Investigating How Communication Breakdowns and Cybersecurity Vulnerabilities Contribute to the High Incidence of Abandoned Public Infrastructure Projects In FCT-Abuja, Nigeria

Ishaq Mighty Baba[1] & Kenneth Adayilo Koce[2], Iko- ojo Gideon[3]

[1]Department of Development Communication

[2]Department of cybersecurity, The federal polytechnic Bida.

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2026.11110037

Received: 02 October 2026; Accepted: 07 October 2026; Published: 24 November 2026

ABSTRACT

This study investigated how communication breakdowns, compounded by cybersecurity vulnerabilities in digital project environments, contribute to the rising incidence of abandoned public infrastructure projects in the Federal Capital Territory (FCT), Abuja, Nigeria. Anchored on Development Support Communication Theory, Stakeholder Theory, Organizational Communication Theory, and principles of information security management, the research employed a descriptive survey design. Data were collected from 40 construction professionals (quantity surveyors, architects, project managers, and related stakeholders) using a structured questionnaire whose content validity was established through expert review and reliability confirmed via Cronbach's alpha ($\alpha = 0.81$). Findings revealed that misinterpretation of working drawings (80%), delays in information flow (77%), inconsistent site meetings (55%), unclear communication channels (50%), language barriers (45%), and cybersecurity-related issues—such as insecure digital platforms, delayed recovery from cyber incidents, and inadequate cybersecurity awareness (ranked highly by respondents)—significantly disrupt project execution. These factors weaken coordination, escalate costs through rework and downtime, and increase the likelihood of project abandonment. The study concludes that communication inefficiencies and associated cybersecurity gaps are important contributing factors to project abandonment in the FCT. It recommends strengthening secure communication structures, integrating cybersecurity training, enhancing information-flow protocols with encrypted digital tools, adopting Building Information Modelling (BIM) with robust access controls, and fostering multi-stakeholder collaboration to support successful project delivery.

Keywords: Communication breakdown, cybersecurity vulnerabilities, project abandonment, public infrastructure, FCT-Abuja, information security, construction project management

INTRODUCTION

Public infrastructure projects form the backbone of national development, enabling economic growth, social welfare, and improved quality of life. In Nigeria, government investments in roads, hospitals, schools, housing, water supply schemes, and power installations remain substantial. Yet the paradox persists: thousands of these projects remain uncompleted or abandoned. Project abandonment has become a recurrent challenge affecting national progress, public trust, and resource management.

While several factors such as corruption, inadequate funding, political changes, and poor planning have been identified as major contributors to project abandonment, an equally critical yet often overlooked factor is communication breakdown. In the contemporary construction environment, communication increasingly relies on digital platforms—email, cloud-based project management software, Building Information Modelling (BIM), and mobile applications. These digital channels introduce a new layer of risk: cybersecurity vulnerabilities. Breaches, ransomware attacks, unauthorized access to project documents, and insecure data-sharing practices

can interrupt information flow, distort technical instructions, and erode stakeholder trust, thereby amplifying traditional communication failures.

Effective communication remains central to development planning and implementation. It ensures alignment between stakeholders, clarity in objectives, coordination across agencies, and feedback mechanisms necessary for monitoring and accountability. However, in Nigeria's public-sector project cycle, both interpersonal and digitally mediated communication failures frequently undermine project execution. Understanding how communication deficits occur, the forms they take (including those induced or exacerbated by cybersecurity weaknesses), and the effects they produce is therefore essential. This study focuses specifically on identifying the communication gaps—together with associated cybersecurity vulnerabilities—that contribute to project abandonment and on recommending integrated communication and cybersecurity solutions that can improve infrastructure delivery in Nigeria.

2. Statement of the Problem

Despite the government's heavy investment in public infrastructure, Nigeria continues to grapple with thousands of abandoned projects scattered across states and sectors. Existing research has focused predominantly on issues such as corruption, inflation, political interference, and management inefficiencies. While these factors are valid, they do not fully account for how communication-related issues—and the cybersecurity risks that increasingly shape modern project communication—influence project outcomes.

Poor communication manifests in several ways: unclear project briefs, lack of coordination between ministries and contractors, inconsistent reporting, inadequate stakeholder engagement, misinformation, and absence of feedback systems. In digital environments these problems are compounded by weak access controls, unencrypted file transfers, phishing attacks targeting project personnel, and limited cybersecurity awareness among site teams and administrative staff. Such gaps often lead to delays, conflict, misallocation of resources, data loss or compromise, and eventual project abandonment. The limited scholarly attention to the interplay between communication failures and cybersecurity vulnerabilities as contributors to abandonment creates a gap that this paper seeks to address.

LITERATURE REVIEW

Empirical studies consistently demonstrate that poor communication significantly impedes the successful implementation of development projects, particularly in developing countries. World Bank (2017) reports that infrastructure projects in sub-Saharan Africa frequently experience delays and cost overruns due to inadequate information flow and weak coordination among stakeholders. Ofori (2015) found that ineffective communication between government agencies and contractors in Ghana led to frequent project misunderstandings, implementation errors, and, in some cases, project abandonment.

In the Nigerian context, research indicates that communication breakdowns within and between ministries, departments, and agencies (MDAs) exacerbate inefficiencies in public infrastructure delivery. Ogunlana et al. (2010) observed that unclear directives, delayed approvals, and limited inter-agency coordination were major contributors to project delays and incomplete projects. Akingbade (2013) highlighted that poor communication between public officials and contractors undermined accountability and increased the likelihood of cost escalations.

Despite these findings, there remains a gap in the literature: few studies explicitly analyse Nigerian infrastructure projects from an integrated communication-and-cybersecurity perspective. Most prior research focuses on technical, financial, or managerial aspects, with limited attention to how information flow, stakeholder engagement, organisational communication practices, and the security of digital communication channels jointly influence project outcomes. This gap underscores the need for studies that examine both traditional communication dynamics and emerging cybersecurity risks as critical factors in the success or failure of public-sector projects in Nigeria.

3.1 Concept of Communication in Construction

Communication is a central component of construction project management because projects depend on the continuous exchange of information among multiple stakeholders. Jergeas and Put (2001) note that effective communication promotes coordination, reduces misunderstandings, and enhances workflow on construction sites. Dainty, Moore, and Murray (2006) argue that communication acts as the connective system linking clients, consultants, contractors, and suppliers throughout the project life cycle. In public projects, communication becomes even more critical due to bureaucratic procedures and the involvement of government agencies (Odesola & Idoro, 2014). Increasingly, this communication occurs through digital media whose integrity depends on sound cybersecurity practices.

3.2 Communication Breakdown and Cybersecurity Vulnerabilities in Construction Projects

Communication breakdown refers to disruptions, distortions, or failures in the flow of information that negatively affect project outcomes. Communication failures rank among the highest contributors to construction disputes and delays. Common manifestations include misinterpretation of drawings, delayed information flow, unclear communication channels, inadequate documentation, and inconsistent site meetings. These breakdowns commonly lead to cost overruns, rework, conflicts, poor-quality delivery, and, ultimately, abandonment.

In the digital era, cybersecurity vulnerabilities constitute an additional and increasingly significant source of communication disruption. Unsecured email systems, weak password practices, absence of multi-factor authentication, ransomware infections that lock project files, and phishing campaigns targeting project managers or quantity surveyors can halt information exchange for days or weeks. When critical drawings, variation orders, or payment certificates are inaccessible or corrupted, work stops, schedules slip, and contractual disputes escalate—conditions that raise the probability of project abandonment. Studies in related sectors indicate that construction organisations often lag behind other industries in cybersecurity maturity, leaving project communication channels exposed (Eastman et al., 2011; related industry reports).

Misinterpretation of Drawings and Technical Information

The inability of project operatives to accurately interpret design drawings is a recognised cause of construction errors. Arain and Pheng (2005) maintain that technical misinterpretation often leads to rework, structural defects, and project abandonment. In developing countries, inadequate training and inexperience magnify this problem. When drawings are stored or shared via insecure digital repositories that become unavailable due to cyber incidents, the problem is compounded.

Delays in Information Flow and Cyber-Induced Disruptions

Timely information dissemination is crucial for decision-making during construction. Meng (2012) asserts that delays in information flow weaken coordination and increase the risk of disputes. Government projects often experience bureaucratic bottlenecks that slow approvals and communication between departments (Olatunji & Aje, 2011). Cybersecurity incidents—such as denial-of-service attacks on agency portals or ransomware locking shared drives—introduce additional, sometimes prolonged, delays that traditional process improvements alone cannot address.

Ineffective Site Meetings, Coordination, and Digital Alternatives

Site meetings serve as the main communication avenue between project stakeholders. Ogunlana, Siddiqui, and Yisa (2004) emphasise that poorly structured meetings, inconsistent attendance, or inadequate documentation contribute to misunderstandings and poor decision-making. Virtual or hybrid meetings conducted over unsecured platforms further expose discussions to interception or disruption.

Unclear Communication Channels and Access Control Failures

In many public projects, communication flows through multiple layers of authority, creating room for distortion. Hwang and Ng (2013) note that unclear channels lead to information loss, duplication of effort, and role conflicts. When digital access rights are poorly managed—granting excessive privileges or failing to revoke access after staff changes—confidential project information can leak or be altered, further confusing legitimate recipients.

Language, Cultural Barriers, and Cybersecurity Awareness Gaps

Public construction sites often employ workers from diverse linguistic and cultural backgrounds. Koskela and Howell (2002) and Loosemore and Lee (2002) observe that language differences can result in misinterpretation of safety instructions and technical guidelines. Parallel to language barriers is a widespread deficit in cybersecurity literacy: many operatives and even mid-level managers lack basic awareness of phishing, secure file-sharing practices, or the importance of strong authentication, thereby increasing the organisation's exposure to cyber-enabled communication failures.

Communication, Cybersecurity, and Project Abandonment

Abandoned projects are frequently linked to communication failures such as delayed approvals, inconsistent directives, and lack of feedback. Aibinu and Jagboro (2002) highlight that poor communication contributes to time overruns, which in turn lead to financial strain and abandonment in public projects. Cybersecurity incidents that interrupt cash-flow documentation, progress reporting, or variation management can accelerate the same pathway from delay to abandonment. Thus, communication breakdown—whether interpersonal or cyber-mediated—functions as both a direct and an indirect contributor to project failure.

THEORETICAL FRAMEWORK

This study adopts four complementary perspectives: Development Support Communication (DSC) Theory, Stakeholder Theory, Organizational Communication Theory, and core principles of information-security management.

Development Support Communication (DSC) Theory

DSC theory emphasises the strategic use of communication as a catalyst for development planning, implementation, and evaluation. It advocates deliberate information flow, stakeholder engagement, and public mobilisation (Quebral, 2012; Melkote & Steeves, 2015). Applied to this study, DSC illuminates how communication weaknesses—including those arising from insecure digital channels—impede project success. When communication systems among ministries, agencies, and contractors are fragmented or compromised, critical information is delayed or distorted, reducing the efficiency of planning and execution.

Stakeholder Theory

Stakeholder theory posits that all individuals and groups affected by or able to influence a project must be adequately considered, informed, and engaged (Freeman, 1984). Effective management requires open communication to align expectations. Communication gaps—whether caused by unclear roles or by cyber incidents that exclude legitimate stakeholders from information platforms—tend to create misunderstandings, reduce trust, and contribute to delays (Aaltonen, 2011).

Organizational Communication Theory

Organizational Communication Theory examines the patterns through which information flows within organisations—upward, downward, and horizontal (Robbins & Judge, 2019). In Nigeria's public sector, failures such as delayed approvals, ambiguous instructions, and poor inter-agency coordination have been identified as major contributors to project inefficiency (Ogunlana et al., 2010; Akingbade, 2013). The security of the channels that carry these flows is an integral, yet frequently neglected, dimension of organisational communication effectiveness.

Information Security Perspective

Drawing on the CIA triad (Confidentiality, Integrity, Availability) that underpins information-security practice, the study recognises that any compromise of the confidentiality, integrity, or availability of project information

constitutes a form of communication failure. Ransomware, for example, attacks availability; unauthorised alteration of drawings attacks integrity; leakage of tender documents attacks confidentiality. Integrating this perspective with the three communication theories provides a comprehensive lens for analysing how both human and technical-security factors contribute to project abandonment.

METHODOLOGY

This study examined how communication breakdowns and related cybersecurity vulnerabilities contribute to the abandonment of public construction projects in the Federal Capital Territory (FCT), Abuja. A descriptive survey design was adopted because the research sought to describe the prevalence and perceived impact of specific communication and cybersecurity factors among practising professionals.

The target population comprised construction professionals actively involved in public infrastructure projects within the FCT, including quantity surveyors, architects, project managers, engineers, and site supervisors. Given the absence of a comprehensive sampling frame and the specialised nature of the respondents, a purposive sampling technique was employed. Forty (40) professionals who met the inclusion criterion of having participated in at least one public infrastructure project in the FCT within the preceding five years were selected. While the sample size is modest, it is considered adequate for an exploratory descriptive study focused on capturing professional perceptions rather than generalising to the entire national construction workforce.

Data were collected by means of a structured questionnaire developed by the researchers. The instrument contained three sections: (A) demographic characteristics; (B) items measuring the perceived effect of traditional communication issues (misinterpretation of drawings, delays in information flow, site-meeting effectiveness, clarity of channels, language barriers, and training of operatives); and (C) items measuring cybersecurity-related communication risks (insecure digital platforms, delayed recovery from cyber incidents, inadequate cybersecurity awareness, and unauthorised access to project documents). All perception items used a five-point Likert-type scale ranging from “Very Low” to “Very High” effect on project delivery/abandonment.

Content validity was established through review by three senior academics specialising in construction project management and one information-security practitioner. Minor revisions were made to wording and item coverage. Reliability was assessed via a pilot administration to ten professionals outside the main sample; Cronbach’s alpha for the combined communication-and-cybersecurity scale was 0.81, indicating acceptable internal consistency.

Data analysis was primarily descriptive. Frequencies and percentages were computed for demographic variables. For the effect items, the percentage of respondents rating each factor as “High” or “Very High” was calculated and used to rank the factors. Mean scores were also computed to support ranking. No inferential statistics were applied, consistent with the exploratory and descriptive purpose of the study. The researchers acknowledge that the design does not permit strong causal claims; findings are therefore interpreted as associations and professional perceptions rather than definitive proof of causation.

RESULTS AND DISCUSSION

6.1 Demographic Characteristics of Respondents

Table 1 presents the demographic profile of the 40 respondents. Males constituted 60 % (n = 24) and females 40 % (n = 16). By designation, quantity surveyors formed the largest group (32 %, n = 13), followed by other professionals (27 %, n = 11), architects (23 %, n = 9), and project managers (18 %, n = 7). With respect to years of experience, 33 % had 0–5 years, 25 % had 6–10 years, 23 % had 11–15 years, and 20 % had more than 15 years. The distribution indicates a reasonably balanced professional mix and a range of experience levels, although the modest sample size limits broad generalisation.

Table 1. Demographic Characteristics of Respondents (N = 40)

Category	Frequency	Percentage

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue XI November 2026

Gender		
Male	24	60%
Female	16	40%
Total	40	100%
Designation		
Quantity Surveyor	13	32%
Project Manager	7	18%
Architects	9	23%
Others	11	27%
Total	40	100%
Years of Experience		
0–5 years	13	33%
6–10 years	10	25%
11–15 years	9	23%
Above 15 years	8	20%
Total	40	100%

Source: Field Survey, 2025

6.2 Perceived Effects of Communication and Cybersecurity Factors

Table 2 summarises the percentage of respondents who rated each factor as having a high or very high effect on project abandonment. Misinterpretation of working drawings ranked highest (80 %), followed by delays in communication (77 %). Cybersecurity-related factors also featured prominently: insecure digital platforms and delayed recovery from cyber incidents were rated high by 62 % and 58 % of respondents respectively, while inadequate cybersecurity awareness was rated high by 52 %. Traditional factors such as site-meeting effectiveness (55 %), late dissemination of information (53 %), unclear channels (50 %), and language problems (45 %) remained important. Training of operatives was perceived as least critical (20 %).

Table 2. Perceived Effect of Communication and Cybersecurity Issues on Project Abandonment

Communication / Cybersecurity Issue	High (%)	Interpretation
Inexperience / Misinterpretation of drawings	80%	Most significant traditional factor
Delay in communication	77%	Major cause of delays
Insecure digital platforms (cyber)	62%	High impact on information availability
Delayed recovery from cyber incidents	58%	Prolongs downtime
Site meetings effectiveness	55%	Important but often under-utilised
Late dissemination of information	53%	Affects site output
Inadequate cybersecurity awareness	52%	Increases vulnerability
Unclear communication channels	50%	Contributes to rework & conflict
Language problems	45%	Moderate barrier
Training of operatives	20%	Least-ranked factor

Source: Field Survey, 2025. Percentages represent respondents rating the factor as High or Very High.

The ranking underscores that technical communication competence (drawing interpretation) and the speed of information flow remain paramount. At the same time, the substantial percentages attached to cybersecurity items indicate that digital-security weaknesses are no longer peripheral; they actively shape the reliability of the communication systems on which modern projects depend. These findings align with the literature on communication-related delays (Aibinu & Jagboro, 2002; Meng, 2012) while extending the discussion into the cybersecurity domain that is increasingly relevant to Nigerian public-sector projects.

It is important to note that the descriptive design and modest sample size preclude strong causal inference. Other well-documented causes of abandonment—funding shortfalls, political interference, and contractor incapacity—operate alongside communication and cybersecurity factors. The present results indicate that communication and cybersecurity issues are associated with, and perceived by professionals as contributing to, higher likelihood of abandonment, rather than being the sole or primary causes.

7. Summary of Findings

The study found that several communication challenges, now intertwined with cybersecurity vulnerabilities, play a major role in elevating the risk of project abandonment in the FCT. Misinterpretation of working drawings remains the most frequently cited problem, leading to mistakes, rework, cost overruns, and frustration that can push projects toward abandonment. Delays in communication—whether caused by bureaucratic bottlenecks or by cyber incidents that render digital platforms temporarily unavailable—disrupt workflow and stall progress. Inconsistent site meetings weaken coordination, while unclear reporting lines and multiple instruction sources generate confusion and conflict. Language barriers continue to affect accuracy of instructions on multicultural sites. Critically, insecure digital platforms, slow recovery from cyber events, and low cybersecurity awareness among project personnel emerged as significant additional stressors on information reliability. Collectively, these factors weaken coordination, escalate costs, and increase the likelihood that public infrastructure projects will be abandoned.

CONCLUSIONS

This study has examined how communication breakdowns, amplified by cybersecurity vulnerabilities in digital project environments, contribute to the persistent problem of abandoned public infrastructure projects in the Federal Capital Territory (FCT), Abuja. The results indicate that misinterpretation of working drawings, delays in information flow, inconsistent site meetings, unclear communication channels, language barriers, and cybersecurity-related disruptions (insecure platforms, recovery delays, and awareness gaps) are all perceived by construction professionals as important contributors to project failure. These issues affect planning, design interpretation, execution, and monitoring stages. Addressing them requires more than technical or financial interventions; it demands deliberate investment in clearer, more secure communication structures, continuous capacity building that includes cybersecurity literacy, and stronger coordination among the diverse stakeholders involved in public projects.

The study acknowledges its limitations—chiefly the modest sample size and the descriptive rather than explanatory design—and therefore presents its conclusions as evidence of association and professional perception rather than definitive causal proof. Nevertheless, the findings provide a useful foundation for policy and practice reforms aimed at reducing the incidence of abandoned infrastructure projects in the FCT and, by extension, in other Nigerian jurisdictions.

RECOMMENDATIONS

Based on the findings, the following recommendations are offered:

1. Strengthen Secure Communication Channels: Government agencies and contractors should establish formal, clear, and unified communication systems that incorporate standardised reporting formats, clear documentation procedures, consistent protocols, and end-to-end encryption for sensitive project documents.

2. Integrate Cybersecurity Training into Construction Communication Capacity Building: Regular workshops should cover interpretation of drawings, site communication etiquette, use of digital tools, documentation procedures, phishing recognition, password hygiene, multi-factor authentication, and secure file-sharing practices.

3. Employ Experienced Personnel and Mentorship: Firms should prioritise professionals with proven competence in design interpretation and construction documentation, supported by mentorship programmes for less-experienced staff.

4. Enhance Timeliness and Resilience of Information Flow: Site meetings should be held regularly and documented; minutes circulated promptly; communication gaps minimised through approved digital platforms that include backup and recovery capabilities to mitigate cyber disruptions.

5. Adopt Secure Technology Solutions: Project-management applications, Building Information Modelling (BIM), and shared cloud platforms should be deployed with robust access controls, regular security audits, and incident-response plans to improve collaboration while protecting data integrity and availability.

6. Reduce Language and Awareness Barriers: Simplified instructions, visual illustrations, safety signage, and interpreters should be used where language differences exist; parallel efforts should raise basic cybersecurity awareness among all site personnel.

7. Strengthen Monitoring, Supervision, and Cyber Oversight: Regulatory bodies should ensure proper documentation, conduct regular audits of both communication reports and cybersecurity compliance, and apply appropriate sanctions for persistent neglect of secure communication procedures.

8. Encourage Collaboration and Trust: A communication climate built on mutual respect, transparency, and cooperation, reinforced by clear data-governance rules, will reduce conflicts and enhance understanding during project execution.

REFERENCES

1. Aaltonen, K. (2011). Project stakeholder analysis as an environmental interpretation process. International Journal of Project Management, 29(2), 165–183.
2. Aibinu, A. A., & Jagboro, G. O. (2002). The effects of construction delays on project delivery in Nigerian construction industry. International Journal of Project Management, 20(8), 593–599.
3. Akinsiku, O. E., & Akinsulire, A. (2012). Stakeholders' perception of the causes and effects of construction delays on project delivery. Journal of Construction Engineering and Management, 138(1), 1–7.
4. Arain, F. M., & Pheng, L. S. (2005). The potential effects of variation orders on institutional building projects. Facilities, 23(11), 496–510.
5. Dainty, A., Moore, D., & Murray, M. (2006). Communication in Construction: Theory and Practice. Taylor & Francis.
6. Eastman, C., Teicholz, P., Sacks, R., & Liston, K. (2011). BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors (2nd ed.). Wiley.
7. Freeman, R. E. (1984). Strategic Management: A Stakeholder Approach. Pitman.
8. Hwang, B., & Ng, W. (2013). Project management knowledge and skills for green construction. Technological and Economic Development of Economy, 19(1), 43–57.
9. Jergeas, G., & Put, J. (2001). Lessons learned from construction industry failures. Journal of Construction Engineering and Management, 127(4), 284–292.
10. Koskela, L., & Howell, G. (2002). The underlying theory of project management is obsolete. PMI Research Conference Proceedings, 293–302.
11. Loosemore, M., & Lee, P. (2002). Communication problems with ethnic minorities in the construction industry. International Journal of Project Management, 20(7), 517–524.
12. Love, P. E. D., Edwards, D., & Irani, Z. (2010). Work accidents and rework in construction projects. Safety Science, 48(6), 674–685.
13. Melkote, S. R., & Steeves, H. L. (2015). Communication for Development: Theory and Practice for Empowerment and Social Justice (3rd ed.). SAGE.
14. Meng, X. (2012). The effect of relationship management on project performance in construction. International Journal of Project Management, 30(2), 188–198.

15. Odesola, I. A., & Idoro, G. I. (2014). Influence of project management communication on public construction project performance in Nigeria. Journal of Construction in Developing Countries, 19(1), 49–67.
16. Ofori, D. (2015). The quality of project management practices and critical success factors in Ghana. International Journal of Business and Management, 8(21), 14–31.
17. Ogunlana, S., Siddiqui, Z., & Yisa, S. (2004). Factors and procedures used in matching project managers to construction projects in Thailand. International Journal of Project Management, 22(2), 107–116.
18. Olatunji, O., & Aje, I. (2011). The roles of communication in construction project delivery. The Built Environment Journal, 7(1), 1–13.
19. Quebral, N. C. (2012). Development Communication Primer. Southbound.
20. Robbins, S. P., & Judge, T. A. (2019). Organizational Behavior (18th ed.). Pearson.
21. World Bank. (2017). Africa's Pulse: An Analysis of Issues Shaping Africa's Economic Future. World Bank Group.