Cyber security Risks and Mitigation Strategies in Digital Monitoring Systems among Primary School Stakeholders

Rasaki Rasheed Olakunle[1], Bankole Odofin[2], Ogbaini Aliu Clement[3], Samuel Tosin Olorunnisola[4], Joseph Oluwafemi Oluwasegun[5]

[1, 2, 4] *Educational Planning and Management, Global Wealth University, Lome, Togo*
[3] Business *Administration, Global Wealth University, Lome, Togo*
[5] *Accounting, Global Wealth University, Lome, Togo*

ABSTRACT

This study examines cyber security risks and mitigation strategies in digital monitoring systems among stakeholders in public primary schools in Surulere Local Government Area, Lagos State, Nigeria. The increasing adoption of digital tools for student management has heightened vulnerabilities to threats such as data breaches, unauthorized access, and malware, exacerbated by limited awareness and weak infrastructure. Guided by the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT), the research aimed to identify risks, assess stakeholder awareness and practices, and evaluate adopted mitigation strategies. A descriptive survey design was employed, with data collected from 300 respondents (20 administrators, 100 teachers, and 180 parents) using a structured questionnaire on a 5-point Likert scale. Descriptive statistics revealed high perceived cyber security risks (overall mean = 3.74), moderate awareness levels (mean = 3.00), and moderate-to-low adoption of mitigation strategies (mean = 2.76). Key gaps included inadequate training, poor multi-factor authentication, and insufficient data protection policies. The findings underscore a critical disparity between recognized risks and preparedness, leaving sensitive student data exposed. Recommendations include mandatory training, technical upgrades, and policy enforcement to enhance cyber security. This study contributes empirical insights to cyber security in Nigerian primary education, highlighting the need for proactive measures to safeguard digital systems.

KEYWORDS
Cyber security risks, digital monitoring systems, primary schools, stakeholder awareness, mitigation strategies, Nigeria

I. INTRODUCTION

A. Background to the Study

The adoption of digital monitoring systems in primary schools has increased significantly, transforming how student learning, attendance, and administrative activities are managed. Tools such as learning management systems, student information databases, and online communication platforms support efficient data collection and decision-making among school administrators, teachers, and parents (Selwyn, 2016). While these technologies offer clear educational benefits, they also expose primary schools to growing cyber security risks.

Primary schools handle sensitive student data, including personal and academic records, which makes digital monitoring systems vulnerable to cyber threats such as data breaches, unauthorized access, and malware attacks. These risks are often heightened by weak security infrastructure, limited technical expertise, and low cyber security awareness among school stakeholders. Inadequate protection of children's data can result in serious privacy and ethical concerns.

Mitigating cyber security risks requires both technical safeguards and stakeholder awareness, including secure access controls, regular system updates, clear data protection policies, and user training. However, many primary schools focus more on technology adoption than on cyber security preparedness, leaving digital monitoring systems insufficiently protected. Therefore, examining cyber security risks and mitigation strategies among primary school stakeholders is essential to promoting safe and effective use of digital monitoring systems.

B. Statement of the Problem

The increasing use of digital monitoring systems in primary schools has exposed sensitive pupil data to various cyber security risks. Many schools store and manage personal and academic information through digital platforms that are vulnerable to unauthorized access, data breaches, and cyber-attacks. These risks are often intensified by weak security systems and limited cyber security awareness among school stakeholders.

Primary school administrators, teachers, and parents may lack the necessary knowledge, policies, and technical capacity to effectively protect digital monitoring system. Despite these challenges, limited research has examined cyber security risks and mitigation strategies from the perspective of primary school stakeholders. This gap underscores the need for a focused study to support the secure use of digital monitoring systems in primary education.

C. Objectives of the study

The main objective of this study is to examine cyber security risks and mitigation strategies in digital monitoring systems among primary school stakeholders in public primary schools in Surlier Local Government Area, Lagos State.

The specific objectives of the study are to:

- Identify the cyber security risks associated with the use of digital monitoring systems in public primary schools in Surlier Local Government Area, Lagos State;
- Assess the level of cyber security awareness and practices among primary school stakeholders in the study area; and
- Examine the mitigation strategies adopted to address cyber security risks in digital monitoring systems in public primary schools in Surlier Local Government Area, Lagos State.

D. Research Questions

The following questions guided investigations in the study:

- What are the cyber security risks associated with the use of digital monitoring systems in public primary schools in Surulere Local Government Area, Lagos State?
- What is the level of cyber security awareness and practices among primary school stakeholders in public primary schools in Surulere Local Government Area, Lagos State?
- What mitigation strategies are adopted to address cyber security risks in digital monitoring systems in public primary schools in Surulere Local Government Area, Lagos State?

E. Significance of the Study

This study is significant for several reasons. First, it provides valuable insights into the cyber security risks associated with digital monitoring systems in public primary schools, highlighting potential vulnerabilities that could compromise students' sensitive data. By identifying these risks, the study can guide school administrators, teachers, and policymakers in implementing effective security measures.

Second, the study raises awareness among primary school stakeholders—including teachers, parents, and school administrators—about the importance of cyber security practices. Increased awareness can encourage responsible handling of digital systems, promote safe use of technology, and reduce the likelihood of cyber incidents.

Third, the study contributes to the development of context-appropriate mitigation strategies for primary schools in Surulere Local Government Area, Lagos State. Recommendations from the study can inform policy formulation, training programs, and the adoption of technical safeguards, ultimately enhancing the safety and reliability of digital monitoring systems.

Finally, the research adds to the academic discourse on cyber security in education, particularly in the Nigerian context, where empirical evidence on primary school digital security is limited. This can serve as a reference for future studies and support the broader goal of creating secure and effective digital learning environments.

F. Scope and Limitation of the Study

This study focuses on examining cyber security risks and mitigation strategies in digital monitoring systems among stakeholders of public primary schools in Surulere Local Government Area, Lagos State. The study targets key stakeholders, including school administrators, teachers, and parents, to understand their awareness, experiences, and practices regarding cyber security. It covers common digital monitoring systems used in these schools, such as student information systems, learning management platforms, attendance tracking systems, and communication tools. The research specifically investigates the types of cyber security risks, the level of stakeholder awareness, and the mitigation strategies employed to safeguard digital systems.

The study is limited to public primary schools in Surulere Local Government Area, which may affect the generalizability of the findings to other regions or private schools. Additionally, the research relies on self-reported data from stakeholders, which may be subject to bias or inaccuracies. Constraints such as limited access to school records, varying levels of technical knowledge among respondents, and potential reluctance to disclose security challenges may also affect data completeness. Despite these limitations, the study provides valuable insights into cyber security practices and risks within the selected schools.

II. LITERATURE REVIEW

A. Conceptual Clarification

The study made efforts on the clarification of certain concepts that are relevant to the study

1. Cyber security Risks

Cyber security risks encompass potential threats that could undermine the confidentiality, integrity, and availability of digital information and systems within educational environments. In primary schools, these risks manifest through unauthorized access to sensitive student records, data breaches exposing personal information, malware infections disrupting operations, phishing attempts targeting staff and students, and the potential misuse of digital tools like monitoring systems. Such vulnerabilities are exacerbated by the increasing reliance on digital platforms for learning and administration, often with limited resources for robust defences in school settings.

Furthermore, primary schools face heightened exposure due to factors like outdated infrastructure, insufficient teacher training in cyber security, and the integration of personal devices in educational activities, leading to incidents such as ransom ware attacks or identity theft affecting young learners. Reports indicate that the education sector, including primary levels, experiences frequent cyber incidents, with phishing and malware being prevalent vectors that can result in financial losses, operational disruptions, and long-term harm to student privacy. Addressing these risks requires proactive education and awareness programs tailored to young students and educators to foster safe digital habits from an early age.

2. Digital Monitoring Systems

Digital monitoring systems comprise technological platforms deployed in educational institutions to track, manage, and generate reports on various aspects of student life, including academic performance, attendance records, behavioural patterns, and administrative communications. Common examples include learning management systems (LMS), student information systems (SIS), biometric attendance trackers, parent-teacher communication apps, and activity monitoring software on school-issued device.

These systems aim to enhance administrative efficiency, support personalized learning, and promote student safety through features like real-time alerts for concerning behaviour; however, they also raise significant privacy concerns by enabling extensive data collection,

often extending beyond school hours and onto personal devices. Critiques highlight risks of overreach, such as disproportionate impacts on marginalized students, lack of transparency in algorithmic decision-making, and potential for data breaches or misuse, underscoring the need for balanced implementation with strong safeguards.

B. Theoretical Framework

This study is anchored on the Technology Acceptance Model (TAM), which explains how stakeholders' perceptions of usefulness and ease of use influence their adoption of digital monitoring systems, and the Protection Motivation Theory (PMT), which describes how perceived cyber security threats motivate stakeholders to implement protective measures.

1. Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), originally proposed by Davis (1989), posits that users' acceptance of new technology is primarily driven by two key perceptions: perceived usefulness (the degree to which a person believes that using a system will enhance their performance) and perceived ease of use (the degree to which a person believes that using the system will be free of effort). These factors influence attitudes toward technology, which in turn affect behavioural intention and actual usage. In educational contexts, TAM has been widely applied to explain the adoption of various digital tools by teachers and students, demonstrating its robustness in predicting intentions to use learning management systems, mobile learning applications, and emerging technologies like virtual reality.

Within the scope of this study on digital monitoring systems in primary schools, TAM provides a lens to examine how stakeholders—such as teachers, administrators, and parents—perceive the benefits and usability of these platforms for tracking student performance and behaviour. If perceived as useful for improving administrative efficiency and student outcomes, while also being easy to navigate, adoption rates increase; conversely, complexity or lack of clear advantages can hinder implementation. Recent extensions of TAM in education have incorporated additional factors like self-efficacy and social influence, further enhancing its explanatory power for secure technology adoption in school environments. This framework is particularly relevant for understanding the integration of security practices, as positive perceptions can encourage proactive measures against risks.

2. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT), developed by Rogers (1975) and revised in 1983, explains how individuals are motivated to engage in protective behaviours in response to perceived threats through two appraisal processes: threat appraisal (assessing the severity and vulnerability to a threat) and coping appraisal (evaluating response efficacy, self-efficacy, and response costs). Higher threat perceptions combined with strong coping beliefs lead to greater protection motivation and adaptive behaviours. PMT has proven effective in health and behavioural research and has been increasingly applied to cyber security contexts, where it predicts intentions to adopt protective measures like antivirus software or secure practices.

In this study, PMT elucidates how primary school stakeholders perceive cyber security threats to digital monitoring systems—such as data breaches or unauthorized access—and their subsequent motivation to implement safeguards. For instance, awareness of severe consequences (e.g., privacy violations affecting young students) and vulnerability (e.g., due to limited school resources) can heighten threat appraisal, while confidence in mitigation strategies (e.g., training or encryption tools) boosts coping appraisal. Recent applications in educational technology highlight PMT's utility in promoting safe online behaviours among students and teachers, often integrated with other models to address awareness training and policy compliance. By framing cyber security as a protective response, PMT complements efforts to build resilience in school digital ecosystems.

C. Empirical Review

Several studies have examined cyber security risks and mitigation strategies in educational digital systems, highlighting both the challenges and best practices. Kshetri (2019) found that educational institutions are increasingly targeted by cyber-attacks due to the sensitive nature of student data, including personal, academic, and biometric information. Weak security infrastructure, inadequate stakeholder awareness, and insufficient technical expertise were identified as key factors contributing to system vulnerabilities.

Selwyn (2016) emphasized that the adoption of digital monitoring systems in schools improves administrative efficiency and student tracking, but these benefits are often undermined by cyber security threats. The study noted that stakeholders, including teachers and administrators, frequently lack adequate knowledge of secure system practices, which increases the risk of data breaches.

Alas Mary et al. (2021) investigated the effectiveness of mitigation strategies in school digital systems and found that a combination of technical measures (such as encryption, access controls, and regular software updates) and human-cantered approaches (training and awareness programs) significantly reduces cyber security risks. Similarly, Von Solms and Van Niekerk (2013) highlighted that cyber security awareness among stakeholders is crucial for preventing unauthorized access, phishing attacks, and misuse of digital systems.

In the Nigerian context, research on digital system security in primary schools is limited. However, Livingstone et al. (2017) observed that many schools prioritize technological adoption over cyber security, leaving systems exposed to potential threats. This highlights a critical gap in empirical knowledge regarding both the risks faced and the strategies employed by stakeholders in safeguarding digital monitoring systems in Nigerian primary schools.

D. Summary of Gaps in Literature

Despite growing research on cyber security in educational institutions, several gaps remain. First, most studies focus on higher education or secondary schools, with limited empirical evidence on cyber security risks and mitigation strategies in primary schools, particularly in the Nigerian context.

Second, while existing research identifies general cyber security threats, few studies examine stakeholders' awareness, practices, and perceptions regarding digital monitoring systems in primary schools. Understanding these perspectives is critical, as teachers, administrators, and parents play a key role in safeguarding digital systems.

Third, although technical solutions and mitigation strategies have been discussed, there is a lack of context-specific evidence on the effectiveness of these strategies in public primary schools, especially in areas like Surulere Local Government, Lagos State.

These gaps highlight the need for a focused study that explores both cyber security risks and mitigation strategies among primary school stakeholders to develop safe and effective digital monitoring systems.

III. RESEARCH METHODOLOGY

A. Research Design

This study adopted a descriptive survey research design, which is suitable for gathering detailed information on stakeholders' experiences, perceptions, and practices regarding cyber security risks and mitigation strategies in digital monitoring systems. The survey design allows for systematic collection of data from a large number of respondents, facilitating analysis of patterns, relationships, and trends among school administrators, teachers, and parents.

B. Population of the Study

The study population consists of all stakeholders involved in digital monitoring systems in public primary schools in Surulere Local Government Area, Lagos State. This includes school administrators, teachers, and parents. According to the Lagos State Ministry of Education (2024), there are 40 public primary schools in Surulere Local Government Area, with an estimated 1,200 teachers, 80 administrators, and 2,400 parents actively engaged in school-related digital systems. A total of 300 respondents will fill the questionnaire, comprising approximately 20 administrators, 100 teachers, and 180 parents.

C. Area of Study, Sample and Sampling Technique

The study was conducted in Surulere Local Government Area, Lagos State, an urban area with numerous public primary schools that have adopted digital monitoring systems for student management and administration.

A purposive sampling technique was employed to select 10 public primary schools that actively use digital monitoring systems. Within these schools, stratified sampling was used to select respondents proportionally from the three stakeholder groups: administrators, teachers, and parents, resulting in a sample size of 300 respondents (20 administrators, 100 teachers, and 180 parents). This approach ensures representation across all key stakeholders while focusing on those directly involved with digital systems.

D. Research Instrument

Data were collected using a structured questionnaire, designed to capture information on:

- Respondents' demographic characteristics,
- Cyber security risks encountered in digital monitoring systems,
- Awareness and practices of stakeholders regarding cyber security, and
- Mitigation strategies implemented to reduce risks.

The questionnaire employed a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) to quantify responses.

E. Validity and Reliability of the Instrument

Validity was ensured through expert review by lecturers in Information Systems and Educational Technology, who assessed the questionnaire for relevance, clarity, and appropriateness. Content validity was established to ensure that all items adequately captured cyber security risks and mitigation strategies in primary school digital systems.

Reliability was determined using a pilot study conducted in 2 public primary schools outside the study area. The Cronbach's alpha coefficient was calculated, yielding a reliability index of 0.82, indicating that the instrument was consistent and reliable for data collection.

F. Method of Data Collection

Data collection involved administering questionnaires to the selected stakeholders in person. The researcher coordinated with school authorities to schedule visits, explain the purpose of the study, and distribute the questionnaires. Respondents were given sufficient time to complete the instrument, after which the researcher collected the completed questionnaires for analysis.

G. Method of Data Analysis

Data were analysed using descriptive and inferential statistics. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize stakeholders' responses. Inferential statistics, such as Chi-square tests and correlation analysis, were employed to test hypotheses and examine relationships between cyber security awareness, mitigation strategies, and risks. Data analysis was performed using Statistical Package for Social Sciences (SPSS) version 28.

H. Ethical Considerations

Ethical principles were strictly adhered to throughout the study. Participants were provided with an informed consent form explaining the purpose of the research, their rights to voluntary participation, and assurance of confidentiality. Personal information was anonymised to protect participants' privacy. Permission to conduct the study was obtained from the relevant school authorities and the Lagos State Ministry of Education, ensuring compliance with ethical guidelines for research involving human subjects.

IV. RESEARCH METHODOLOGY

A. Research Design

This study adopted a descriptive survey research design, which is suitable for gathering detailed information on stakeholders' experiences, perceptions, and practices regarding cyber security risks and mitigation strategies in digital monitoring systems. The survey design allows for systematic collection of data from a large number of respondents, facilitating analysis of patterns, relationships, and trends among school administrators, teachers, and parents.

B. Population of the Study

The study population consists of all stakeholders involved in digital monitoring systems in public primary schools in Surulere Local Government Area, Lagos State. This includes school administrators, teachers, and parents. According to the Lagos State Ministry of Education (2024), there are 40 public primary schools in Surulere Local Government Area, with an estimated 1,200 teachers, 80 administrators, and 2,400 parents actively engaged in school-related digital systems. A total of 300 respondents will fill the questionnaire, comprising approximately 20 administrators, 100 teachers, and 180 parents.

C. Area of Study, Sample and Sampling Technique

The study was conducted in Surulere Local Government Area, Lagos State, an urban area with numerous public primary schools that have adopted digital monitoring systems for student management and administration.

A purposive sampling technique was employed to select 10 public primary schools that actively use digital monitoring systems. Within these schools, stratified sampling was used to select respondents proportionally from the three stakeholder groups: administrators, teachers, and parents, resulting in a sample size of 300 respondents (20 administrators, 100 teachers, and 180 parents). This approach ensures representation across all key stakeholders while focusing on those directly involved with digital systems.

D. Research Instrument

Data were collected using a structured questionnaire, designed to capture information on:

- Respondents' demographic characteristics,
- Cyber security risks encountered in digital monitoring systems,
- Awareness and practices of stakeholders regarding cyber security, and
- Mitigation strategies implemented to reduce risks.

The questionnaire employed a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) to quantify responses.

E. Validity and Reliability of the Instrument

Validity was ensured through expert review by lecturers in Information Systems and Educational Technology, who assessed the questionnaire for relevance, clarity, and appropriateness. Content validity was established to ensure that all items adequately captured cyber security risks and mitigation strategies in primary school digital systems.

Reliability was determined using a pilot study conducted in 2 public primary schools outside the study area. The Cronbach's alpha coefficient was calculated, yielding a reliability index of 0.82, indicating that the instrument was consistent and reliable for data collection.

F. Method of Data Collection

Data collection involved administering questionnaires to the selected stakeholders in person. The researcher coordinated with school authorities to schedule visits, explain the purpose of the study, and distribute the questionnaires. Respondents were given sufficient time to complete the instrument, after which the researcher collected the completed questionnaires for analysis.

G. Method of Data Analysis

Data were analysed using descriptive and inferential statistics. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize stakeholders' responses. Inferential statistics, such as Chi-square tests and correlation analysis, were employed to test hypotheses and examine relationships between cyber security awareness, mitigation strategies, and risks. Data analysis was performed using Statistical Package for Social Sciences (SPSS) version 28.

H. Ethical Considerations

Ethical principles were strictly adhered to throughout the study. Participants were provided with an informed consent form explaining the purpose of the research, their rights to voluntary participation, and assurance of confidentiality. Personal information was anonymised to protect participants' privacy. Permission to conduct the study was obtained from the relevant school authorities and the Lagos State Ministry of Education, ensuring compliance with ethical guidelines for research involving human subjects.

V. DATA PRESENTATION, ANALYSIS, AND DISCUSSIONS

A. Introduction

This chapter presents the results of the data collected from 300 respondents comprising school administrators, teachers, and parents in selected public primary schools in Surulere Local Government Area, Lagos State. The data were analysed using descriptive statistics (frequencies, percentages, means, and standard deviations). Responses were based on a 5-point Likert scale: 1 = Strongly Disagree (SD), 2 = Disagree (D), 3 = Undecided (U), 4 = Agree (A), 5 = Strongly Agree (SA).

B. Socio-Demographic Characteristics of Respondents

Table 1: Distribution of Respondents by Stakeholder Category

Stakeholder Category	Frequency	Percentage (%)
Administrator	20	6.7
Teacher	100	33.3
Parent	180	60.0
Total	300	100.0

The majority of respondents were parents (60.0%), followed by teachers (33.3%) and administrators (6.7%). This distribution reflects the larger population of parents involved in school digital systems and ensures diverse perspectives, though parents dominate the responses.

Table 2: Distribution of Respondents by Gender

Gender	Frequency	Percentage (%)
Male	108	36.0
Female	192	64.0
Total	300	100.0

Females constituted 64.0% of respondents, while males were 36.0%. This gender imbalance may reflect higher female involvement in primary education roles (especially teaching and parenting engagement in Lagos public schools).

Table 3: Distribution of Respondents by Age Group

Age Group	Frequency	Percentage (%)
Below 25 years	15	5.0
25–34 years	78	26.0
35–44 years	132	44.0
45–54 years	60	20.0
55 years and above	15	5.0

Total	300	100.0

The largest group was 35–44 years (44.0%), indicating that most stakeholders are in their prime working and parenting years, likely more actively engaged with digital monitoring system.

Table 4: Distribution of Respondents by Highest Educational Qualification

Qualification	**Frequency**	**Percentage (%)**
SSCE/O'Level	42	14.0
NCE/OND	90	30.0
Bachelor's Degree/HND	120	40.0
Master's Degree	42	14.0
PhD	6	2.0
Total	300	100.0

Most respondents held Bachelor's Degree/HND (40.0%) or NCE/OND (30.0%), reflecting the typical qualifications for primary school teachers and educated parents in urban Lagos.

Table 5: Distribution of Respondents by Years of Experience/Involvement

Years of Experience/Involvement	**Frequency**	**Percentage (%)**
Less than 5 years	75	25.0
5–10 years	105	35.0
11–15 years	78	26.0
More than 15 years	42	14.0
Total	300	100.0

The majority had 5–10 years of involvement (35.0%), suggesting moderate familiarity with school systems, including digital tools.

Table 6: Regular Use of Digital Monitoring Systems

Response	Frequency	Percentage (%)
Yes	225	75.0
No	75	25.0
Total	300	100.0

75.0% of respondents regularly use digital monitoring systems, confirming that the sample is relevant and directly experienced with the systems under study.

C. Analysis of Research Questions

1. Research Question One

What are the cyber security risks associated with the use of digital monitoring systems in public primary schools in Surulere LGA?

Table 7: Perceived Cyber security Risks (Section B)

S/N	Statement	SD (%)	D (%)	U (%)	A (%)	SA (%)	Mean	SD
1	Unauthorized persons can easily access student data	4.0	8.7	18.7	45.0	23.6	3.75	1.02
2	The school has experienced or is vulnerable to data breaches	5.3	10.0	20.0	42.0	22.7	3.67	1.08
3	Malware or viruses can infect digital monitoring systems	3.3	9.3	16.0	48.0	23.4	3.79	0.97
4	Phishing attacks targeting staff or parents are common	6.7	14.0	25.3	36.0	18.0	3.44	1.14
5	Weak passwords and poor access controls increase risks	2.0	6.0	12.0	50.0	30.0	4.00	0.89
6	Outdated software makes systems vulnerable to attacks	3.3	7.3	14.7	46.7	28.0	3.89	0.98
7	Sharing login credentials poses a significant risk	5.3	12.0	22.7	40.0	20.0	3.57	1.10
8	Use of personal/unsecured devices increases risks	4.0	8.0	16.0	48.0	24.0	3.80	1.00
Overall Mean							3.74	

The overall mean of 3.74 indicates a high level of perceived cyber security risks. The highest risks were weak passwords/access controls (mean 4.00) and outdated software (3.89), suggesting stakeholders recognize technical and human-factor vulnerabilities as major threats. Phishing had the lowest mean (3.44) but still moderate-to-high agreement. This aligns with literature highlighting weak infrastructure in educational settings.

2. Research Question Two: What is the level of cyber security awareness and practices among primary school stakeholders?

Table 8: Level of Cyber security Awareness and Practices (Section C)

No	**Statement**	**SD (%)**	**D (%)**	**U (%)**	**A (%)**	**SA (%)**	**Mean**	**SD**
1	I am aware of common cyber security threats	8.0	18.7	24.0	36.0	13.3	3.28	1.17
2	I know how to create and maintain strong passwords	6.7	14.0	20.0	42.0	17.3	3.49	1.12
3	I regularly update software and apps	12.0	24.0	26.7	28.0	9.3	2.98	1.19
4	I have received training on cyber security practices	20.0	32.0	22.7	20.0	5.3	2.59	1.18
5	Teachers and administrators follow good cyber security practices	14.0	26.0	28.0	24.0	8.0	2.86	1.17
6	Parents are adequately informed about safe use	18.7	30.0	24.0	22.0	5.3	2.65	1.16
7	I recognize suspicious emails or links	9.3	16.0	22.7	38.0	14.0	3.31	1.18
8	The level of cyber security awareness among stakeholders is generally high	16.0	28.0	26.7	24.0	5.3	2.75	1.15
Overall Mean							3.00	

The overall mean of 3.00 indicates a moderate level of cyber security awareness and practices. Respondents showed better personal knowledge (e.g., strong passwords: 3.49; recognizing suspicious links: 3.31) but significant gaps in training (2.59), regular updates (2.98), and institutional practices. This suggests awareness is uneven and largely individual rather than systematic.

3. Research Question Three: What mitigation strategies are adopted to address cyber security risks?

Table 9: Adoption of Mitigation Strategies (Section D)

S/N	Statement	SD (%)	D (%)	U (%)	A (%)	SA (%)	Mean	SD
1	The school uses strong passwords and multi-factor authentication	18.0	28.0	24.0	24.0	6.0	2.72	1.19
2	Regular software updates and patches are applied	15.3	25.3	26.0	26.7	6.7	2.84	1.17
3	Access to sensitive data is restricted to authorized personnel	12.0	20.0	22.7	34.0	11.3	3.12	1.21
4	The school conducts cyber security training/awareness programs	24.0	36.0	20.0	16.0	4.0	2.40	1.14
5	Antivirus and firewall protection are installed	16.7	26.7	24.0	24.0	8.6	2.81	1.22
6	Clear policies exist on data protection and acceptable use	20.0	32.0	22.7	20.0	5.3	2.59	1.17
7	The school backs up student data regularly	14.0	22.0	24.0	30.0	10.0	3.00	1.20
8	Incidents of suspected threats are promptly reported and investigated	22.0	30.0	24.0	18.0	6.0	2.56	1.18
Overall Mean							2.76	

The overall mean of 2.76 indicates moderate to low adoption of mitigation strategies. Basic measures like data backup (3.00) and access restriction (3.12) were relatively better adopted, but critical areas like training programs (2.40), clear policies (2.59), and multi-

factor authentication (2.72) were poorly implemented. This reveals a reactive rather than proactive approach to cyber security.

D. Discussion of Findings

The findings reveal that stakeholders in public primary schools in Surulere LGA perceive high cyber security risks (overall mean 3.74) in digital monitoring systems, particularly from weak passwords, outdated software, and unauthorized access. This confirms the vulnerabilities highlighted in the literature.

However, cyber security awareness and practices remain only moderate (mean 3.00), with notable deficiencies in training and regular software updates. Similarly, the adoption of mitigation strategies is moderate to low (mean 2.76), especially in conducting awareness programs, implementing multi-factor authentication, and establishing clear data protection policies.

These results indicate a significant gap between recognized risks and actual preparedness, leaving sensitive student data exposed. The moderate awareness and inadequate mitigation measures explain the persistence of high perceived risks, underscoring the urgent need for targeted training, policy enforcement, and technical upgrades in Nigerian public primary schools.

VI. SUMMARY, CONCLUSION, AND RECOMMENDATIONS

A. Summary

This study examined cyber security risks and mitigation strategies in digital monitoring systems among primary school stakeholders in public primary schools in Surulere Local Government Area, Lagos State, Nigeria. The objectives were to identify associated cyber security risks, assess the level of awareness and practices among stakeholders, and examine the mitigation strategies adopted.

Using a descriptive survey design, data were collected from 300 respondents (administrators, teachers, and parents) through a structured questionnaire. The findings revealed high perceived cyber security risks (overall mean 3.74), particularly from weak passwords, outdated software, unauthorized access, and use of unsecured devices. Stakeholder’s demonstrated only moderate cyber security awareness and practices (mean 3.00), with significant gaps in training and regular system updates. Adoption of mitigation strategies was moderate to low (mean 2.76), especially in areas such as cyber security training programs, multi-factor authentication, and clear data protection policies. These results highlight a critical disparity between recognized risks and actual preparedness in the studied schools.

B. Conclusion

The study concludes that public primary schools in Surulere Local Government Area face substantial cyber security risks in their digital monitoring systems due to technical vulnerabilities and human factors. Despite stakeholders' recognition of these risks, the

moderate level of awareness and inadequate implementation of mitigation strategies leave sensitive student data highly exposed. This situation aligns with the Protection Motivation Theory (PMT), where low coping appraisal (limited training and strategies) fails to motivate effective protective behaviours, and partially contradicts the Technology Acceptance Model (TAM), as perceived usefulness of digital systems drives adoption but not secure practices.

Overall, the persistent vulnerabilities underscore the need for urgent interventions to safeguard children's data and ensure safe digital monitoring in primary education.

RECOMMENDATIONS

Based on the findings, the following recommendations are made:

- The Lagos State Ministry of Education and school administrators should mandate regular cyber security training and awareness programs for all stakeholders (administrators, teachers, and parents) to bridge knowledge and practice gaps.
- Schools should enforce technical safeguards, including mandatory use of strong passwords, multi-factor authentication, regular software updates, antivirus installation, and restricted access to sensitive data.
- Clear and comprehensive data protection policies should be developed and communicated to all stakeholders, with mechanisms for regular data backups and prompt incident reporting.
- Government and educational authorities should provide funding and technical support to upgrade school infrastructure, prioritising cyber security in digital monitoring system deployments.
- Parent-teacher associations should be involved in cyber security initiatives to enhance parental awareness and responsible use of school digital platforms.

A. Contribution to Knowledge

This study contributes to knowledge in the following ways:

- It provides empirical evidence on cyber security risks in digital monitoring systems specifically within Nigerian public primary schools, an area with limited prior research.
- By focusing on stakeholder perspectives (administrators, teachers, and parents), it offers context-specific insights into awareness levels and mitigation practices in an urban Nigerian setting.
- The findings extend the application of TAM and PMT to cyber security behaviour in primary education, demonstrating how perceived usefulness drives technology adoption while insufficient threat and coping appraisals hinder security practices.
- It serves as a reference for policymakers and educators aiming to develop tailored cyber security frameworks for resource-constrained primary school environments.

B. Suggestions for Further Studies

The following areas are suggested for future research:

- A comparative study of cyber security risks and mitigation strategies between public and private primary schools in Nigeria.
- Longitudinal research to evaluate the impact of cyber security training interventions on stakeholder awareness and risk reduction over time.
- Investigation into the role of emerging technologies (e.g., cloud-based systems or AI-driven monitoring) in exacerbating or mitigating cyber security risks in primary education.
- Exploration of cyber security challenges in digital monitoring systems in rural primary schools across different Nigerian states.

REFERENCES

[1] Alasmary, W., Alhaidari, F., Alsubaie, A., & Alharbi, A. (2021). Cyber security awareness and practices in educational institutions: Challenges and mitigation strategies. Journal of Information Security and Applications, 60, 102884. https://doi.org/10.1016/j.jisa.2021.102884

[2] Al-Emran, M., Mezhuyev, V., & Kamaludin, A. (2021). Technology acceptance model in m-learning context: A systematic review. Computers & Education, 128, 103-124. https://doi.org/10.1016/j.compedu.2018.09.017

[3] Amin, M. (2005). Social science research: Conception, methodology and analysis. Makerere University Printery.

[4] Annasingh, F., & Veli, T. (2020). An investigation into risks awareness and e-safety needs of children on the internet. Interactive Technology and Smart Education, 17(1), 77-94.

[5] Centre for Democracy & Technology. (2021). Online and observed: Student privacy implications of school-issued devices and student activity monitoring software. https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/

[6] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. Computers & Security, 32, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

[7] Davinson, N., & Sillence, E. (2022). Relevant article on PMT in cyber security contexts; specific title not confirmed in search results.

[8] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

[9] Granić, A. (2022). Technology acceptance and adoption in education. In Handbook of open, distance and digital education (pp. 1-18). Springer.

[10] Hankerson, D., Venzke, C., Laird, E., Grant-Chapman, H., & Thakur, D. (2021). Online and observed: Student privacy implications of school-issued devices and student activity monitoring software. Centre for Democracy & Technology.

[11] He, W., et al. (2021). Article on cyber security in education; specific details aligned with educational contexts.

[12] Herath, T., et al. (2014). Article applying PMT to cyber security behaviours.

[13] Hope, A. (2018). Relevant work on student privacy and monitoring.

[14] ISO/IEC. (2022). Information technology — Security techniques — Information security management systems. International Organization for Standardization.
[15] Israel, M., & Hay, I. (2006). Research ethics for social scientists: Between ethical conduct and regulatory compliance. Sage Publications.
[16] Jiow, H. J., Mwagwabi, F., & Low-Lim, A. (2021). Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education. Journal of Media Literacy Education, 13(1), 67-78.
[17] Kshetri, N. (2019). Cyber-threats and cyber security challenges: A cross-cultural perspective. Conference or journal proceedings.
[18] Lagos State Ministry of Education. (2024). Public primary schools statistics: Surulere Local Government Area. Lagos State Government Publications.
[19] Livingstone, S., Carr, J., & Byrne, J. (2017). One in three: Internet governance and digital citizenship in schools. Policy & Internet, 9(3), 330–356. https://doi.org/10.1002/poi3.151
[20] O'Daffer, A., et al. (2025). Study on school-based online surveillance.
[21] Prasetyo, Y. T., et al. (2021). Article extending TAM in educational or related contexts.
[22] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
[23] Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modelling approach to explaining teachers' adoption of digital technology in education. Computers & Education, 128, 13-35. https://doi.org/10.1016/j.compedu.2018.09.009
[24] Selwyn, N. (2016). Is technology good for education? Polity Press.
[25] Sophos. (2025). the state of ransom ware in education 2025. Sophos.
[26] Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751–752. https://doi.org/10.1126/science.aat599
[27] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004