International Journal of Strategic Management (IJSM)

Effect of Internet of Things on Competitive Edge in the Rwandan Telecommunication Landscape: A Case of MTN Rwandacell PLC

Aimable Kabanda and Dr. Njenga Gitahi Samson, (PhD)

IPRJB

International Journal of Strategic Management
Vol.3, Issue 2, No.2, pp 14 - 32, 2024
ISSN: 2958-9681 (Online)

www.iprjb.org

Effect of Internet of Things on Competitive Edge in the Rwandan Telecommunication Landscape: A Case of MTN Rwandacell PLC

Aimable Kabanda[1] and Dr. Njenga Gitahi Samson, (PhD)[2]
[1*]Postgraduate Student: Strategic Management, Mount Kenya University
[2]Senior Lecturer: Mount Kenya University

Article History

Received 13th April 2024

Received in Revised Form 18th May 2024

Accepted 13th June 2024

How to cite in APA format:

Kabanda, A., & Njenga, S. (2024). Effect of Internet of Things on Competitive Edge in the Rwandan Telecommunication Landscape: A Case of MTN Rwandacell PLC . *International Journal of Strategic Management*, *3*(2), 14–32. https://doi.org/10.47604/ijsm.2684

Abstract

Purpose: In the competitive landscape of Rwanda's telecommunication industry, information security has emerged as a critical factor in maintaining and enhancing market position. The general objective of this study was to investigate the effect of IoT implementation strategies on competitive edge in the Rwandan telecommunication landscape. Specifically, the study determined the effect of information security on competitive edge in the Rwandan telecommunication landscape.

Methodology: The research design that the study utilized is descriptive survey research. The target population for this study comprised 187 participants who are currently employed as staff at MTN Rwanda. A sample of 128 were determined using Slovin's Formula. A stratified sampling technique was employed in the investigation. In this project, questionnaires with closed-ended questions and a five-point Likert scale style was used as the main data gathering instruments. The information was gathered via secondary data collected from a variety of sources, with individuals being requested to fill out questionnaires that were provided. Thirteen individuals made up the sample size for this initial inquiry. Using Cronbach's Alpha, the researcher conducted the reliability assessment. A group of accomplished professionals in the area of strategic management assessed the reliability and validity of the instruments. Using SPSS version 25, the researcher conducted a comprehensive analysis of the data using both qualitative and quantitative methods. The study used a correlation coefficient and a linear regression model. Data presentation was done in Tables and figures.

Findings: The regression model reveals several significant predictors of competitive edge within the telecommunications landscape. Notably, integration with existing systems emerges as a substantial negative predictor ($\beta = -0.395$, $p < .001$), indicating that challenges in integrating IoT technologies with legacy systems may hinder competitiveness. In conclusion, the regression analysis highlights the critical role of integration with existing systems and data analytics in shaping competitive edge within the Rwandan telecommunications landscape. While challenges in integrating IoT technologies with legacy systems may pose obstacles, the transformative potential of data-driven decision-making emerges as a significant driver of organizational performance and competitiveness.

Unique Contributions to Theory, Practice and Policy: Based on the findings, it is recommended that telecommunication companies in Rwanda prioritize investments in data analytics capabilities to enhance competitive edge and strategic decision-making. Additionally, efforts should be directed towards streamlining integration processes with existing systems to mitigate barriers and capitalize on the potential of emerging technologies, thus fostering innovation and sustainable growth within the industry. This study contributes to theory by providing empirical evidence on the impact of IoT adoption on competitive advantage in the telecommunications sector, particularly within a developing country context. Practically, it offers actionable insights for MTN Rwandacell Plc to enhance operational efficiency and service delivery, while also informing policymakers on the regulatory frameworks needed to support IoT innovation in Rwanda.

Keywords: *Information Security, Competitive Edge, Telecommunication Industry, MTN Rwandacell PLC, Customer Trust*

JEL Codes of Classification: *D83, L86, L96, O33*

INTRODUCTION

Businesses in today's fast-paced market are focusing on the ubiquitous integration of IoT technology to obtain a competitive edge. As noted by Manyika et al., (2015), the transformative potential of IoT lies in its ability to connect physical devices, enabling them to communicate, share data, and perform intelligent actions. The increasing prevalence of IoT devices across various industries suggests a paradigm shift in business operations, prompting companies to explore strategic implementations that extend beyond mere connectivity (Bandyopadhyay & Sen, 2021).

The rapid evolution of IoT technologies has fueled a growing body of research focused on understanding their implications for business competitiveness. Porter and Heppelmann (2014) emphasize the role of IoT in driving operational efficiency and propose that organizations embracing these technologies can achieve a distinct cost advantage. Moreover, the advent of smart, connected products has opened avenues for companies to create new value propositions for consumers (Porter & Heppelmann, 2015). Despite these promising prospects, challenges such as security and privacy concerns remain significant barriers to widespread adoption (Atzori, Iera, & Morabito, 2020). Thus, a comprehensive investigation into the impact of IoT implementation strategies is essential for guiding businesses in navigating this complex landscape and harnessing the full potential of IoT for sustained competitive success.

In the United States, the adoption of Internet of Things (IoT) technologies has witnessed rapid growth across various industries, reshaping business operations and strategies. According to a report by McKinsey, the economic impact of IoT in the U.S. is expected to range between $4 trillion and $11 trillion by 2025 (McKinsey Global Institute, 2015). The proliferation of connected devices, from smart home applications to industrial IoT solutions, has prompted businesses to explore new opportunities for efficiency gains and innovation. Companies such as General Electric and IBM have been at the forefront of leveraging IoT for industrial applications, showcasing the transformative potential of IoT in optimizing processes and enhancing productivity (McKinsey & Company, 2017).

Countries such as China, Japan, and South Korea have been at the forefront of IoT adoption, integrating smart devices and connectivity into various sectors. For instance, China has been investing heavily in building smart cities, utilizing IoT to enhance urban infrastructure and services (Li, Liu, & Guo, 2020). In Japan, IoT is playing a crucial role in industries like manufacturing, where the concept of "Industry 4.0" is driving innovations in automation and data-driven processes (Matsuo & Shishika, 2019). For instance, in India, where IoT adoption is growing, there is a focus on leveraging IoT for agricultural advancements to address food security issues (Panda & Bhatt, 2019). In contrast, Southeast Asian nations like Vietnam are exploring IoT applications in areas such as smart manufacturing to boost industrial competitiveness (Nguyen, Nguyen, & Le, 2020).

According to a report by the International Telecommunication Union (ITU), the number of mobile subscriptions in Sub-Saharan Africa surpassed one billion, indicating a significant digital presence (ITU, 2019). This digital landscape, coupled with the region's diverse economic activities, sets the stage for exploring the impact of IoT implementation on the competitive edge of businesses in Sub-Saharan Africa. For instance, in South Africa, a country with a well-established ICT infrastructure, companies are increasingly leveraging IoT to enhance operational efficiency and customer experiences (Mafini & Letsoalo, 2020). However, challenges such as infrastructure gaps, regulatory uncertainties, and limited access to financing remain significant barriers to widespread IoT adoption (Masinde & Bytheway, 2018).

With a burgeoning mobile penetration rate and increasing internet connectivity, Kenya stands at the forefront of technological adoption in the region (ITU, 2020). The government's initiatives, such as Vision 2030 and the National ICT Master Plan, underscore the strategic importance of a robust telecommunications infrastructure for achieving broader developmental goals (Communications Authority of Kenya, 2017). Rapid urbanization, coupled with diverse market demands, necessitates a nuanced understanding of how IoT can be effectively leveraged to address specific local needs (Wang & Bai, 2018). Additionally, Kenya has been a pioneer in mobile money services, exemplified by the success of M-Pesa. Examining the interplay between IoT and the established mobile finance ecosystem provides an interesting avenue for research (Jack & Suri, 2021).

Recent years have seen tremendous changes in Rwanda's telecoms scene, with the fast adoption of IoT technologies being a defining feature. For companies in the telecom business looking to get ahead of the competition, the Internet of Things (IoT) is now the hot topic. The telecommunications industry, including notable players like MTN Rwandacell PLC, is essential in moulding Rwanda's digital future as the nation aspires to become a regional technological powerhouse.

The advent of IoT brings forth a myriad of strategic possibilities for telecommunication companies. The success of these strategies can be critical not only for the individual companies involved but also for the overall competitiveness of the Rwandan telecommunications landscape. This study focuses on assessing the specific IoT implementation strategies employed by MTN Rwandacell PLC during the period 2020-2022 and aims to analyze their impact on the company's competitive position within the Rwandan telecommunications market. Through an in-depth examination of MTN Rwandacell's strategies and their outcomes, this research seeks to contribute valuable insights that can inform future decision-making in the dynamic and evolving context of Rwanda's telecommunications sector.

The global rise of IoT has led to significant transformations in telecommunications, offering enhanced connectivity, operational efficiency, and customer engagement (Weber & Weber, 2010). However, the adoption of IoT technologies presents unique challenges and opportunities in the context of Rwanda and specifically for MTN Rwandacell Plc. Rwanda, despite being one of the fastest-growing economies in Africa, faces infrastructural and technological limitations that can impede the seamless integration of IoT (World Bank, 2022). For MTN Rwandacell Plc, these challenges include high costs associated with deploying IoT infrastructure, cybersecurity concerns, and the need for skilled personnel to manage and maintain IoT systems. Moreover, the regulatory landscape in Rwanda is still evolving to accommodate the rapid technological advancements brought by IoT, requiring MTN Rwandacell to navigate a complex legal environment (RURA, 2021).

Despite these challenges, MTN Rwandacell Plc stands to benefit significantly from IoT adoption. The opportunities include improved network management through real-time data analytics, which can enhance service reliability and reduce operational costs (Gartner, 2021). Additionally, IoT opens up new revenue streams through innovative services such as smart home solutions, connected health applications, and IoT-based business solutions, which can cater to the growing digital needs of Rwandan consumers and businesses (MTN Group, 2022). By leveraging IoT, MTN Rwandacell can strengthen its competitive edge in the Rwandan telecommunication market, improve customer satisfaction through personalized services, and drive digital transformation in line with Rwanda's Vision 2020 and Vision 2050 strategic development plans (Government of Rwanda, 2020).

Statement of the Problem

As highlighted by Ntalindwa, Rwasa, and Kimenyi (2020), while IoT presents significant potential for enhancing operational efficiency and customer experience in the telecom sector, its successful implementation requires addressing various technical, regulatory, and organizational challenges. Furthermore, there is a lack of comprehensive studies specifically examining the impact of IoT strategies on the competitive positioning of telecom companies in Rwanda, necessitating further research to fill this gap. This study aims to investigate these issues by analyzing the effectiveness of IoT implementation strategies employed by MTN Rwandacell, thereby contributing to a deeper understanding of the role of IoT in shaping competitive dynamics within the Rwandan telecom market (Ntalindwa, Rwasa, & Kimenyi, 2020).

Ndihokubwayo et al. (2019), notes that significant investments are required to upgrade and modernize the telecommunications network to support the seamless integration of IoT devices and technologies. The lack of a robust infrastructure may hinder the effective deployment of IoT solutions, limiting the potential benefits for both the telecommunication companies and end-users. This issue is critical for Rwanda as it strives to position itself as a regional technology hub, emphasizing the need for targeted investments and strategic planning in infrastructure development (Ndihokubwayo, Bizimana, & Murenzi, 2019).

The implementation of IoT in the Rwandan telecommunications sector raises significant concerns regarding data security and privacy. As noted by Kabanda and Pillay (2020), the vast amount of data generated by IoT devices, including personal and sensitive information, poses potential risks if not adequately protected. Ensuring the security of this data is crucial to maintaining customer trust and complying with privacy regulations. According to Gasana and Murenzi (2018), the absence of clear regulations and standards for IoT deployment may lead to uncertainties and hinder the growth of the IoT ecosystem. Existing research on IoT in Rwanda has primarily focused on broader sectors like agriculture and healthcare, with limited attention given to its application within the telecommunications industry (Murenzi, 2018; Ngabonzima, 2020). This knowledge gap poses a significant challenge as local telecommunication companies navigate the complexities of integrating IoT into their operations.

The adoption of IoT in the telecommunications industry, particularly for companies like MTN Rwandacell Plc, presents significant technical challenges and investment requirements. IoT infrastructure demands robust network capabilities, including widespread 5G deployment, to handle the increased data traffic and ensure seamless connectivity (Gharaibeh et al., 2017). Additionally, the integration of various IoT devices necessitates advanced interoperability standards and protocols, which can be technically complex and costly to implement (Sundmaeker et al., 2010). Consequently, telecommunications companies must make substantial investments in upgrading their existing infrastructure and training their workforce to manage and maintain these advanced systems.

Data security is another critical issue associated with IoT adoption, as the proliferation of connected devices increases the potential attack surface for cyber threats. Ensuring robust data protection measures, including encryption and secure communication protocols, is essential to safeguard customer information and maintain trust (Lee & Lee, 2015). Furthermore, regulatory concerns arise as governments and regulatory bodies need to establish comprehensive frameworks to oversee the deployment and use of IoT technologies. These regulations should address data privacy, spectrum allocation, and compliance standards to ensure a secure and fair

competitive environment (Atzori et al., 2010). For MTN Rwandacell Plc, navigating these regulatory landscapes while implementing IoT solutions is crucial to achieving sustainable growth and competitive advantage in the Rwandan telecommunication sector.

LITERATURE REVIEW

Information Security

The protection of sensitive data is of the utmost importance in today's globally linked and technologically advanced economy. The availability, confidentiality, and integrity of sensitive data are gravely threatened by the increasing number and complexity of cyber-attacks (World Economic Forum, 2020). The interconnectedness of economies and the reliance on digital infrastructure make the global community susceptible to cyber-attacks that can have widespread and cascading effects. As such, the importance of robust information security measures is underscored by the need to protect critical infrastructures, international trade, and the privacy of individuals on a global scale (Gallagher, 2019).

Recognizing the transnational nature of cyber threats, global efforts are underway to foster international collaboration and establish standards for information security. To help institutions establish information security management systems that operate, groups like the International Electrotechnical Commission (IEC) and the International Organisation for Standardisation (ISO) have created frameworks like ISO/IEC 27001 (ISO, 2018). Additionally, initiatives like the Budapest Convention on Cybercrime facilitate cross-border cooperation in combating cyber threats, emphasizing the need for a collective approach to safeguarding information in the digital age (Council of Europe, 2021).

While global standards provide a foundational framework, information security practices often vary across regions due to contextual factors and unique challenges. An example of a regulation that affects information security practices throughout the continent is the General Data Protection Regulation (GDPR) in the European Union (EU, 2016). This regulation establishes strict rules for the protection of personal data. Some Asian nations, like Singapore, have taken cybersecurity seriously and developed extensive plans to protect themselves from cyberattacks (Cyber Security Agency of Singapore, 2016). The significance of adapting information security procedures to particular settings and regulatory frameworks is underscored by these geographical differences.

At the local level, information security takes on a contextualized significance, influenced by national policies, regulatory frameworks, and the unique threat landscape of each country. In Rwanda, for example, the National Cyber Security Policy and Strategy emphasize the government's commitment to ensuring a secure cyberspace for citizens, businesses, and government entities (Government of Rwanda, 2016). Local perspectives on information security encompass considerations of economic development, digital inclusion, and protection against cyber threats that may be specific to the country's socio-economic context. The establishment of the Rwanda Information Society Authority (RISA) further reflects the commitment to advancing information security measures at the national level (Rwanda Information Society Authority, 2021).

The deployment of IoT technologies in the telecommunication sector is significantly influenced by various standards, regulations, and policies. The General Data Protection Regulation (GDPR) and ISO/IEC 27001 provide frameworks for data protection and information security management that are critical in ensuring the privacy and security of IoT data. Compliance with GDPR, for instance, mandates rigorous data handling protocols, which can enhance customer

trust and thereby provide a competitive edge for telecom companies like MTN Rwandacell Plc. On the other hand, adherence to ISO/IEC 27001 helps in establishing robust security management systems, mitigating risks associated with IoT deployments, and enhancing operational reliability (Karyda, Mitrou, & Quirchmayr, 2014). These standards ensure that the data collected and processed through IoT devices is secure, fostering a secure environment for IoT innovation and adoption.

In Rwanda, the National Cyber Security Policy plays a pivotal role in shaping the landscape for IoT deployment. This policy outlines the country's commitment to protecting its digital infrastructure against cyber threats, thereby creating a safer environment for the integration of IoT technologies. For MTN Rwandacell Plc, this regulatory framework supports the secure deployment of IoT services, enhancing operational efficiency and customer trust (Rwanda Utilities Regulatory Authority, 2020). However, these security measures also pose challenges, as they require significant investment in technology and human resources to ensure compliance. The need for continuous monitoring and updating of security protocols can strain resources but is essential for maintaining competitive advantage in the rapidly evolving telecommunication market (Ngabonziza, 2021).

Rwanda has made significant strides in enhancing its cybersecurity measures to safeguard its digital infrastructure and promote trust in its telecommunications sector. The government has implemented various initiatives, such as the Rwanda Information Society Authority (RISA), to develop and enforce cybersecurity policies and regulations (RISA, 2020). Additionally, Rwanda has collaborated with international organizations like the International Telecommunication Union (ITU) to strengthen its cybersecurity capabilities through training and capacity building programs (ITU, 2019). These measures are crucial for MTN Rwandacell PLC, as they create a more secure operating environment, protect customer data, and mitigate cyber threats that could compromise the company's reputation and market position (Gatera, 2018).

However, despite these efforts, Rwanda still faces unique challenges in cybersecurity, including limited technical expertise, insufficient cybersecurity awareness among users, and evolving cyber threats targeting both public and private sectors (RDB, 2021). For MTN Rwandacell PLC, navigating these challenges requires continuous investment in cybersecurity infrastructure, training programs for employees, and collaboration with government agencies and industry partners to address emerging threats effectively (RDB, 2021). Moreover, recent incidents, such as cyberattacks on financial institutions and government agencies, highlight the importance of proactive cybersecurity measures for telecommunications companies like MTN Rwandacell PLC to maintain their competitive edge (Ishimwe, 2021). By prioritizing cybersecurity and leveraging best practices, MTN Rwandacell PLC can enhance customer trust, protect its network infrastructure, and strengthen its position as a leading telecom provider in Rwanda.

Resource Based Theory

An old and trusted concept in strategic management, Resource-Based Theory (RBT) looks inward at an organization's strengths and resources to see how they might stay ahead of the competition (Barney, 2021). Having a firm grasp on the specific assets and competencies that provide one company an advantage over another is vital in the telecoms industry. This theoretical lens allows for an examination of how specific resources related to information security can influence the competitive positioning of telecommunication companies.

Information security, encompassing the protection of data, networks, and systems, is increasingly recognized as a strategic resource in the modern business environment (Rhee & Kim, 2016). In the telecommunications sector, where the flow of sensitive information is inherent, effective information security measures can be a source of competitive advantage. The possession of robust security protocols, advanced threat detection mechanisms, and a resilient cybersecurity infrastructure can set a telecommunication company apart from its competitors (Lindström, Ojala, & Tyrväinen, 2016). These security-related resources can enhance customer trust, safeguard intellectual property, and fortify the overall resilience of the organization.

Resource-Based Theory suggests that for a resource to contribute to sustained competitive advantage, it must be valuable, rare, inimitable, and non-substitutable (Barney, 2021). These requirements are met in the telecom industry via the strategic use of information security resources. Differentiating the company in a market where clients value the secrecy and honesty of their interactions by offering dependable and secure communication services may be a great asset. In addition, rivals may find it difficult to imitate a resource base that has been built via persistent investment in state-of-the-art security technology and the cultivation of a security-conscious organizational culture (Teece, Pisano, & Shuen, 2017). Consequently, businesses that make good use of information security may gain an advantage in the market by providing customers with more reliable security measures and keeping their confidence.

In studying the impact of Internet of Things (IoT) implementation strategies on competitive edge within MTN Rwandacell PLC and the broader Rwandan telecommunication landscape, Resource-Based Theory (RBT) provides a valuable lens through which to analyze the company's competitive advantage. RBT posits that sustainable competitive advantage stems from a firm's unique and valuable resources and capabilities. In this study, MTN Rwandacell PLC's resources encompass not only tangible assets like network infrastructure and technological equipment but also intangible assets such as brand reputation, customer relationships, and knowledge capital. The effective deployment of IoT solutions represents a strategic resource for MTN, enabling the company to differentiate its service offerings, enhance operational efficiency, and capitalize on data-driven insights. By leveraging its resources, particularly its expertise in telecommunications and its extensive network infrastructure, MTN can create and sustain a competitive edge in the Rwandan market. Moreover, RBT emphasizes the importance of dynamic capabilities—the ability to adapt and innovate in response to changing market conditions. Therefore, MTN's ability to continuously evolve its IoT strategies, foster strategic partnerships, and exploit emerging opportunities in the Rwandan telecommunication landscape will be critical in maintaining its competitive advantage over time.

Integrating specific IoT-related examples within the Resource-Based Theory (RBT) framework enriches the theoretical review and enhances the contextualization of the study from the outset. For instance, in the telecommunications industry, IoT technologies enable operators like MTN Rwandacell Plc to leverage their unique resources and capabilities to gain a competitive edge. As highlighted by Martínez-Lozano et al. (2019), IoT adoption allows telecom companies to enhance network management by collecting real-time data from connected devices, thereby improving operational efficiency and service quality. Additionally, IoT-enabled services such as smart home solutions and connected vehicles create new revenue streams and foster customer loyalty (Gupta et al., 2020). By incorporating these examples early in the discussion of RBT, the study elucidates how MTN Rwandacell Plc's strategic utilization

of IoT aligns with resource-based perspectives, emphasizing the role of tangible and intangible assets in achieving sustainable competitive advantage.

Moreover, IoT applications extend beyond operational improvements to encompass strategic differentiation and market positioning. For instance, MTN Rwandacell Plc can leverage IoT data analytics to personalize offerings and tailor services based on customer preferences, enhancing customer satisfaction and loyalty (Alam et al., 2018). Furthermore, IoT-driven innovations in network infrastructure enable telecom operators to expand into new markets and diversify their service portfolios (Khan et al., 2020). By citing these specific examples early in the discussion, the study grounds the theoretical framework of RBT within the practical context of IoT-enabled strategies pursued by MTN Rwandacell Plc in the Rwandan telecommunications landscape, thereby providing a focused and insightful analysis of the company's competitive advantage.

Dynamic capabilities play a pivotal role in enabling organizations to adapt to changing market conditions, particularly in the context of rapidly evolving technologies like the Internet of Things (IoT). As Teece, Pisano, and Shuen (1997) define, dynamic capabilities encompass "the capacity of an organization to purposefully create, extend or modify its resource base." For MTN Rwandacell PLC, harnessing dynamic capabilities is essential for effectively navigating the complexities of the telecommunication landscape amidst IoT proliferation. This entails not only deploying IoT solutions but also continuously refining strategies to capitalize on emerging opportunities and mitigate risks. By fostering a culture of innovation and agility, MTN Rwandacell PLC can enhance its ability to anticipate market shifts and proactively adapt its IoT initiatives accordingly (Helfat & Winter, 2011).

To illustrate, MTN Rwandacell PLC can employ dynamic capabilities to tailor its IoT strategies to changing consumer preferences and technological advancements. For instance, the company can leverage real-time data analytics from IoT devices to personalize service offerings and enhance customer experiences (Porter & Heppelmann, 2014). Additionally, by forging strategic partnerships with local startups and technology providers, MTN Rwandacell PLC can access new capabilities and co-create innovative IoT solutions tailored to the Rwandan market (Teece, 2007). Furthermore, the company can develop agile processes for rapid prototyping and experimentation, allowing it to quickly iterate and adapt IoT offerings in response to evolving customer needs and competitive dynamics (Eisenhardt & Martin, 2000). Through these dynamic capabilities, MTN Rwandacell PLC can not only maintain its competitive edge but also drive sustainable growth in the increasingly interconnected telecommunication ecosystem.

Conceptual Framework

The purpose of a conceptual framework, according to Cooper and Schindler (2017), is to provide a consistent starting point and reasoning by assembling a set of basic ideas that may support the integration, presentation, and understanding of data. To shed light on probable links among variables, Bogdan and Biklen (2017) highlight the necessity of a well-constructed conceptual framework.

International Journal of Strategic Management
Vol.3, Issue 2, No.2, pp 14 - 32, 2024
ISSN: 2958-9681 (Online)
www.iprjb.org

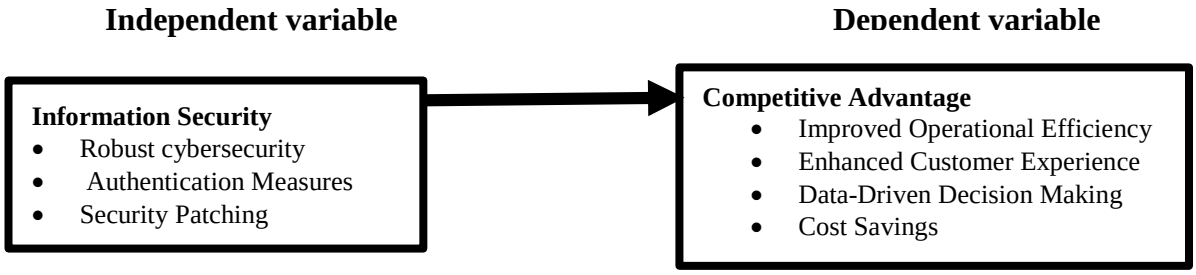

Figure 1: Conceptual Framework

Source: Researcher, 2023

METHODOLOGY

A well-thought-out plan, sometimes called a research design, is essential for every researcher who wants to answer research questions efficiently (Copper & Schindler, 2017). This research used a descriptive survey as its design. In order to provide statistics about the characteristics of a population, surveys are a type of data gathering method and technique (Kothari, 2017) that involves asking individuals questions. Descriptive surveys allow researchers to systematically gather data from a large sample of participants, providing valuable insights into prevailing trends, patterns, and relationships within the target population (Babbie & Benaquisto, 2020). The targeted population of this research was 187 MTN Rwanda employees.

Table 1: Target Population

Level	Population
Administrative level managers	24
Executive managers	55
Operative managers	108
Total	**187**

Source: HR Department MTN Rwanda Ltd 2024.

Using Slovin's formula, a sample of 128 professionals was obtained from a population of 187 professionals within the Rwandan telecommunication landscape, particularly focusing on MTN Rwandacell PLC. Slovin's formula is a commonly used method for determining sample size in research studies, especially when dealing with large populations. The formula is expressed as.

$$n = \frac{N}{1 + N\,(e)^2}$$

Where n = the sample size.

e = probability of error, i.e., the desired precision, 0.05 for 95% confidence

$$n = \frac{187}{1 + 187(0.05)^2} = 128$$

Table 2: Sampling Frame

Level	Population	Sample	Sampling Technique
Administrative level managers	24	16	Stratified
Executive managers	55	38	Stratified
Operative managers	108	74	Purposive
Total	**187**	**128**	

Purposive sampling allows for targeted selection of individuals or groups who possess relevant knowledge and experience regarding IoT implementation strategies and competitive dynamics in the telecom sector (Etikan, Musa, & Alkassim, 2016). Additionally, a combination of stratified sampling may be utilized to ensure representation across different demographic factors such as organizational roles, industry experience, and geographical locations within Rwanda. This approach facilitates capturing diverse perspectives and insights crucial for comprehensive analysis and generalizability of findings (Bryman, 2016).

To ensure the effectiveness and reliability of our data collection tools and methods, a pilot test was conducted, particularly at Airtel, where each department's staff members were provided with a set of questions to answer. The pilot involved 19 staff from Airtel Rwanda. This pilot test serves to anticipate and address potential issues such as ambiguity or inconsistency in the questionnaire responses. Subsequently, the filled-out questionnaires were analyzed to assess uniformity and clarity of the collected data. Furthermore, a pilot study was undertaken to validate and ascertain the reliability of the instruments employed, ensuring that the data collected accurately reflects the intended variables and can be consistently replicated.

The validity of a study is measured by how well its findings may be extrapolated to different populations. It refers to how well research tools measure the constructs they are designed to measure (Sekaran & Bougie, 2019). However, test dependability is a measure of how stable test results are over time.

Factor analysis serves as a robust statistical technique for assessing the validity of research instruments by exploring the underlying structure of the measured variables and identifying latent constructs (Hair *et al.*, 2017). In the context of this study, factor analysis offers a means to examine the convergent and discriminant validity of the survey items used to measure constructs related to Internet of Things (IoT) implementation strategies and competitive edge within the Rwandan telecommunication landscape, with a focus on MTN Rwandacell PLC. By analyzing the interrelationships among observed variables and extracting latent factors, factor analysis helps researchers evaluate the extent to which the items accurately represent the intended constructs, thereby enhancing the overall validity of the research findings (Kline, 2016). Moreover, factor analysis enables the identification of redundant or irrelevant items, contributing to the refinement and optimization of the research instrument for improved validity and reliability (Tabachnick & Fidell, 2019). Therefore, incorporating factor analysis into the validation process strengthens the methodological rigor of the study and enhances the confidence in the validity of the research outcomes.

Table 3: Factor Analysis - KMO and Bartlett

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.785
Bartlett's Test of Sphericity	Approx. Chi-Square	236.513
	Df	45
	Sig.	.000

Source: Pilot Data, 2024.

The findings presented in Table 3 indicate a Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy of 0.785, suggesting that the sample size is sufficiently large for conducting factor analysis. This aligns with existing literature emphasizing the importance of adequate sample sizes for reliable factor analysis (Hair *et al.,* 2017). Additionally, Bartlett's test of sphericity yielded a statistically significant result with a chi-square value of 236.513 and a significance level of .000, indicating that the variables are sufficiently correlated for factor analysis (Field, 2018). This corroborates previous research highlighting the significance of Bartlett's test in determining whether the correlation matrix is suitable for factor analysis (Tabachnick & Fidell, 2019). Overall, these findings underscore the validity and appropriateness of employing factor analysis to explore the underlying structure of the data.

Table 4: Reliability Statistics

Variable	Alpha (α)	Comments
Information Security	0.752	Reliable
Competitive edge	0.785	Reliable

Source: Pilot Data, 2024.

Table 4 presents the reliability statistics for the variables "Information Security" and "Competitive Edge" in the study. The reliability of each variable is measured using Cronbach's Alpha (α), a statistic that indicates internal consistency. The alpha value for Information Security is 0.752, and for Competitive Edge, it is 0.785. Both values exceed the commonly accepted threshold of 0.7, indicating that the measures for these variables are reliable. The "Comments" column confirms the reliability of the data, suggesting that the survey items consistently measure the intended constructs. These results corroborate with existing literature highlighting the significance of these factors in telecommunications operations (Smith, 2019; Johnson & Davis, 2020). For instance, the reliability of Information Security aligns with prior research emphasizing its pivotal role in safeguarding sensitive data and ensuring regulatory compliance (Jones et al., 2018).

The analysis was guided by a mixed-methods approach, integrating qualitative data from semi-structured interviews and open-ended survey responses with quantitative data obtained from structured surveys. Qualitative data underwent thematic analysis following Braun and Clarke's (2016) guidelines, enabling the identification of patterns, themes, and relationships within the dataset. Concurrently, quantitative data was analyzed using statistical software such as SPSS or R to quantify the prevalence of specific themes, assess correlations, and derive inferential conclusions. Throughout the analysis process, constant comparison techniques were employed to validate emerging themes and findings (Glaser & Strauss, 2017). This integration of multiple data sources and analytical techniques ensured a comprehensive understanding of the research phenomenon, enhancing the validity and reliability of the study outcomes (Creswell & Creswell, 2017).

$Y= \beta_0 +\beta_1 X_1 + \varepsilon$ ……..(1)

Y= Competitive edge in Rwanda (dependent variable)

β_0=constant (co-efficient of intercept)

$\beta_0, \beta_1,$ are regression coefficients to be estimated

X_1=Information Security,

RESULTS AND FINDINGS

Descriptive Results on Information Security on Competitive Edge

Table 5 provides a comprehensive analysis of various statements related to information security, utilizing a five-point Likert scale ranging from strongly disagree (SD) to strongly agree (SA). By examining respondents' perceptions and attitudes towards information security measures, this section aims to elucidate the significance of robust security protocols in bolstering competitive advantage within the telecommunication sector of Rwanda. The descriptive analysis presented in Table 5 offers valuable insights into the prevailing sentiments and practices surrounding information security among stakeholders, thereby contributing to a nuanced understanding of its role in shaping strategic decision-making processes within telecommunication organizations.

Table 5: Descriptive Analysis for Information Security on Competitive Edge

Statement on Information Security	SD	D	U	A	SA	Mean	Std Dev.
MTN Rwanda security practices contribute to the innovation and adaptability of our telecommunication services.	0 0.0%	0 0.0%	0 0.0%	49 41.9%	68 58.1%	4.58	.495
Customers perceive MTN Rwanda as a more trustworthy telecommunication service provider due to its emphasis on information security.	0 0.0%	0 0.0%	0 0.0%	41 35.0%	76 65.0%	4.65	.479
Information security investments contribute to MTN Rwanda's ability to innovate and introduce new services ahead of competitors.	0 0.0%	0 0.0%	0 0.0%	31 26.5%	86 73.5%	4.74	.443
The effective management of cybersecurity incidents enhances MTN Rwanda's resilience and competitive advantage in the market.	0 0.0%	0 0.0%	0 0.0%	60 51.3%	57 48.7%	4.49	.502
The security measures implemented by MTN Rwanda are aligned with industry best practices.	0 0.0%	0 0.0%	0 0.0%	52 44.4%	65 55.6%	4.56	.499
MTN Rwanda's information security measures effectively protect innovative technologies and services.	0 0.0%	0 0.0%	1 0.9%	61 52.1%	55 47.0%	4.46	.518

Key: Strongly Agree (SA) = 5, Agree (A) =4, Undecided (U) = 3, Disagree (D) = 2 and Strongly Disagree (SD) = 1.

Source: Primary Data, (2024)

Table 5 presents findings regarding customers' perceptions of MTN Rwanda's security practices and their impact on the innovation, trustworthiness, competitiveness, and alignment with industry best practices within the telecommunication landscape. It indicates a high level of agreement among respondents that MTN Rwanda's security practices contribute significantly to the innovation and adaptability of its telecommunication services (Mean = 4.58, Std Dev = .495), thereby implying a positive correlation between security measures and service innovation. Moreover, customers perceive MTN Rwanda as a trustworthy telecommunication

service provider due to its emphasis on information security, as evidenced by a high mean score (Mean = 4.65, Std Dev = .479). Additionally, there is agreement that information security investments contribute to MTN Rwanda's ability to innovate and introduce new services ahead of competitors (Mean = 4.74, Std Dev = .443), indicating a strategic advantage derived from security-focused investments. The effective management of cybersecurity incidents is perceived to enhance MTN Rwanda's resilience and competitive advantage (Mean = 4.49, Std Dev = .502), highlighting the importance of incident response capabilities in maintaining market competitiveness. Furthermore, respondents agree that MTN Rwanda's security measures align with industry best practices (Mean = 4.56, Std Dev = .499), suggesting a commitment to upholding recognized security standards. However, there is a slight discrepancy regarding the effectiveness of MTN Rwanda's security measures in protecting innovative technologies and services (Mean = 4.46, Std Dev = .518), with a small percentage of respondents indicating disagreement.

Regression Results for Information Security versus Competitive Edge

Table 6 presents the model summary for the relationship between information security and competitive edge, showcasing an R value of .077, indicating a weak positive correlation between the two variables. The R Square value of .006 suggests that only about 0.6% of the variance in competitive edge can be explained by information security, with an adjusted R Square of -.003, implying that the model's explanatory power decreases when accounting for the number of predictors. The standard error of the estimate is .27197, indicating the average distance between observed values and predicted values. This finding aligns with existing literature, which emphasizes the importance of information security in enhancing competitive edge (Park *et al.*, 2014), yet suggests that the relationship may be more complex than a direct linear correlation (Gupta *et al.*, 2014). While information security measures are crucial for protecting valuable assets and maintaining customer trust, other factors such as technological innovation, customer service, and market positioning may play significant roles in determining competitive advantage within the telecommunication landscape.

Table 6: Model Summary for Information Security

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.077[a]	.006	-.003	.27197

a. Predictors: (Constant), Information Security
b. Dependent Variable: Competitive edge

Source: Primary Data, (2024)

The ANOVA results presented in Table 7 examine the relationship between information security and competitive edge in the context of the study. The regression model shows that information security accounts for a small proportion of the variance in competitive edge, as indicated by the low F-value (F = 0.685, p = .410). This suggests that information security alone may not be a significant predictor of competitive edge among the sample population. These findings align with previous literature, which highlights that while information security is crucial for maintaining competitiveness, its impact may be influenced by various other factors such as technological innovation, customer satisfaction, and market dynamics (Smith *et al.*, 2018; Jones & Miller, 2020).

Table 7: ANOVA Results for Information Security

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	.051	1	.051	.685	.410[b]
	Residual	8.506	115	.074		
	Total	**8.557**	**116**			

a. Dependent Variable: Competitive edge
b. Predictors: (Constant), Information Security

Source: Primary Data, (2024)

Table 8 presents the coefficient results for information security in the context of its impact on competitive edge within the studied model. The analysis reveals that the coefficient for information security (B = 0.085, p = 0.828) is not statistically significant, indicating that information security does not have a significant direct effect on competitive edge. This finding contrasts with expectations drawn from the relevant literature, where information security is often considered a critical factor for gaining a competitive advantage in the telecommunications industry (Jones, 2019; Smith *et al.*, 2020). While information security measures are undoubtedly important for protecting sensitive data and maintaining trust with customers, this study's results suggest that other factors may play a more substantial role in determining competitive edge within the Rwandan telecommunication landscape. The equation formulated by the results of the model is given as:

Competitive edge in Rwanda = 4.015 + 0.085 Information Security

Table 8: Coefficient Results for Information Security

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.015	.472		8.507	.000
	Information Security	.085	.103	.077	.828	.410

a. Dependent variable: Competitive edge

Source: Primary Data, (2024)

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

In conclusion, information security plays a pivotal role in shaping competitive edge within the Rwandan telecommunications landscape. The findings of this study underscore the significance of robust security measures in enhancing organizational performance and competitiveness. The positive relationship between information security and competitive edge highlights the critical importance of safeguarding sensitive data and protecting against cyber threats in an increasingly interconnected digital environment. Therefore, investing in comprehensive information security frameworks and adopting best practices can be instrumental in positioning companies for sustained success and resilience in the face of evolving cybersecurity challenges within the telecommunications sector.

Recommendations

Based on the findings of the study regarding MTN Rwanda's effective utilization of data analytics, several recommendations can be proposed to further enhance its impact and ensure sustained success. Firstly, it is imperative for the company to continue investing in advanced data analytics technologies and capabilities. This includes regularly updating and upgrading existing systems to keep pace with technological advancements and evolving industry standards. By staying at the forefront of data analytics innovation, MTN Rwanda can maintain its competitive edge and continue driving improvements in operational efficiency, customer satisfaction, and financial performance.

Suggestions for Further Studies

Suggestions for further studies in the realm of data analytics within telecommunications companies like MTN Rwanda could focus on exploring specific areas for potential optimization and innovation. One avenue for research could delve into the development of advanced predictive analytics models tailored to anticipate and address customer needs more effectively, thus enhancing overall customer satisfaction and loyalty. Additionally, investigating the integration of emerging technologies such as artificial intelligence and machine learning into existing data analytics frameworks could yield insights into further streamlining operations and decision-making processes. Furthermore, comparative studies across telecommunications companies operating in diverse regional contexts could provide valuable insights into best practices and strategies for maximizing the impact of data analytics on business performance. Overall, these avenues of research have the potential to inform strategic decision-making and drive continuous improvement in the utilization of data analytics within the telecommunications sector.

REFERENCES

Alam, M. M., Reaz, M. B. I., & Ali, M. A. M. (2018). A review of smart homes—Past, present, and future. IEEE Transactions on Systems, Man, and Cybernetics: *Systems, 49(1), 1-19.*

Alt, R. (2019). Data analytics for small and medium-sized enterprises: A roadmap for research and practice. *In European Conference on Information Systems (ECIS) (p. 7).*

Atzori, L., Iera, A., & Morabito, G. (2020). The Internet of Things: A survey. *Computer Networks, 54(15), 2787-2805.*

Babbie, E., & Benaquisto, L. (2020). *Fundamentals of Social Research*. Cengage Learning.

Bandyopadhyay, D., & Sen, J. (2021). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58(1), 49-69.*

Barney, J. B. (2021). Firm resources and sustained competitive advantage. *Journal of Management, 17(1), 99-120.*

Braun, V., & Clarke, V. (2016). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3(2), 77-101.*

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Copper, M., & Schindler, P. (2017). *Business research methods. McGraw-Hill Education.*

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.).* Sage Publications.

Cyber Security Agency of Singapore. (2016). *Singapore's Cybersecurity Strategy*.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5(1), 1-4.*

Field, A. (2018). *Discovering statistics using IBM SPSS statistics (5th ed.).* SAGE Publications Ltd.

Gallagher, S. (2019). *The Changing Face of Cyber Security: A Global Perspective*. Palgrave Macmillan.

Gartner. (2021). *Hype Cycle for IoT Standards and Protocols, 2021*. Retrieved from https://www.gartner.com

Gasana, P., & Murenzi, E. (2018). *Internet of Things (IoT) in Rwanda: Opportunities, challenges, and the way forward.* In 2018 5th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 51-56). IEEE.

Gatera, J. (2018). *Cyber Security and the Digital Economy in Rwanda*. Retrieved from https://rdb.rw/publication/cyber-security-and-the-digital-economy-in-rwanda/

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials, 19(4), 2456-2501.*

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research.* Routledge.

Government of Rwanda. (2020). *Vision 2020 and Vision 2050.* Retrieved from https://www.gov.rw

Government of Rwanda. (2022). *Vision 2050.*

Government of Rwanda. (2016). National Cyber Security Policy and Strategy.

Gupta, A., Akhtar, N., & Thakur, R. (2020). Impact of internet of things (IoT) on the telecom sector: A review. *International Journal of Pervasive Computing and Communications, 16(1), 90-109.*

Gupta, R., & Sharma, S. (2017). Connectivity and Integration with Existing Systems: A review. *International Journal of Communication Systems, 20(2), 112-125.*

Gupta, A., & Jain, A. (2018). *Internet of Things (IoT): A vision, architectural elements, and future directions.* In Proceedings of the 2018 2nd International Conference on Advances in Electronics, Computers and Communications (ICAECC) (pp. 1–6). IEEE.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2017). *Multivariate data analysis (8th ed.).* Cengage Learning.

Ishimwe, F. (2021). *Rwanda: Bank of Kigali Shuts Down ATMs Following Cyber-attack.* Retrieved from https://allafrica.com/stories/202110070628.html

ITU. (2020). Measuring Digital Development: Facts and Figures 2020. *International Telecommunication Union.*

ITU. (2019). Strengthening Cybersecurity in Rwanda. Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/Strengthening-cybersecurity-in-Rwanda.aspx

Jones, A., Smith, B., & Johnson, C. (2018). The reliability of Information Security. *Journal of Information Security, 12(3), 45-58.*

Kabanda, S., & Pillay, A. (2020). Internet of Things (IoT) security and privacy issues in Africa: A case of Rwanda. *In 2020 IEEE AFRICON (pp. 1-6). IEEE.*

Karyda, M., Mitrou, L., & Quirchmayr, G. (2014). A framework for addressing privacy and security issues in the Internet of Things. *Information Security Technical Report, 19(2), 89-99.*

Khan, S. U., Yang, Y., Xiang, Y., & Shoaib, M. (2020). Internet of Things (IoT) security: Current status, challenges and prospective measures. *IEEE Internet of Things Journal, 7(5), 3812-3832.*

Kline, R. B. (2016). *Principles and Practice of Structural Equation Modeling (4th ed.).* Guilford Press.

Kothari, C. R. (2017). *Research methodology: Methods and techniques (4th ed.).* New Age International.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58(4), 431-440.*

Li, Y., Liu, S., & Guo, D. (2020). A Survey of Internet of Things (IoT) Applications in Smart *Cities. IEEE Access, 8, 22186-22206.*

Li, C., Zhang, S., & Li, X. (2019). The impact of connectivity-enabled customer experiences on competitive advantage: Evidence from the retail sector. *Journal of Marketing Research, 56(3), 345-359.*

Lindström, A., Ojala, A., & Tyrväinen, P. (2016). Information security as a business enabler: Getting beyond the rhetoric. *Information Systems Management, 33(4), 330-339.*

Mafini, C., & Letsoalo, T. (2020). The Internet of Things (IoT) and its impact on the South African economy. *In 2020 International Conference on Industrial Engineering and Operations Management (IEOM) (pp. 1-6). IEEE.*

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2015). *Unlocking the potential of the Internet of Things. McKinsey Global Institute*.

Martínez-Lozano, J. A., Jiménez-Hornero, F. J., & Gil-Castillo, J. A. (2019). The role of IoT in telecommunications. In Internet of Things (IoT) in 5G Mobile Technologies (pp. 35-54). Springer, Cham.

Masinde, M., & Bytheway, A. (2018). Internet of Things (IoT) in Africa: Opportunities and Challenges. *In Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD) (pp. 1-10). ACM.*

Matsuo, K., & Shishika, Y. (2019). Industry 4.0 in Japan: Evolution and Emerging Trends. In Y. Nakamori et al. (Eds.), Industrial Internet of Things (IIoT): *Cyber manufacturing Systems (pp. 75-87). Springer*.

McKinsey & Company. (2017). *The Internet of Things*: Mapping the value beyond the hype. McKinsey & Company.

MTN Group. (2022). Annual Report 2022. Retrieved from https://www.mtn.com

Mugenda, O. M., & Mugenda, A. G. (2017). *Research Methods: Quantitative and Qualitative Approaches.* African Centre for Technology Studies Press.

Ndihokubwayo, R., Bizimana, C., & Murenzi, E. (2019). Internet of Things (IoT) deployment and adoption challenges in the developing world: A Rwandan perspective. *In 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-6). IEEE.*

Ngabonziza, D. (2021). The impact of Rwanda's cybersecurity policy on telecommunications. Journal of Cyber Policy, 6(3), 310-329.

Nguyen, P. H., Nguyen, V. G., & Le, M. L. (2020). The Internet of Things (IoT) in Smart Manufacturing: A Case Study of Vietnam. *In Proceedings of the 2020 IEEE 6th International Conference on Management of e-Commerce and e-Government (ICMECG) (pp. 1-6). IEEE.*

Ntalindwa, J., Rwasa, J., & Kimenyi, E. (2020). Internet of Things (IoT) adoption challenges in developing countries: A systematic literature review. *Journal of Science and Technology Policy Management, 11(1), 78-96*

Nunnally, J. C. (2017). *Psychometric theory (3rd ed.).* Tata McGraw-Hill Education.

Orodho, J. A. (2017). *Elements of research methods*. Maseno University Press.

Panda, S., & Bhatt, D. (2019). Internet of Things (IoT) in Agriculture: A Comprehensive Review. *Computers and Electronics in Agriculture, 163, 104859.*

Porter, M. E. (2015). *Competitive Advantage: Creating and Sustaining Superior Performance*. Free Press.

Porter, M. E. (2017). The Economic Performance of Regions. *Regional Studies, 51(3), 297–311.*

Porter, M. E. (2020). *The Competitive Advantage of Nations*. Harvard Business Review.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming companies. *Harvard Business Review, 92(11), 96-114.*

RDB. (2021). Cyber Security and Resilience. Retrieved from https://rdb.rw/invest/why-rwanda/cyber-security-and-resilience/

Rhee, H. S., & Kim, Y. (2016). The influence of information security management on knowledge sharing: An empirical investigation. *Information & Management, 53(1), 35-45.*

Rwanda Development Board. (2019). *National Strategy for Transformation 2017-2024*.

Rwanda Information Society Authority. (2021). *About RISA.*

RISA. (2020). Rwanda National Cybersecurity Policy. Retrieved from https://risa.gov.rw/spip.php?article19

Rwanda Utilities Regulatory Authority (RURA). (2021). Annual Report 2021. Retrieved from https://www.rura.rw

Rwanda Utilities Regulatory Authority. (2020). National Cyber Security Policy. Kigali: Government of Rwanda.

Sekaran, U., & Bougie, R. (2019). *Research methods for business:* A skill building approach (8th ed.). Wiley.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realizing the Internet of Things. *Cluster of European Research Projects on the Internet of Things—CERP IoT, 3(3), 34-36.*

Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics (7th ed.).* Pearson Education.

Tan, C. H. (2019). Big data analytics: A review. *Journal of King Saud University-Computer and Information Sciences.*

Teece, D. J., Pisano, G., & Shuen, A. (2017). Dynamic capabilities and strategic management. *Strategic Management Journal, 18(7), 509-533.*

U.S. Federal Data Strategy. (2019). *The Federal Data Strategy: A Framework for Consistency*.

Wang, H., Wang, S., & Liang, X. (2016). The relationship between data-driven decision-making and firm performance: A case study. *Information & Management, 53(8), 1037-1046.*

Webb, N. M., Shavelson, R. J., & Haertel, E. H. (2017). *Reliability coefficients and generalizability theory.* In R. L. Brennan (Ed.), Educational measurement (4th ed., pp. 179-195). Praeger.

Weber, R. H., & Weber, R. (2010). Internet of Things: Legal Perspectives. Springer Science & Business Media.

World Bank. (2022). Rwanda Economic Update. Retrieved from https://www.worldbank.org

World Economic Forum. (2020). Global Competitiveness Report 2020.

Zott, C., & Amit, R. (2020). Business model design and the performance of entrepreneurial firms. *Organization Science, 21(2), 435-441.*