IKR Publishers

IKR Journal of Economics, Business and Management
(IKRJEBM)
Journal homepage: https://ikrpublishers.com/ikrjebm/
Volume-2, Issue-1 (January-February) 2026

OPEN ACCESS
ISSN: 3107-8052 (Online)

Cyber Security and Data Protection in Educational Management

Akintayo Oluwatoyin Olusola Alex (Ph.D)[1*] & Akintayo Ifedolapo Moyosore[2]

[1]Department of Accounting, Faculty of Management Sciences, Bamidele Olumilua University of Education Science & Technology Ikere Ekiti, Ekiti State, Nigeria

[2]Department of Educational Management Faculty of Education, Ekiti State University, Ado Ekiti, Ekiti State, Nigeria.

DOI:10.5281/zenodo.19318144

ARTICLE INFO

Article history:

Received : 02-03-2026
Accepted : 11-03-2026
Available online : 29-03-2026

Citation: Akintayo, O. O. A., & Akintayo, I. M. (2026). Cyber Security and Data Protection in Educational Management. *IKR Journal of Economics, Business and Management (IKRJEBM), 2*(1), 21-31.

ABSTRACT **Original Research Article**

The study investigated the influence of Cyber Security factors such as awareness, infrastructure security, regulatory compliance, and incident response capability on data protection effectiveness in federal and state universities in Nigeria. The purpose was to assess how these factors contribute to safeguarding institutional data. A quantitative research design was adopted, with data collected from 195 educational management staff and institution's management personnel. Data were collected using a structured questionnaire and analyzed using descriptive and inferential statistics with the use of mean, STD, and structural equation modeling (SEM) via SPSS and AMOS 24. Descriptive analysis revealed high perceived levels of cyber security awareness (mean = 4.18), infrastructure security (mean = 4.17), regulatory compliance (mean = 4.20), incident response capability (mean = 4.20), and data protection effectiveness (mean = 4.20). however, hypothesis testing showed that none of the constructs significantly predicted data protection effectiveness cyber security awareness (β = -0.077, p = 0.254), infrastructure security (β = -0.014, p = 0.838), regulatory compliance (β = -0.074, p = 0.269), and incident response capability (β = 0.094, p = 0.159) with the model explaining only 2.3% of the variance. Based on these findings, the study concludes that awareness, infrastructure, policy compliance, and incident response alone are insufficient to ensure effective data protection without practical enforcement, resources, and skilled personnel. Therefore, it is recommended that government and institution management implement regular cybersecurity training, upgrade IT infrastructure, enforce compliance policies, and develop strong incident response plans to enhance data security in all educational institutions.

Keywords: Cybersecurity Awareness, Infrastructure Security, Regulatory Compliance, Incident Response Capability, Data Protection, Educational Management, Nigeria.

**Corresponding author: Akintayo Oluwatoyin Olusola Alex (Ph.D)*
Department of Accounting, Faculty of Management Sciences, Bamidele Olumilua University of Education Science & Technology Ikere Ekiti, Ekiti State, Nigeria

Introduction

The rapid digital transformation of educational management systems has profoundly reshaped how institutions operate, leading to enhanced efficiency in administration, teaching, and learning. Globally, educational institutions now routinely store, process, and manage vast amounts of personal and institutional data including student records, financial information, research outputs, and staff data using digital platforms and cloud-based services. However, this increased reliance on digital technologies has simultaneously expanded the attack surface for cyber threats by exposing educational institutions to complex vulnerabilities and data breaches (Afolalu & Tsoeu, 2025).

Cybersecurity refers to set of practices, policies, and technologies deployed to protect system information and data from unauthorized access, damage, or disruption (Malasowe et al., 2024). The frequency and sophistication of cyberattacks against big organization and educational institutions have risen significantly, with common attack methods including ransomware, phishing schemes, insider threats, and malware, all of which pose persistent and damaging risks to critical data.

Institutions that once operated within predominantly closed and offline administrative environments are increasingly required to function in open and highly interconnected digital ecosystems. This rapid digital transformation has significantly expanded their exposure to cyber threats, including unauthorized access, data breaches, ransomware attacks, and identity theft. However, many of these institutions have transitioned to digital platforms without corresponding investments in robust cybersecurity infrastructure, staff training, and institutional awareness. Consequently, the gap between technological adoption and security preparedness continues to widen, by this means heightening vulnerability to cyber incidents and compromising the confidentiality, integrity, and availability of sensitive educational data (Afolalu & Tsoeu, 2025).

In addition, Kifaru et al. (2023) emphasize that cybersecurity breaches significantly compromise the confidentiality, integrity, and availability of sensitive institutional data, by exposing students, staff, and administrative records to unauthorized access and misuse. Such violations not only disrupt institutional operations but also erode stakeholder confidence in the institution’s ability to safeguard personal and academic information. Moreover, persistent data breaches may result in noncompliance with national and international data protection frameworks, leading to legal liabilities, financial penalties, and institutional reputational damage.

In response to these threats, educational management must integrate cybersecurity measure that ensure comprehensive data protection that align with best practices and regulatory standards. In addition, one important thing to note even according to Agalit et al. (2023) is that cybersecurity governance involves not only technological safeguards such as firewalls, encryption, and intrusion detection systems but also institutional policies, user awareness, and incident response strategies

Given these backdrops, empirical research that investigates the relationships between cybersecurity practices and data protection outcomes is urgently needed. This study aims to fill that gap by examining how various facets of cybersecurity influence data protection effectiveness in educational management.

Statement of the Problem

Globally, the redoubling integration of digital technologies into educational system has meaningfully improved most institutions administrative efficiency, student record management, online learning coordination, and financial operations. In spite of this, digital transformation has simultaneously heightened the vulnerability of educational institutions to cyber threats and data breaches. Despite growing investments in educational technologies, many institutions keep on operate without comprehensive cybersecurity or effective data protection mechanisms. This gap exposes sensitive institutional and personal data such as academic records, financial information, and research databases to unauthorized access, ransomware attacks, phishing schemes, and insider threats.

Of late, some empirical studies indicate that the education sector remains one of the most targeted industries for cyberattacks globally. For example, Afolalu and Tsoeu (2025) reported that tertiary institutions increasingly experience ransomware and phishing attacks due to weak security governance structures and insufficient user awareness. Similarly, Kifaru et al. (2023) found that inadequate cybersecurity infrastructure significantly conceded student information management systems, resulting in data exposure and operational disruptions. These studies conjure up that even though digital platforms have expanded through the world, institutional capabilities, cybersecurity preparedness has not yet advanced proportionately.

In addition, regulatory frameworks such as data protection laws require institutions to implement adequate safeguards to protect personal information. In spite of this, compliance levels among educational institutions remain inconsistent, particularly in developing countries where cybersecurity budgets and technical expertise are limited. This absence of integrated security policies in some country’s tertiary institution as well as limited staff training, weak incident response, and outdated technological infrastructure collectively undermine data protection effectiveness.

Even though some prior studies have examined cybersecurity challenges in education, yet, there is limited empirical research that structurally examines how cybersecurity dimensions such as awareness, infrastructure security, regulatory compliance, and incident response capability jointly influence data protection effectiveness. As a result of these, this study therefore concentrate on this gap by empirically investigate the structural relationships between cybersecurity mechanisms and data protection effectiveness in educational management systems.

Objectives of the Study

The main purpose of this study is to examine the influence of cyber security practices on data protection effectiveness in educational management. Specifically, the study seeks to:

1. Examine the effect of cyber security awareness on data protection effectiveness in educational management systems.
2. Assess the influence of technological infrastructure security on data protection effectiveness.
3. Evaluate the impact of regulatory compliance on data protection effectiveness.
4. Determine the effect of incident response capability on data protection effectiveness.

Research Questions

1. What is the level of cyber security awareness among staff and management in educational institutions?
2. How does infrastructure security affect data protection effectiveness in educational management?
3. How does Regulatory Compliance affect Data Protection Effectiveness in educational institutions?
4. What is the influence of Incident Response Capability on Data Protection Effectiveness?

Research Hypotheses

In line with the objectives, the following hypotheses are proposed for testing in this study:

H$_{01}$: Cyber security awareness has no significant effect on data protection effectiveness in educational management systems.

H$_{02}$: Technological infrastructure security has no significant effect on data protection effectiveness in educational management systems.

H$_{03}$: Regulatory compliance has no significant effect on data protection effectiveness in educational management systems.

H$_{04}$: Incident response capability has no significant effect on data protection effectiveness in educational management systems.

Literature Review

Cyber Security

Cyber security refers to the protection of information systems, networks, and data from unauthorized access, cyber attacks, and damage. Cyber security in educational management refers to the systematic protection of digital assets, information systems, and institutional data from cyber threats, unauthorized access, misuse, and disruption within educational environments. In supporting this definition, Afolalu and Tsoeu (2025) also describe cyber security in higher education as a coordinated framework of technological tools, risk management strategies, and awareness programs designed to safeguard digital infrastructures against evolving cyber threats. As educational institutions throughout the world increasingly rely on digital technologies for teaching, learning, research, and administration, the need for structured cyber security has become critical. Institutions now manage large volumes of sensitive data, including student academic records, financial information, research data, and personal identification details, all of which require strong protection mechanisms. Research indicates that educational institutions are disproportionately targeted by cybercriminals because of their open network environments, resource limitations, diverse user populations, and often outdated security infrastructure (Afolalu & Tsoeu, 2025).

Educational institutions operate unique digital ecosystems that include online learning platforms, student information systems, financial records, research databases, and administrative networks. These interconnected systems make them attractive targets for cyber-attacks, which can disrupt educational delivery and compromise personal and institutional data (Hinton, 2024). Besides, global cybersecurity surveys samples of UK educational institutions complied by Maddy and Saman (2024) show that a high proportion of schools and universities have experienced breaches or attempted attacks, with many institutions lacking adequate incident response plans or comprehensive security policies.

The prevalence of cyber threats in education is underscored by the increased frequency of incidents such as malware proliferation and ransomware attacks. For example, Nicholas (2026) global threat reports revealed significant rises in malware targeting educational networks in 2022, with educational institutions facing over 3,000 attacks weekly and ransomware incidents rising sharply in 2023 and 2024 (Nicholas, 2026). These threats not only jeopardize data confidentiality but can also lead to prolonged operational downtimes and substantial financial costs for remediation which over and over again diverting scarce resources away from core educational functions.

In response to these trends, different scholars have emphasize the importance of adopting robust cybersecurity bases that balance technological defenses with human centered strategies. For example, Mouwers and Musikavanhu (2024) stress that continuous cybersecurity training and awareness programs for faculty, staff, and students are essential for mitigating cyber risks, strengthening vigilance, and reducing susceptibility to social engineering attacks. In addition, Keller (2024) recommends the adoption of advanced security models such as Zero Trust Architecture, which enhances protection against evolving threats by eliminating implicit trust within and outside institutional network perimeters.

Data Protection in Educational Institutions

Data protection in educational institutions refers to the practices and measures adopted to safeguard personal and institutional information from unauthorized access, misuse, loss, or exploitation. With many institution hasty adoption of digital tools such as learning management systems, cloud storage, student information systems, and online assessment platforms, educational institutions progressively manage more large volumes of sensitive data, including student academic records, staff personal details, financial information, and research outputs. In which the loss or compromise of such data can lead to institution's reputational damage, legal consequences, financial liabilities, and erosion of trust among stakeholders which in this case rustle up vital data protection mechanisms essential.

Many recent research has highlights the multifaceted nature of data protection in education. For example, Raval (2023) explored how increased digitization exposes institutions to cybersecurity risks such as ransomware, phishing attacks, and data breaches while data protection laws like the General Data Protection Regulation and the Family Educational Rights and Privacy Act aim to guard personal data, albeit with varying implementation challenges. The study underscores the need for policies that align technological safeguards with legal requirements to protect institutional data and user privacy. In addition, Mwamlangala (2025) also examined compliance with Tanzania's Personal Data Protection Act among universities. Using doctrinal legal research, the study found that compliance levels were low due to the absence of data protection policies, lack of awareness training, and the non-appointment of dedicated data protection officers, despite the presence of the law. These two studies suggests that legal frameworks alone are not sufficient without institutional implementation, awareness, and governance structures.

Similarly, Binitie et al. (2025) investigated EdTech security and student privacy concerns in Nigerian higher education. Their survey revealed strong student concerns about data breaches, limited trust in existing privacy practices, and a need for stronger encryption, training, and institutional data protection policies. The findings emphasize that effective data protection must combine technical measures with awareness and governance strategies to enhance institutional resilience.

Lastly, research by Xu and Zhou (2025) identified ongoing challenges as institutions transform digitally, including inconsistent compliance with data protection regulations and limited cybersecurity resources. They recommend comprehensive data governance frameworks to address privacy and security risks as part of educational transformation processes. Taken together, these studies illustrate that effective data protection in educational institutions requires an integrated approach with strong legal compliance, advanced technical controls (e.g., encryption and access management), continuous awareness training, and institutional governance to implement and enforce policies consistently.

Theoretical Framework

This study is anchored on the Technology Organization Environment theory and the Information Security Governance theory to explain how educational institutions adopt and manage cyber security and data protection practices.

The Technology Organization Environment theory developed by Tornatzky and Fleischer in 1990 and widely applied in contemporary technology adoption studies, posits that three interrelated factors including technological, organizational, and environmental determine the adoption, integration, and effectiveness of innovations within organizations (Abdurrahman et al., 2024). The technological part of this theory involves the characteristics of available technologies, such as usability, compatibility, and security features, which influence adoption. The organizational includes internal factors like institutional size, leadership support, resource availability, and workforce skills that determine readiness for implementing technological measures. While environmental comprises external pressures, such as regulatory requirements, industry standards, and stakeholder expectations, which shape adoption decisions. In educational management, TOE provides a structured lens to evaluate how digital platforms, security infrastructures, and data protection measures are adopted and maintained.

Complementing TOE, the Information Security Governance theory emphasizes the critical role of institutional leadership in establishing policies, accountability mechanisms, risk management frameworks, and compliance protocols to ensure effective data protection (Von Solms & Van Niekerk, 2022). ISG theory highlights that technological safeguards alone are insufficient effective institutional data protection measure but the success of cyber security initiatives depends on managerial oversight, organizational culture, and adherence to structured governance practices. In backing these, research by Afolalu & Tsoeu (2025) shown that institutions with strong ISG frameworks usually display better protection of sensitive student and staff data, enhanced compliance with regulations, and higher resilience against cyber threats.

By integrating TOE and ISG, this study acknowledges that effective cyber security and data protection in educational management arise from both structural governance mechanisms and related technological, organizational, and environmental factors. This combined theoretical lens provides a holistic method in understanding how institutions can enhance cybersecurity awareness, implement robust infrastructure, comply with regulations, and ensure the confidentiality, integrity, and availability of institutional data.

Empirical Review

Different studies have highlighted the critical role of cybersecurity awareness, data protection policies, and educational interventions in smoothing safe digital practices within educational institutions by integrating awareness, policy compliance, and technology management as an essential factor for safeguarding intuitional data. For example, Alqarni (2025) investigated the relationship between cybersecurity awareness and protective behaviors among Saudi secondary school students, focusing on the mediating effect of cyber threat perception and the moderating role of internet usage duration. A sample of 1,980 students across multiple regions was studied using structural equation modeling (SEM) via AMOS24. Findings indicated that cybersecurity awareness ($\beta = 0.38$, $p < 0.001$) and internet usage duration ($\beta = 0.27$, $p < 0.001$) significantly predicted cyber threat perception, which in turn predicted protective behaviors ($\beta = 0.44$, $p < 0.001$). Cyber threat perception mediated the awareness-behavior link (indirect $\beta = 0.17$, $p < 0.001$), while longer internet usage strengthened the direct and indirect effects. The study concluded that interactive cybersecurity modules and targeted interventions for high internet users optimize protective behaviors.

Eshetu et al (2024) examined cybersecurity vulnerabilities in 16 Ethiopian university websites using automated vulnerability assessment tools (Nmap, Nessus, Vega) and a cybersecurity awareness survey. Vega reported 11,286 findings, and Nessus identified 1,749 vulnerabilities, including outdated software, weak passwords, and insufficient encryption. The study proposed tailored countermeasures for each vulnerability, emphasizing proactive cybersecurity measures and strategic planning to safeguard sensitive academic data.

Kaleli (2024) measured digital data security awareness among students and staff at Ardahan University using a validated awareness scale with 324 participants. Results showed medium to high awareness across password security, safe internet use, data backup, and software updates. The study concluded that while awareness levels were satisfactory, continuous institutional efforts are needed to maintain secure practices and inform policy decisions.

Oroni et al. (2024) explored cyber safety in e-learning environments using PLS-SEM and fsQCA with 398 virtual students. Cybersecurity awareness and information security policy compliance significantly enhanced cyber safety measures. The fsQCA analysis revealed multiple effective pathways; high awareness combined with policy compliance consistently led to safer digital behaviors, even with moderate e-learning engagement. The study recommended integrated strategies that combine awareness, engagement, and policy enforcement.

Martin et al. (2026) evaluated multimedia-based cybersecurity professional development for 50 K-12 personnel. Pre- and post-tests showed significant knowledge gains using Wilcoxon signed-rank tests. Participants reported enhanced ability to recognize and act against potential cyber threats, although technical and resource challenges were noted. The study concluded that targeted professional development significantly improves cybersecurity literacy among educators.

Sapanca and Kanbul (2022) assessed teachers' information security awareness in Turkey through a survey of 394 educators. Results revealed moderate awareness, with lower levels among female teachers and higher levels among trained and IT-specialist teachers. The study concluded that professional training is vital to enhance teacher awareness and overall institutional cybersecurity posture.

Essien and Edun (2024) examined digitalizing cybersecurity for data management in Nigerian higher education among 400 students. Findings revealed that educators' lack of cyberspace expertise negatively influenced cybersecurity knowledge and data protection, contributing to risks such as cyberbullying and online fraud. The study concluded that institutional policies and curriculum reforms are critical to improving cybersecurity education and protective behaviors.

Ogunode et al (2025) analyzed cybersecurity education in Nigerian schools, highlighting systemic challenges such as inadequate funding, poor infrastructure, lack of trained personnel, and insufficient professional development. The study emphasized the importance of targeted training, policy reform, and curriculum integration to establish safer digital environments for students.

Methodology

This study adopted a quantitative research design to examine the influence of cybersecurity awareness, infrastructure security, regulatory compliance, and incident response capability on data protection effectiveness among educational management staff in Nigerian universities. This study focused on staff and management personnel from federal and state universities across Nigeria. A multistage sampling technique was employed. In the first stage, a stratified sampling approach was used to categorize Nigeria into its six geopolitical zones namely; North Central, North East, North West, South West, South East, and South South. This stratification ensured that all regions of the country were included in the study. In the second stage, five (5) universities (comprising both federal and state institutions) were purposively selected from each geopolitical zone, based on their accessibility, and the availability of educational management staff. This resulted in a total of thirty (30) universities. At the third stage, this study aimed to target at least eight (8) respondents from each university. This provided a total target population of 240 educational management staff and personnel across universities in Nigeria. Out of the targeted population of 240, 195 respondents successfully completed the online questionnaire representing a response rate of 81.25%. Data were collected using a questionnaire administered through a Google Forms. The instrument was subjected to content validation by three experts; one from Ekiti State University and two from Bamidele Olumilua University of Education, Science and Technology, Ado Ekiti. Their input ensured that the items were clear, relevant, and adequately captured the constructs under investigation. The questionnaire was divided into sections covering demographic information and the main study variables, namely cybersecurity awareness, infrastructure security, regulatory compliance, incident response capability, and data protection effectiveness. Each construct was measured using five (5) items, giving a total of twenty five (25) items, all adapted from relevant literature and aligned with the objectives of this study. Cybersecurity Awareness items assessed respondents' knowledge and understanding of cyber threats, safe online practices, and compliance with institutional cybersecurity policies. Infrastructure Security items measured the perceived robustness and reliability of digital systems, including monitoring, firewalls, and encryption mechanisms.

Regulatory Compliance items captured adherence to institutional policies and national/international data protection frameworks. Incident Response Capability items evaluated the ability of staff and institutions to respond effectively to cyber incidents, including reporting, mitigation, and recovery procedures. Data Protection Effectiveness items reflected the extent to which institutional data is safeguarded from unauthorized access, breaches, or loss, emphasizing confidentiality, integrity, and availability of sensitive information. Responses were captured using a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5) so as to allow respondents to express their level of agreement with each statement. Data analysis was conducted using SPSS and AMOS 24 for Structural Equation Modeling. Descriptive statistics, including mean and standard deviation, were used to assess the central tendency and dispersion of responses. Model fit was evaluated using indices such as Chi-square/df, CFI, NFI, RMSEA, and SRMR, with thresholds adhering to Hair et al. (2022) recommendations. While reliability and validity of the constructs were evaluated using CR and AVE before SEM was then applied to test the hypothesized relationships, providing unstandardized (B) and standardized (β) coefficients, critical ratios, and p-values for hypothesis evaluation. The R² value was used to assess the explanatory power of the model. Ethical considerations, including informed consent, confidentiality, and voluntary participation were all strictly observed throughout the study and stated in the form.

Result

Analysis of Research Questions

Question one: What is the level of cyber security awareness among staff and management in educational institutions?

Table 1: Respondent’s perception of Cyber Security Awareness on Data Protection

S/N	Items	N	Mean	Std
1.	I am aware and knowledgeable about different types of cyber threats, such as phishing attacks, malware, ransomware and their potential impacts on data.	195	4.20	0.401
2.	I understand the importance of creating strong, unique passwords and consistently updating them to prevent unauthorized access to institutional accounts.	195	4.19	0.393
3.	I am aware of safe internet browsing practices and usually avoid visiting suspicious websites or downloading unverified files / link on institutional devices.	195	4.18	0.389
4.	I have a clear understanding of my institution’s cybersecurity policies, guidelines, and rules regarding the use of digital resources and online platforms.	195	4.17	0.380
5.	I regularly follow security protocols, such as locking devices and logging out of accounts, to protect institutional and personal data from cyber threats.	195	4.17	0.380
	Average Mean		**4.18**	**0.389**

The response in table 1 indicate a consistently high level of cyber security awareness among respondents. Item 1 (Mean = 4.20, SD = 0.401) shows strong awareness of cyber threats and their implications to institution data. Item 2 (Mean = 4.19, SD = 0.393) reflects sound knowledge of password security practices. Item 3 (Mean = 4.18, SD = 0.389) confirms safe browsing behavior. Items 4 and 5 with the same (Mean = 4.17, SD = 0.380) also demonstrate understanding of institutional policies and adherence to security protocols. Overall, these findings suggest that respondents perceive themselves as highly knowledgeable and compliant with cybersecurity practices. However, the relatively low standard deviation across items indicates limited variability in responses, which may have implications for further inferential analysis.

Question Two: How does infrastructure security affect data protection effectiveness in educational management?

Table 2: Respondent’s perception of Infrastructure Security on Data Protection

S/N	Items	N	Mean	STD
1.	Access to our institution sensitive information is strictly restricted to authorized personnel only, with proper authentication.	195	4.17	0.380
2.	Our computers, servers, and devices are regularly updated with software patches and system upgrades to mitigate security vulnerabilities.	195	4.17	0.380
3.	Reliable backup systems, including cloud and physical storage, are implemented to ensure rapid recovery of institutional data in the event of system failures or attacks.	195	4.17	0.380
4.	Our institution’s IT infrastructure is equipped with robust firewalls, antivirus software, and intrusion detection systems that prevent unauthorized access.	195	4.17	0.376
5.	All sensitive data stored on our institutional servers, databases, or cloud systems are encrypted using standard encryption protocols to ensure confidentiality and integrity.	195	4.18	0.385
	Average Mean		**4.17**	**0.380**

Table 2 findings reveal a very strong perception of infrastructure security within the institution. Item 1 (Mean = 4.17, SD = 0.380) indicates confidence in restricted access and authentication controls. Item 2 (Mean = 4.17, SD = 0.380) reflects regular system updates to address vulnerabilities. Item 3 (Mean = 4.17, SD = 0.380) confirms reliable backup mechanisms. Item 4 (Mean = 4.17, SD = 0.376) suggests robust protective systems such as firewalls and antivirus tools. Item 5 (Mean = 4.18, SD = 0.385) shows strong data encryption practices.

Question Three: How does Regulatory Compliance affect Data Protection Effectiveness in educational institutions?

Table 3: Respondent's perception of Regulatory Compliance on Data Protection

S/N	Items	N	Mean	STD
1.	Our institution actively complies with national and international data protection regulations, such as GDPR and FERPA, to safeguard students' and staff personal information.	195	4.21	0.405
2.	Policies and procedures regarding data protection and privacy are clearly communicated to all staff and students in a consistent and accessible manner.	195	4.21	0.409
3.	All staffs and students receive periodic training and workshops to enhance understanding of data protection regulations and ensure institutional compliance.	195	4.20	0.401
4.	Audits compliance are conducted regularly to evaluate adherence to data protection policies and to identify areas that needed improvement.	195	4.19	0.393
5.	Instances of regulatory non-compliance or violations are promptly addressed and sanctioned.	195	4.19	0.397
	Average Mean		**4.20**	**0.401**

The table 3 results furthermore show evidence of high level of perceived regulatory compliance within Nigerian institution as both items 1 and 2 same mean value of 4.21 indicate strong agreement that their institution always complies with data protection regulations and clearly cyber security related policies. Also, item 3 (Mean = 4.20, SD = 0.401) reflects consistent training efforts being made by the institutions while items 4 and 5 indicate their institution do regularly involve in audit compliance and prompt handling of any cyber violations or threats.

Question Four: What is the influence of Incident Response Capability on Data Protection Effectiveness?

Table 4: Respondent's perception of Incident Response Capability on Data Protection

S/N	Items	N	Mean	STD
1.	Our institution has a formally documented incident response plan that outlines step-by-step procedures to follow in the event of a cyberattack or data breach.	195	4.17	0.380
2.	Staff and students are trained to respond effectively and efficiently during cybersecurity incidents, including reporting threats and minimizing data loss.	195	4.17	0.380
3.	Our institution has monitoring tools in place to detect, analyze, and report any data breaches or unauthorized access in real-time.	195	4.24	0.426
4.	Recovery procedures are in place to restore data and systems after incidents.	195	4.18	0.385
5.	Lessons from past cyber incidents are thoroughly reviewed and incorporated into updated strategies to improve future cybersecurity resilience.	195	4.18	0.389
	Average Mean		**4.19**	**0.392**

As presented in Table 4 above, the overall mean of 4.19 suggests that respondents perceive incident response capability as relatively strong. Items 1 and 2, with mean values of 4.17, indicate that respondents believe their institutions have incident response plans in place and that IT staff are trained to respond to cyber incidents. Item 3, with a mean of 4.24, reflects respondents' confidence in the availability of real time monitoring and cyber breach detection tools at their institutions. Similarly, items 4 and 5, with mean values of 4.18, suggest that respondents perceive their institutions to have effective recovery procedures and practices for continuous improvement in the event of cyber incidents.

Table 5: Model Fit and Reliability Summary Table

Model Fit		
Fit Index	**Estimate**	**Notes / Range interpretation**
Chi-Square (CMIN)	339.684	DF = 265, p = .001
CMIN/DF	1.282	Acceptable if < 3
Standardized RMR	0.0416	< 0.08 indicates good fit
NFI	0.911	> 0.90 indicates good fit
RFI	0.900	> 0.90 indicates good fit
RMSEA	0.032	LO 90 = 0.020, HI 90 = 0.041, PCLOSE = 1.000

Reliability and Validity Measures			
Construct	**CR**	**AVE**	**Notes / Validity Concerns**
Cyber Security Awareness	0.874	0.584	CR > 0.7, AVE > 0.5, convergent validity acceptable
Infrastructure Security	0.881	0.598	CR and AVE indicate strong reliability and validity
Regulatory Compliance	0.880	0.595	Good convergent and discriminant validity
Incident Response Capability	0.870	0.572	All validity measures acceptable
Data Protection Effectiveness	0.894	0.628	Highest reliability, AVE > 0.6, strong construct validity

The Model Fit Summary in table 5 indicates an excellent fit between the hypothesized model and the observed data. The Chi-Square (CMIN = 339.684, DF = 265, p = 0.001<0.05) shows significant, with CMIN/DF ratio of 1.282 well below the recommended threshold of 3, further highlight a good relative fit. In addition, absolute fit indices, including the SRMR (0.0416) and RMSEA (0.032, 90% CI: 0.020–0.041, PCLOSE = 1.000), confirm minimal residuals and excellent approximation.

Furthermore, the reliability and validity assessment show that all constructs exhibit strong psychometric properties. Composite reliability (CR) values range from 0.870 to 0.894, exceeding the 0.70 threshold, confirmed internal consistency among the variable. Average Variance Extracted (AVE) values span 0.572 to 0.628, all above 0.50 further confirm satisfactory convergent validity. Remarkably results shows that all the constructs are reliable and valid for structural modeling and hypothesis testing.

Hypotheses Testing

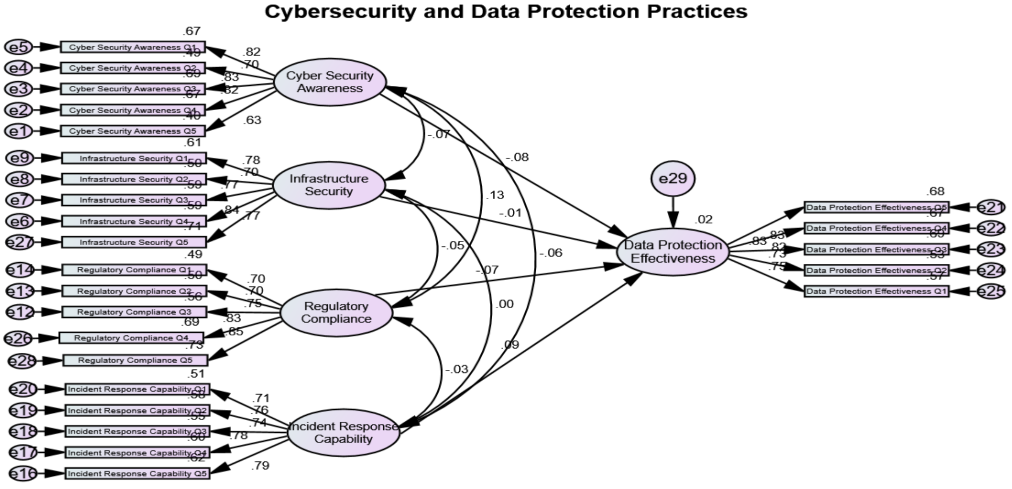
Cybersecurity and Data Protection Practices
Cyber Security Awareness
Infrastructure Security
Regulatory Compliance
Incident Response Capability
Data Protection Effectiveness
e29
.02
Cyber Security Awareness Q1
Cyber Security Awareness Q2
Cyber Security Awareness Q3
Cyber Security Awareness Q4
Cyber Security Awareness Q5
Infrastructure Security Q1
Infrastructure Security Q2
Infrastructure Security Q3
Infrastructure Security Q4
Infrastructure Security Q5
Regulatory Compliance Q1
Regulatory Compliance Q2
Regulatory Compliance Q3
Regulatory Compliance Q4
Regulatory Compliance Q5
Incident Response Capability Q1
Incident Response Capability Q2
Incident Response Capability Q3
Incident Response Capability Q4
Incident Response Capability Q5
Data Protection Effectiveness Q5
Data Protection Effectiveness Q4
Data Protection Effectiveness Q3
Data Protection Effectiveness Q2
Data Protection Effectiveness Q1
e5
e4
e3
e2
e1
e9
e8
e7
e6
e27
e14
e13
e12
e26
e28
e20
e19
e18
e17
e16
e21
e22
e23
e24
e25
.67
.49
.69
.67
.40
.82
.70
.83
.82
.63
.61
.50
.59
.59
.71
.78
.70
.77
.84
.77
.49
.50
.56
.69
.73
.70
.70
.75
.83
.85
.51
.58
.55
.60
.62
.71
.76
.74
.78
.79
.68
.67
.69
.53
.57
.83
.83
.82
.73
.75
-.07
-.08
.13
-.01
-.05
-.06
-.07
.00
.09
-.03

Figure 1: Standardized Estimate

Table 6: Summary of Structural Path Results and Hypotheses Testing

H_0	Path	B (Unstd.)	S.E	C.R	P-value	β (Std.)	Decision
H_{01}	Data Protection Effectiveness ← Cyber Security Awareness	-0.104	0.091	-1.141	0.254	-0.077	Not Rejected
H_{02}	Data Protection Effectiveness ← Infrastructure Security	-0.015	0.075	-0.204	0.838	-0.014	Not Rejected
H_{03}	Data Protection Effectiveness ← Regulatory Compliance	-0.086	0.078	-1.106	0.269	-0.074	Not Rejected
$H0_4$	Data Protection Effectiveness ← Incident Response Capability	0.100	0.071	1.410	0.159	0.094	Not Rejected
R^2	Data Protection Effectiveness			0.023			

From the table 6 and figure 1 above, the hypothesis testing results indicate that none of the independent variables significantly influence Data Protection Effectiveness. Specifically, Cyber Security Awareness (H_{01}: β = -0.077, p = 0.254), Infrastructure Security (H_{02}: β = -0.014, p = 0.838), Regulatory Compliance (H_{03}: β = -0.074, p = 0.269), and Incident Response Capability (H_{04}: β = 0.094, p = 0.159) all have p-values above the 0.05 statistical level of significance. Consequently, the four null hypotheses cannot be rejected. The R^2 value of 0.023 further indicates that these constructs together explain only 2.3% of the variance in Data Protection Effectiveness, suggesting that other factors may have more substantial impact that these factors.

Discussion of Findings

The findings from the hypothesis testing indicate that none of the examined independent variables, including cybersecurity awareness, infrastructure security, regulatory compliance, and incident response capability, significantly influenced data protection effectiveness. Specifically, the standardized coefficients were weak, ranging from -0.077 to 0.094, and all p-values exceeded the 0.05 level of significance. Consequently, all the null hypotheses were not rejected. The R^2 value of 0.023 further suggests that these variables jointly explain only a very small proportion of the variance in data protection effectiveness. This implies that other factors not captured in the current model may play a more substantial role in determining the effectiveness of institutional data protection.

A critical observation in this study, however, is the apparent contradiction between the high descriptive mean scores reported across all constructs and the non significant structural relationships. While respondents generally perceived cybersecurity awareness, infrastructure security, regulatory compliance, and incident response capability to be highly effective (with mean values above 4.0), these perceptions did not translate into statistically significant predictive relationships in this study. This inconsistency may be attributed to several factors. First, social desirability bias may have influenced respondents to provide favorable responses that reflect expected institutional standards rather than actual practices. Also, the findings may reflect symbolic compliance, where institutions formally adopt cybersecurity policies and frameworks without fully implementing them in practice.

The empirical evidence from prior studies offers both complementary and contrasting perspectives on these findings. Previous research has consistently emphasized the importance of cybersecurity awareness in shaping protective behaviors and promoting secure digital practices. For instance, Alqarni (2025) reported a significant positive relationship between cybersecurity awareness and cyber threat perception among Saudi secondary school students, which subsequently enhanced protective behaviors. Similarly, Oroni et al. (2024) found that cybersecurity awareness and adherence to information security policies collectively improved cyber safety among virtual learners, demonstrating multiple pathways through which awareness can influence outcomes. These findings support the theoretical expectation that awareness and compliance are critical components of effective data protection.

In contrast, the non-significant findings in this study may reflect contextual and practical limitations within the sampled institutions. Unlike the structured interventions and comprehensive awareness programs reported in studies such as Alqarni (2025), Kaleli (2024), and Martin et al. (2026), the institutions examined in this study may lack consistent training programs, effective monitoring systems, or strong enforcement mechanisms. Evidence from Nigerian higher education supports this interpretation. Essien and Edun (2024) and Ogunode et al. (2025) identified systemic challenges such as inadequate infrastructure, limited technical expertise, insufficient funding, and weak institutional enforcement as key barriers to effective cybersecurity implementation in many institutions. These structural constraints may result in a situation where awareness and policies exist in principle but do not translate into actual data protection outcomes.

Furthermore, the weak and, in some cases, negative coefficients observed for constructs such as cybersecurity awareness (-0.077) and infrastructure security (-0.014) suggest that awareness and technical measures alone may not directly lead to measurable improvements in data protection effectiveness. This finding aligns with Sapanca and Kanbul (2022), who argued that awareness does not automatically translate into behavioral compliance without continuous professional development and targeted interventions. Similarly, Eshetu et al. (2024) emphasized that effective cybersecurity requires a combination of proactive vulnerability management, technical controls, and organizational commitment. This indicates that data protection effectiveness is a multidimensional outcome influenced by deeper institutional factors such as enforcement culture, leadership commitment, resource allocation, and integration of cybersecurity practices into daily operations.

On the whole, the findings of this study imply that even though educational institutions may demonstrate relatively high levels of perceived preparedness in terms of cyber security awareness, infrastructure security, regulatory compliance, and incident response capability, these factors alone are insufficient to explain actual data protection effectiveness. This proposes a possible disconnect between perceived readiness and realworld implementation of effective data protection practices within educational management systems. It further indicates that institutional efforts may be more theoretical or policydriven rather than practically enforced or technologically supported.

Conclusion

Based on the findings of the study, it can be concluded that educational managements staffs in both Federal and State University exhibit high levels of cyber security awareness, strong infrastructure security, strong regulatory compliance, effective incident response capabilities, and overall data protection effective measure. Respondents consistently reported high understanding level of cyber threats, adhering to security protocols, and following institutional policies, while infrastructure and monitoring systems were perceived as reliable and secure. However, the hypothesis testing revealed that these constructs did not significantly predict data protection effectiveness, which automatically advocate that other organizational factors may play a more essential role in safeguarding institutional data. Therefore, in spite of the fact that awareness, policies, and technical controls are important, institutional commitment, continuous training, and proactive organizational support are essential to transform these measures into tangible improvements in data protection. These by so doing highlight the need of comprehensive, multi-dimensional strategies to strengthen cybersecurity practices and protect sensitive institutions information effectively.

Recommendations

Based on the findings of this study, the following recommendations are put forward:

1. To enhance the effect of cybersecurity awareness on data protection effectiveness, government agencies and university management should implement regular and comprehensive training programs for staff and students. These programs should focus on recognizing cyber threats, practicing safe online behavior, and understanding institutional cybersecurity policies to translate awareness into improved data protection practices.
2. University management should invest in upgrading and maintaining IT infrastructure, including firewalls, encryption protocols, intrusion detection systems, and reliable backup solutions, to improve the overall security of institutional data.
3. Institutions and management should establish clear policies aligned with national and international data protection frameworks, conduct regular audits, and monitor adherence. Continuous staff and student training on data protection regulations will ensure compliance translates into improved security outcomes.
4. To improve the effect of incident response capability on data protection, institutions management should develop formal incident response plans, conduct periodic simulation exercises, and provide ongoing training to IT staff and relevant personnel. Lessons learned from past incidents should be incorporated into updated procedures to enhance institutional resilience and rapid recovery in case of cyberattacks.

References

1. Abdurrahman, A., Gustomo, A., & Prasetio, E. A. (2024). Impact of dynamic capabilities on digital transformation and innovation to improve banking performance: A TOE framework study. *Journal of Innovation & Knowledge Management.*https://www.sciencedirect.com/science/article/pii/S2199853124000O9X
2. Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. *Future Internet, 17*(12), 575. https://doi.org/10.3390/fi17120575
3. Agalit, M. A., Chakir, E. M., Issam, T., & Idrissi Khamlichi, Y. (2023). A review of cybersecurity management standards applied in higher education institutions. *International Journal of Cyber Security and Safety Education.* https://doi.org/10.18280/ijsse.130614
4. Alqarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: The mediating role of cyber threat perception and the moderating role of internet usage duration. *Humanities and Social Sciences Communications, 12*, 1837. https://doi.org/10.1057/s41599-025-06122-x
5. Binitie Amaka Patience, Onyemenem, S. I., & Okoh, F. J. (2025). Enhancing security and privacy in EdTech tools: Safeguarding student data in the digital learning era. *Journal of Science Innovation and Technology Research, 9*(9). https://doi.org/10.70382/ajsitr.v9i9.041
6. Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *Journal of Big Data, 11*, 118. https://doi.org/10.1186/s40537-024-00980-z
7. Essien, E. S., & Edun, E. E. (2024). Digitalizing cyber security for data management in higher education: Implications for educational management in Nigeria. *Journal of Advances in Education and Philosophy, 8*(4), 234–238. https://doi.org/10.36348/jaep.2024.v08i04.001
8. Hinton, M. (2024). Cybersecurity challenges intensify for educational institutions amid cyberattack surge – Report. *Cyber Insurance News.*https://cyberinsurancenews.org/cybersecurity-challenges-intensify-for-educational-institutions-amid-surge-in-cyberattacks/
9. Kaleli, S. S. (2024). Measuring digital data security awareness: The case of higher education institution. *Journal of Studies in Advanced Technologies, 2*(2), 108–119. https://doi.org/10.63063/jsat.1591281
10. Keller, J. (2024). How zero trust can protect against evolving cybersecurity threats in higher ed. *EdTech Magazine.*https://edtechmagazine.com/higher/article/2

024/07/how-zero-trust-can-protect-against-evolving-cybersecurity-threats-higher-ed

11. Kifaru, F., Kavuta, K., & Semlambo, A. (2023). Assessment of the impacts of cyber security on student information management systems: A case of Ruaha Catholic University. *The Journal of Informatics, 3*(1). https://doi.org/10.59645/tji.v3i1.127
12. Maddy, E., & Saman, R. (2024). Cyber Security Breaches Survey 2024: Education institutions annex. *GOV.UK*.https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex
13. Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., & Ojugo, A. A. (2024). Techniques and best practices for handling cybersecurity risks in educational technology environment. *Journal of Science and Technology Research*, *6*(2), 293–311. https://doi.org/10.5281/zenodo.12617068
14. Martin, F., Zhuang, M., Byker, E., Wang, W. C., Bacak, J., & Ahlgrim-Delzell, L. (2026). Multimedia-based cybersecurity and privacy professional development on educational technology for K-12 personnel. *Educational Technology Research and Development*.https://doi.org/10.1007/s11423-025-10575-x
15. Mouwers Singh, C., & Musikavanhu, T. (2024). A narrative review on enhancing cybersecurity in higher education institutions: The role of continuous training and awareness. *Expert Journal of Business and Management, 12*(2), 67–73. https://business.expertjournals.com/ark:/16759/EJBM_1206mouwers67-73.pdf
16. Mwamlangala, D. F. (2025). Are universities compliant? A study of Tanzania’s Personal Data Protection Act in higher learning institutions. *African Journal of Law and Practice*, *1*(2), 66–83. https://doi.org/10.61538/afjlp.v1i2.1791
17. Nicholas, S. (2026). The 5 biggest cyber threats for the education sector in 2026. *UpGuard Blog*.https://www.upguard.com/blog/cyber-threats-education
18. Ogunode, N. J., Edinoh, K., & Felicia, A. O. (2025). Cyber security education in Nigerian schools: Importance, problems and way forward. *Web of Scholars: Multidimensional Research Journal*, *4*(1), 25–32. https://journals.innoscie.com/index.php/wos/article/view/38
19. Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2024). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. *Computers & Security*, *150*, 104276. https://doi.org/10.1016/j.cose.2024.104276
20. Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers’ information security awareness levels. *Frontiers in Psychology*, *13*, 986561. https://doi.org/10.3389/fpsyg.2022.986561
21. Von Solms, R., & Van Niekerk, J. (2022). Information security governance: A comprehensive review. *Computers & Security, 112*, 102509. https://doi.org/10.1016/j.cose.2022.102509
22. Xu, N., & Zhou, X. (2025). Guarding the digital education era: Unraveling the data security and privacy dilemmas in educational transformation. *International Journal of Sociologies and Anthropologies Science Reviews*, *5*(5), 733–744. https://doi.org/10.60027/ijsasr.2025.7209