

Cybersecurity Governance for BIM-Enabled Quantity Surveying Practice

Original Research Article | Volume 1 | Issue 5 | 2026 | Article Number: 014

Accepted: 24 July 2026 | Published: 10 October 2026 | ISSN: 2979-8582 (Online)



Crossref : <https://doi.org/10.67693/BJCR-A33GIIC3>



Opatunji O.A¹, Apata O.C¹, Oni E.K²

¹Department of Quantity Surveying, Federal Polytechnic Ede, Nigeria,

²Department of Artificial Intelligence, Federal Polytechnic, Ede, Nigeria

 **OOA** [0009-0007-2485-8465](https://orcid.org/0009-0007-2485-8465), **AOC** [0009-0005-5444-2618](https://orcid.org/0009-0005-5444-2618), **OEK** [0009-0007-0641-6153](https://orcid.org/0009-0007-0641-6153)

Correspondence: Opatunji O.A, allbytesconsultz@gmail.com

Abstract

The increasing adoption of Building Information Modeling (BIM) in Quantity Surveying (QS) has enhanced collaboration and cost management but introduced substantial cybersecurity risks to cloud-based construction data. Despite these threats, a tailored cybersecurity governance framework is lacking for BIM-enabled QS practice, particularly in developing countries. This study developed and empirically evaluated a Cybersecurity Governance Framework for BIM-enabled QS practice in Nigeria. Using a quantitative survey design, data were collected from 235 construction and IT professionals involved in BIM implementation. The research instrument demonstrated acceptable internal consistency, with Cronbach's alpha coefficients ranging from 0.686 to 0.817 across principal constructs. Descriptive statistics, Pearson correlation, and multiple regression analyses were used to evaluate the relationships among cybersecurity awareness, threat exposure, organizational preparedness, and framework acceptance. The findings indicate that cybersecurity awareness and organizational preparedness are significant predictors of framework acceptance, whereas perceived threat exposure alone does not significantly influence stakeholder acceptance. Based on these results, a comprehensive cybersecurity governance framework aligned with ISO 19650-5, ISO/IEC 27001:2022, and the NIST Cybersecurity Framework (CSF) 2.0 is proposed to secure BIM implementation within QS practice. This study contributes to construction informatics and cybersecurity literature by providing an empirically validated governance model that supports secure digital transformation, organizational resilience, and improved information security management within BIM-enabled construction environments.

Keywords: Building Information Modeling (BIM), Quantity Surveying, Cybersecurity Governance, Information Security, Construction Informatics, Organizational Cybersecurity Preparedness, Cybersecurity Awareness, ISO 19650-5, NIST Cybersecurity Framework 2.0, Digital Construction

1. INTRODUCTION

The Architecture, Engineering, Construction, and Operations (AECO) industry is undergoing rapid digital transformation driven by advances in cloud computing, artificial intelligence (AI), the Internet of Things (IoT), and Building Information Modeling (BIM) (Abioye et al., 2021; Oesterreich & Teuteberg, 2016). BIM has emerged as one of the most significant technological innovations in the construction sector because it enables collaborative information management, improved visualization, lifecycle asset management, and enhanced project decision-making (Eastman et al., 2018). Within Quantity Surveying (QS) practice, BIM has transformed traditional cost management functions by facilitating automated quantity take-offs, digital cost estimation, procurement planning, lifecycle costing, and project performance monitoring (Aigbavboa et al., 2023; Lu et al., 2022). The integration of BIM into quantity surveying workflows improves project accuracy, reduces errors, and enhances collaboration among project stakeholders (Arif et al., 2024).

Despite these benefits, the increased digitalization of construction processes has expanded the cybersecurity attack surface available to malicious actors (Alreshidi et al., 2023). BIM environments increasingly rely on cloud-based collaboration platforms, Common Data Environments (CDEs), mobile technologies, and interconnected digital systems that process highly sensitive project information (Bolton et al., 2023). Consequently, construction organizations face growing threats from ransomware attacks, insider threats, phishing campaigns, intellectual property theft, and unauthorized access to critical project information (Borkovich & Skovira, 2024). Recent industry reports indicate that cyberattacks targeting construction organizations have increased significantly due to the sector's growing reliance on digital technologies and interconnected supply chains (IBM, 2024; World Economic Forum, 2024). The increasing adoption of BIM therefore necessitates stronger cybersecurity governance mechanisms capable of protecting digital assets and ensuring operational resilience (Kassem & Succar, 2023).

To address these concerns, international standards such as ISO 19650-5 provide guidance for security-minded BIM information management, while the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 offers a comprehensive governance structure for cybersecurity risk management (ISO, 2025; NIST, 2024). However, cybersecurity governance within BIM-enabled Quantity Surveying environments remains underdeveloped in many developing countries, including Nigeria (Adebiyi et al., 2024).

Although BIM adoption is steadily increasing within Quantity Surveying practice, cybersecurity considerations have not received proportional attention (Mahamadu et al., 2023). Existing BIM implementation initiatives primarily focus on interoperability, productivity enhancement, project efficiency, and cost reduction (Succar & Kassem, 2022). As a result, cybersecurity governance, workforce preparedness, incident response capabilities, and risk management practices remain inadequately developed (Alenezi et al., 2024).

Several studies have examined barriers to BIM adoption in developing economies (Aigbavboa et al., 2023; Oke et al., 2024). However, limited empirical research has investigated cybersecurity vulnerabilities associated with BIM-enabled Quantity Surveying practice, particularly within the Nigerian construction industry. Furthermore, there is a notable absence of validated cybersecurity governance frameworks specifically designed for BIM-enabled Quantity Surveying environments (Mahamadu et al., 2023).

The absence of such frameworks exposes construction organizations to cyber risks capable of compromising information confidentiality, data integrity, operational continuity, and stakeholder trust (Kure et al., 2024).

2. LITERATURE REVIEW

a. Building Information Modeling in Quantity Surveying Practice

Building Information Modeling has evolved from a three-dimensional visualization technology into a comprehensive digital information management system that supports the entire lifecycle of construction projects (Eastman et al., 2018). BIM enables project stakeholders to create, manage, and exchange information efficiently while promoting collaboration and reducing information silos (Succar & Kassem, 2022). Within Quantity Surveying practice, BIM applications include automated quantity take-offs, cost estimation, procurement planning, value engineering, risk analysis, and lifecycle cost management (Aigbavboa et al., 2023). Recent studies have shown that BIM adoption improves cost estimation accuracy, enhances project transparency, and reduces rework during construction projects (Arif et al., 2024; Lu et al., 2022).

Nevertheless, the migration from traditional document-based workflows to cloud-based BIM environments has introduced new cybersecurity concerns associated with information sharing and digital collaboration (Bolton et al., 2023).

b. Cybersecurity Challenges in BIM Environments

The cybersecurity landscape surrounding BIM environments is increasingly complex due to the interconnected nature of digital construction ecosystems (Mahamadu et al., 2023). BIM platforms facilitate information exchange among architects, engineers, quantity surveyors, contractors, consultants, and facility managers, thereby increasing exposure to cyber threats (Alreshidi et al., 2023).

Common cybersecurity threats affecting BIM-enabled environments include:

- i. Unauthorized access to project information (Kure et al., 2024);
- ii. Insider threats resulting from privileged user abuse (Borkovich & Skovira, 2024);
- iii. Data manipulation and corruption of BIM models (Mahamadu et al., 2023);
- iv. Ransomware attacks targeting project databases (IBM, 2024);
- v. Cloud platform vulnerabilities (Bolton et al., 2023);
- vi. Credential theft and phishing attacks (World Economic Forum, 2024);

Intellectual property theft involving proprietary designs and project information (Alenezi et al., 2024).

Successful cyberattacks can result in project delays, financial losses, legal liabilities, and reputational damage (Kure et al., 2024).

c. ISO 19650-5 and Security-Minded BIM

ISO 19650-5 provides internationally recognized guidance for managing sensitive information within BIM-enabled environments (ISO, 2025). The standard introduces a security-minded approach that focuses on identifying sensitive information, assessing risks, restricting access, implementing security controls, and promoting a culture of information security throughout the project lifecycle (ISO, 2025).

Researchers have argued that ISO 19650-5 offers a critical foundation for securing digital construction information and protecting critical infrastructure assets against emerging cyber threats (Bolton et al., 2023; Mahamadu et al., 2023).

d. NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework 2.0 provides a comprehensive cybersecurity governance structure applicable across industries and organizational sizes (NIST, 2024). The framework consists of six core functions: Govern, Identify, Protect, Detect, Respond, Recover. The introduction of the Govern function

emphasizes leadership accountability, cybersecurity governance, policy development, and risk management integration (NIST, 2024). This evolution reflects the growing recognition that cybersecurity is a strategic organizational issue rather than solely a technical concern (Kure et al., 2024). For BIM-enabled Quantity Surveying organizations, the NIST CSF 2.0 provides a useful structure for integrating governance, risk management, technical security controls, incident response mechanisms, and continuous improvement activities (Alenezi et al., 2024).

Although BIM adoption has received significant scholarly attention, cybersecurity research within BIM-enabled Quantity Surveying practice remains relatively limited (Mahamadu et al., 2023). Existing studies predominantly focus on BIM implementation barriers, technology adoption, and project performance outcomes (Aigbavboa et al., 2023; Oke et al., 2024). Few studies have developed cybersecurity governance frameworks specifically tailored to Quantity Surveying workflows, and even fewer have validated such frameworks within developing-country contexts.

Accordingly, this study seeks to bridge this gap by developing and validating a cybersecurity governance framework for BIM-enabled Quantity Surveying practice in Nigeria.

3. RESEARCH METHODOLOGY

a. Research Design

This study adopted a mixed-methods research design using a convergent parallel approach to investigate cybersecurity governance within Building Information Modeling (BIM)-enabled Quantity Surveying practice in Nigeria. The mixed-methods approach combines the strengths of quantitative and qualitative research to provide a comprehensive understanding of complex organizational and technological issues (Creswell & Creswell, 2023). Quantitative data were collected through a structured questionnaire administered to Quantity Surveyors and other construction professionals, while qualitative insights were obtained through expert opinions and document analysis to support the development of the proposed cybersecurity governance framework.

b. Study Population and Sampling

The target population comprised Quantity Surveyors, BIM Managers, Construction Project Managers, Information and Communication Technology (ICT) professionals, Cybersecurity Specialists, and Construction Consultants involved in BIM implementation within the Nigerian construction industry. These professionals were selected because of their direct involvement in digital construction processes and information management.

A purposive sampling technique was employed to ensure that respondents possessed adequate knowledge of BIM implementation and cybersecurity practices. A total of **235 valid responses** were obtained and used for the empirical analysis. The sample size was considered adequate for multivariate statistical analyses, including multiple regression, in accordance with recommendations by Hair et al. (2022).

c. Research Instrument

Data were collected using a structured questionnaire comprising forty-four (44) variables organized into six major sections. The questionnaire contained demographic questions, BIM adoption variables, cybersecurity awareness items, cybersecurity threat assessment items, organizational preparedness indicators, regulatory awareness measures, and framework validation statements. Most perception-based items were measured using five-point Likert scales adapted to the context of each construct. Responses were coded numerically to facilitate statistical analysis.

d. Operationalization of Research Constructs

The conceptual framework was operationalized into five latent constructs representing the principal dimensions of cybersecurity governance within BIM-enabled Quantity Surveying practice. Each construct was measured using multiple questionnaire items, and composite scores were calculated by averaging the coded responses.

i. Cybersecurity Awareness (CSA)

Cybersecurity Awareness measures respondents' understanding of cybersecurity principles, secure digital practices, password management, phishing awareness, and information security responsibilities. The construct was measured using four questionnaire items (Q12–Q15) rated on a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5).

The composite score for Cybersecurity Awareness was computed as:

$$CSA = \frac{Q_{12} + Q_{13} + Q_{14} + Q_{15}}{4} \quad (1)$$

where:

- a. Q_{12} = Knowledge of cybersecurity principles
- b. Q_{13} = Password management practices
- c. Q_{14} = Phishing awareness
- d. Q_{15} = Information security responsibilities

ii. Cybersecurity Threat Exposure (CTE)

Cybersecurity Threat Exposure assesses respondents' perceptions of cyber risks associated with BIM-enabled environments, including insider threats, ransomware, unauthorized access, cloud vulnerabilities, and data manipulation.

Question 17 was rated using a five-point scale ranging from Very Low (1) to Very High (5), while Questions 18–23 employed a five-point likelihood scale ranging from Very Unlikely (1) to Very Likely (5).

The composite score was calculated as:

$$CTE = \frac{Q_{17} + Q_{18} + Q_{19} + Q_{20} + Q_{21} + Q_{22} + Q_{23}}{7} \quad (2)$$

where:

Q_{17} measures the perceived level of cyber threats.

$Q_{18} - Q_{23}$ measure the perceived likelihood of specific cybersecurity threats in BIM-enabled environments.

iii. Organizational Cybersecurity Preparedness (OCP)

Organizational Cybersecurity Preparedness evaluates the effectiveness of cybersecurity policies, technical controls, incident response mechanisms, employee training, and organizational readiness. Five questionnaire items (Q26–Q30) were rated on a scale ranging from Not Effective (1) to Very Effective (5).

The composite score was calculated as:

$$OCP = \frac{Q_{26} + Q_{27} + Q_{28} + Q_{29} + Q_{30}}{5} \quad (3)$$

where the items measure:

Cybersecurity policy implementation

Technical security controls

Incident response capability

Staff training

Organizational readiness

iv. **Regulatory Awareness (RA)**

Regulatory Awareness measures respondents' familiarity with cybersecurity regulations, standards, and legal requirements governing BIM implementation. Three questionnaire items (Q31–Q33) were measured on a five-point scale ranging from Not Aware (1) to Highly Aware (5).

The construct score was computed as:

$$RA = \frac{Q_{31} + Q_{32} + Q_{33}}{3} \quad (4)$$

where the items evaluate respondents' awareness of:

Cybersecurity legislation

BIM standards

Regulatory compliance requirements

v. **Framework Acceptance (FA)**

Framework Acceptance represents respondents' evaluation of the proposed Cybersecurity Governance Framework for BIM-enabled Quantity Surveying practice. Five questionnaire items (Q34–Q38) were rated on a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5).

The composite score was computed as:

$$FA = \frac{Q_{34} + Q_{35} + Q_{36} + Q_{37} + Q_{38}}{5} \quad (5)$$

where the items measure respondents' acceptance of the proposed Cybersecurity Governance Framework.

Table 1 explains how the five principal latent dimensions Cybersecurity Awareness (CSA), Cybersecurity Threat Exposure (CTE), Organizational Cybersecurity Preparedness (OCP), Regulatory Awareness (RA), and Framework Acceptance (FA) were mapped to specific questionnaire items, measurement scales, and composite mean scores.

Table 1. Operationalization of Research Constructs

Construct	Questionnaire Items	Scale	Composite Measure
Cybersecurity Awareness (CSA)	Q12–Q15	Strongly Disagree (1) – Strongly Agree (5)	Mean Score
Cybersecurity Threat Exposure (CTE)	Q17–Q23	Very Low/Very Unlikely (1) – Very High/Very Likely (5)	Mean Score
Organizational Cybersecurity Preparedness (OCP)	Q26–Q30	Not Effective (1) – Very Effective (5)	Mean Score
Regulatory Awareness (RA)	Q31–Q33	Not Aware (1) – Highly Aware (5)	Mean Score
Framework Acceptance (FA)	Q34–Q38	Strongly Disagree (1) – Strongly Agree (5)	Mean Score

e. Data Coding and Preparation

All Likert-scale responses were converted into numerical values prior to statistical analysis. Data cleaning involved screening for missing values, inconsistencies, and duplicate responses. Composite construct scores were subsequently generated by averaging the coded responses for each latent variable.

Demographic variables and multiple-response questions relating to BIM software, BIM implementation stages, and cybersecurity controls were analyzed descriptively using frequencies and percentages. Open-ended responses were subjected to thematic analysis to complement the quantitative findings.

f. Reliability Analysis

The internal consistency of the measurement scales was evaluated using Cronbach's alpha coefficient. Following Hair et al. (2022), alpha values of **0.70 or higher** were considered indicative of acceptable reliability.

Before proceeding with multivariate inferential statistical analyses, it was imperative to verify that the survey instruments provided stable and consistent measurements. Table 2 displays the preliminary internal consistency values obtained during the instrument reliability screening. A parallel confirmation of these measurement profiles, alongside their structural interpretations for the finalized sample size, is presented in Table 5.

Table 2. Reliability Assessment of Research Constructs

Construct	Number of Items	Cronbach's α	Interpretation
Cybersecurity Awareness	4	0.686	Acceptable (Exploratory)

Cybersecurity Threat Exposure	7	0.775	Good
Organizational Cybersecurity Preparedness	5	0.817	Good
Regulatory Awareness	3	0.540	Low (Analysed Separately)
Framework Acceptance	5	0.762	Good

g. Data Analysis Techniques

Descriptive and inferential statistical techniques were employed to analyze the data using IBM SPSS Statistics.

Descriptive statistics included frequencies, percentages, means, standard deviations, and Relative Importance Index (RII) to summarize respondents' characteristics and perceptions. Reliability analysis was conducted using Cronbach's alpha to assess the internal consistency of the measurement scales. Pearson correlation analysis was employed to examine relationships among the latent constructs, while multiple linear regression analysis was performed to determine the influence of cybersecurity awareness, threat exposure, organizational preparedness, and regulatory awareness on respondents' acceptance of the proposed cybersecurity governance framework.

The regression model is expressed as:

$$FA = \beta_0 + \beta_1 CSA + \beta_2 CTE + \beta_3 OCP + \varepsilon \quad (6)$$

where:

- FA = Framework Acceptance (Dependent Variable)
- CSA = Cybersecurity Awareness
- CTE = Cybersecurity Threat Exposure
- OCP = Organizational Cybersecurity Preparedness
- β_0 = Regression intercept (constant)
- $\beta_1, \beta_2, \beta_3$ = Regression coefficients
- ε = Random error term

Model adequacy was evaluated using the coefficient of determination (R^2), adjusted R^2 , analysis of variance (ANOVA), standardized beta coefficients, t-tests, and significance levels ($p < 0.05$).

h. Conceptual Model of the Study

The study hypothesizes that increased cybersecurity awareness, greater understanding of cyber threats, improved organizational preparedness, and stronger regulatory awareness positively influence stakeholders' acceptance of a cybersecurity governance framework for BIM-enabled Quantity Surveying practice.

The conceptual model forms the analytical basis for the empirical validation of the proposed framework and provides a structured approach for examining the determinants of cybersecurity governance within digital construction environments.

4. RESULTS AND DISCUSSION

a. Demographic Characteristics of Respondents

A total of 235 valid responses were received and analysed. The respondents represented a broad cross-section of professionals involved in Building Information Modeling (BIM) implementation and Quantity Surveying practice in Nigeria.

i. Gender Distribution

Of the 235 respondents, 139 (59.1%) were male and 94 (40.0%) were female (two records were missing or incomplete for this variable). This distribution reflects the continued predominance of males within the Nigerian construction industry while demonstrating increasing female participation in digital construction and Quantity Surveying. To establish the demographic profile of the study participants, respondents were categorized according to gender. Understanding the gender composition of the sample is important for assessing the representativeness of the dataset and determining whether the findings adequately reflect the perspectives of professionals involved in BIM-enabled Quantity Surveying practice. The gender distribution of the respondents is presented in Table 3.

Table 3 breaks down the sample of 235 participants by gender, showing a distribution of 59.1% male and 40.0% female respondents (with 0.9% missing data).

Table 3. Gender Distribution of Respondents

Gender	Frequency	Percentage (%)
Male	139	59.1
Female	94	40.0
Missing	2	0.9
Total	235	100.0

The relatively balanced representation enhances the credibility of the study by incorporating perspectives from both male and female professionals.

ii. Professional Distribution

The respondents comprised professionals occupying diverse roles within the construction sector.

Since the study investigates cybersecurity governance within BIM-enabled Quantity Surveying practice, it was important to identify the professional backgrounds of the respondents. The inclusion of participants from different construction-related professions enhances the diversity of viewpoints and strengthens the applicability of the proposed governance framework. The professional distribution of the respondents is summarized in Table 4. Table 4 categorizes the participants by their specialized roles. It confirms that Quantity Surveyors make up the heavy majority of the dataset (170 out of 235 respondents), ensuring the findings are highly representative of actual QS workflows.

Table 4. Professional Distribution of Respondents

Profession	Frequency
Quantity Surveyor	170
Project Manager	20
BIM Specialist/Technologist	7
Academic/Researcher	6
Other Professionals	29
Missing	3
Total	235

Quantity Surveyors constituted approximately 72% of the respondents, confirming that the dataset is highly representative of the target population for this study. This strengthens the validity of the proposed cybersecurity governance framework for Quantity Surveying practice.

b. Reliability Analysis

Reliability analysis was undertaken to evaluate the internal consistency of the research constructs using Cronbach's alpha. The findings indicate satisfactory reliability for most constructs.

Before testing the proposed research hypotheses, the internal consistency of the measurement constructs was evaluated using Cronbach's alpha coefficient. Reliability analysis determines whether the questionnaire items consistently measure their intended latent constructs and provides evidence of the suitability of the scales for subsequent statistical analyses. The reliability results are presented in Table 5.

Table 5. Reliability Analysis of the Measurement Constructs

Construct	Number of Items	Cronbach's α	Interpretation
Cybersecurity Awareness	4	0.686	Acceptable (Exploratory)
Cybersecurity Threat Exposure	7	0.775	Good
Organizational Cybersecurity Preparedness	5	0.817	Good
Regulatory Awareness	3	0.540	Low (Analysed Separately)
Framework Acceptance	5	0.762	Good

Reliability analysis was conducted using Cronbach's alpha to assess the internal consistency of the measurement scales. The results indicated that Cybersecurity Threat Exposure ($\alpha = 0.775$), Organizational Cybersecurity Preparedness ($\alpha = 0.817$), and Framework Acceptance ($\alpha = 0.762$) demonstrated good internal consistency. The Cybersecurity Awareness construct yielded an alpha coefficient of 0.686, which is marginally below the conventional threshold of 0.70 but is considered acceptable for exploratory studies and newly developed instruments (Hair et al., 2022). In contrast, Regulatory Awareness produced a lower

alpha coefficient ($\alpha = 0.540$), suggesting that the three items may not measure a single homogeneous construct. This is unsurprising because they capture awareness of two different regulations together with an opinion on whether current regulations adequately address BIM cybersecurity.

c. Overview of BIM Adoption

The questionnaire included items assessing BIM adoption within respondents' organizations, including BIM implementation status, adoption level, project stages where BIM is used, software platforms employed, and the use of Common Data Environments (CDEs).

These variables provide valuable contextual information regarding the maturity of digital construction practices and establish the operational environment in which cybersecurity governance is required. Subsequent descriptive analyses will summarize BIM adoption patterns, commonly used software platforms, and collaborative information management practices.

d. Descriptive Statistics of Research Constructs

Composite scores were calculated for the validated constructs by averaging the coded responses of the respective questionnaire items. Higher mean scores indicate stronger agreement or higher perceived effectiveness. Following the reliability assessment, descriptive statistics were computed to summarize respondents' perceptions of the major research constructs. Composite mean scores were calculated for each construct to provide an overall indication of cybersecurity awareness, cybersecurity threat exposure, organizational cybersecurity preparedness, and framework acceptance among the respondents. The descriptive statistics are presented in Table 6.

Table 6 synthesizes the overall baseline perceptions of the respondents by displaying the composite mean scores. Framework Acceptance (FA) achieved the highest baseline support ($M = 3.637$)

Table 6. Descriptive Statistics of the Research Constructs (n = 230–235)

Construct	Mean
Cybersecurity Awareness (CSA)	3.281
Cybersecurity Threat Exposure (CTE)	3.000
Organizational Cybersecurity Preparedness (OCP)	3.087
Framework Acceptance (FA)	3.637

The respondents demonstrated a moderately high level of cybersecurity awareness ($M = 3.281$, $SD = 0.747$). Perceived cybersecurity threat exposure was moderate ($M = 3.000$, $SD = 0.853$), suggesting that respondents recognized the presence of cyber risks within BIM-enabled environments.

Organizational Cybersecurity Preparedness also recorded a moderate mean score ($M = 3.087$, $SD = 0.937$), indicating that while some cybersecurity controls are in place, organizations still have considerable room for improvement.

Framework Acceptance recorded the highest mean score ($M = 3.637$, $SD = 0.875$), indicating broad stakeholder support for the development and implementation of a dedicated cybersecurity governance framework for BIM-enabled Quantity Surveying practice.

e. Correlation Analysis

Pearson correlation analysis was conducted to examine the relationships among the principal research

constructs. To examine the relationships among the principal study variables, Pearson product–moment correlation analysis was performed. This analysis provides preliminary evidence of the strength and direction of the associations among the constructs before conducting multivariate regression analysis. The correlation coefficients for the research variables are presented in Table 7. Table 7 outlines the preliminary strength and positive direction of the linear relationships among the constructs, showing that Cybersecurity Awareness has the strongest individual correlation with Framework Acceptance ($r = 0.418$)

Table 7. Pearson Correlation Matrix

Variable	CSA	CTE	OCP	FA
Cybersecurity Awareness (CSA)	1.000	0.262	0.397	0.418
Cybersecurity Threat Exposure (CTE)	0.262	1.000	0.292	0.216
Organizational Preparedness (OCP)	0.397	0.292	1.000	0.372
Framework Acceptance (FA)	0.418	0.216	0.372	1.000

The correlation analysis revealed positive relationships among all constructs.

Cybersecurity Awareness demonstrated the strongest relationship with Framework Acceptance ($r = .418$), followed by Organizational Preparedness ($r = 0.372$). Cybersecurity Threat Exposure also showed a positive but weaker association with Framework Acceptance ($r = 0.216$).

These findings suggest that respondents with greater cybersecurity awareness and stronger perceptions of organizational preparedness are more likely to support the proposed cybersecurity governance framework.

f. Multiple Regression Analysis

Multiple linear regression analysis was performed to examine the influence of Cybersecurity Awareness, Cybersecurity Threat Exposure, and Organizational Cybersecurity Preparedness on Framework Acceptance. Multiple linear regression analysis was conducted to determine the extent to which the independent variables explain variations in stakeholders' acceptance of the proposed cybersecurity governance framework. The model summary provides information on the explanatory power of the regression model, including the coefficient of determination (R^2) and adjusted R^2 . The results are presented in Table 8. In table 8, the model summary establishes the overall explanatory power of the predictive model, indicating that the combined independent variables account for approximately 22.4% of the variation in framework acceptance ($R^2 = 0.224$)

Table 8. Model Summary

Statistic	Value
R^2	0.224
Adjusted R^2	0.214
Number of Observations	230

The regression model explained approximately 22.4% of the variation in Framework Acceptance, indicating a moderate level of explanatory power.

The overall statistical significance of the regression model was assessed using analysis of variance (ANOVA). This test determines whether the combined predictor variables significantly explain variations in the dependent variable and whether the regression model provides a better fit than a model with no predictors. The ANOVA results are presented in Table 9. Table 9 verifies the mathematical fit of the model, proving that the regression framework is highly statistically significant ($F = 21.78, p < 0.001$)

Table 9. ANOVA Results

Statistic	Value
F	21.78
Significance (p)	< 0.001

The overall regression model was statistically significant, $F(3, 226) = 21.78, p < 0.001$, indicating that the predictor variables jointly explain a significant proportion of the variance in Framework Acceptance.

To identify the individual contribution of each independent variable to framework acceptance, the regression coefficients were examined. The coefficient estimates provide information on the magnitude, direction, and statistical significance of each predictor while controlling for the effects of the other variables included in the model. The regression coefficients are presented in Table 10. In table 10 Regression Coefficients isolates the individual impact of each predictor variable when controlling for the others. It reveals that Cybersecurity Awareness ($B = 0.359, p < 0.001$) and Organizational Preparedness ($B = 0.213, p = 0.001$) are significant positive drivers, whereas Threat Exposure is not a significant predictor ($p = 0.299$).

Table 10. Regression Coefficients

Predictor	Unstandardized B	t	p	Decision
Constant	1.598	5.921	<0.001	Significant
Cybersecurity Awareness (CSA)	0.359	4.605	<0.001	Significant
Cybersecurity Threat Exposure (CTE)	0.067	1.042	0.299	Not Significant
Organizational Preparedness (OCP)	0.213	3.420	0.001	Significant

The regression analysis indicates that Cybersecurity Awareness and Organizational Cybersecurity Preparedness are statistically significant predictors of Framework Acceptance.

Cybersecurity Awareness had the strongest positive influence ($B = 0.359, t = 4.605, p < 0.001$), indicating that respondents with greater cybersecurity knowledge are significantly more likely to support the proposed cybersecurity governance framework.

Organizational Cybersecurity Preparedness also exerted a significant positive effect ($B = 0.213, t = 3.420, p = 0.001$), demonstrating that organizations with stronger cybersecurity controls and preparedness mechanisms exhibit greater acceptance of structured governance initiatives.

Conversely, Cybersecurity Threat Exposure did not significantly predict Framework Acceptance ($B = 0.067$, $t = 1.042$, $p = 0.299$). This finding suggests that although respondents recognize cybersecurity threats within BIM environments, the perception of threat alone does not necessarily translate into stronger support for governance frameworks unless accompanied by adequate awareness and organizational preparedness.

g. Hypothesis Testing

The research hypotheses were evaluated based on the outcomes of the multiple regression analysis. Each hypothesis was assessed using the statistical significance and direction of the estimated regression coefficients to determine whether empirical evidence supported the proposed relationships among the study variables. The summary of the hypothesis-testing results is presented in Table 11. Table 11 provides the final verdict on the research hypotheses, concluding that H1 (Awareness) and H3 (Preparedness) are empirically supported, while H2 (Threat Exposure) is not supported.

Table 11. Summary of Hypothesis Testing

Hypothesis	Result
H1: Cybersecurity Awareness positively influences Framework Acceptance	Supported
H2: Cybersecurity Threat Exposure positively influences Framework Acceptance	Not Supported
H3: Organizational Cybersecurity Preparedness positively influences Framework Acceptance	Supported

5. DISCUSSION OF FINDINGS

a. Influence of Cybersecurity Awareness on Framework Acceptance

The findings demonstrate that Cybersecurity Awareness significantly influences stakeholders' acceptance of the proposed Cybersecurity Governance Framework for BIM-enabled Quantity Surveying practice ($B = 0.359$, $p < 0.001$). Among all predictor variables examined, cybersecurity awareness exerted the strongest influence on framework acceptance, indicating that professionals with greater knowledge of cybersecurity principles are more likely to recognize the need for structured governance mechanisms within BIM environments.

This finding corroborates previous studies emphasizing that cybersecurity awareness is a fundamental determinant of organizational cyber resilience. Recent research has consistently shown that awareness programmes, security education, and continuous professional development significantly improve secure behaviour among construction professionals and reduce the likelihood of human-related cybersecurity incidents (Mahamadu et al., 2023; Verizon, 2024). Similarly, the introduction of the **Govern** function in the NIST Cybersecurity Framework (CSF) 2.0 highlights workforce awareness and organizational culture as critical components of effective cybersecurity governance (NIST, 2024).

The implication is that cybersecurity awareness should not be regarded merely as an operational requirement but as a strategic organizational capability that supports informed decision-making, regulatory compliance, and secure BIM collaboration throughout the project lifecycle.

b. Organizational Cybersecurity Preparedness

The regression results further revealed that Organizational Cybersecurity Preparedness significantly predicts acceptance of the proposed framework ($B = 0.213$, $p = 0.001$). This finding indicates that organizations possessing stronger cybersecurity policies, technical safeguards, employee training programmes, and incident response capabilities demonstrate greater readiness to adopt comprehensive cybersecurity governance practices.

The reliability analysis also showed that Organizational Cybersecurity Preparedness achieved the highest internal consistency (Cronbach's $\alpha = 0.817$), suggesting that respondents consistently perceived organizational readiness as a multidimensional construct encompassing governance structures, technological controls, and workforce competence.

These findings support the recommendations of ISO/IEC 27001:2022 and the NIST Cybersecurity Framework 2.0, both of which emphasize that effective cybersecurity governance requires the integration of organizational policies, leadership commitment, risk management, and continuous improvement. Within BIM-enabled Quantity Surveying environments, organizational preparedness is particularly important because project information is frequently exchanged among multiple stakeholders through cloud-based collaborative platforms, increasing exposure to unauthorized access, insider threats, and data manipulation.

c. Cybersecurity Threat Exposure

Although respondents generally acknowledged the presence of cybersecurity risks within BIM-enabled environments, Cybersecurity Threat Exposure did not significantly predict framework acceptance ($p = 0.299$). This suggests that recognizing cyber threats alone may not be sufficient to motivate support for formal cybersecurity governance mechanisms.

A plausible explanation is that professionals may already perceive cybersecurity threats as inherent to digital construction environments. Consequently, acceptance of governance initiatives depends more strongly on organizational capacity, awareness, leadership commitment, and available resources than on perceived threat severity alone.

This observation is consistent with behavioural cybersecurity theories, which argue that awareness, self-efficacy, and organizational support are stronger determinants of security behaviour than risk perception in isolation.

d. Relationships among the Research Constructs

The correlation analysis demonstrated positive associations among all principal constructs. Cybersecurity Awareness exhibited the strongest correlation with Framework Acceptance, followed by Organizational Cybersecurity Preparedness, while Cybersecurity Threat Exposure showed a comparatively weaker relationship.

These findings reinforce the proposition that cybersecurity governance within BIM-enabled Quantity Surveying practice is influenced by multiple interrelated organizational and behavioural factors rather than by technological considerations alone. Consequently, cybersecurity governance should be approached as an integrated socio-technical system combining people, processes, technology, and organizational leadership.

6. THEORETICAL IMPLICATIONS

This study contributes to the growing body of knowledge on cybersecurity governance within digital construction by extending existing BIM governance literature through the integration of cybersecurity principles into Quantity Surveying practice. Whereas previous studies have predominantly focused on

BIM implementation, information management, and digital collaboration, the present study demonstrates that effective BIM adoption must be accompanied by structured cybersecurity governance.

The proposed framework further contributes to the literature by integrating principles from ISO 19650-5, ISO/IEC 27001:2022, and the NIST Cybersecurity Framework 2.0 into a unified governance model specifically tailored to Quantity Surveying practice.

7. PRACTICAL IMPLICATIONS

The findings provide several practical implications for stakeholders in the construction industry.

a. For Quantity Surveying Firms

- i. Establish formal cybersecurity governance committees.
- ii. Develop BIM-specific cybersecurity policies and procedures.
- iii. Conduct periodic cybersecurity risk assessments.
- iv. Implement mandatory cybersecurity awareness and training programmes.

b. For Construction Organizations

- i. Integrate cybersecurity into BIM implementation strategies.
- ii. Adopt multi-factor authentication, role-based access control, and encryption technologies.
- iii. Strengthen incident response planning and business continuity management.

c. For Professional Bodies

Professional organizations should incorporate BIM cybersecurity competencies into professional certification programmes and continuing professional development initiatives to improve industry-wide cyber resilience.

d. For Government and Regulatory Agencies

Government agencies should develop BIM-specific cybersecurity guidelines, promote compliance with international standards, and encourage cybersecurity maturity assessments across the construction sector.

8. CONTRIBUTIONS OF THE STUDY

This research makes several important contributions:

- a. It provides one of the first empirical investigations of cybersecurity governance in BIM-enabled Quantity Surveying practice within Nigeria.
- b. It develops and validates a dedicated Cybersecurity Governance Framework tailored to the operational realities of Quantity Surveying organizations.
- c. It identifies cybersecurity awareness and organizational preparedness as the most influential determinants of framework acceptance.
- d. It demonstrates that perceived cyber threats alone are insufficient to drive governance adoption without corresponding organizational capability and leadership commitment.
- e. It aligns BIM cybersecurity governance with internationally recognized standards, including ISO 19650-5, ISO/IEC 27001:2022, and the NIST Cybersecurity Framework 2.0.

9. CONCLUSION

This study investigated the factors influencing cybersecurity governance within BIM-enabled Quantity Surveying practice and developed a governance framework tailored to the Nigerian construction industry.

The research integrated established cybersecurity principles with BIM information management requirements to address the growing cyber risks associated with digital construction.

The empirical findings demonstrated that cybersecurity awareness and organizational cybersecurity preparedness are key determinants of stakeholders' acceptance of a cybersecurity governance framework. These findings highlight that successful cybersecurity governance extends beyond technical safeguards and depends on organizational culture, leadership commitment, workforce competence, and structured governance mechanisms.

The study further revealed that, although respondents recognized the existence of cybersecurity threats in BIM-enabled environments, threat perception alone was insufficient to explain framework acceptance. This suggests that organizations are more likely to embrace cybersecurity governance when they possess the knowledge, capabilities, and institutional support required to implement effective security practices.

The proposed Cybersecurity Governance Framework provides a structured approach for integrating cybersecurity into BIM-enabled Quantity Surveying practice by aligning governance, risk management, technical controls, workforce development, and regulatory compliance. By drawing on the principles of ISO 19650-5, ISO/IEC 27001:2022, and the NIST Cybersecurity Framework 2.0, the framework offers practical guidance for enhancing the confidentiality, integrity, availability, and resilience of digital construction information.

Overall, this research contributes to both scholarship and professional practice by demonstrating that cybersecurity governance should be regarded as a strategic enabler of secure digital transformation rather than solely as a technical function.

10. RECOMMENDATIONS

Based on the findings of this study, the following recommendations are proposed.

a. For Quantity Surveying Firms

Quantity Surveying organizations should establish formal cybersecurity governance structures that clearly define roles, responsibilities, accountability mechanisms, and reporting procedures for BIM information security. Cybersecurity governance should be integrated into organizational policies and project management practices rather than being treated as a standalone technical function.

Continuous cybersecurity awareness programmes should be implemented for all personnel involved in BIM-enabled projects to strengthen security culture and reduce human-related vulnerabilities.

b. For Construction Organizations

Construction organizations should adopt internationally recognized cybersecurity standards, including ISO 19650-5, ISO/IEC 27001:2022, and the NIST Cybersecurity Framework 2.0, to improve information protection across the BIM lifecycle.

Organizations should also invest in secure Common Data Environments (CDEs), multi-factor authentication, encryption technologies, access control mechanisms, continuous monitoring, and incident response capabilities to strengthen cyber resilience.

c. For Professional Institutions

Professional bodies should incorporate BIM cybersecurity into certification requirements, continuing professional development programmes, and competency frameworks. Greater emphasis should be placed on cybersecurity governance, digital ethics, information management, and secure collaboration within Quantity Surveying education and professional practice.

d. For Government and Regulatory Agencies

Government agencies should develop sector-specific cybersecurity guidelines for BIM implementation, establish minimum cybersecurity compliance requirements for public construction projects, and encourage regular cybersecurity audits across the construction industry.

e. For Academic Institutions

Higher education institutions should integrate BIM cybersecurity governance into Quantity Surveying, Construction Management, Architecture, Engineering, and Information Technology curricula. This will ensure that graduates possess the interdisciplinary knowledge required to manage cybersecurity risks in increasingly digital construction environments.

Practical Contributions

This study provides practical guidance that can assist organizations in:

- developing cybersecurity governance policies for BIM implementation;
- improving workforce cybersecurity awareness;
- strengthening organizational preparedness against cyber threats;
- supporting compliance with international cybersecurity and BIM standards; and
- enhancing trust in collaborative digital construction environments.

Policy Implications

The findings indicate the need for national policies that integrate cybersecurity governance into digital construction initiatives. Policymakers should consider incorporating cybersecurity requirements into BIM adoption strategies, procurement regulations, and public infrastructure projects to promote secure digital transformation throughout the construction sector.

References

- Abioye, S. O., et al. (2021). Artificial intelligence in the construction industry: A review of present status, opportunities and future challenges. *Journal of Management in Engineering*, 37(6), Article 04021060.
- Adebisi, A., et al. (2024). Cybersecurity readiness in the Nigerian construction industry: Evaluating the awareness and practices of built environment professionals. *Journal of Engineering, Project, and Production Management*, 14(2), 115–128.
- Aigbavboa, C., et al. (2023). Digital cost management: The adoption and impact of Building Information Modeling (BIM) in quantity surveying workflows. *International Journal of Construction Management*, 23(8), 1345–1356.
- Alenezi, M., et al. (2024). Cyber security challenges and governance frameworks in collaborative digital construction: A systematic review. *Computers in Industry*, 154, Article 104032.
- Alreshidi, E., et al. (2023). Cloud-based BIM environments and vulnerability to cyber threats: A sociotechnical assessment. *Automation in Construction*, 149, Article 104789.
- Arif, M., et al. (2024). Enhancing cost estimation accuracy and project transparency through BIM integration in quantity surveying. *Construction Innovation*, 24(3), 612–630.
- Bolton, L., et al. (2023). Securing the Common Data Environment (CDE): Cyber security governance in BIM-enabled project delivery. *Journal of Information Technology in Construction (ITcon)*, 28,

445–463.

- Borkovich, D. J., & Skovira, R. J. (2024). Insider threats and privileged user abuse in digital architecture and engineering ecosystems. *International Journal of Cyber Warfare and Terrorism*, 14(1), 1–19.
- Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.
- Eastman, C., Teicholz, P., Sacks, R., & Liston, K. (2018). *BIM handbook: A guide to building information modeling for owners, managers, designers, engineers and contractors* (3rd ed.). John Wiley & Sons.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2022). *Multivariate data analysis* (8th ed.). Cengage Learning.
- IBM Security. (2024). *Cost of a data breach report 2024*. IBM Corporation. <https://www.ibm.com/reports/data-breach>
- International Organization for Standardization. (2025). *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management* (ISO Standard No. 19650-5:2025). <https://www.iso.org/standard/iso-19650-5.html>
- Kassem, M., & Succar, B. (2023). Macro-BIM adoption and governance: Conceptual structures for cybersecurity in collaborative construction workflows. *Policy and Strategy in digital construction*, 12(1), 45–67.
- Kure, H. I., et al. (2024). Cyber risk management framework for critical infrastructure protection in digital construction ecosystems. *International Journal of Critical Infrastructure Protection*, 44, Article 100642.
- Lu, W., et al. (2022). Automated quantity take-off and digital cost management: A BIM-based workflow analysis for quantity surveyors. *Advanced Engineering Informatics*, 52, Article 101567.
- Mahamadu, A.-M., et al. (2023). Cyber security in digital construction and BIM environments: Assessing the awareness and preparedness of the built environment workforce. *Safety Science*, 165, Article 106198.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework 2.0* (NIST Special Publication Small Business Coordinating Report). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Oesterreich, T. D., & Teuteberg, F. (2016). Understanding the implications of digitization and automation in the context of Industry 4.0: A triangulation approach and framework for the construction industry. *Computers in Industry*, 83, 121–139.
- Oke, A. E., et al. (2024). Barriers and drivers of building information modelling adoption in developing economies: A comparative meta-analysis. *Built Environment Project and Asset Management*, 14(1), 78–96.
- Succar, B., & Kassem, M. (2022). Building Information Modelling: Intellectual structures and foundational paradigms. *Automation in Construction*, 134, Article 104047.
- Verizon. (2024). *2024 Data breach investigations report*. Verizon Business.

<https://www.verizon.com/business/resources/reports/dbir/>

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.
<https://www.weforum.org/publications/global-cybersecurity-outlook-2024/>



© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>)