Al Dhaheri MS, Madan R, Dzandu MD. How to counter organisational inertia to enable knowledge management practices adoption in public sector organisations. Journal of knowledge management. 2021 Nov 17; 25(9):2245-73.

[23] Akinbowale OE, Mashigo MP, Zerihun P. Understanding and mitigating cyberfraud in Africa. AOSIS; 2024.

[24] Al-Emran M, Al-Qaysi N, Al-Sharafi MA, Alhadawi HS, Ansari H, Arpaci I, Ali NA. Factors shaping physicians' adoption of telemedicine: a systematic review, proposed framework, and future research agenda. International Journal of Human–Computer Interaction. 2025 Jul 3; 41(13):8495-514.

[25] Hlahla S, Ngidi M, Duma SE, Sobratee-Fajurally N, Modi AT, Slotow R, Mabhaudhi T. Policy gaps and food systems optimization: a review of agriculture, environment, and health policies in South Africa. Frontiers in sustainable food systems. 2023 Aug 17; 7:867481.

[26] Shapoval Y. Relationship between financial innovation, financial depth, and economic growth. Investment Management & Financial Innovations. 2021; 18(4):203.

[27] Anderson, Marcus Aurelius. *International Cyber Cooperation: Coalition of the Willing*. Diss. Capitol Technology University, 2025.

[28] Do Manh T, Dang D, Falch M, Tran Minh T, Vu Phi T. The role of stakeholders and their relationships in the sustainability of telecentres. Digital Policy, Regulation and Governance. 2023 Mar 7; 25(2):104-19.

[29] Guma A. An assessment of information security and awareness levels in small to medium organizations: a case study of Masvingo. Available at ssrn 5318922. 2024 Aug 15.

[30] Ghonim MA, Goda AE, Khashaba NM, Elsotouhy MM, Khashan MA. Impact of organizational energy on digital transformation in healthcare services: the movement of human resources from inertia to flexibility. EuroMed Journal of Business. 2025 Nov 19; 20 (4):945-73.

[31] Falayi M, Gambiza J, Schoon M. A scoping review of environmental governance challenges in southern Africa from 2010 to 2020. Environmental Conservation. 2021 Dec; 48(4):235-43.

[32] Cheong CL. Research on AI security strategies and practical approaches for risk management. Journal of Computer, Signal, and System Research. 2025 Dec 31; 2(7):98-115.

[33] J Nair A, Manohar S, Mittal A. Reconfiguration and transformation for resilience: Building service organizations towards sustainability. Journal of Services Marketing. 2024 Apr 25;38(4):404-25.

[34] Jahanbakht M, Mostafa R. Coevolution of policy and strategy in the development of the mobile telecommunications industry in Africa. Telecommunications Policy. 2020 May 1;44(4):101906.

[35] Bawa S, Benin IW, Yongping X. Digital innovation and knowledge management involvement: a study of Ghana's economy. Kybernetes. 2025 May 12.

[36] Khadka K, Ullah AB. Human factors in cybersecurity: an interdisciplinary review and framework proposal. International Journal of Information Security. 2025 Jun; 24(3):1-3.

[37] Li D. Global Governance of Space Cyber Security: Regulatory and Institutional Aspects. Taylor & Francis; 2024 Nov 25.

[38] Shah SS, Shah SA. Trust as a determinant of Social Welfare in the Digital Economy. Social Network Analysis and Mining. 2024 Apr 5; 14(1):79.

[39] Okolo FC, Etukudoh EA, Ogunwole O, Osho GO, Basiru JO. Strategic approaches to building digital workforce capacity for cybersecure transportation operations and policy compliance. Journal Name Missing. 2023 Mar.

[40] Paredes O, Melo D, Guamán AR, García M, Guamán-Guevara F. Which Innovative Solutions of Non-Technological and Technological Nature are needed to Improve Tourism Services? A Case of Tungurahua Province in Ecuador. Tourism: An International Interdisciplinary Journal. 2021 Nov 25; 69(4):559-77.