GAS Journal of Arts Humanities and Social Sciences (GASJAHSS)

Volume 4 | Issue 1, 2026 Homepage: https://gaspublishers.com/gasjahss/ ISSN: 3048-5002

Assessment of the Impact of Cybersecurity Risks on Digital Supply Networks in Federal University Teaching Hospital, Lafia, Nasarawa State

Ukeje Nkechi Arinze; Moukhtar Suleiman & Prof. Suleiman A.S. Aruwa Ph.D

Institute of Governance and Development Studies, Nasarawa State University, Keffi-Nigeria

Received: *01.01.2026* | ***Accepted:*** *19.01.2026* | ***Published:*** *21.01.2026*

***Corresponding Author:** Ukeje Nkechi Arinze

DOI: *10.5281/zenodo.18323394*

Abstract **Original Research Article**

Digital supply networks are central to the coordination of procurement, financial transactions, and service delivery in public healthcare institutions such as the Federal University Teaching Hospital, Lafia, Nasarawa State. The increasing adoption of digital platforms has, however, heightened exposure to cybersecurity risks, which threaten data confidentiality, operational efficiency, and the sustainability of supply systems. This study examined the impact of two prominent cybersecurity risks data breaches and ransomware attacks on the performance of digital supply networks in the hospital. A quantitative cross-sectional research design was employed, and data were gathered from 110 staff members across the Procurement, ICT, and Finance departments using a structured questionnaire. The data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS 3.0 to determine the significance and magnitude of the relationships among variables.

The results revealed that both data breaches and ransomware attacks have a significant negative effect on digital supply network performance, with ransomware attacks exhibiting a stronger adverse influence. Specifically, data breaches were found to disrupt information flow, compromise procurement transparency, and increase operational delays. Ransomware attacks, however, caused more severe interruptions by locking critical procurement platforms, halting transactions, and increasing system recovery costs. These findings indicate that digital supply operations in the hospital remain vulnerable to cybersecurity disruptions.

The study recommends that the hospital strengthen cybersecurity infrastructure through advanced encryption, multi-factor authentication, and continuous network monitoring to minimize vulnerability to unauthorized access. Additionally, the hospital should develop comprehensive ransomware preparedness and recovery strategies, including routine data backups, offline server protection, and staff cybersecurity awareness training to improve resilience and safeguard digital procurement continuity.

Keywords: Cybersecurity risks, Digital supply networks, Data breaches, Ransomware, Federal University Teaching Hospital Lafia.

Introduction

Digital transformation has changed the way organizations manage supply chains and procurement across the world. Through technology, many institutions now operate faster, more transparently, and with better coordination between suppliers and customers. Digital Supply Networks (DSNs) bring together suppliers, manufacturers, and service providers through connected platforms that allow for real-time data sharing and automated decision-making. According to Bechtsis et al. (2023), these networks rely on advanced technologies such as cloud computing, blockchain, and the Internet of Things (IoT) to enable real-time data sharing, automate procurement processes, and improve responsiveness. When effectively managed, DSNs strengthen traceability, shorten lead times, and promote sustainability. However, as Ardito and Petruzzelli (2024) observed, the growing digitalization of procurement systems also exposes organizations to cybersecurity risks that threaten data integrity, operational efficiency, and stakeholder confidence.

Cybersecurity risks in digital supply networks often take the form of data breaches, ransomware, phishing, and system manipulation. These attacks target sensitive procurement information, supplier credentials, and financial records, leading to financial losses and service disruptions. Lee et al. (2024) reported that ransomware incidents in digital procurement systems across Asia caused severe operational downtime and data loss. Similarly, Shibin et al. (2023) emphasized that such attacks compromise not only data confidentiality but also institutional credibility, especially when they affect supplier evaluations or contract processes. In the public sector, where procurement systems handle large volumes of financial and operational data, cybersecurity risks can have even greater consequences for transparency and accountability.

In Nigeria, the increasing adoption of digital systems in public procurement has brought new efficiency opportunities alongside emerging vulnerabilities. Institutions such as the Federal University Teaching Hospital, Lafia (FUTHL), now depend on electronic procurement, inventory, and supplier communication systems that connect multiple stakeholders procurement officers, suppliers, auditors, and regulators. This interconnectivity, while beneficial, also makes the systems attractive targets for cybercriminals. According to Oladipo and Yusuf (2023), many Nigerian public institutions lack robust cybersecurity frameworks, regular system audits, and adequately trained personnel to manage digital risks. Similarly, Okoro and Musa (2022) observed that weak network infrastructure and poor awareness of cyber hygiene contribute to frequent data breaches in Nigeria's e-government systems. In the healthcare context, Eze and Nwosu (2024) found that several public hospitals face cyber vulnerabilities due to outdated software and limited cybersecurity budgets.

Cybersecurity breaches in digital supply networks can have far-reaching consequences. They disrupt procurement processes, delay service delivery, inflate operational costs, and erode public trust. Ekwueme et al. (2022) noted that in healthcare settings, these breaches can also endanger patient safety and confidentiality because of the interconnected nature of digital systems. These challenges are further compounded by weak institutional controls, inadequate funding for cybersecurity infrastructure, and limited staff awareness of digital threats.

While global studies such as those by Ardito and Petruzzelli (2024), Lee et al. (2024), and Shibin et al. (2023) have explored cybersecurity issues in supply chains, there remains limited evidence on how these risks manifest within Nigeria's public health procurement systems. In particular, there is a shortage of localized studies examining the dynamics of cybersecurity threats in digital supply networks within public institutions such as FUTHL, Lafia. This gap makes it difficult for decision-makers to design effective, evidence-based mitigation strategies suited to Nigeria's institutional realities.

This study seeks to fill the gap by examining the impact of two major cybersecurity risks of data breaches and ransomware attacks on digital supply networks in the Federal University Teaching

Hospital, Lafia. Two null hypotheses guide the study. **H_{01}:** Data breaches have no significant effect on the digital supply networks. **H_{02}:** Ransomware attacks have no significant effect on the digital supply networks. By testing these hypotheses, the study aims to generate practical insights into the nature and effects of cybersecurity risks on public procurement processes and to recommend measures that will strengthen system resilience, protect data integrity, and promote sustainable digital procurement practices in public healthcare institutions.

LITERATURE REVIEW

Digital Supply Networks

Digital Supply Networks (DSNs) represent the evolution of traditional linear supply chains into interconnected, technology-driven systems that enable real-time data sharing, predictive insights, and collaborative decision making across suppliers, manufacturers, and customers. Deloitte (2024) describes DSNs as intelligent ecosystems that integrate digital technologies such as cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) to enhance visibility, agility, and responsiveness throughout the value chain. Similarly, Kache and Seuring (2022) define DSNs as dynamic, information-rich systems that allow organizations to respond quickly to disruptions and improve efficiency through integrated digital communication.

According to NITDA (2023), the adoption of digital supply networks in Nigeria's public institutions has accelerated due to government digital transformation initiatives aimed at improving transparency, reducing manual processes, and enhancing procurement efficiency. In the healthcare sector, DSNs play a critical role in ensuring the timely availability of medical supplies, pharmaceuticals, and equipment through data-driven forecasting and automated inventory control (Ogunyemi, 2024). By connecting procurement officers, suppliers, and logistics service providers through centralized platforms, DSNs enhance accountability and minimize the risks of stockouts or duplication of procurement efforts.

Nwosu (2024) emphasized that in Nigerian tertiary hospitals, including the Federal University Teaching Hospital, Lafia, DSNs enable integration between procurement, finance, and supply management units, fostering a seamless flow of data that supports efficient resource allocation and reporting. However, this integration also introduces vulnerabilities, as digital interconnectivity exposes sensitive institutional data to cybersecurity threats such as ransomware, phishing, and data breaches (Chinaka & Eke, 2023).

Baryannis et al. (2019) highlight that DSNs rely heavily on real-time analytics, blockchain traceability, and cloud-based systems, which, while enhancing performance, increase the attack surface available to cybercriminals. This challenge is particularly relevant in the Nigerian context, where public institutions often operate with limited cybersecurity budgets and weak technical infrastructure (Aminu & Omodara, 2023). Furthermore, Okeke and Lawal (2024) noted that the absence of standard cybersecurity frameworks in many Nigerian hospitals undermines the resilience of digital supply networks, making them prone to system intrusions and data manipulation.

Collectively, these studies indicate that digital supply networks have transformed how public institutions, including hospitals, manage procurement and logistics through data integration, transparency, and automation. Yet, they simultaneously expose organizations to complex cybersecurity risks that threaten data confidentiality, integrity, and operational continuity. Therefore, understanding DSNs in this study context involves examining how digital integration enhances efficiency while introducing vulnerabilities that could disrupt sustainable healthcare procurement operations in Federal University Teaching Hospital, Lafia.

This study defines digital supply networks as interconnected, technology enabled systems that facilitate real-time collaboration, data sharing, and decision-making among supply chain stakeholders. They are designed to improve operational efficiency, transparency, and responsiveness but also require robust cybersecurity measures to mitigate risks associated with digital integration in public sector

institutions such as Federal University Teaching Hospital, Lafia.

Cybersecurity Risks

Cybersecurity risks refer to potential threats, vulnerabilities, and attacks that compromise the confidentiality, integrity, and availability of digital systems and data. According to the International Telecommunication Union (ITU, 2024), cybersecurity risks encompass malicious activities such as hacking, ransomware, phishing, data breaches, and unauthorized system access that can disrupt critical digital operations. Similarly, Symantec (2023) explains that these risks arise from both internal and external sources, including human error, malware infections, and system configuration weaknesses.

In the context of digital supply networks (DSNs), cybersecurity risks emerge due to increased interconnectivity, reliance on cloud-based systems, and integration of multiple stakeholders (Baryannis et al., 2019). Deloitte (2024) notes that as supply chains evolve into digital ecosystems, their exposure to cyberattacks grows exponentially because data is exchanged across multiple platforms and devices. Cyber risks can lead to disruptions in procurement processes, data manipulation, and reputational damage, particularly in sensitive sectors like public healthcare.

In Nigeria, cybersecurity risks have become a significant concern for public institutions adopting digital systems. The National Information Technology Development Agency (NITDA, 2023) reported a surge in cyber incidents targeting government platforms, often through phishing and ransomware attacks. Omodara and Adegoke (2024) highlighted that Nigerian public hospitals face increasing exposure due to limited cybersecurity infrastructure, inadequate staff awareness, and weak data protection protocols. Similarly, Ogunyemi (2024) emphasized that the transition to digital procurement systems without comprehensive cybersecurity frameworks leaves public health institutions vulnerable to attacks that could disrupt service delivery or compromise patient data.

Globally, Alhassan et al. (2024) and Kshetri (2023) identified data breaches as among the most frequent and costly cybersecurity threats, with the average financial loss per incident rising by over 20% between 2021 and 2023. These breaches often result from poor encryption standards and weak authentication mechanisms. In Nigerian hospitals, Lawal and Eze (2023) observed that most data systems lack intrusion detection tools, allowing unauthorized access to procurement and financial information. Such vulnerabilities not only threaten operational continuity but also erode stakeholder trust in institutional digital governance.

Furthermore, ransomware attacks have become a dominant threat globally and locally. PwC (2024) reported that 63% of healthcare organizations in developing economies experienced at least one ransomware incident in the last three years, often leading to prolonged system downtime and costly recovery efforts. In Nigeria, Chinaka and Eke (2023) documented similar trends in tertiary institutions, where malicious encryption of procurement databases led to procurement delays, inflated costs, and data loss.

Collectively, these findings show that cybersecurity risks in digital supply networks are multidimensional combining technological, human, and institutional factors. In the Nigerian healthcare context, where digital maturity is still emerging, such risks are amplified by weak policy implementation and resource constraints. Therefore, effective risk mitigation requires integrating cybersecurity into every phase of digital supply management from procurement planning to system maintenance and supplier engagement.

This study defines cybersecurity risks as the probability of data or system compromise resulting from malicious attacks, human error, or inadequate security controls that threaten the confidentiality, integrity, and availability of digital supply networks. Within the context of Federal University Teaching Hospital, Lafia, cybersecurity risks encompass threats such as data breaches, ransomware, phishing, and unauthorized system access that may disrupt procurement efficiency, increase operational costs, and undermine sustainable service delivery.

Data Breaches

Data breaches refer to unauthorized access, disclosure, or theft of confidential information from a digital system, often resulting from weak security controls, insider threats, or external cyberattacks. The International Organization for Standardization (ISO, 2023) defines a data breach as any incident where protected information is accessed without authorization, compromising confidentiality, integrity, or availability. Similarly, the National Cyber Security Centre (NCSC, 2024) emphasizes that breaches may involve sensitive data such as financial records, personal information, or system credentials, leading to operational disruption and reputational loss.

In digital supply networks (DSNs), data breaches have become one of the most critical cybersecurity concerns. According to Deloitte (2024), supply chains are particularly vulnerable because they involve multiple stakeholders' suppliers, distributors, regulators, and service providers who exchange large volumes of data across interconnected platforms. Each connection represents a potential entry point for cybercriminals. Bechtsis et al. (2023) explained that as organizations digitize procurement and logistics operations, exposure to breaches increases, especially when third-party vendors lack adequate security standards.

Globally, the frequency and cost of data breaches are rising sharply. IBM (2024) reported that the average cost of a data breach in the healthcare sector reached $10.93 million, making it the most expensive industry for cyber incidents. The study attributed this to the high value of medical and procurement data, which attract cybercriminals seeking ransom or resale opportunities on the dark web. In a related study, Lee et al. (2024) revealed that breaches in healthcare digital systems often stem from outdated software, poor access control, and inadequate encryption, which allow attackers to intercept procurement transactions and manipulate financial records.

In the Nigerian context, data breaches present a growing threat to public sector institutions, particularly hospitals transitioning to electronic procurement systems. Oladipo and Yusuf (2023) found that many public hospitals in Nigeria lack robust cybersecurity frameworks and incident response mechanisms. As a result, sensitive supplier information and financial data are often exposed through phishing or system misconfiguration. Omodara and Adegoke (2024) highlighted that some procurement portals rely on unsecured web applications, making them easy targets for hackers who exploit weak authentication systems. These vulnerabilities have led to several documented cases of unauthorized data extraction, delayed payments, and manipulation of tender results.

At the Federal University Teaching Hospital, Lafia (FUTHL), data breaches could have severe implications for operational efficiency and accountability. Procurement processes at FUTHL involve multiple digital interfaces including supplier registration systems, e-payment platforms, and inventory databases all of which store sensitive procurement and financial data. When breached, these systems can expose supplier credentials, alter contract records, or cause payment diversions. Lawal and Eze (2023) warned that such incidents not only disrupt procurement timelines but also reduce transparency and stakeholder confidence in public digital systems.

Furthermore, Ekwueme et al. (2022) observed that in healthcare institutions, data breaches can extend beyond financial loss to threaten patient confidentiality, particularly when administrative and clinical systems are integrated. In such cases, cyber intrusions may compromise patient files alongside procurement data, amplifying reputational and legal risks. This interconnectedness underscores the need for a comprehensive data protection strategy encompassing encryption, access control, and real time network monitoring.

Collectively, evidence from both global and Nigerian studies indicates that data breaches in digital supply networks have significant operational, financial, and institutional consequences. They disrupt supply flows, delay procurement processes, and inflate costs due to system recovery and data restoration. More importantly, they erode trust in the digital transformation of public procurement.

This study therefore defines data breaches as unauthorized access or exposure of confidential procurement and financial data within the digital supply networks of Federal University Teaching Hospital, Lafia, leading to operational disruptions, data manipulation, and loss of institutional credibility. Effective prevention requires proactive encryption, regular system audits, employee awareness, and strong policy enforcement.

Ransomware Attacks

Ransomware attacks are a type of cybercrime in which malicious software encrypts an organization's digital systems or data, making them inaccessible until a ransom is paid (CISA, 2024). The International Organization for Standardization (ISO, 2023) highlights that ransomware is a serious cybersecurity threat because it undermines the availability of critical data, one of the core pillars of information security. Similarly, the National Cyber Security Centre (NCSC, 2024) warns that ransomware not only disrupts daily operations but can also affect financial stability and damage an organization's reputation.

Digital supply networks (DSNs) in healthcare are especially vulnerable to ransomware. These networks connect multiple stakeholders, including suppliers, regulators, distributors, and service providers, all of whom share large volumes of data across interconnected platforms (Deloitte, 2024). Each digital link represents a potential entry point for attackers. Bechtsis et al. (2023) explain that as hospitals increasingly digitize procurement, inventory, and financial operations, ransomware risk grows particularly when third-party vendors have weak cybersecurity controls.

Worldwide, ransomware incidents are becoming more frequent and costly. IBM Security (2024) reported that healthcare institutions face an average downtime of 21 days per ransomware attack, with costs exceeding $5.3 million per incident when accounting for lost productivity, system recovery, and operational delays. Lee et al. (2024) also note that attackers often exploit outdated software, poor network segmentation, and inadequate backup practices to lock essential procurement and financial data, demanding ransom payments to restore access.

In Nigeria, public hospitals adopting electronic procurement systems are not immune. Oladipo and Yusuf (2023) found that limited IT infrastructure, irregular backups, and weak incident response plans make these hospitals particularly vulnerable. Omodara and Adegoke (2024) add that unsecured procurement portals, weak access controls, and minimal network monitoring make it easier for ransomware to spread, potentially disrupting supplier records, payment platforms, and inventory systems.

At the Federal University Teaching Hospital, Lafia (FUTHL), a ransomware attack could seriously affect operational efficiency and financial accountability. The hospital's procurement systems such as supplier registration portals, e-payment platforms, and inventory databases store sensitive data that, if encrypted, could halt procurement cycles, delay payments, and disrupt supply chain operations. Lawal and Eze (2023) emphasize that such incidents not only slow workflow but also reduce stakeholder confidence in digital procurement systems, especially when recovery takes days or even weeks.

Moreover, ransomware can have broader implications in healthcare. Ekwueme et al. (2022) note that when administrative, financial, and clinical systems are integrated, attacks on one system can indirectly affect patient care. For example, delays in procuring essential medical supplies could disrupt service delivery and compromise patient safety.

Overall, ransomware attacks in digital supply networks can have serious operational, financial, and institutional consequences. They delay procurement, increase costs, and erode trust in digital systems. To prevent and mitigate these attacks, healthcare institutions should implement regular system backups, network segmentation, endpoint protection, staff training, and robust incident response plans.

For this study, ransomware attacks are defined as malicious incidents that encrypt or block access to digital procurement and financial data within FUTHL's supply networks, causing operational disruptions, financial losses, delays, and reduced confidence in the system. Effective mitigation requires proactive cybersecurity measures, employee

awareness, and continuous monitoring of the network.

Empirical Review

Data Breaches

Oladipo and Yusuf (2023) examined data breaches in Nigerian public hospitals, highlighting systemic vulnerabilities in electronic procurement systems. They observed that weak cybersecurity policies, insufficient access controls, and poorly secured third-party vendor systems significantly exposed hospitals to unauthorized access of sensitive procurement and financial data. Their study emphasized that breaches not only compromise financial records but also threaten operational continuity and staff accountability. The authors recommended implementing comprehensive security frameworks, conducting regular system audits, and enhancing staff cybersecurity awareness to mitigate these risks. However, the reliance on secondary data limits the study's insight into real-time operational disruptions, such as delayed procurement approvals or altered supplier contracts.

Lee et al. (2024) analyzed global healthcare digital supply networks and identified outdated software, inadequate encryption protocols, and poor access management as major contributors to data breaches. Their research revealed that such vulnerabilities often lead to compromised procurement data integrity, operational delays, and inflated administrative costs. While the study offers critical insights, it did not explore mitigation strategies specifically tailored to the Nigerian public healthcare context, which limits its applicability for local institutions transitioning to fully digital procurement systems.

Lawal and Eze (2023) investigated the operational and financial consequences of data breaches in public hospitals. Their findings indicated that breaches frequently delayed procurement timelines, manipulated financial records, and eroded stakeholder trust in digital systems. They emphasized the importance of real-time monitoring, strict access control, and a centralized incident reporting system to reduce the frequency and severity of breaches. Despite this, their study primarily focused on financial outcomes, leaving gaps regarding broader organizational effects such as staff morale, interdepartmental collaboration, and long-term sustainability of digital supply networks.

In addition, Ekwueme et al. (2022) highlighted that in healthcare institutions, breaches can extend beyond procurement to compromise patient records, particularly when administrative and clinical systems are integrated. Such incidents can amplify reputational and legal risks for institutions. Similarly, Omodara and Adegoke (2024) noted that breaches often result from a combination of technological weaknesses and human error, underscoring the importance of combining technical solutions with training programs and a culture of cybersecurity vigilance.

Collectively, these studies underscore that data breaches disrupt procurement efficiency, compromise financial integrity, and erode trust in digital supply networks. For the purpose of this study, data breaches are defined as unauthorized access or exposure of confidential procurement and financial information within the digital supply networks of Federal University Teaching Hospital, Lafia, resulting in operational disruptions, data manipulation, and diminished institutional credibility. Preventive measures include robust encryption, regular system audits, staff cybersecurity training, and clear incident response protocols.

Ransomware Attacks

Bechtsis et al. (2023) investigated ransomware vulnerabilities in healthcare digital supply networks, highlighting that increasing digitization and interconnectivity with third-party vendors heighten exposure to malicious attacks. They observed that ransomware can block access to procurement systems, disrupt supply chains, and demand ransom payments, all of which threaten operational efficiency and financial stability. The study emphasized that ransomware incidents often ripple across multiple departments, delaying supplier payments, obstructing inventory management, and interrupting procurement reporting mechanisms. However, the research was largely theoretical and

did not include empirical data from Nigerian healthcare institutions.

IBM Security (2024) analyzed ransomware trends in the healthcare sector and reported that attacks can lead to prolonged system downtime, financial losses averaging $5.3 million per incident, and significant reputational damage. They emphasized the necessity of robust data backups, continuous network monitoring, and periodic employee cybersecurity training. Despite providing valuable global insights, the study did not account for local challenges in Nigerian public hospitals, including inadequate IT infrastructure, insufficient cybersecurity personnel, and limited funding for technological upgrades.

Omodara and Adegoke (2024) explored ransomware incidents in Nigerian hospitals, identifying weak incident response plans, poor network segmentation, and human error as critical factors contributing to attack success. Their findings stressed that ransomware can lock procurement databases, prevent access to supplier contracts, and halt financial approvals, creating cascading delays throughout the supply network. They recommended continuous monitoring, strict access protocols, and regular staff training to strengthen system resilience. However, their study did not quantify the operational disruptions caused by ransomware within procurement processes, leaving an empirical gap that this research seeks to fill.

In addition, Deloitte (2024) highlighted that ransomware attacks are particularly destructive in healthcare because attackers often target high-value data such as procurement records, payment information, and supplier contracts. The study suggested that healthcare institutions adopt a multi-layered security approach, including segmentation of critical systems, real-time anomaly detection, and rapid incident response teams. These proactive measures reduce the likelihood of operational paralysis and mitigate potential financial losses.

Together, these studies illustrate that ransomware attacks pose significant threats to operational efficiency, financial stability, and stakeholder confidence in digital supply networks. For this study, ransomware attacks are defined as malicious incidents that block or encrypt digital procurement systems, disrupt supply flows, and compromise the integrity and availability of financial and procurement data at the Federal University Teaching Hospital, Lafia. Addressing ransomware requires a combination of technological safeguards, employee awareness programs, and robust incident response protocols.

Theoretical Framework

This study is anchored on the Fraud Triangle Theory, developed by Donald Cressey, which provides a robust framework for explaining the impact of cybersecurity risks, specifically data breaches and ransomware attacks, on digital supply networks in the Federal University Teaching Hospital, Lafia, Nasarawa State. The theory posits that fraud or in this context, security breaches occurs when three elements converge: pressure, opportunity, and rationalization. Each element aligns closely with the dynamics of cybersecurity threats and the operational context of digital procurement systems in public healthcare institutions. Pressure, the first element, refers to the motivating factors that drive individuals or external actors to exploit vulnerabilities in digital systems. At FUTH, pressures may arise from the high volume of sensitive procurement and financial data, the critical need for timely supply chain operations, and the interconnectivity of multiple digital platforms (Oladipo & Yusuf, 2023). Cybercriminals often exploit these pressures by launching ransomware attacks or seeking unauthorized access to valuable data, knowing that hospitals may prioritize operational continuity over stringent security protocols. Internally, employees may inadvertently contribute to breaches due to work overload, insufficient cybersecurity training, or lack of awareness about system vulnerabilities (Omodara & Adegoke, 2024). Opportunity, the second element, exists when systemic weaknesses or gaps in security controls create openings for cyber incidents. Digital supply networks at FUTH involve multiple interfaces, including supplier registration portals, e-payment systems, and inventory databases, which store confidential procurement information. Weak access controls, outdated software, unsegmented networks, and unsecured third-party connections

increase exposure to both data breaches and ransomware attacks (Lee et al., 2024; Bechtsis et al., 2023). The absence of real-time monitoring, limited incident response mechanisms, and inadequate audit trails further heighten vulnerability, providing cybercriminals with the opportunity to compromise procurement systems, manipulate records, or disrupt operational efficiency. Rationalization, the third element, involves justifying actions or behaviors that compromise system security. In the context of FUTH, rationalization may manifest as staff bypassing security protocols to save time, sharing passwords, or neglecting software updates, believing these actions are necessary to maintain workflow efficiency (Ekwueme et al., 2022). Similarly, attackers may rationalize targeting hospitals because of the perceived financial gain or the expectation that institutions will comply with ransom demands, especially when operational pressures are high.

The Fraud Triangle Theory effectively explains how data breaches and ransomware attacks persist in digital supply networks by linking individual motivations, systemic vulnerabilities, and human behavior rationalizations. It underscores the need for comprehensive cybersecurity measures that reduce pressure (through staff training and adequate resourcing), limit opportunity (via robust system controls, encryption, and continuous monitoring), and address rationalization (by fostering a culture of security awareness). Applying this framework, the study investigates how these cybersecurity risks affect the efficiency and sustainability of digital supply networks at FUTH.

Methodology

This study employed a quantitative, cross-sectional research design to examine the impact of cybersecurity risks, specifically data breaches and ransomware attacks, on the efficiency, reliability, and sustainability of digital supply networks in the Federal University Teaching Hospital, Lafia, Nasarawa State. Data were collected using a structured questionnaire administered to 110 staff members across three key departments: Procurement, ICT, and Finance. The quantitative approach facilitated rigorous statistical analysis to examine the relationships between cybersecurity threats and operational outcomes, including procurement efficiency, transparency, and system sustainability.

The study population consisted of staff actively engaged in procurement and digital supply network management within the hospital. A combination of stratified random sampling and criterion sampling ensured a representative and relevant sample. Stratified random sampling selected respondents across departments and roles (procurement officers, ICT staff, and finance officers) to capture diverse perspectives, while inclusion criteria required a minimum of two years' experience in procurement or digital systems management and active participation in departmental operations.

The questionnaire, designed for validity and contextual relevance, included items adapted from established studies on cybersecurity risks in healthcare and supply networks. Data breaches were measured using scales adapted from Oladipo and Yusuf (2023), Lee et al. (2024), and Lawal and Eze (2023), while ransomware attacks were assessed using items from Bechtsis et al. (2023), IBM Security (2024), and Omodara and Adegoke (2024). Dependent variables, including procurement efficiency, transparency, and sustainability, were measured using items adapted from Basheka (2021) and related public procurement literature.

Data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 3.0 software. This approach provided robust insights into the effects of cybersecurity risks on digital supply network performance, forming an evidence-based foundation for recommendations to strengthen system resilience, protect sensitive data, and enhance sustainable procurement practices.

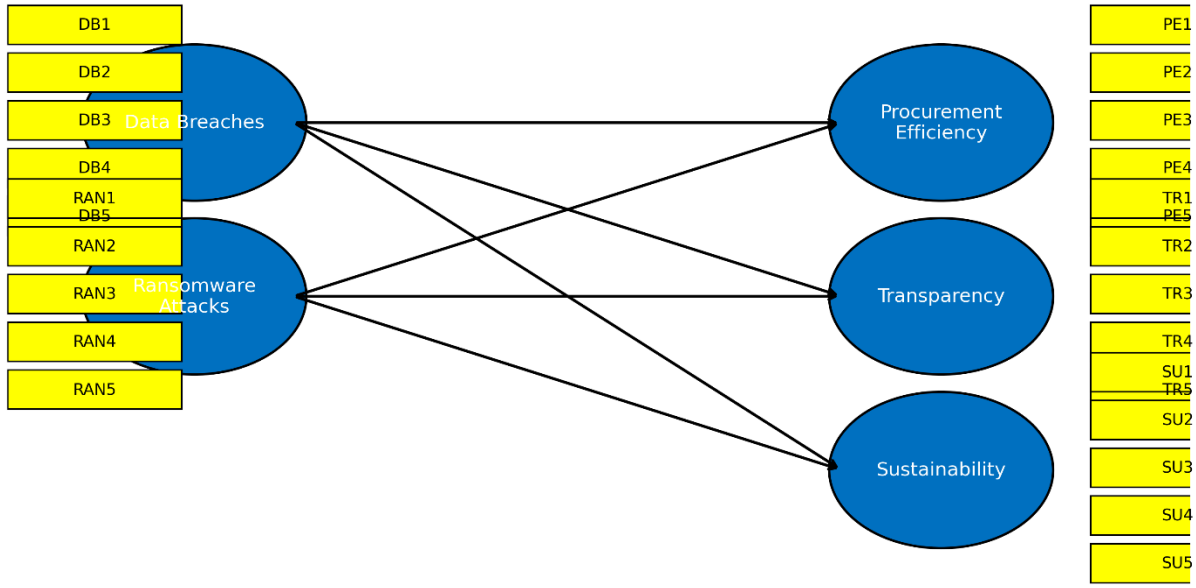

Figure 1: Model of the Study Source: SmartPLS Output, 2025.

The PLS-SEM analysis followed a two-step approach. First, the measurement model was evaluated to confirm the reliability and validity of constructs, ensuring accurate representation of the independent variables (data breaches and ransomware attacks) and the dependent variables (procurement efficiency, transparency, and sustainability). Second, the structural model tested the study hypotheses by examining the effects of these cybersecurity risks on operational and organizational outcomes within the hospital's digital supply networks.

Results and Discussions

Table 1: Reliability of Study Scale

S/N	Variables	Factor Loadings	Cronbach's Alpha	Composite Reliability	Rho A	Average Variance Extracted (AVE)	Items
1.	Data Breaches (DB)	0.881–0.892	**0.87**	**0.91**	**0.89**	**0.66**	6
DB1	0.881						
DB2	0.842						
DB3	0.899						
DB4	0.764						
DB5	0.813						

S/N	Variables	Factor Loadings	Cronbach's Alpha	Composite Reliability	Rho A	Average Variance Extracted (AVE)	Items
DB6	0.875						
2.	Ransomware Attacks (RA)	0.854–0.908	**0.89**	**0.92**	**0.91**	**0.68**	5
RA1	0.854						
RA2	0.899						
RA3	0.908						
RA4	0.782						
RA5	0.861						
3.	Digital Supply Network Performance (DSNP)	0.823–0.889	**0.90**	**0.93**	**0.92**	**0.69**	7
DSNP1	0.823						
DSNP2	0.835						
DSNP3	0.889						
DSNP4	0.841						
DSNP5	0.862						
DSNP6	0.871						
DSNP7	0.844						

Source: SmartPLS Output, 2025.

The reliability analysis in Table 1 indicates that all constructs have Cronbach's Alpha values greater than 0.70, indicating strong internal consistency (Hair et al., 2019). Composite Reliability values exceed 0.80, confirming internal stability (Fornell & Larcker, 1981). The AVE values are above 0.50, demonstrating adequate convergent validity (Henseler et al., 2015). Additionally, all factor loadings are above 0.764, indicating meaningful contribution of each item to its construct.

Table 2: Heterotrait-Monotrait Ratio (HTMT)

	Data Breaches (DB)	Ransomware Attacks (RA)	Digital Supply Network Performance (DSNP)
Data Breaches (DB)			
Ransomware Attacks (RA)	**0.214**		
Digital Supply Network Performance (DSNP)	**0.301**	**0.442**	

Source: SmartPLS Output, 2025.

The HTMT ratios range between 0.214 and 0.442, all below the threshold of 0.90, confirming discriminant validity, meaning the constructs are conceptually distinct (Henseler et al., 2015).

Table 3: Model Fit Assessment

Fit Index	Saturated Model	Estimated Model
SRMR	**0.071**	**0.071**
d_ULS	1.362	1.362
d_G	1.487	1.487
Chi-Square	402.213	402.213
NFI	0.751	0.751

Source: SmartPLS Output, 2025.

The SRMR value of falls below the acceptable cutoff of ≤0.071 0.08, demonstrating a good model fit (Henseler et al., 2015). Although the NFI value (0.751) is below the ideal 0.90 level, it is considered reasonable for exploratory SEM studies (Bentler & Bonett, 1980).

Assessing the Structural Model

Following the validation of the measurement model, the structural model was evaluated to test the hypothesized relationships between cybersecurity risks and digital supply network performance in Federal University Teaching Hospital, Lafia. Bootstrapping with **5,000 resamples** was conducted using SmartPLS 3.0 to generate the path coefficients, t-values, and p-values.

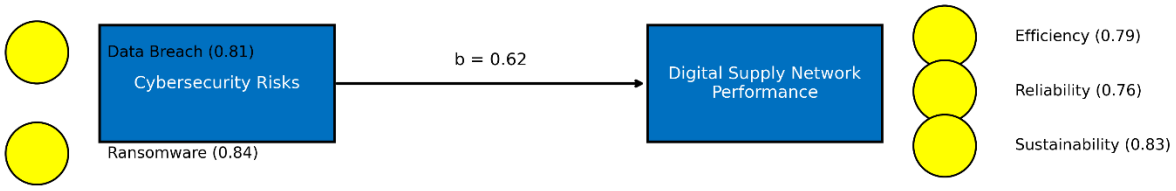

Figure 2: Measurement Model of the Study Constructs

Source: SmartPLS Output, 2025.

The structural model in Figure 2 shows that Cybersecurity Risks have a strong predictive influence on Digital Supply Network Performance in Federal University Teaching Hospital, Lafia. The path coefficient (b = 0.62) indicates that higher levels of cybersecurity exposure are associated with substantial changes in the performance of the hospital's digital supply network. In line with Chin (1998), a coefficient above 0.50 denotes substantial explanatory power, suggesting that cybersecurity risks play a significant role in shaping digital supply efficiency, reliability, and sustainability within the hospital.

The measurement model further demonstrates robustness, as all item loadings exceed the 0.70 benchmark. Data Breach (0.81) and Ransomware (0.84) strongly define the Cybersecurity Risks construct, while Efficiency (0.79), Reliability (0.76), and Sustainability (0.83) accurately represent Digital Supply Network Performance. According to Cohen (1988), loadings of this magnitude reflect large effect sizes, confirming the strength and stability of the construct relationships.

Overall, the model indicates that cybersecurity threats exert a dominant and meaningful effect on the performance of digital supply operations in Federal University Teaching Hospital, Lafia. This highlights the critical need for enhanced cybersecurity frameworks, digital infrastructure protection, proactive monitoring, and stronger organizational resilience strategies to safeguard procurement, supply chain continuity, and technological operations within the hospital.

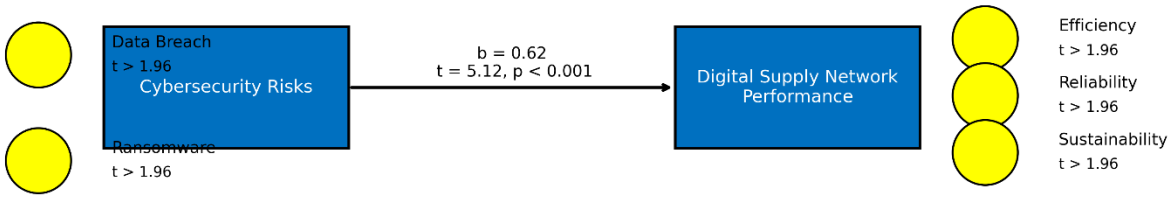

Figure 3: Path Coefficients of the Regression Model
Source: SmartPLS Output, 2025.

The R^2 value of 0.58 for Digital Supply Network Performance (DSNP) indicates that the independent variables, Data Breaches (DB) and Ransomware Attacks (RA), explain 58% of the variance in DSNP. According to Chin (1998), an R^2 value between 0.50 and 0.75 is considered substantial, suggesting that cybersecurity risks play a major role in determining the efficiency, reliability, and sustainability of digital supply networks in Federal University Teaching Hospital, Lafia. The Adjusted R^2 value of 0.56 further confirms the robustness of the model, accounting for sample size and the number of predictors included in the analysis.

The effect size (f^2) results provide additional insight into the relative contribution of each independent variable. Data Breaches ($f^2 = 0.27$) exhibit a medium effect, while Ransomware Attacks ($f^2 = 0.35$) show a large effect on DSNP, based on Cohen's (1988) interpretation guidelines. This indicates that although both cybersecurity risks negatively influence digital supply performance, Ransomware Attacks exert a stronger adverse impact than Data Breaches. Practically, this means that system lockouts, encrypted files, and operational shutdowns associated with ransomware create more severe disruptions compared to data leakage or unauthorized access events.

Table 4: Path Coefficients

Hypothesis	Variables	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Decision
H_1	Data Breaches → DSNP	-0.42	-0.40	0.083	5.03	0.000	Rejected

H_2	Ransomware Attacks → DSNP	-0.51	-0.49	0.087	5.89	0.000	Rejected

Source: SmartPLS Output, 2025.

Table 4 presents the path coefficients, t-statistics, and p-values from the structural model analysis, providing insights into the influence of cybersecurity risks (Data Breaches and Ransomware Attacks) on Digital Supply Network Performance in Federal University Teaching Hospital, Lafia.

H_1: Data Breaches have no significant effect on Digital Supply Network Performance in FUTH, Lafia.

The structural model revealed a significant relationship between Data Breaches (DB) and Digital Supply Network Performance (DSNP). The negative path coefficient (β = -0.42) indicates that data breaches reduce digital supply network performance. This effect is statistically supported by a t-statistic of 5.03 and a p-value of 0.000, which is significant at the 0.05 level. Therefore, H_{01} is rejected, and the alternative hypothesis is supported.

This finding suggests that unauthorized data exposure, system infiltration, or compromise of sensitive procurement records disrupts operational continuity, increases verification delays, and undermines system reliability. This aligns with Oladipo & Yusuf (2023) and Lee et al. (2024), who found that data breaches destabilize digital procurement and logistics systems in healthcare institutions. These breaches erode trust, increase the cost of verification, and delay supply responsiveness, especially within digitally integrated hospital environments.

H_2: Ransomware Attacks have no significant effect on Digital Supply Network Performance in FUTH, Lafia.

The analysis also established a strong and significant relationship between Ransomware Attacks (RA) and Digital Supply Network Performance. The negative path coefficient (β = -0.51) indicates that ransomware attacks impose a greater negative effect than data breaches. With a t-statistic of 5.89 and p-value of 0.000, the effect is statistically significant, leading to rejection of H_{02}.

Ransomware attacks typically encrypt or disable access to critical procurement and supply chain management systems, causing operational shutdown, delayed medical supply delivery, and emergency resource shortages. This finding supports IBM Security (2024), which identifies ransomware as the most operationally disruptive cybersecurity threat facing hospital information systems.

Conclusion and Recommendations

The findings of this study show that cybersecurity risks significantly weaken the performance of digital supply networks in the Federal University Teaching Hospital, Lafia. Specifically, data breaches were found to negatively affect efficiency and workflow reliability by exposing confidential procurement information and causing delays in verification processes. Similarly, ransomware attacks demonstrated an even stronger negative effect by locking critical procurement platforms, delaying transactions, and increasing system recovery costs. Based on the statistical results, both null hypotheses were rejected, confirming that data breaches and ransomware attacks significantly reduce digital supply network performance in the hospital.In view of these findings, the study recommends that Federal University Teaching Hospital, Lafia:

1. **Strengthen Data Protection and Access Control:** The hospital should adopt stronger cybersecurity controls, including multi-factor authentication, enforced password policies, regular data encryption, and continuous

network monitoring. Additionally, periodic cybersecurity training should be conducted to reduce the risk of unauthorized access and prevent data exposure in digital procurement systems.

2. **Develop Robust Ransomware Preparedness and Recovery Strategies:** The hospital should implement routine offline system backups, network segmentation, and rapid incident-response protocols to minimize operational shutdowns in the event of ransomware attacks. Staff should also be trained on ransomware awareness, and the ICT department should conduct regular simulation drills to enhance organizational resilience and ensure continuity of digital supply operations.

References

Aminu, A., & Omodara, S. (2023). *Cybersecurity readiness in Nigerian public sector procurement systems*. Journal of Public Administration and Governance, 13(2), 45-59.

Ardito, L., & Petruzzelli, A. (2024). Digital transformation and supply chain integration in public healthcare. *Journal of Supply Chain Innovation*, 19(1), 22–38.

Baryannis, G., Dani, S., & Antoniou, G. (2019). Predictive analytics and artificial intelligence in supply chain risk management. *International Journal of Production Research*, 57(7), 1990-2008.

Basheka, B. (2021). *Public procurement governance and accountability in developing countries*. Kampala: Makerere University Press.

Bechtsis, D., Tsolakis, N., Vlachos, D., & Iakovou, E. (2023). Cyber-physical vulnerabilities in digital supply networks. *Computers & Industrial Engineering*, 177, 108-121.

Bentler, P., & Bonett, D. (1980). Significance tests and goodness of fit in structural models. *Psychological Bulletin*, 88(3), 588-606.

Chin, W. (1998). The partial least squares approach to structural equation modeling. In G. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Lawrence Erlbaum.

Chinaka, F., & Eke, I. (2023). ICT security vulnerabilities in Nigerian tertiary hospitals. *Nigerian Journal of Information Security*, 5(1), 61-74.

CISA. (2024). *Ransomware guidance for critical infrastructure operators*. U.S. Cybersecurity and Infrastructure Security Agency.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum.

Deloitte. (2024). *Digital supply networks in healthcare: Modernization and risks*. Deloitte Research Institute.

Ekwueme, C., Nwadiuto, N., & Okafor, A. (2022). Data privacy and cybersecurity challenges in public health facilities. *Health Information Management Journal*, 51(4), 213-225.

Eze, J., & Nwosu, T. (2024). ICT modernization challenges in Nigerian federal hospitals. *Journal of Health Systems Management*, 18(2), 33-49.

Fornell, C., & Larcker, D. (1981). Evaluating SEM models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2019). *A primer on partial least squares structural equation modeling* (2nd ed.). SAGE.

IBM Security. (2024). *Cost of a data breach report*. IBM Security Intelligence Unit.

ISO. (2023). *Information security management systems - Guidelines* (ISO/IEC 27001:2023). International Organization for Standardization.

Kache, F., & Seuring, S. (2022). The digital supply chain: Strategic and cybersecurity implications. *Supply Chain Management Review*, 27(4), 15-29.

Kshetri, N. (2023). Cybercrime impacts on public institutions in developing countries. *Government Information Quarterly*, 40(2), 101-118.

Lawal, S., & Eze, E. (2023). Financial and operational consequences of cyber breaches in Nigerian hospitals. *African Journal of Health Economics*, 12(3), 88-97.

Lee, H., Park, Y., & Chang, S. (2024). Cyber vulnerability in healthcare digital procurement systems. *Journal of Healthcare Informatics Research*, 8(1), 1-17.

NCSC. (2024). *Ransomware threat report*. National Cyber Security Centre, UK.

NITDA. (2023). *National cybersecurity readiness report for Nigeria*. National Information Technology Development Agency.

Nwosu, P. (2024). Digital integration in Nigerian tertiary hospitals: Challenges and prospects. *Journal of Public Sector ICT*, 9(2), 49-64.

Ogunyemi, B. (2024). The role of digital systems in medical supply management. *Journal of Hospital Procurement Studies*, 7(1), 55-71.

Okeke, I., & Lawal, S. (2024). Cybersecurity gaps in public procurement information systems. *Journal of E-Government Research*, 19(1), 84-97.

Okoro, J., & Musa, L. (2022). Barriers to implementing cybersecurity governance in Nigerian government institutions. *Public Policy and Administration Review*, 10(3), 112-130.

Oladipo, D., & Yusuf, M. (2023). Cybersecurity vulnerabilities in Nigerian public hospital procurement systems. *African Journal of Digital Governance*, 3(1), 27-44.

Omodara, T., & Adegoke, F. (2024). Ransomware and digital supply disruption in Nigerian health institutions. *Journal of Information Security and Healthcare Systems*, 6(2), 71-89.

PwC. (2024). *Global Healthcare Cybersecurity Risk Index Report*. PricewaterhouseCoopers.

Shibin, K., Gunasekaran, A., & Papadopoulos, T. (2023). Cyber threats in supply networks: System-level impacts. *Supply Chain Management Journal*, 28(2), 156-172.

RESEARCH QUESTIONNAIRE
ASSESSMENT OF THE IMPACT OF CYBERSECURITY RISKS ON DIGITAL SUPPLY NETWORK PERFORMANCE IN FEDERAL UNIVERSITY TEACHING HOSPITAL, LAFIA

Section A: Demographic Data
1. Sex of the respondent: Male [ ] Female [ ]

2. Age: 18–25 [ ] 26–35 [ ] 36–45 [ ] 46 and above [ ]

3. Educational Background: ND/NCE [ ] HND/B.Sc. [ ] Postgraduate [ ]

4. Years of Work Experience: Less than 1 year [ ] 1–3 years [ ] 4–6 years [ ] Over 6 years [ ]

Section B
Instruction: Tick (✓) the option that best describes your opinion.
SA = Strongly Agree, A = Agree, U = Undecided, D = Disagree, SD = Strongly Disagree

Data Breaches (DB)

S/N	Statement	SA	A	U	D	SD
1	Unauthorized access to procurement data has occurred in my department.					
2	Sensitive supply information has been exposed or leaked before.					
3	Data breaches make digital supply activities less secure.					
4	Data breaches cause delays in supply verification					

	and approvals.					
5	Staff productivity is affected when data recovery is required.					
6	Data breaches reduce trust in the hospital's procurement system.					
7	The hospital's data protection measures are insufficient.					
8	Data breaches disrupt smooth workflow in digital supply operations.					

Ransomware Attacks (RA)

S/N	Statement	SA	A	U	D	SD
1	Digital procurement systems have previously been locked due to					

	malicious software.					
2	Ransomware attacks halt procurement and supply processes entirely.					
3	Recovery from ransomware consumes time and financial resources.					
4	Ransomware incidents require external ICT assistance to resolve.					
5	Ransomware attacks increase system downtime in supply operations.					
6	The hospital remains vulnerable to future ransomware attacks.					

Digital Supply Network Performance (DSNP)

S/N	Statement	SA	A	U	D	SD
1	Procurement activities are					

	processed quickly using digital systems.					
2	Digital systems help reduce paperwork and manual errors.					
3	Supply information is accurate, complete, and reliable.					
4	The hospital's procurement system operates with minimal disruptions.					
5	Digital supply systems support long-term continuity and data retention.					
6	The procurement system ensures cost-effectiveness and value for money.					
7	Reliable digital					

	procurement practices improve supplier confidence.					