Addressing the Digital Resilience Challenge in the Electricity Sector in Nigeria: From Risk to Resilience

Pius M Achuama
Coventry University, Priory Street Coventry, United Kingdom

achuamap@coventry.ac.uk

Abstract: The electricity sector in Nigeria stands at the crossroads of an ever-evolving digital landscape and the pressing need for resilience in the face of dynamic challenges. This paper explores Nigeria's electricity sector, navigating its evolving digital landscape with a focus on resilience amid growing challenges. Shifting from risk reduction to resilience building, the study utilizes stakeholder interviews to assess cyber resilience. Unveiling technological advancements, it addresses interdependencies, vulnerabilities, and cyber threats in the connected grid. The study discusses some enabling practices to solve these issues including the role of policy and regulatory frameworks in fostering a culture of resilience and collaboration among various stakeholders. Amid the digital revolution, it advocates readiness, responsiveness, and rehabilitation for Nigeria's electricity sector. The study serves as a strategic roadmap for public and private decision-makers to tackle digital resilience challenges.

Keywords: Digital Resilience, Electricity Sector, Risk Mitigation, Cyber Resilience.

1. Introduction

The implementation of technological innovations has caused revolutionary opportunities and new challenges in Nigeria's electricity sector, which is characterized by a dynamic landscape. The convergence of digitalization and electricity systems gains prominence as the country endeavors to achieve sustainable electricity provision. Electricity generation in Nigeria traces back to 1896 in Lagos, with the first power plant installed in 1929 (Awosope, 2014). The sector saw slow development until 1999, marked by minimal investment and deteriorating infrastructure, leading to a drastic decrease in installed capacity from 5,600MW to an average of 1,750MW (Onuoha, 2010), (Adedeji, 2017). The industry's dire state prompted significant reforms. The Electricity Corporation of Nigeria (ECN) was established in 1951, followed by the formation of the Niger Dams Authority (NDA) in 1962, eventually merging into the National Electric Power Authority (NEPA) in 1972 (Nwaiwu, 2021). NEPA took on the integrated responsibilities of electricity generation, transmission, and distribution in Nigeria. One of the document highlights how susceptible the Nigeria's electricity sector is prone to cyberattacks, especially when it comes to new digital systems and outdated equipment. Cyberthreats that affect generation, transmission, and distribution systems, and attacks that happened like phishing, malware, and data breaches, present serious hazards (Ogundari, 2020).

The current electricity sector situation in Nigeria reflects significant technological innovations for enhanced service delivery. The sector has deployed technological solutions in improving electricity supply and enhancing their service delivery. For instance, in billing and accounting, the use of accounting software and electronic billing, demonstrates modernization efforts. The use of advanced Metering Infrastructure (AMI) facilitates remote meter connection for operational insights while. Communication and marketing tools have been integrated making it easier to have wider and quicker reach to employees in various locations and customers. Customer Relationship Management (CRM) tools streamline customer management, while Geographic Information System (GIS) aids in asset mapping and real-time location tracking. Monitoring systems like SCADA and ETAP contribute to proactive system security and management though only one distribution company in Nigeria can afford SCADA system at the moment. These organizations have tried to build some digital resilience measures to cater for the prevalent issues with technological adoption such as include building redundancy through backup servers and diverse hosting. Strict authorized access controls, multiple communication channels, collaboration with multiple internet service providers, and the implementation of security features such as firewalls contribute to system resilience. Skilled human resources, smart monitoring with devices like smart meters, and comprehensive training programs for all users further enhance the sector's digital resilience.

Generally, Nigeria's electricity sector showcases technological advancements for enhanced service delivery and operational resilience. From the adoption of advanced metering infrastructure to the integration of communication tools and digital resilience measures, organizations are proactively modernizing their operations. Despite these efforts, ongoing investments in scalable solutions, collaboration with service providers, and workforce skill development remain imperative for sustaining progress and effectively navigating future challenges. By prioritizing innovation and resilience-building initiatives, the sector can fortify its position

to meet the evolving demands of the nation's energy landscape and drive sustainable growth. This study undertakes a thorough investigation and a critical evaluation of the problems of digital resilience in the context of Nigeria's electricity sector.

2. Literature Review

It is impossible to overestimate the role that energy plays in promoting economic development in countries like Nigeria (Oyedepo, 2014). Today, technology is essential to both socioeconomic advancement and worldwide operations. Digital technologies are being used by critical infrastructure sectors increasingly to improve their services, yet this dependence creates vulnerabilities. Improving legislative and regulatory measures' cybersecurity and resilience in the electricity sector is becoming increasingly important on a global scale (Heymann, 2022). Like many other critical infrastructure companies, the Nigerian electricity sector uses technology for both power generation and distribution. Cybercriminals, however, pose a threat to cybersecurity due to the fact that they strive to get access to its digital infrastructure (Rothrock, 2018). The Nigerian power sector has changed and faced many difficulties throughout the years, reflecting the country's larger dynamics (Alley, 2016). The Nigerian power industry has adopted digital technology to enhance operations, much like other sectors. Cybercriminals have been regarded as a major threat to the industry, therefore there are cybersecurity issues associated with this increased reliance on digital technology (Mbamaluikem, 2016). Any human organization must effectively manage risk, which is defined as the possibility of undesirable events. In order to reduce risks and react positively to their effects, resilience is crucial as the future is dynamic and unpredictable. As per (Rehak, 2020) findings, the process of organizational innovation holds considerable importance in strengthening the resilience of essential infrastructure components. In article by (Nwaiwu, 2021) that focuses on the African location, the digitization of energy systems is investigated, and technologies like blockchain, digital platforms, and smart grids for enabling sustainable energy transitions are critically evaluated. The implementation of intelligent grids has resulted in increased power system efficiency; nevertheless, it also poses security risks related to natural disasters, cyberattacks, and physical attacks. Blackouts, privacy violations, and infrastructure failure can result from these attacks (Otuoze, 2018). While a number of studies have attempted to offer analyses of resilience definitions, evaluation standards, and improvement techniques, the works by (Gholami, 2018), (Jufri, 2019), (Hussain, 2019)) primarily concentrate on reviews and definitions of engineering and ecological resilience. Cybersecurity solutions must progress in tandem with the sector's continuous technological breakthroughs to tackle the escalating threats and vulnerabilities (Tagarev, 2021). The majority of the research on energy system resilience and how it intersects with energy security focuses on particular kinds of threats (Chandramowli, 2014) (Pryor, 2010), (Cadini, 2016), (Li). By detecting possible threats to the business, Business Continuity Management (BCM) is a complete process designed to enhance resilience and ensure effective response to protect the interests of key stakeholders, reputation, brand, and value-creating activities (Ekaette, 2006). Robust protection against cyberthreats must be put in place to address digital resilience in the electricity sector. A thorough cybersecurity plan should be based on standards like ISO/IEC 27001 or the NIST Cybersecurity Framework (Shen, 2014). The sector makes use of drills, training, and exercises to pinpoint assets that require reliability enhancements and to hone crisis response plans. While strategies differ according to resources and region, companies use comparable techniques to train staff for increased resilience (Berkeley, 2010. Based on a literature review (Poonen, 2018), (Jasiunas, 2021), the digital resilience of the electricity industry relies on crucial determinant factors vital for safeguarding power systems against potential threats and disruptions. Thus, the infrastructure management, organizational strategies, and cybersecurity system management are critical for maintaining digital resilience, according to literature insights and factors found.

3. Methodology

This paper adopts a pragmatic approach, relying on qualitative research methods to assess digital resilience in Nigeria's electricity sector. The research design includes stakeholder interviews to perform a survey as the primary data collection method, aligning with an ontological focus on real events and an epistemological belief in knowledge derived from human activities. A convergent mixed method design enhances the assessment depth. The primary data collection involves interviews with key stakeholders in the Nigerian electricity sector. Participants include senior officers from Electricity Distribution Companies (Discos) in Nigeria, and data is analysed using Nvivo 12 software. It was specifically used to investigate the themes and subthemes that emerged from the information gathered from questionnaire responses and stakeholder interviews. The qualitative data was analyzed using the thematic analysis approach, which made it possible to find patterns,

trends, and insights on digital resilience in Nigeria's electrical industry. This method made it easier to comprehend the intricate problems relating to digital resilience and made it possible to draw insightful conclusions. The questionnaire, refined through a pilot study, is administered on senior employees of electricity sector in Nigeria.

4. Results Discussion

In the dynamic landscape of Nigeria's electricity sector, technological adoption emerges as a critical catalyst for operational advancement and service optimization. However, this transition is not devoid of challenges, as stakeholders encounter a spectrum of obstacles inherent in the assimilation of new technologies. The journey towards technological integration is rife with complexities. Furthermore, the sector contends with the nuanced nuances of regulatory frameworks, infrastructural deficiencies, and the looming spectre of cybersecurity threats. Therefore, it becomes imperative to contextualize these challenges within the broader narrative of sectoral transformation, acknowledging their multifaceted impacts on operational efficacy and strategic planning. Interviews with stakeholders in the power industry have shown a number of obstacles to advancement in technology and efficiency in operations as shown in Table 3.1.

These issues come in many forms, such as poor communication between stakeholders that impedes effective information exchange. Furthermore, there is a clear reluctance to adopt new technologies, as evidenced by the widespread preference for human operations over automated ones. Additionally, there is a noticeable lack of IT proficiency among industrial workers, which hinders their capacity to handle and understand new technology. Concerns about cybersecurity have also surfaced, as incidences of fraudulent activity and illegal access have been reported, jeopardizing the security of the system and the financial integrity of the clients.

In addition, insufficient IT infrastructure and irregular internet connectivity in rural regions present formidable obstacles to the effective assimilation and application of novel technology. Patent rights for software used in the industry have also been a source of concern. This has resulted in longer wait times for software upgrades and maintenance, which has limited organizational control over software assets. The issues are made worse by inadequate training and awareness initiatives, which deprive staff of the essential knowledge on cyber dangers and appropriate software usage.

The dynamic nature of customer demands introduces an additional level of intricacy, necessitating prompt adaptation and response from the sector in order to maintain competitiveness. Furthermore, because physical and cyber infrastructure are integrated, there is an increased risk of external threats, which calls for strong cybersecurity measures. In addition to these difficulties, poor data management techniques have been found, which lead to inadequate decision-making procedures and lost chances for organizational expansion.

The lack of a well-defined approach to technology adoption and business planning exacerbates these issues, posing challenges for firms to successfully align their goals and leverage technological improvements. Employee satisfaction and sector performance are further hampered by a lack of specialized IT skills. Lastly, a major barrier to the sector's ability to safely and successfully use cutting-edge technologies for operational development and expansion is the absence of comprehensive industry and government policies around technology integration.

Table 3.1 : Identified challenges in the Electricity sector by the participants

Identified Challenge	Participant 1	Participant 2	Participant 3	Participant 4	Participant 5
Communication Breakdown		✓			
Technology-Related Fear	✓	✓			
Inadequate IT Skills			✓	✓	
Cyber Fraud Incidents			✓		✓
Lack of IT Infrastructure					✓
Lack of Internet Access		✓	✓	✓	
Lack of Patent Rights			✓		✓
Lack of Training and Awareness		✓			✓
Evolving Customer Needs			✓		
Increased Threats	✓			✓	

Ineffective Data Management		✓	✓		
Lack of a Defined Strategy				✓	✓
Lack of Dedicated IT Skills		✓		✓	
Lack of Policies			✓		✓

5. Approaches to Promote the Electricity Sector: Suggestions and Perspectives by the Participants

In order to effectively manage technical issues, the participants emphasized the vital need of having a highly skilled staff in the electric power industry. They stressed how important it is to have knowledgeable staff members who can identify, address, and anticipate technical challenges that the industry may face. A compelling recommendation was also made for the establishment of a strategy roadmap to address challenges in the electrical power sector. This plan should include early detection and quick fixes for problems, utilizing digitalization to expedite the process of identifying issues. It is believed that successfully navigating the quickly changing technical landscape in the electrical power industry requires a proactive and strategic strategy.

The necessity of ongoing training and retraining programs for human resources was emphasized because of how rapidly modern technologies are evolving. The adoption of continuing education programs to guarantee staff competency in using new technology was supported by the participants. In addition, they suggested adding certificates of participation and refresher courses to reward and acknowledge staff members who complete training.

Participants suggested an integrated approach to strengthen the security of systems within the energy power industry against cyber threats. Deploying programs with cutting-edge security features, such multifactor authentication modules and enterprise-wide digital security solutions, is part of this all-encompassing strategy. Other recommended actions included the use of SCADA systems for real-time monitoring and the identification and prevention of energy meter tampering in smart meters. It was highlighted that SMART Grid Security should be integrated with reporting sensors for power and electrical infrastructures in order to provide strong cybersecurity measures such authentication, tampering prevention, real-time monitoring, and strategic zoning.

Participants promoted cross-departmental cooperation in order to foster a security-conscious culture while addressing operational and geographic imbalances. They recommended industry-wide avenues for dissemination and emphasized the significance of good communication and technological understanding for issue resolution. It was also decided that creating a culture that could change with technology would be crucial, meaning that cooperation between the energy sector's stakeholders would be required to change perceptions about tech integration.

In addition, participants stressed the importance of giving priority to the deployment of customer-centric technologies in order to improve productivity and customer satisfaction. They advocated for the use of user-friendly technology and a "customer-first" approach, demonstrating a commitment to technical innovations that address the requirements and experiences of customers. In order to successfully integrate technology, participants emphasized the value of working as a team and integrating all relevant parties. It was determined that industry-wide cooperation was essential to maintaining IT and operational technology networks as well as real-virtual link protection.

Participants emphasized the need of regulatory oversight and the function that rules and regulations enforced by regulatory bodies play in guaranteeing thorough data gathering and knowledgeable advice. They also supported disruptive digital technology as a means of satisfying consumer needs and expanding markets, but they stressed that its implications for the electrical industry should be carefully considered. In order to lower risks in the ever-changing digital ecosystem, participants recommended proactive security measures and strategic intelligence on threats. To ensure cybersecurity resilience in the electrical power industry, it was determined that security considerations needed to be incorporated into choices about infrastructure and expansion.

6. Conclusion and Future Directions

This paper investigates the digital resilience landscape within Nigeria's electricity sector. The sector's strides in adopting advanced technologies for service delivery are commendable, yet the persistence of challenges such as communication breakdowns, cyber fraud, and technological hesitancy underscores the complexity of the digital transformation journey. These findings contribute to advancing understanding in the fields of digital resilience, cybersecurity, and organizational management by highlighting the nuanced interplay between technological adoption and resilience-building efforts.

Practical implications of the research findings are manifold, calling for strategic planning, investment in human resources, and robust cybersecurity measures. Addressing digital challenges, including evolving customer needs and insufficient IT skills, necessitates a holistic approach that encompasses human resource availability, targeted training initiatives, strategic roadmaps, and secure technology use.

Moving forward, recommendations for improvement encompass awareness strategies, customer-focused technology adoption, fostering a culture change, industry-wide collaboration, regulatory measures, and reflection on disruptive digital technology. Embracing digital resilience is pivotal for the sustainability and efficiency of Nigeria's electricity sector, offering opportunities for growth and innovation amidst challenges. Future research endeavours could explore the long-term impact of these measures, analyze global best practices, and assess economic implications, thus further enriching the scholarly discourse on digital resilience in the context of the electricity sector.

References

Adedeji, A. O. (2017). Privatisation and performance of electricity distribution companies in Nigeria. *Journal of Public Administration and Governance, 7*, 190--203.

Alley, I. a. (2016). Electricity supply, industrialization and economic growth: evidence from Nigeria. *International Journal of Energy Sector Management, 10*, 511--525.

Awosope, C. A. (2014). Nigeria electricity industry: issues, challenges and solutions. *Covenant University Public Lecture Series, 3*, 5--36.

Cadini, F. a. (2016). A Bayesian Monte Carlo-based algorithm for the estimation of small failure probabilities of systems affected by uncertainties. *Reliability Engineering \& System Safety*, 15--27.

Chandramowli, S. N. (2014). Impact of climate change on electricity systems and markets--A review of models and forecasts. *Sustainable Energy Technologies and Assessments, 5*, 62--74.

(2015). *CYBERCRIME ACT.*

Ekaette, E. U.-L. (2006). Risk analysis in radiation treatment: application of a new taxonomic structure. *Radiotherapy and Oncology, 80*, 282--287.

Gholami, A. a. (2018). Toward a consensus on the definition and taxonomy of power system resilience. *IEEE Access, 6*, 32035--32053.

Heymann, F. e. (2022). Cybersecurity and resilience in the swiss electricity sector: Status and policy options. *Utilities Policy, 79*, 101432.

Hussain, A. a.-H.-M. (2019). Microgrids as a resilience resource and strategies used by microgrids for enhancing resilience. *Applied energy, 240*, 56--72.

Jasiunas, J. a. (2021). Energy system resilience--A review. *Renewable and Sustainable Energy Reviews*, 111476.

Jufri, F. H. (2019). tate-of-the-art review on power grid resilience to extreme weather events: Definitions, frameworks, quantitative assessment methodologies, and enhancement strategies. *Applied energy, 239*, 1049--1065.

Li, Y. a. (n.d.). Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. *Accident Analysis \& Prevention, 121*, 148--156.

Mbamaluikem, P. a. (2016). *AN OVERVIEW OF SMART GRID: A NECESSARY SYSTEM FOR NIGERIAN TODAY AND FUTURE ELECTRICITY.*

Nwaiwu, F. (2021). Digitalisation and sustainable energy transitions in Africa: assessing the impact of policy and regulatory environments on the energy sector in Nigeria and South Africa. *Energy, Sustainability and Society, 11*, 1--16.

Onuoha, K. C. (2010). The electricity industry in Nigeria: What are the challenges and options available to improve the sector? *Available at SSRN 1664788*.

Otuoze, A. O. (2018). Journal of Electrical Systems and Information Technology. *Smart grids security challenges: Classification by sources of threats.*, 468-483.

Oyedepo, S. O. (2014). Towards achieving energy for sustainable development in Nigeria. *Renewable and sustainable energy reviews , 34*, 255--272.

Poonen, J. a. (2018). Application of cyber resilience review to an electricity company. In *ECCWS 2018: proceedings of the 17th European conference on cyber warfare and security* (pp. 380--389).

Pryor, S. C. (2010). Climate change impacts on wind energy: A review. *Renewable and sustainable energy reviews, 14*.

Rehak, a. D. (2020). Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. *Safety Science, 123*, 104573.

Rothrock, R. A. (2018). *Digital Resilience: What You can Do—now.* Amacom.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer, 10*, 16.

Tagarev, T. (2021). Understanding hybrid influence: emerging analysis frameworks. *Digital Transformation, Cyber Security and Resilience of Modern Societies*, 449--463.