UKR Journal of Economics, Business and Management (UKRJEBM)
Homepage: https://ukrpublisher.com/ukrjebm/
Email: submit.ukrpublisher@gmail.com
Volume 2, Issue 5, 2026
ISSN: 3049-429X (Online)

Physical Espionage and Competitiveness of Nigerian Telecommunication Firms

Prince Godswill Akhimien

Department of Business Administration, Nnamdi Azikiwe University, Awka, Nigeria. *ORCID No: 0000-0002-4730-5827*

***Corresponding Author**: Prince Godswill Akhimien

DOI: *https://doi.org/10.5281/zenodo.20398296*

Article History

Original Research Article

Received: 01-04-2026

Accepted: 05-05-2026

Published: 26-05-2026

Citation: Prince Godswill Akhimien. (2026). Physical Espionage and Competitiveness of Nigerian Telecommunication Firms. UKR Journal of Economics, Business and Management (UKRJEBM), 2(5), 168-177.

Abstract

This study investigates the relationship between physical espionage and competitiveness among Nigerian telecommunication firms, specifically MTN, GLO, and Airtel. Despite substantial investments in digital infrastructure, Nigerian telecom firms continue to suffer security lapses that compromise business continuity and competitive positioning through unauthorized physical access to facilities, data centres, and restricted operational areas. Adopting a descriptive survey research design, primary data were collected through structured questionnaires administered to 245 respondents across operational centres in Edo State, Nigeria. The study employed Crime Prevention Through Environmental Design (CPTED) Theory as its theoretical framework, positing that environmental design and management of physical spaces significantly influence espionage prevention and organizational competitiveness. Statistical analysis employed Pearson Product Moment Correlation. Findings revealed a weak but statistically significant positive relationship between physical espionage and competitiveness ($r = 0.137$, $p = 0.032$), indicating that unauthorized physical access to facilities and sensitive infrastructure subtly undermines firms' competitive positioning. Descriptive analysis showed high mean scores for physical espionage ($M = 3.77$, $SD = 1.11$), with 71.4% of respondents acknowledging tampering or theft of sensitive documents, while 67.4% recognized that espionage threats affected competitive advantage. The study concludes that despite technological advancements, physical security breaches remain relevant threats to corporate performance in Nigeria's telecommunications sector. Recommendations include enhanced biometric access controls, comprehensive surveillance systems, robust visitor management protocols, and integration of CPTED principles into organizational security architecture to safeguard sustainable competitive advantage.

Keywords: *Physical Espionage, Competitiveness, Telecommunications, Corporate Security, Crime Prevention Through Environmental Design, Nigeria.*

***JEL CODES**: L86, M19, O32, K42, D23*

Introduction

Organizational espionage, also known as corporate or industrial espionage, encompasses a range of covert and unauthorized actions aimed at acquiring sensitive, proprietary, or classified information from business entities for strategic or competitive gain (Anderson & James, 2023). While modern discourse often emphasizes cyber threats, physical espionage involving unauthorized access to facilities, data centres, and restricted operational areas remains a persistent and potentially damaging form of corporate intelligence theft. Physical espionage refers to covert, unauthorized access to an organization's physical facilities, such as offices, data centres, or restricted operational areas, with the deliberate intent to acquire sensitive or proprietary information. This form of espionage may involve techniques such as surveillance, impersonation, bribery of insiders, installation of hidden recording devices, or direct physical infiltration by hostile actors (Adetola & Oladele, 2022). In the context of

Nigeria's increasingly competitive telecommunications sector, physical espionage has become a growing concern, particularly among major operators like MTN, GLO, and Airtel. As these firms expand their infrastructure, including base transceiver stations, network operation centres, and customer data facilities the physical touchpoints for potential breaches multiply (Okon & Abasi, 2023). Competitiveness refers to an organization's capacity to maintain, improve, or defend its market position in relation to existing and emerging rivals. It embodies a firm's ability to deliver value to customers better than its competitors through superior products, services, pricing strategies, branding, and operational efficiency (Ekong & Ibeh, 2024). In the dynamic landscape of the telecommunications industry, competitiveness is a critical performance indicator that directly influences customer loyalty, revenue growth, and long-term sustainability. The Nigerian telecommunications sector contributes approximately 14.13% to the country's Gross Domestic Product (NCC, 2024), making its security and stability vital for national economic development. However, rapid digital transformation has increased vulnerability to espionage-related threats. Physical espionage compromises corporate security by exposing critical business secrets and customer data, enabling competitors to undercut services or pre-empt market moves (Uchenna & Abubakar, 2023). Despite substantial investments in digital infrastructure, Nigerian telecom firms continue to suffer security lapses that compromise business continuity and competitive positioning. This study examines the specific relationship between physical espionage and competitiveness in Nigerian telecommunication firms, addressing a critical gap in understanding how traditional, non-digital security threats continue to affect corporate performance in an increasingly digital economy.

The Nigerian telecommunications sector, while being one of the fastest-growing segments of the country's economy, faces an escalating threat from organizational espionage. As firms like MTN, GLO, and Airtel expand their digital infrastructure and customer base, they also become more exposed to covert practices aimed at stealing sensitive information, disrupting operations, and undermining competitive advantage (Okeke & Adebayo, 2023). Physical espionage, often carried out through unauthorized access to data centres or surveillance of proprietary operations, has led to leaks of pricing models and strategic plans, eroding the first-mover advantage of key market players (Adetola & Oladele, 2022). Several Nigerian firms have experienced unauthorized access incidents that led to the exposure of customer databases, strategic pricing models, and vendor contracts. In some cases, breaches were facilitated by former employees or contractors who retained unauthorized access credentials after their exit (Okon & Abasi, 2023). One significant challenge with physical espionage is its often-undetected nature. Unlike cyber-attacks that may trigger digital alarms or leave audit trails, physical breaches can occur subtly, especially in organizations lacking robust access control systems. This includes outdated security infrastructure, poor visitor management protocols, and inadequate surveillance coverage (Chukwu, 2023). The International Association of Corporate Security (2023) reported that over 30% of recent corporate espionage cases globally involved some form of physical access breach, reflecting the persistent relevance of this tactic even in a digital-first business environment. The consequences of physical espionage are multi-dimensional. Apart from the loss of critical documents or devices, there is a risk of long-term strategic disadvantage if competitors gain insights into business development plans or client acquisition strategies. Furthermore, such breaches often compromise customer trust, particularly when personal or financial information is accessed unlawfully (Eze & Ogunleye, 2023). Resources that would otherwise be allocated to innovation, talent development, or market expansion may be redirected toward enhancing surveillance, conducting internal investigations, or managing post-breach recovery, diminishing a firm's agility and limiting its ability to respond to competitive threats (Adeyemi & Oladipo, 2023). Despite these challenges, there remains insufficient empirical evidence specifically examining how physical espionage affects competitiveness in Nigeria's telecommunications sector. Most existing studies either focus on cyber-espionage or adopt sector-agnostic approaches that fail to capture the unique operational context of telecom firms. This study addresses this gap by investigating the specific relationship between physical espionage and competitiveness among MTN, GLO, and Airtel in Nigeria.

Research Question

What is the relationship between physical espionage and competitiveness of Nigerian Telecommunication Firms?

Research Hypotheses

H_0: There is no significant relationship between physical espionage and competitiveness of Nigerian Telecommunication Firms.

Literature Review (Conceptual Review)

Physical Espionage

Physical espionage refers to covert, unauthorized access to an organization's physical facilities, such as offices, data centres, or restricted operational areas, with the deliberate intent to acquire sensitive or proprietary information. This form of espionage may involve techniques such as surveillance, impersonation, bribery of insiders, installation of hidden recording devices, or direct physical infiltration by hostile actors (Adetola & Oladele, 2022). In the context

of Nigeria's increasingly competitive telecommunications sector, physical espionage has become a growing concern, particularly among major operators like MTN, GLO, and Airtel. As these firms expand their infrastructure including base transceiver stations, network operation centres, and customer data facilities the physical touchpoints for potential breaches multiply exponentially, creating numerous vulnerabilities that malicious actors can exploit. Okon and Abasi (2023) reported that several Nigerian firms have experienced unauthorized access incidents that led to the exposure of customer databases, strategic pricing models, and vendor contracts. In some cases, breaches were facilitated by former employees or contractors who retained unauthorized access credentials after their exit, highlighting the insider threat dimension of physical espionage. One significant challenge with physical espionage is its often-undetected nature. Unlike cyber-attacks that may trigger digital alarms or leave comprehensive audit trails, physical breaches can occur subtly and remain undiscovered for extended periods, especially in organizations lacking robust access control systems, comprehensive visitor management protocols, and adequate surveillance coverage (Chukwu, 2023). The International Association of Corporate Security (2023) argued that over 30% of recent corporate espionage cases globally involved some form of physical access breach, a statistic that reflects the persistent relevance of this tactic even in a digital-first business environment. This finding underscores that despite technological advancements; traditional espionage methods remain effective and widely employed. The consequences of physical espionage are multi-dimensional and far-reaching. Apart from the immediate loss of critical documents or devices, there is substantial risk of long-term strategic disadvantage if competitors gain insights into business development plans, merger and acquisition strategies, or client acquisition methodologies. Uchenna and Abubakar (2023) argue that physical espionage in Nigeria's telecom sector has directly led to market distortions, where competitors use stolen intelligence to undercut services, replicate innovations, or pre-empt market moves, thereby eroding the victim firm's competitive positioning and market share. The financial implications extend beyond direct losses to include reputational damage, regulatory penalties, and the substantial costs of remediation and enhanced security measures.

Competitiveness

Competitiveness refers to an organization's capacity to maintain, improve, or defend its market position in relation to existing and emerging rivals. It embodies a firm's ability to deliver value to customers better than its competitors through superior products, services, pricing strategies, branding, and operational efficiency (Ekong & Ibeh, 2024). In the dynamic landscape of the telecommunications industry, competitiveness is a critical performance indicator that directly influences customer loyalty, revenue growth, and long-term sustainability. At its core, competitiveness is shaped by multiple internal and external factors that interact in complex ways to determine market outcomes. Internally, it depends on a firm's ability to leverage its resources effectively including financial capital, human talent, technological capabilities, and intellectual property to create distinctive value propositions that resonate with target customers. Externally, competitiveness is influenced by market trends, regulatory pressures, customer expectations, and the intensity of rivalry in the industry, all of which require continuous monitoring and strategic adaptation. Innovation plays a central role in sustaining competitiveness, as it enables firms to differentiate themselves and adapt to changing consumer preferences in an increasingly crowded marketplace. Strategic resource management such as cost optimization, process improvement, and talent retention also contributes significantly to maintaining a competitive edge by ensuring operational excellence and organizational resilience. Customer retention, driven by consistent service quality and customer engagement, ensures recurring revenue and brand loyalty, which are essential for sustainable profitability (Afolabi & Njoku, 2023). Additionally, network quality, coverage expansion, and pricing flexibility remain critical competitive weapons in the Nigerian telecommunications sector where subscriber acquisition costs are high and customer switching behaviour is prevalent. However, competitiveness is increasingly vulnerable to external threats, particularly organizational espionage. Acts of espionage ranging from unauthorized data access to theft of strategic documents can expose a firm's business plans, pricing models, and customer insights to rivals, neutralizing carefully cultivated competitive advantages. Chidiebere and Hassan (2023) argue that such exposure undermines a firm's ability to defend its market position, as competitors can exploit stolen information to mimic strategies, launch countermeasures, or pre-empt market initiatives. In Nigeria's telecommunications sector, where firms invest heavily in infrastructure expansion and service innovation, the loss of strategic intelligence through physical espionage can result in significant competitive displacement, market share erosion, and diminished returns on investment. The protection of competitive information therefore becomes not merely a security concern but a strategic imperative for long-term market survival and growth.

Physical Espionage and Competitiveness

Physical espionage poses a direct and often underestimated threat to an organization's competitiveness, particularly in

knowledge-intensive industries where proprietary information constitutes a significant portion of firm value. In Nigeria's telecommunications sector, competitiveness is closely tied to the protection of physical assets such as customer data repositories, pricing strategies, research labs, and server rooms. The ability to safeguard these resources is critical in sustaining a firm's strategic advantage in a highly saturated and fast-paced market where customer loyalty is fragile and switching costs are minimal. As telecommunications firms increasingly rely on data-driven decision-making and personalized service offerings, the physical security of information assets becomes paramount to maintaining competitive differentiation. Chidiebere and Hassan (2023) assert that physical breaches often expose critical business intelligence such as rollout plans, service innovations, and infrastructure blueprints which rivals can exploit to dilute market dominance or undercut service offerings. For instance, if a competitor gains access to unreleased pricing schemes or marketing strategies through physical infiltration, they may pre-emptively launch competing products or alter their prices, eroding the first-mover advantage and market positioning of the original firm. This temporal displacement of competitive initiatives can result in substantial revenue losses and wasted investment in aborted market entry strategies. Furthermore, stolen infrastructure blueprints can enable competitors to replicate network expansion plans at lower research and development costs, effectively free-riding on the victim firm's innovation investments. Moreover, physical espionage undermines investor and customer confidence in ways that extend far beyond immediate financial losses. Breaches of this nature suggest weak internal control and security protocols, which can deter potential partnerships, joint ventures, and strategic alliances that are essential for growth in the telecommunications sector. Institutional investors increasingly incorporate security risk assessments into their valuation models, and firms with documented physical security lapses may face higher capital costs or reduced market valuations. This reputational damage is especially dangerous in the telecom industry, where data privacy and service reliability are top customer priorities (Eze & Ogunleye, 2023). Subscriber churn following security incidents can be substantial, as customers migrate to competitors perceived as more trustworthy guardians of personal information. The cumulative effect of these competitive injuries lost market opportunities, eroded pricing power, damaged reputation, and increased cost of capital demonstrates that physical espionage represents a systemic threat to sustainable competitive advantage that demands proactive managerial attention and substantial protective investment.

Theoretical Framework

This study is anchored on Crime Prevention Through Environmental Design (CPTED) Theory, developed by criminologist C. Ray Jeffery in 1971. CPTED suggests that the design and management of physical spaces can significantly reduce the likelihood of crime, including unauthorized access, theft, and espionage activities within organizational premises. The theory posits that by carefully designing and controlling environmental factors, organizations can deter potential intruders, making it more challenging for individuals to gain unauthorized physical access (Jeffery, 1971). CPTED operates on key principles that make it particularly relevant to this study's focus on physical espionage and its impact on organizational competitiveness:

1. **Natural Surveillance:** Emphasizes maximizing visibility to deter potential intruders. Organizations can leverage design layouts, CCTV placements, and strategically placed windows to enhance natural visibility, reducing the opportunity for unauthorized entry.
2. **Access Control:** Focuses on managing points of entry and restricting access to sensitive areas. Physical barriers, security protocols, and keycard systems help limit unauthorized access to critical organizational assets and information.
3. **Territorial Reinforcement:** Seeks to establish a clear distinction between private and public spaces, thereby creating a sense of ownership and accountability. Demarcating restricted areas with clear signage or structural barriers can discourage individuals from attempting unauthorized entry.
4. **Maintenance:** Involves keeping spaces orderly and well-maintained to signal vigilance and deter intrusions. Well-maintained premises with visible security measures communicate to potential intruders that the organization actively monitors and protects its environment.

Applying CPTED principles can help companies like MTN, GLO, and Airtel strengthen their defences against physical espionage. By incorporating this theory, the study gains insight into how environmental factors and organizational design can directly impact the effectiveness of espionage prevention strategies and, subsequently, the performance and competitiveness of an organization (Crowe, 2000; Clarke & Eck, 2005).

Empirical Review

Akhimien (2023) conducted a study on the relationship between organizational espionage and performance in Nigerian manufacturing firms, using a descriptive survey method. The study focused on Seven-Up Bottling Company, with a sample of 112 respondents determined by

Taro Yamane's formula. Analysis involved descriptive statistics, correlation, and regression. Findings showed a mean espionage score of 28.5 and a performance score of 72.4, with a significant positive correlation ($r = 0.72$, $p < 0.05$). Regression results indicated that espionage accounted for 52% of performance variability. The study recommended strengthening cybersecurity and promoting ethical awareness.

Ogunyemi and Falade (2024) focused on the impact of physical espionage on strategic performance in selected Nigerian financial institutions. The study adopted a descriptive survey research design, targeting security managers, operations officers, and IT administrators across ten major banks in Lagos and Abuja. Using stratified random sampling, 180 respondents were drawn from departments vulnerable to espionage risks. Results revealed that physical espionage had a statistically significant negative correlation with strategic performance ($r = -0.68$, $p < 0.01$). Regression analysis indicated that physical espionage accounted for 46% of the variance in strategic performance outcomes. The study recommended enhancing physical access control through biometrics and installing surveillance cameras with remote monitoring.

Okon and Abasi (2023) conducted a study on the impact of organizational espionage on contract competitiveness in the Nigerian oil and gas sector. The study employed a qualitative case study approach, focusing on the role of leaked tender documents and proprietary data in influencing bidding outcomes. Data were collected from five multinational and indigenous oil firms in Rivers and Akwa Ibom States, with 25 participants selected through purposive sampling. Content analysis revealed that over 30% of lost contracts were traced to intelligence leaks during bidding processes. The study recommended implementing encrypted bid submission platforms and deploying forensic audit tools.

Garrett and Holmes (2024) conducted a qualitative and quantitative study on the impact of physical espionage on logistics companies in Germany. The study analysed field reports and security breach records from 15 major logistics firms over a three-year period. Findings revealed that physical espionage, particularly facility breaches, was used to sabotage delivery timelines and reroute sensitive consignments. On average, companies experienced a 22% increase in delayed shipments following espionage incidents, with estimated financial losses of €7.8 million annually per firm. The study recommended implementing biometric access controls and comprehensive employee background checks.

Miller and Thompson (2024) conducted a quantitative study to investigate the impact of corporate espionage on market positioning among technology firms in the UK. The study utilized panel data analysis covering 40 technology companies over a five-year period. Findings revealed that firms affected by espionage experienced an average annual decline of 12% in market share growth compared to firms with no reported espionage activities. The negative effect was more pronounced in small- and medium-sized firms lacking robust intellectual property protections. The study recommended strengthening cybersecurity and competitive intelligence safeguards.

Schneider and Becker (2023) conducted a quantitative study analysing the impact of cross-border cyber-espionage on the performance of European defence contractors. The study examined a panel dataset of 30 defence firms across five European countries over a six-year period. Using logistic regression and performance benchmarking, the study found that firms targeted by espionage were 40% more likely to underperform relative to industry benchmarks. Specifically, affected firms showed an average 18% decline in annual revenue growth and a 25% reduction in contract renewals. The study recommended enhanced international cooperation on cybersecurity and investment in threat intelligence sharing.

Methodology

This study adopted a descriptive survey research design to investigate the relationship between physical espionage and competitiveness among Nigerian telecommunication firms. The survey design was appropriate for collecting primary data through questionnaires from employees of MTN, GLO, and Airtel, enabling the measurement of respondents' experiences, perceptions, and internal organizational practices regarding physical security threats and competitive positioning.

The study was conducted in Esan West and Esan Central Local Government Areas of Edo State, Nigeria. These areas were selected because they host several branch offices and operational units of major telecommunications firms, particularly MTN Nigeria, GLO Nigeria, and Airtel Nigeria. The concentration of these firms in the area makes it a relevant site for investigating the effects of physical espionage on firm competitiveness. The population of the study comprised employees from three major telecommunications companies operating within Esan West and Esan Central LGAs:

Company	**Number of Employees**
MTN Nigeria	85
GLO Nigeria	82
Airtel Nigeria	78
Total	**245**

The population consisted of employees in managerial, IT security, and strategic decision-making roles, targeted because of their involvement in operational strategy, data protection, and corporate security. Due to the relatively manageable size of the population (245), the study adopted a census sampling technique, which involves collecting data from the entire population. This method ensures comprehensive data coverage and minimizes sampling bias. The study utilized primary data obtained through structured questionnaires administered to selected respondents. The questionnaire was developed on a five-point Likert scale: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1). The questionnaire consisted of: Section A: Demographic Information (gender, age, educational qualification, years of experience, department), Section B: Physical Espionage (4 items measuring unauthorized access, facility breaches, surveillance risks, and visitor monitoring), Section C**:** Competitiveness (4 items measuring market position, service delivery performance, impact of espionage on competitive advantage, and strategic information security). Data were analysed using both descriptive and inferential statistics: Descriptive Statistics: Mean, standard deviation, and frequency distributions were used to summarize respondents' demographic characteristics and provide a general overview of the study variables. Inferential Statistics: Pearson Product Moment Correlation (PPMC) was employed to test the hypothesis and determine the strength and direction of association between physical espionage and competitiveness. The analysis was conducted using SPSS Version 23, with a 5% level of significance ($\alpha = 0.05$). The decision rule was: If p-value < 0.05, reject the null hypothesis (significant relationship exists), If p-value ≥ 0.05, fail to reject the null hypothesis (no significant relationship)

Data Analysis and Results

Analysis of Retrieved Questionnaires

A total of 245 questionnaires were administered to the sampled respondents across the selected telecommunication firms. All 245 questionnaires were duly completed and returned, representing a retrieval rate of 100%.

Table 1: Analysis of Questionnaire

Questionnaire Status	**Frequency**	**Percentage (%)**
Retrieved	245	100.00
Not Retrieved	0	0.00
Total	**245**	**100**

Source: Field Survey (2026)

9.2 Demographic Characteristics of Respondents

Table 2: Gender Distribution

Gender	**Frequency**	**Percentage (%)**
Male	160	65.31%
Female	85	34.69%
Total	**245**	**100%**

Source: Field Survey (2026)

Table 3: Age Distribution

Age Range	**Frequency**	**Percentage (%)**
18–25 years	25	10.20%
26–35 years	95	38.78%
36–45 years	80	32.65%
46 and above	45	18.37%
Total	**245**	**100%**

Source: Field Survey (2026)

Table 4: Years of Experience

Experience Range	Frequency	Percentage (%)
Less Than 1 year	25	10.20%
1–5 years	50	20.41%
6–10 years	95	38.78%
11 years and above	75	30.61%
Total	**245**	**100%**

Source: Field Survey (2026)

9.3 Descriptive Statistics of Research Variables

Table 5: Physical Espionage (Items 1–4)

S/N	Statement	5 (SA)	%	4 (A)	%	3 (N)	%	2 (D)	%	1 (SD)	%	Total
1	Unauthorized individuals have accessed restricted areas	90	36.7%	75	30.6%	40	16.3%	25	10.2%	15	6.1%	245
2	Physical security measures are inadequate	100	40.8%	85	34.7%	30	12.2%	20	8.2%	10	4.1%	245
3	Sensitive documents/devices have been tampered with or stolen	85	34.7%	90	36.7%	35	14.3%	20	8.2%	15	6.1%	245
4	Visitors/contractors are not always properly monitored	95	38.8%	80	32.7%	40	16.3%	20	8.2%	10	4.1%	245

Source: Field Survey (2026)

Table 6: Descriptive Statistics for Physical Espionage

Statement	Mean	Std. Dev.
Item 1	3.69	1.15
Item 2	3.84	1.07
Item 3	3.72	1.12
Item 4	3.84	1.08
Average	**3.77**	**1.11**

Source: Field Survey (2026)

Table 7: Competitiveness (Items 17–20)

S/N	Statement	5 (SA)	%	4 (A)	%	3 (N)	%	2 (D)	%	1 (SD)	%	Total
17	Our company maintains strong market position	100	40.8%	85	34.7%	30	12.2%	20	8.2%	10	4.1%	245
18	We outperform competitors in service delivery	95	38.8%	90	36.7%	35	14.3%	15	6.1%	10	4.1%	245

19	Espionage threats have affected competitive advantage	85	34.7%	80	32.7%	40	16.3%	25	10.2%	15	6.1%	245
20	We enhance competitiveness through strategic information security	100	40.8%	90	36.7%	30	12.2%	15	6.1%	10	4.1%	245

Source: Field Survey (2026)

Table 8: Descriptive Statistics for Competitiveness

Statement	**Mean**	**Std. Dev.**
Item 17	3.84	1.08
Item 18	3.86	1.06
Item 19	3.66	1.14
Item 20	3.86	1.06
Average	**3.81**	**1.09**

Source: Field Survey (2026)

Table 9: Mean and Standard Deviation of Key Constructs

Variable	**Mean**	**Std. Deviation**
Physical Espionage	3.84	0.69
Competitiveness	3.88	0.73

Source: Field Survey (2026)

Hypothesis Testing

Table 10: Hypothesis One Correlations

		physical_esp	**competitiveness**
physical_esp	Pearson Correlation	1	.137*
	Sig. (2-tailed)		.032
	N	245	245
competitiveness	Pearson Correlation	.137*	1
	Sig. (2-tailed)	.032	
	N	245	245

*. Correlation is significant at the 0.05 level (2-tailed).

Source: SPSS Statistics v23

Interpretation: Table 10 shows a weak but statistically significant positive correlation between physical espionage and competitiveness (r = 0.137, p = 0.032). This suggests that physical espionage activities, though subtle, affect firms' market performance. The positive direction indicates that as perceptions of physical espionage increase, there is a corresponding slight increase in reported competitiveness concerns likely reflecting that firms experiencing physical security breaches must invest more heavily in competitive positioning to maintain market standing. Since the p-value (0.032) is less than the 0.05 significance level, the null hypothesis is rejected. There is a statistically significant relationship between physical espionage and competitiveness of Nigerian Telecommunication Firms.

Summary of Findings

1. **Demographic Profile:** The study comprised 245 respondents from MTN (85), GLO (82), and Airtel

(78). The majority were male (65.31%), aged 26–35 years (38.78%), with 6–10 years of experience (38.78%), indicating a mature workforce with significant institutional knowledge.

2. **Physical Espionage Prevalence:** Descriptive analysis revealed high mean scores for physical espionage (M = 3.77, SD = 1.11). Notably, 71.4% of respondents acknowledged that sensitive documents or devices had been physically tampered with or stolen, and 71.5% believed visitors or contractors were not consistently monitored.

3. **Competitiveness Perceptions:** Competitiveness showed positive mean scores (M = 3.81, SD = 1.09), with 75.5% agreeing their company maintains strong market position. However, 67.4% acknowledged that espionage threats have affected competitive advantage, indicating awareness of security-performance linkages.

4. **Hypothesis Testing:** Pearson correlation analysis revealed a weak but statistically significant positive relationship between physical espionage and competitiveness ($r = 0.137$, $p = 0.032$). The null hypothesis was rejected, confirming that physical espionage significantly influences competitiveness in Nigerian telecommunication firms.

5. **Theoretical Validation:** The findings support CPTED Theory (Jeffery, 1971), demonstrating that inadequate environmental design and access control in physical spaces create opportunities for espionage that subsequently undermine competitive positioning.

Conclusion

This study investigated the relationship between physical espionage and competitiveness among Nigerian telecommunication firms. The findings establish that physical espionage represents a significant, albeit often underestimated, threat to corporate competitiveness in the sector. The weak but statistically significant positive correlation ($r = 0.137$, $p = 0.032$) confirms that unauthorized physical access, inadequate surveillance, and poor visitor management contribute to competitive vulnerabilities.

The study demonstrates that despite the digital transformation of the telecommunications industry, physical security breaches remain relevant threats that can expose critical business intelligence, erode customer trust, and divert resources from strategic initiatives to crisis management. The findings validate the applicability of Crime Prevention Through Environmental Design (CPTED) Theory in understanding how environmental factors influence espionage opportunities and competitive outcomes.

The research contributes to the limited body of empirical literature on corporate espionage in sub-Saharan Africa, particularly Nigeria, by providing evidence-based insights into the physical dimension of security threats. The study underscores that competitiveness in telecommunications is not merely a function of digital infrastructure and service quality, but also depends critically on the protection of physical assets and operational environments.

Recommendations

Based on the findings, the following recommendations are proposed:

1. **Enhanced Physical Access Controls:** Telecommunication firms should implement strict facility access controls, including biometric authentication systems, keycard protocols, and multi-factor verification for entry to restricted areas such as data centres, network operation centres, and research facilities.

2. **Comprehensive Surveillance Systems:** Organizations should invest in advanced CCTV surveillance with AI-based facial recognition capabilities, strategically positioned to maximize natural surveillance and eliminate blind spots in critical operational areas.

3. **Robust Visitor Management Protocols:** Firms must establish stringent visitor and contractor monitoring systems, including pre-registration requirements, escorted access, badge tracking, and real-time logging of all physical entries and exits.

4. **Regular Security Audits:** Organizations should conduct routine physical security audits and vulnerability assessments to identify potential breach points, evaluate existing control effectiveness, and implement continuous improvements based on CPTED principles.

5. **Employee Vetting and Awareness:** Comprehensive background checks should be mandatory for all employees with access to sensitive areas, complemented by regular security awareness training that emphasizes the risks of physical espionage and individual accountability in maintaining secure environments.

6. **Territorial Reinforcement:** Clear demarcation between public and restricted zones, supported by visible signage, structural barriers, and

environmental design that signals ownership and vigilance, should be implemented across all organizational premises.

7. **Integration of Physical and Cyber Security:** Firms should adopt holistic security frameworks that integrate physical security measures with cybersecurity protocols, recognizing that physical breaches often serve as entry points for broader espionage activities.

References

1. Adetola, J., & Oladele, S. (2022). Corporate espionage in emerging markets: The Nigerian experience. *African Journal of Strategic Business Studies, 8*(2), 89–105.
2. Adeyemi, R., & Oladipo, I. (2023). Strengthening organizational culture for physical espionage resilience. *West African Journal of Management and Security, 11*(3), 45–60.
3. Afolabi, T., & Njoku, E. (2023). Organizational agility and performance under security threats. *Nigerian Journal of Telecom Strategy, 6*(4), 17–30.
4. Akhimien, P. G. (2023). The relationship between organizational espionage and performance in Nigerian manufacturing firms. *International Journal of Recent Research in Commerce Economics and Management, 10*(4), 84–92.
5. Anderson, J., & James, L. (2023). Cybersecurity strategies in African telecommunications. *African Journal of Cyber Policy, 7*(1), 33–49.
6. Chidiebere, U., & Hassan, B. (2023). Espionage and competitiveness in Nigerian telecoms. *Nigerian Journal of Business Security, 12*(2), 40–58.
7. Chukwu, K. (2023). Security infrastructure and physical breach patterns in Nigeria. *Journal of Physical Security Management, 7*(1), 11–26.
8. Clarke, R. V., & Eck, J. E. (2005). *Crime analysis for problem solvers in 60 small steps*. Washington, DC: U.S. Department of Justice.
9. Crowe, T. D. (2000). *Crime prevention through environmental design: Applications of architectural design and space management concepts* (2nd ed.). Oxford, UK: Butterworth-Heinemann.
10. Ekong, B., & Ibeh, K. (2024). Legal and strategic measures for IP protection. *Journal of Intellectual Property and Innovation, 8*(1), 50–67.
11. Eze, C., & Ogunleye, D. (2023). Physical espionage and customer trust in Nigeria. *Journal of Telecom Risk and Ethics, 6*(1), 25–41.
12. Garrett, R., & Holmes, A. (2024). Logistics under espionage threats in Europe. *Journal of Supply Chain Security, 10*(2), 66–83.
13. International Association of Corporate Security. (2023). *Global espionage incident review 2023*. Geneva, Switzerland: IACS Press.
14. Jeffery, C. R. (1971). *Crime prevention through environmental design*. Beverly Hills, CA: Sage Publications.
15. Miller, S., & Thompson, D. (2024). Market share loss from corporate espionage. *European Journal of Technology and Strategy, 15*(1), 70–87.
16. Nigerian Communications Commission. (2024). *Annual report on telecommunications in Nigeria*. Abuja, Nigeria: NCC.
17. Ogunyemi, Y., & Falade, S. (2024). Physical espionage and performance in Nigerian banks. *Journal of Strategic Security Studies, 9*(2), 93–109.
18. Okeke, V., & Adebayo, T. (2023). Corporate espionage and competition in Nigeria. *Journal of Emerging Market Ethics, 8*(2), 61–78.
19. Okon, D., & Abasi, G. (2023). Espionage and contract loss in oil & gas firms. *Nigerian Journal of Strategic Procurement, 6*(3), 74–90.
20. Schneider, F., & Becker, M. (2023). Cybersecurity behaviour in organizations: An empirical study. *Journal of Information Security Research, 12*(2), 101–117.
21. Uchenna, E., & Abubakar, H. (2023). Market distortion through physical espionage. *West African Journal of Competitive Strategy, 7*(1), 38–55.