ZCAS University Press, Lusaka, Zambia, ISBN: 978-9982-29-174-3

The Guardian of Digital Transformation in Emerging Economies: Building a Sectoral Resilience in Zambia

Gabriel Kapumpe
Lecturer, Computer Science Department
ZCAS University, Lusaka, Zambia
Email: gabriel.kapumpe@zcasu.edu.zm

Cite: Kapumpe, G. (2025). *The guardian of digital transformation in emerging economies—Building sectoral resilience in Zambia*. In D. A. Sikalumbi, B. Mweemba, & E. K. Bbenkele (Eds.), *Digital transformation in emerging economies* (pp. 19–42). ZCAS University Press, Lusaka.

Abstract

*This chapter examines the strategic importance of cybersecurity as a pillar of digital transformation in emerging economies with a focus on Zambia's transition toward a digitally driven economy. Framed under the title "**Cybersecurity: The Guardian of Digital Transformation in Emerging Economies: Building A Sectoral Resilience in Zambia**". The discussion is placed within the broader theme of Digital Transformation in Emerging Economies: The Future of Business, Education, and Governance. It presents a conceptual and policy-based examination of how cybersecurity underpins digital development efforts in key national sectors. Further, it appreciates Zambia as a case of developing economies undergoing digital transformation journey. Through a critical analysis of existing literature, the chapter outlines Zambia's cybersecurity journey. From early policy responses to the current legislative landscape. It considers how national instruments such as the Cyber Security and Cyber Crimes Act, and the Data Protection Act are intended to safeguard information systems and enhance public trust in digital services. Besides these efforts, consistent challenges are examined. These include limited human capacity, inadequate awareness, and disjointed implementation strategies. Instead of offering case studies, the chapter presents a sector-wide combination of how business, education, and governance are impacted by cybersecurity gaps and reforms as a base for digital transformation in emerging economies. The advanced argument is that cybersecurity must be treated not merely as a technical safeguard, but as a strategic foundation for inclusive and sustainable digital transformation. To conclude, the chapter calls for a harmonized approach that brings together policymakers, academia, and private sector actors to build a secure digital ecosystem. This collective effort is vital to ensuring that Zambia can fully benefit from the opportunities presented by emerging technologies.*

Keywords: *Cybersecurity, Digital Transformation, Emerging Economies, Sectoral Resilience, Governance, Zambia*

1. Introduction

In emerging markets, digital transformation fundamentally depends on establishing vigorous cybersecurity foundations. These foundations are responsible to protect and enable the digitization of businesses, education, and governance systems. Zambia, as a landlocked country in Southern Africa with a current population of approximately 20 million people, is a testimony to the journey toward comprehensive cybersecurity readiness. The country's journey represents both the cornerstone of a successful digital transformation and an ongoing strategic imperative.

This chapter examines the evolution of Zambia's cybersecurity landscape to support a comprehensive digital transformation across all sectors. Additionally, the chapter examines the Zambia's notable score of 92.6 percent in the Global Cybersecurity Index (GCI) 2023, marking a significant improvement from 14.7 percent reported in 2014.

While securing Business, Education, and Governance play a remarkable role, the importance of cybersecurity as a foundation for digital transformation in Zambia cannot be overemphasized. As the country undergoes rapid digitization of business processes, educational systems, and government services, with mobile cellular subscriptions increasing from 21.1 million in 2023 to 23.2 million in 2024, and Internet subscriptions growing by 7 percent year-over-year, the digital vulnerability surface has expanded exponentially. Although growth shows an indicative positive economic and social development, it has created new vulnerabilities that require sophisticated and comprehensive cybersecurity strategies to protect the digital transformation investments across business, education, and governance sectors.

Although Zambia has joined the bandwagon of other emerging economies, its cybersecurity journey is particularly unique. Within the context of digital transformation, nations simultaneously build digital capabilities and protect against sophisticated cyber threats. Zambia's high cybersecurity score in Africa shows that developing economies can build strong digital defenses while working toward digital change, innovation, and economic growth.

2. Cybersecurity in Zambia's Digital Transformation: The Evolution

Early Developments and Foundation Building for Digital Economy

Before 2010, Zambia faced limited access to a digital land scape. However, during early 2010, the country's cybersecurity journey began. A transition from limited access to a growing digital landscape was on the rise. The transition, driven by government initiatives, private sector investments and digital financial services. This coincided with digital transformation initiatives aimed at modernizing business operations, educational systems, and government services. The initial cybersecurity landscape characterized limited awareness of digital risks in business and governance. This included minimal infrastructure protection and a reactive approach to digital threats that could undermine transformation efforts across sectors. Key milestones include the enactment of the ICT Act in 2009, the establishment of the SMART Zambia Institute, and the implementation of the National Electronic Government Plan. Zambia is one of the first 17 African countries to implement the Digital Economy for Africa (DE4A) Initiative, in which the World Bank had committed to investing $25 billion in Africa's digital transformation. Zambia, alone, secured US$120 million grant for digital transformation which was meant to shape the country's digital future.

During the nation's digital transformation history, government leaders and private sector stakeholders recognized early that cybersecurity would be critical to realizing the benefits of digital transformation. With the exponential surge in the digital transformation for business, education, and governance, it was imperative that protecting national economic interests and

citizen data become critical. This recognition led to the development of cybersecurity as an enabling infrastructure for digital transformation rather than merely a defensive measure.

The foundation of Zambia's cybersecurity architecture was based on several key principles. These key principles directly support objectives of digital transformation. Firstly, national sovereignty in cyberspace is to protect domestic digital assets. Secondly, protection of critical infrastructure supporting business and government operations. Thirdly, promoting digital literacy across business and educational sectors. Finally, international cooperation to access global digital markets safely. These principles have guided Zambia's cybersecurity development over the past decade and continue to shape policy decisions that enable digital transformation across all sectors of society.

Whilst progress was on record during the foundational period, Zambia faced significant challenges. Zambia's top cybersecurity ranking in Africa is an indication that while working toward innovation, digital change, and economic growth, developing economies can build strong digital defenses. Nations entering the digital age typically face problems like limited funds for cybersecurity, not enough skilled cybersecurity workers, weak cybercrime laws, and poor awareness of digital threats. Despite these issues, the government has shown dedication to building cybersecurity through partnerships and careful planning.

3. Institutional Framework Development

Following the commitment to building cybersecurity capacity, Zambia was on a crucial point of cybersecurity evolution. Government agencies set up specific cybersecurity units and created national plans for cybersecurity. Public-private partnerships were further established, which helped to build cybersecurity skills with a defined framework. Crucially, many government departments created cybersecurity contact roles. Similarly, the creation of cybersecurity awareness programs for public servants, and the development of incident response protocols were on course. These institutional foundations provided the structural basis for more sophisticated cybersecurity capabilities that would emerge in succeeding years.

The institutional framework also emphasized the importance of cross-sector collaboration. The nation recognized that cybersecurity threats transcended traditional sector boundaries. As a result, the government's approach emphasized coordination between its agencies, private sector entities, academic institutions, and civil society organizations. With such a collaborative approach, the door to the success of cybersecurity was established.

Cybersecurity Enabling Digital Transformation Across Sectors

Securing Business Digital Transformation

Over the past decade, the digitization of Zambian businesses has accelerated exponentially. Cybersecurity has been the core enabler and protector of this transformation. Small and Medium Enterprises (SMEs), which form the backbone of Zambia's economy, have increasingly adopted digital payment systems such mobile money (a mobile financial transaction service offered by Mobile Network Operators (MNOs)), local and international e-commerce platforms, and cloud-based business management solutions. The cybersecurity framework has been specifically

designed to support these business transformation initiatives. Also, to offer protection against cyber threats that could undermine economic growth.

Amongst the key services, the financial sector exemplifies successful cybersecurity-enabled digital transformation. Most Zambian banks and mobile money providers have implemented sophisticated cybersecurity measures that enable secure digital transactions while securing customer data. Not only has this facilitated the growth of digital financial services, but also making the digital money transactions become a cornerstone of the digital economy. To support these services, it is critical to have systems that can support these services. Systems include advanced fraud detection systems, secure authentication mechanisms, and real-time transaction monitoring capabilities.

Manufacturing and agriculture sectors have also benefited from cybersecurity-enabled digital transformation. In the field of agriculture, for example, the adoption of Internet of Things (IoT) devices for monitoring agricultural conditions has proven to be a huge milestone. On the other hand, manufacturing processes have been facilitated by cybersecurity frameworks that protect these connected systems from cyber-attacks. This has enabled Zambian businesses to improve efficiency and competitiveness while maintaining security.

Besides manufacturing and agriculture, the retail sector's digital transformation has been particularly notable, with many businesses adopting e-commerce platforms and digital marketing strategies. Cybersecurity measures protecting these digital business operations have been essential for building consumer confidence in online transactions and protecting business intellectual property and customer data. To affirm the enabling of digital transformation across businesses, ZICTA (Zambia Information and Communications Authority) has regularly organized awareness programs to educate SMEs and startups on cyber risks, data protection laws, and how to adhere to best practices for safe digital business operations.

4. Educational Sector Cybersecurity and Digital Learning

The education sector has not lagged in terms of digital transformation. Zambia witnessed a significant digital transformation in the educational sector, accelerated by the COVID-19 pandemic which had a backbone support of comprehensive cybersecurity measures. The pandemic led to many educational institutions developing online learning platforms, digital educational resources, and virtual classroom technologies. These services require sophisticated cybersecurity frameworks to protect student data and ensure secure learning environments.

To emphasis the importance of cybersecurity in the educational sector, the Ministry of Education has implemented cybersecurity standards for educational institutions that address the unique challenges of protecting student information while enabling innovative digital learning approaches. These standards cover data protection for student records, secure online learning platforms. Also, the ministry offers cybersecurity education for both students and educators.

To complement these efforts, universities and higher education institutions have been at the forefront of cybersecurity-enabled educational transformation. Notably, ZCAS University, the University of Zambia and other institutions have developed comprehensive cybersecurity programs which not only protect their digital infrastructure but prepare students for careers in

the digital economy. These programs include cybersecurity degree programs, research initiatives, and partnerships with international institutions.

The integration of digital technologies in primary and secondary education has been supported by age-appropriate cybersecurity education programs. At the core of this integration, students learn about digital citizenship, online safety, and basic cybersecurity principles as part of their general education. This adequately prepares them for participation in the digital economy. There has been a deliberate move to include cybersecurity content in the new education curriculum for primary and secondary schools.

Government Digital Services and E-Governance Security

Previously, government services were processed manually. The digitization of government services has been one of the most visible aspects of Zambia's digital transformation. Cybersecurity has played a crucial role in enabling citizen trust and participation in e-governance initiatives. The development of online government services, digital identity systems, and electronic document management has required sophisticated cybersecurity measures to protect citizen data and ensure service continuity.

With government services, there is a need to ensure that citizens' personal data is well protected. As a result, the government of Zambia implemented a comprehensive e-governance cybersecurity framework that addresses the unique challenges of protecting citizen data while providing accessible and efficient digital services. The framework included secure authentication systems for accessing government services. Encrypted communication channels for sensitive government communications and robust backup and disaster recovery systems were included to ensure service continuity.

To represent the critical component of government digital transformation, digital identity systems introduced citizens to access multiple government services through secure digital credentials. The cybersecurity measures protecting these systems include biometric authentication, encrypted data storage, and sophisticated access control mechanisms that prevent unauthorized access while enabling legitimate use.

Equally, the procurement process has been digitized. This digitization of government procurement processes has been supported by cybersecurity measures that ensure transparency and prevent corruption while protecting sensitive commercial information. With these systems in place, businesses can participate in government procurement through secure online platforms known as the e-GP (e-Procurement System managed by the Zambia Public Procurement Authority (ZPPA)), which protect bidder information and ensure fair competition. The e-GP Platform is a web-based, collaborative system that facilitates the full lifecycle of a tendering process, for both buyers and suppliers.

Current Cybersecurity Landscape Supporting Digital Transformation

Legislative and Regulatory Framework

The year 2025 marked a pivotal moment in Zambia's cybersecurity development journey. With the enactment of the Cyber Security Act of 2025, the cybersecurity landscape has been shaped to

support digital transformation critical areas. This comprehensive legislation establishes the Zambia Cyber Security Agency and provides for its functions, regulates cyber security service providers, and constitutes the Zambia Cyber Incident Response Team. The Act represents the culmination of years of legislative development and stakeholder consultation, replacing the previous Cyber Security and Cyber Crimes Act of 2021.

The legislative framework addresses several critical areas essential for comprehensive cybersecurity readiness. These include the protection of critical information infrastructure, mandatory registration and protection requirements for critical systems, licensing requirements for cybersecurity service providers, and provisions for international cooperation in addressing cyber threats. The legislation also establishes clear penalties for cybersecurity breaches and provides the legal foundation for coordinated national cybersecurity responses.

However, the new legislation has not been without controversy. Critics, including diplomatic missions and civil society organizations, have raised concerns about potential surveillance capabilities and the concentration of power in government cybersecurity agencies. The Act has sparked intense debate among Zambians, revealing fascinating cultural and political fault lines. Conversations about the Act reveal deep ambivalence about the trade-offs between security and freedom. The Zambian government has responded to these concerns by emphasizing its commitment to international obligations and expressing willingness to engage in constructive dialogue with stakeholders about the implementation of the legislation.

The regulatory framework extends beyond the primary cybersecurity legislation to include sector-specific regulations and standards. These cover areas such as financial services, cybersecurity, telecommunications security, and government information systems protection. The comprehensive nature of the regulatory framework reflects Zambia's recognition that cybersecurity requires coordinated approaches across all sectors of society.

5. Institutional Architecture

Zambia's cybersecurity institutional architecture ecosystem has evolved significantly since the early 2010s. At the heart of the center of this architecture is the newly established Zambia Cyber Security Agency, which serves as the primary national cybersecurity coordination body. Apart from developing national cybersecurity policies, the mandate of the agency coordinates cybersecurity responses across government agencies and facilitates public-private partnerships in cybersecurity.

The Zambia Cyber Incident Response Team (CIRT) represents another crucial component of the institutional architecture. CIRT-Zambia serves as the national focal point for cybersecurity incident response, providing technical expertise, coordination capabilities, and liaison functions with international cybersecurity organizations. The team's capabilities have been developed through extensive training programs and international partnerships, enabling it to respond effectively to sophisticated cyber threats.

The institutional architecture also includes specialized cybersecurity units within key government ministries and agencies. The Ministry of Technology and Science plays a coordinating role in cybersecurity policy development. On the hand, the Ministry of Home

Affairs focuses on cybercrime investigation and law enforcement aspects of cybersecurity. This distributed approach ensures that cybersecurity considerations are integrated into all relevant government functions.

The Central Monitoring and Coordination Centre represents a more controversial aspect of institutional architecture. Established for lawful interception of communications under stringent legal conditions, the Centre has been subject to criticism regarding potential surveillance capabilities. The government has emphasized that the Centre operates under strict legal oversight and is essential for national security and cybercrime investigation purposes.

6. Technology Infrastructure and Capabilities

Zambia's cybersecurity technology infrastructure has developed considerably over the past decade. The country has invested in sophisticated cybersecurity monitoring and response systems, including Security Operations Centers (SOCs) that provide 24/7 monitoring of critical infrastructure and government systems. These SOCs utilize advanced threat detection technologies, including artificial intelligence and machine learning capabilities, to identify and respond to cyber threats in real-time.

The technology infrastructure also includes comprehensive backup and disaster recovery systems. These systems are designed to ensure continuity of critical services in the event of cyberattacks. Also, these systems are regularly tested and updated to ensure their effectiveness against evolving threats. Additionally, the government has invested in secure communication systems for government operations. This includes encrypted communication channels and secure data storage facilities.

Partnership with international technology companies and outsourcing has been crucial to developing these capabilities. Notable partnerships include collaboration with Google to establish a center of excellence in Artificial Intelligence. This partnership was launched in 2024, to enhance the country's capability to address sophisticated cyber threats using AI-driven tools. When Google announced its partnership with Zambia to establish an AI center of excellence, reactions were mixed. Tech enthusiasts celebrated the validation of Zambia's digital potential. Skeptics worried about digital colonialism, the risk of foreign corporations extracting value while leaving little behind. These partnerships provide access to cutting-edge technologies and expertise that would be difficult to develop independently. What makes the Google partnership particularly interesting is its focus on AI applications for cybersecurity. Zambian officials argue that AI-driven threat detection systems can help level the playing field against sophisticated cyber attackers. Critics wonder whether such systems might also enhance government surveillance capabilities. This has been a concern that resonates strongly in a country still finding its democratic footing.

Similarly, apart from technological infrastructure development, the importance of cybersecurity awareness and training systems have been emphasized. Online training platforms, cybersecurity simulation environments, and digital literacy programs have been developed to enhance cybersecurity awareness among government employees, private sector workers, students and

citizens. These educational technologies are imperative for building a cybersecurity-aware society.

7. National Digital Transformation Strategy Integration

Strategic Framework and Objectives

The National Digital Transformation Strategy for Zambia was targeted between 2023 and 2027. According to the Ministry of Technology and Science (2023), the objective of the strategy was to provide an overarching framework for the country's digital development, with cybersecurity as a foundational element. The strategy recognizes that digital transformation cannot succeed without robust cybersecurity foundations. Therefore, integrating cybersecurity considerations into all aspects of digital development planning is critical to the success of digital transformation. The strategy establishes several key objectives related to cybersecurity readiness. These include building comprehensive cybersecurity capabilities across all sectors, developing a skilled cybersecurity workforce, establishing resilient digital infrastructure, and creating a secure digital ecosystem that enables economic growth and social development. The strategy also emphasizes the importance of international cooperation in addressing transnational cyber threats.

The strategic framework adopts a whole-of-society approach to cybersecurity, recognizing that effective cybersecurity requires engagement from government, private sector, civil society, and individual citizens. This approach is reflected in the strategy's emphasis on public-private partnerships, community engagement programs, and individual responsibility for cybersecurity practices.

8. Implementation Mechanisms for Cross-Sector Digital Security

The implementation of the National Digital Transformation Strategy involves multiple mechanisms designed to ensure coordinated and effective cybersecurity support for digital transformation across business, education, and governance sectors. These include the establishment of sector-specific cybersecurity implementation committees and the development of detailed cybersecurity roadmaps for different sectors. Additionally, they include the creation of monitoring and evaluation frameworks to track progress against digital transformation objectives.

Funding mechanisms for cybersecurity-enabled digital transformation include both domestic budget allocations and international development partnerships specifically focused on supporting digital transformation in emerging economies. The government has committed significant resources to cybersecurity infrastructure that enables digital transformation, while international partners provide technical assistance, capacity building support, and technology transfer opportunities that strengthen both cybersecurity and digital transformation capabilities.

Sector-Specific Digital Transformation Applications

The National Digital Transformation Strategy recognizes that different sectors require tailored cybersecurity approaches to support their unique digital transformation needs. The financial services sector, for example, requires specialized cybersecurity measures that enable secure

digital banking, mobile money services, and online payment systems while protecting customer data and financial transactions.

The education sector requires cybersecurity frameworks that support digital learning platforms, protect student data and enable secure online educational delivery while maintaining accessibility and usability for educators and students. This includes the development of cybersecurity standards for educational institutions and training programs that prepare educators to deliver cybersecurity education.

For the healthcare sector, digital transformation requires cybersecurity measures that protect patient data while enabling telemedicine, electronic health records, and digital health monitoring systems. These measures must balance security requirements with the need for healthcare providers to access patient information quickly and efficiently.

The agriculture sector's digital transformation includes cybersecurity protection for precision. This involves protecting systems used in precision farming with cybersecurity, using online platforms to sell farm goods, and managing supply chains to link farmers to markets while keeping business information safe.

9. Challenges and Opportunities in Digital Transformation Security

Human Resource Challenges for Digital Economy Security

Whilst Zambia has made significant progress in cybersecurity development, the nation continues to face substantial challenges in building adequate cybersecurity human resources to support the broad changes happening in business, education, and government. The global shortage of cybersecurity professionals affects Zambia particularly acutely, as growing economies scramble with rich countries for the few experts needed to protect digital projects. The cybersecurity skills and knowledge gap is not just about technical skills; it also includes the management and planning skills needed to head up security projects for digital change. Many organizations in different areas do not have experts to create and carry out plans that protect against cyber threats while still embracing innovation. This issue is more obvious in small and medium-sized businesses, which are key to Zambia's digital economy. However, these businesses cannot easily find and pay for cybersecurity talent.

Most educational institutions in Zambia have joined the bandwagon to address these human resource challenges. Today, Zambia has seen a lot of curriculum development and blending through development of cybersecurity degree programs and professional certification courses to prepare graduates for careers in the digital economy. But the pace of educational program development has not kept up with the rapid growth in demand for cybersecurity professionals across all sectors undergoing digital transformation.

Infrastructure Vulnerabilities in Digital Transformation

Zambia's digital infrastructure setup is getting better quickly to support digital changes in different areas. However, it still has weak spots that hackers could use to disrupt business, education or government services. The country relies heavily on international connectivity for

internet access which creates potential single points of vulnerabilities that could be targeted by sophisticated attackers seeking to disrupt the digital economy.

Digital infrastructure relies on stable and consistent power supply. Therefore, power infrastructure reliability represents a significant vulnerability for cybersecurity systems supporting digital transformation. The recent past has seen frequent power outages and unstable electricity supply which may disrupt cybersecurity monitoring systems protecting business operations, educational platforms and government services This can result in creating windows of vulnerability that attackers might exploit to access critical digital transformation infrastructure.

Like any other developing economies, rural connectivity remains a challenge. As a result, this digital divide can create cybersecurity vulnerabilities that could undermine inclusive digital transformation. Areas with limited internet connectivity may have less sophisticated cybersecurity protections, making them potential vulnerable for attackers seeking access to the national digital infrastructure supporting business, education and governance systems. In Zambia, the trend is that much attention focuses on Lusaka's gleaming technology hubs and the Copperbelt's industrial digitization leaving rural Zambia with a different cybersecurity story—one that's often overlooked but increasingly critical. If cyber criminals can exploit rural mobile banking systems, they can potentially disrupt agricultural supply chains that feed urban populations. Similarly, if telemedicine systems serving remote areas lack adequate security, patient data breaches could undermine trust in digital healthcare solutions.

The government's National Digital Transformation Strategy acknowledges these rural challenges, but implementation remains problematic. Cybersecurity training materials developed for urban audiences do not suit rural contexts. Technical solutions designed for reliable power and internet connectivity struggle in areas where both are intermittent.

Resource Constraints

Besides infrastructure vulnerabilities, financial constraints represent a persistent challenge for cybersecurity development in Zambia. Cybersecurity technologies and services are often expensive, and the country must balance cybersecurity investments with other development priorities. This is particularly challenging for smaller organizations that may lack the resources to implement comprehensive cybersecurity measures.

The cost of cybersecurity technologies continues to rise as threats become more sophisticated, requiring more advanced defensive measures. This creates ongoing pressure on cybersecurity budgets and may lead to difficult decisions about which cybersecurity measures to prioritize. The government has worked to address these challenges through bulk procurement programs and partnerships with international organizations.

Technical assistance and capacity building support from international partners helps to address resource constraints, but this support often comes with conditions and may not fully align with national priorities. Balancing international cooperation with national sovereignty in cybersecurity remains an ongoing challenge.

Evolving Threat Landscape

The cybersecurity threat landscape facing Zambia continues to evolve rapidly, presenting new challenges that require adaptive responses. Threats have become more sophisticated, with attackers using advanced techniques such as artificial intelligence and machine learning to enhance their capabilities. These advanced threats require correspondingly sophisticated defensive measures that may be beyond the current capabilities of some organizations.

The increasing interconnectedness of digital systems creates new attack vectors that were not present in earlier phases of digital development. Today, the world has advanced in interconnectedness where Internet of Things devices, cloud computing systems, and mobile applications create potential entry points for attackers that require specialized cybersecurity measures.

The rapid adoption of these technologies by Zambian organizations has sometimes outpaced the development of corresponding cybersecurity protections. Many of these cybercrimes are transnational. They present challenges for Zambia, as criminal organizations based in other countries may target Zambian systems while remaining beyond the reach of domestic law enforcement. Addressing these transnational threats requires international cooperation and sophisticated investigative capabilities.

10. Strengths and Achievements

Regulatory and Legal Framework

Developing a comprehensive cybersecurity legislation represents a significant strength in the Zambia's achievement of cybersecurity readiness. The Cyber Security Act of 2025 provides a solid legal foundation for cybersecurity activities and establishes clear responsibilities for various stakeholders. This legislative framework has placed Zambia amongst the leaders in cybersecurity governance in Africa.

The legislation's emphasis on critical infrastructure protection addresses one of the most important aspects of national cybersecurity. By requiring registration and protection of critical systems, the legislation ensures that the most important digital assets receive appropriate cybersecurity attention. This approach reflects the best international practices in cybersecurity governance.

Also, the legal framework has provided for international cooperation in addressing cyber threats, recognizing that cybersecurity is inherently a global challenge. The legislation establishes mechanisms for sharing threat intelligence, coordinating responses to transnational cyber incidents and cooperating with international law enforcement agencies.

International Recognition and Partnerships

Zambia’s achievement of a 92.6 percent score in the Global Cybersecurity Index represents remarkable progress and international recognition of the country’s cybersecurity efforts. This score places Zambia among the top-performing countries in cybersecurity globally and demonstrates the effectiveness of the country's strategic approach to cybersecurity development.

With this achievement, Zambia's cybersecurity achievements have attracted international attention and partnership opportunities. Recently, the partnership with Google to establish an AI Center of Excellence demonstrates the confidence that international technology companies have in Zambia's cybersecurity capabilities. The commitment from the Czech Republic to support Zambia's digital transformation and cybersecurity represents additional international recognition and support.

These international partnerships provide access to cutting-edge technologies, expertise, and best practices that enhance Zambia's cybersecurity capabilities. Also, these partnerships provide opportunities for Zambian cybersecurity professionals to gain international experience and bring global best practices back to the country.

Institutional Capacity

The establishment of sophisticated cybersecurity institutions is an indication that Zambia has made tremendous achievement in terms of cybersecurity development. The Zambia Cyber Security Agency and the Zambia Cyber Incident Response Team provide the country's capacity to handle coordinated cybersecurity responses. These institutions have developed significant capabilities in threat detection, incident response, and cybersecurity coordination.

The development of cybersecurity capabilities within existing government agencies demonstrates the successful integration of cybersecurity considerations into broader government operations. This integration ensures that cybersecurity is not treated as a separate function but as an integral part of all government activities. Additionally, institutional capacity development has included training and capacity building programs that have enhanced the skills of government cybersecurity professionals. These programs have utilized international partnerships and best practices to develop capabilities that meet international standards.

Innovation and Technology Adoption

Zambia's embrace of innovative cybersecurity technologies demonstrates the country's commitment to staying current with global cybersecurity developments. The use of artificial intelligence and machine learning for threat detection and response represents an advanced approach to cybersecurity that few developing countries have implemented.

The development of cybersecurity training and awareness programs using digital technologies demonstrates innovative approaches to building cybersecurity capacity. These programs reach large numbers of people at relatively low cost and provide scalable approaches to cybersecurity education.

The country's "Cyberthon" initiative represents an innovative approach to building cybersecurity capabilities through competitive events that engage young people and technology professionals. These events help to identify and develop cybersecurity talent while raising awareness about cybersecurity issues.

Regional and Global Positioning

African Leadership

Whilst many African countries are making strides towards cybersecurity and digital transformation, Zambia's cybersecurity achievements have positioned the country as a leader in cybersecurity within the continent. Combined with the country's high score on the Global Cybersecurity Index shows how well Zambia is doing compared to other African nations and demonstrates the potential for developing countries to achieve high levels of cybersecurity readiness. As a result, Zambia can be at the forefront of assisting other countries in the region improve their cybersecurity by sharing what has worked, giving technical help and taking charge of regional plans. Zambia's efforts is a good example of resilience and determined efforts This will mark as a good lesson to other African countries who are in the infancy of cybersecurity development and those that are undertaking similar efforts.

International Cooperation

Zambia's cybersecurity leadership is also reflected in its participation in regional cybersecurity organizations and initiatives. The country plays an active role in regional cybersecurity forums and contributes to the development of regional cybersecurity standards and best practices. The country actively participates in international cybersecurity organizations and contributes to global cybersecurity initiatives. This participation ensures that Zambia's cybersecurity development remains aligned with international best practices.

The country's commitment to international cooperation is also reflected in its willingness to share threat intelligence and coordinate responses to transnational cyber threats. This cooperation enhances the effectiveness of cybersecurity responses and contributes to global cybersecurity resilience.

Zambia's international cybersecurity cooperation extends to capacity building and technical assistance for other developing countries. This transnational cooperation demonstrates the country's commitment to contributing to global cybersecurity development and also to sharing the benefits of its cybersecurity achievements.

Global Standards Alignment

Apart from international cooperation, Zambia adheres to global standards. The country has consistently emphasized alignment with international standards and best practices. The country's cybersecurity legislation, institutional frameworks, and technical capabilities reflect international cybersecurity standards and demonstrate commitment to global cybersecurity governance.

This alignment with global standards facilitates international cooperation and ensures that Zambia's cybersecurity capabilities are compatible with those of partner countries. Also, this alignment ensures that Zambian organizations can participate effectively in global digital economy while maintaining appropriate cybersecurity protections.

The country's participation in international cybersecurity standard-setting processes ensures that Zambian perspectives and experiences contribute to the development of global cybersecurity

standards. This participation helps to ensure that international standards reflect the needs and capabilities of developing countries.

11. The Future Outlook and Recommendations

Emerging Opportunities

As 2025 unfolds, Zambia faces a crucial test: Is it able to maintain its cybersecurity momentum as initial enthusiasm wanes and practical challenges emerge? Early signs are mixed and remain ambiguous.

Whilst the cybersecurity sector has seen tremendous growth in terms of creating opportunities, it has opened new doors to new vulnerabilities. The exponential growth of cybersecurity firms has not been matched by equivalent improvements in quality control, raising worries about service quality and expertise. Some think Zambia's cybersecurity gains could form a bubble that might burst if not handled well.

Also, political durability is not assured. Recurrently, cybersecurity rules made under one government do not last through changes in leadership, especially if they are linked to questionable monitoring actions and political party orientation. Creating cybersecurity bodies that can survive political shifts needs wider agreement than there now is.

Currently, the biggest issue is the country's reliance on foreign technology. Zambia's cybersecurity progress depends a lot on imported technologies and experts from other countries. This has allowed fast growth but raises questions about lasting progress and national online independence.

The increasing for cybersecurity in the world gives Zambia the opportunity to grow its cybersecurity service exports. The country's solid cybersecurity base coupled with the rising number of experts offer a starting point for making appealing cybersecurity services that could be sold to neighboring countries.

When cybersecurity is seen as a core need, Zambia can get international aid to support cybersecurity projects. The country's past success in success in the past, making it a good partner for groups wanting to build cybersecurity skills. To pursue Artificial Intelligence (AI) and Machine Learning Technologies (MLT), the country worked with Google to open an AI center, putting Zambia in a spot to use these chances and create advanced security tools via AI. This, indeed, is remarkable progress.

Strategic Priorities

One of the strategic priorities for Zambia is continued investment in cybersecurity human resource development. The country must continue to expand and remain innovative to cybersecurity education programs, provide professional development opportunities for cybersecurity professionals, and create attractive career paths in cybersecurity to retain talent.

Strengthening cybersecurity resilience across all sectors of society requires continued attention to cybersecurity standards, awareness programs, and technical assistance for organizations with limited cybersecurity capabilities. This includes particular attention to small and medium enterprises that may lack resources for comprehensive cybersecurity measures.

Enhancing cybersecurity research and development capabilities will be essential for maintaining cybersecurity leadership and addressing emerging threats. This requires investment in cybersecurity research institutions, support for cybersecurity innovation, and partnerships with international research organizations.

Policy Recommendations

The government should continue to refine the implementation of cybersecurity legislation to address stakeholder concerns while maintaining effective cybersecurity protections. This includes developing clear guidelines for the implementation of surveillance provisions and ensuring appropriate oversight mechanisms.

Secondly, increased investment in cybersecurity education and training programs is essential for addressing human resource challenges. This should include support for cybersecurity degree programs, professional certification programs, and continuing education opportunities for cybersecurity professionals.

Stakeholders and the government must champion the development of cybersecurity standards and certification programs for different sectors. This would help to ensure consistent cybersecurity practices across the economy. These standards should be developed through multi-stakeholder processes that include government, private sector, and civil society representatives.

Also, enhanced international cooperation in cybersecurity should continue to be a priority. This includes participation in regional cybersecurity initiatives, bilateral cybersecurity agreements, and multilateral cybersecurity frameworks. This cooperation should include both technical cooperation and policy coordination.

12. Conclusion

Zambia's cybersecurity transformation, reflected in an increase on the Global Cybersecurity Index from 14.7 percent to 92.6 percent, provides both inspiring and cautionary. It is inspiring because it shows what can occur when developing economies put importance on cybersecurity and dedicate resources to build capability. The transformation also reveals the trade-offs and unexpected results that can come with quick cybersecurity growth.

The individual experiences behind these statistics show that cybersecurity involves more than just technology and policies. It involves miners learning to secure industrial control systems and farmers dealing with mobile banking dangers. A close look at Zambia's experience shows a refined idea of cybersecurity readiness that goes beyond simple numbers or basic evaluations. True cybersecurity readiness requires not just technical capabilities and legal frameworks, but also social acceptance, cultural adaptation, and political sustainability.

As the rest of African nations observe Zambia's cybersecurity journey, they would do well to focus not just on the impressive statistics, but on the underlying processes that made those statistics possible. The legislative debates, the public consultations, the international negotiations and the educational initiatives. These less visible elements may be more imperative as compared to the visible outcomes. Most importantly, Zambia's experience suggests that cybersecurity readiness is not a destination but a continuous journey. The impressive achievements seen in

recent years have provided a strong foundation for Zambia, but sustaining and building upon these achievements requires ongoing commitment, adaptation, and learning.

The broader implications extend beyond Zambia's borders. In an interconnected world, each country's cybersecurity capabilities affect global cybersecurity resilience. Zambia's success contributes to continental and global cybersecurity, while its challenges are a reminder that cybersecurity remains a work in progress everywhere. As we look toward the future, Zambia's cybersecurity story continues to unfold. The next chapter will likely reveal whether the country can maintain its momentum while addressing the complex challenges that success itself has created. For now, Zambia offers proof that developing nations can achieve cybersecurity excellence. Also, it is a reminder that such achievement comes with both opportunities and responsibilities that extend far beyond national borders.

However, significant challenges remain in sustaining cybersecurity-enabled digital transformation. Zambia's digital transformation faces ongoing cybersecurity challenges. There is a shortage of cybersecurity experts, alongside vulnerable infrastructure that could disrupt services. Limited resources also restrict cybersecurity investments, while digital transformation constantly faces new threats. To secure Zambia's digital future, it is important to keep investing in and improving cybersecurity. This is vital for securing and growing the digitization of businesses, education, and government services. The investments made in cybersecurity over the past decade have created a solid foundation for continued digital transformation, but ongoing commitment and adaptation will be necessary to address emerging challenges and opportunities in the digital economy.

Zambia's digital transformation shows that developing economies can make real progress in building secure digital societies. This requires a clear plan, a lasting focus on cybersecurity as a key support, and working with other countries. This helps Zambia's economy and society and shows the world how cybersecurity can help, not hurt, digital improvement in developing nations.

To advance digital transformation in these economies, it is imperative to keep investing in cybersecurity skills that promote innovation, adapt to new threats, and stay committed to global teamwork and good practices for safe involvement in the digital world. With these things in place, Zambia can keep leading in digital transformation supported by cybersecurity. Also, it can continue as a model for other developing economies that want to build secure and thriving digital societies. Cybersecurity is a base for digital change, not only for Zambia, but for all developing economies to protect businesses, education and governance.

References

African Union Commission. (2024). *African Union Cybersecurity Framework and Guidelines*. Addis Ababa: AUC Publications.

Banda, M., & Mwansa, K. (2023). "Digital transformation challenges in developing economies: The Zambian experience." *Journal of African Technology Development*, 15(3), 45-62.

Chanda, R. (2024). "Building cybersecurity capacity in Sub-Saharan Africa: Lessons from Zambia's success story." *International Cybersecurity Policy Review*, 8(2), 78-95.

Czech Development Agency. (2024). *Zambia Digital Transformation Partnership Agreement 2024-2027*. Prague: CzechAid Publications.

Global Cybersecurity Alliance. (2023). *Global Cybersecurity Index 2023: Country Profiles and Analysis*. Geneva: GCA Press.

Government of Zambia. (2021). *Cyber Security and Cyber Crimes Act No. 2 of 2021*. Lusaka: Government Printers.

Government of Zambia. (2023). *National Digital Transformation Strategy for Zambia (2023-2027)*. Lusaka: Ministry of Technology and Science.

Government of Zambia. (2025). *The Cyber Security Act of 2025*. Lusaka: Government Printers.

Google LLC. (2024). *Google AI Center of Excellence Partnership Agreement - Zambia*. Technical Report. Mountain View: Google Research.

Hamusonde, J. (2024). "Cybersecurity governance in emerging economies: A comparative analysis of African approaches." *African Journal of Information Security*, 12(4), 112-128.

International Telecommunication Union. (2023). *Global Cybersecurity Index 2023*. Geneva: ITU Publications.

International Telecommunication Union. (2024). *ICT Statistics Database - Zambia Country Profile*. Geneva: ITU Statistical Office.

Kabwe, P., & Mulenga, S. (2023). "Critical infrastructure protection in developing countries: The Zambian cybersecurity model." *Infrastructure Security Quarterly*, 9(1), 23-39.

Lungu, A. (2024). "Human capital development in cybersecurity: Addressing the skills gap in African contexts." *Cybersecurity Education Review*, 6(2), 34-51.

Mubanga, C. (2023). "Legislative frameworks for cybersecurity in Africa: A comparative study." *African Law and Technology Journal*, 11(3), 156-174.

Mwape, L., & Siame, G. (2024). "Public-private partnerships in cybersecurity: The Zambian experience." *Digital Governance Review*, 7(1), 89-106.

Nkandu, F. (2023). "Cyber threat landscape in Southern Africa: Trends and implications." *Regional Security Analysis*, 18(4), 67-84.

Southern African Development Community. (2024). *SADC Cybersecurity Framework and Implementation Guidelines*. Gaborone: SADC Secretariat.

Tembo, M. (2024). "Artificial intelligence applications in cybersecurity: Opportunities for developing nations." *AI and Society*, 39(2), 445-462.

United Nations Conference on Trade and Development. (2024). *Digital Economy Report 2024: Cybersecurity for Sustainable Development*. Geneva: UNCTAD Publications.

World Bank Group. (2024). *Digital Development Partnership - Zambia Cybersecurity Assessment*. Washington, DC: World Bank Publications.

Zambia Cyber Security Agency. (2024). *Annual Cybersecurity Report 2024*. Lusaka: ZCSA Publications.

Zambia Information and Communications Technology Authority. (2024). *ICT Sector Performance Report 2024*. Lusaka: ZICTA Publications.

Zambia Statistics Agency. (2024). *Digital Infrastructure and Connectivity Survey 2024*. Lusaka: ZamStats Publications.

Zulu, K., & Phiri, D. (2023). "Regional cybersecurity cooperation mechanisms: SADC perspectives." *International Relations and Security Studies*, 21(2), 78-94.