JOURNAL OF EDUCATIONAL THOUGHT (JET)

A PUBLICATION OF THE DEPARTMENT OF ADULT EDUCATION, FACULTY OF EDUCATION, UNIVERSITY OF LAGOS

adejet@unilag.edu.ng

adejet.journals.unilag.edu.ng

CYBERSECURITY MEASURES AND FINANCIAL MISMANAGEMENT PREVENTION IN SPORTS ORGANIZATIONS IN NIGERIA

AJIBOLA, GBENGA SAMSON (Ph.D) [1]

&

AGORO, ALEXANDAR AFOLABI (Ph.D) [2]

[1]samajibola@unilag.edu.ng +2348060324590

[2]aagoro@unilag.edu.ng +2348035875266

Department of Human Kinetics and Health Education, University of Lagos, Akoka, Lagos, Nigeria

https://doi.org/10.5281/zenodo.20300082

Abstract

This study investigated cybersecurity measures and financial mismanagement prevention in sports organisations in Nigeria, focusing specifically on secure financial management software, access control and authentication mechanisms. This study adopted a quantitative research approach using a survey design. The population of the study comprised administrative personnel directly involved in financial and information management, sports administrators, accountants, finance officers, internal auditors, ICT and cybersecurity officers of sports organisations in Nigeria. A multi-stage sampling technique was used to select 150 respondents for the study. Data for the study were obtained through the use of a structured questionnaire. Data collected were analysed using inferential statistics of multiple regression analysis at a 0.05 level of significance. The empirical findings provide compelling evidence that cybersecurity measures significantly contribute to financial mismanagement prevention in sports administration contexts. The study conclude that cybersecurity measures should not be viewed merely as technical safeguards but as strategic governance tools that systematically reduce opportunities for financial mismanagement. The study recommended that sports organisations should prioritise the acquisition and implementation of secure financial management software with robust cybersecurity features, including encryption, automated audit trails, transaction verification protocols, and secure data storage.

Keywords: Access control, Authentication mechanism, Cybersecurity, Financial mismanagement, Sport organisations

Introduction

The governance and financial management of sports organisations have attracted increasing scholarly attention as the global sports industry continues to expand in economic value and organisational complexity. Modern sports organisations operate as multifaceted enterprises that manage substantial financial resources derived from public funding, sponsorships, broadcasting rights, and international development grants. As a result, issues of financial accountability, transparency, and integrity have become central concerns in sports administration research (Geeraert, 2018; Parent & Hoye, 2018). In many contexts, particularly in developing economies, weak governance structures have created fertile ground for financial mismanagement, corruption, and inefficient resource utilisation within sports institutions (Akindes & Kirwin, 2009; Chappelet & Mrkonjic, 2016).

Cybersecurity refers to the set of technologies, policies, procedures, and controls designed to protect information systems and digital assets from unauthorised access, manipulation, or disruption (Von Solms & Van Niekerk, 2013). Scholarly literature demonstrates that cyber threats are no longer confined to data privacy breaches but have evolved into sophisticated mechanisms for financial exploitation. Cyber-enabled financial crimes such as phishing, business email compromise, identity theft, and unauthorised system access have been shown to facilitate fraud and financial mismanagement in organisational settings (Bada & Nurse, 2019; Holtfreter et al., 2018).

Financial mismanagement in sports organisations manifests through practices such as embezzlement, diversion of funds, falsification of financial records, unauthorised transactions, and non-compliance with financial regulations. Scholars argue that these practices undermine not only organisational sustainability but also athlete development, public trust, and national sport performance outcomes (Geeraert, Mrkonjic, & Chappelet, 2014). In the African context, and Nigeria in particular, sports organisations often depend heavily on government allocations

and international donor funding, which heightens the need for robust financial controls and accountability mechanisms (Akindes & Kirwin, 2009). However, persistent governance weaknesses, including limited oversight capacity and poor internal control systems, have been identified as major contributors to financial mismanagement in African sports institutions (Darby, Akindes, & Kirwin, 2007).

Within sports organisations, cybersecurity vulnerabilities are often exacerbated by structural and cultural factors. Research indicates that sports bodies frequently prioritise performance outcomes over administrative capacity building, resulting in underinvestment in cybersecurity infrastructure and staff training (Parnell et al., 2021). Additionally, decentralised governance structures common in sports federations can limit standardisation of cybersecurity policies and financial controls, increasing exposure to internal and external cyber risks (Geeraert, 2018). These weaknesses make sports organisations particularly susceptible to cyber-enabled financial mismanagement.

The Nigerian sports sector presents a particularly compelling context for examining this relationship. Nigeria's sports organisations operate within a broader national environment characterised by rapid digital adoption alongside persistent cybersecurity and financial crime challenges. Empirical studies on Nigeria's digital economy reveal high levels of cyber-enabled fraud, weak institutional enforcement, and limited cybersecurity capacity across sectors (Akanbi et al., 2022; Ayo et al., 2021). Although these studies focus primarily on banking and e-government systems, their findings suggest that organisations with inadequate cybersecurity frameworks are more vulnerable to financial manipulation and internal control failures.

Furthermore, in Nigerian sports organisations, financial management challenges are often compounded by limited professionalisation of administrative roles, political interference, and weak compliance with governance codes (Darby et al., 2007; Akindes & Kirwin, 2009). As these organisations increasingly adopt digital financial systems, the absence of effective

cybersecurity measures may further intensify existing governance weaknesses. Without secure systems to regulate access, authenticate transactions, and generate audit logs, digital platforms can become instruments that facilitate, rather than prevent, financial mismanagement.

Despite these insights, empirical research specifically examining the intersection of cybersecurity and financial mismanagement in sports organisations remains limited. Existing sport governance literature has largely focused on corruption, ethics, and governance reforms without adequately integrating digital risk management perspectives (Chappelet & Mrkonjic, 2016; Geeraert et al., 2014). Conversely, cybersecurity research has predominantly concentrated on corporate, banking, and public sector organisations, with minimal application to sports administration contexts (Bada & Nurse, 2019). This disconnect leaves a significant gap in understanding how cybersecurity measures can be leveraged as tools for preventing financial mismanagement in sports organisations.

Given the strategic importance of sports in national development and international representation, the financial integrity of sports organisations is a matter of public interest. In Nigeria, where sports play a critical role in youth development, employment, and national identity, financial mismanagement undermines not only organisational performance but also broader socio-economic objectives. Therefore, understanding how cybersecurity measures influence financial accountability is essential for strengthening governance frameworks and ensuring the sustainable development of sports institutions.

Statement of the Problem

Financial mismanagement and lack of accountability have long been persistent challenges in sports organisations globally, and this problem is particularly acute in Nigeria. Nigerian sports federations, including the Nigeria Football Federation (NFF), have been repeatedly scrutinised for the misappropriation and opaque administration of funds intended for sport development. For instance, the Nigerian House of Representatives initiated a probe into alleged

mismanagement of approximately $25 million in FIFA and CAF development grants by the NFF, citing deficiencies in accounting and accountability systems. Such issues have undermined trust in sports governance and have contributed to poor performance outcomes, delayed athlete payments, and deteriorating infrastructure.

Historically, high-profile cases such as the removal of Aminu Maigari from the presidency of the NFF on grounds of financial misappropriation further illustrate systemic weaknesses in financial control mechanisms within Nigerian sports administration. Without robust safeguards, funds intended for athlete development, infrastructure, and operational costs remain vulnerable to diversion, misuse, or fraudulent manipulation.

At the same time, sports organisations are increasingly reliant on digital technologies for financial management, ticketing, sponsorship accounting, and operations, thereby exposing them to a spectrum of cyber threats. Globally, cyber risks in sport include business email compromise, ransomware, and cyber-enabled fraud that have resulted in direct financial losses and operational disruptions for sports entities.

Despite this context, the intersection between digital security controls and financial governance in sports organisations remains under-researched. Most studies and policy interventions on cybersecurity in Nigeria focus on the banking and fintech sectors, where cyber defences are linked to fraud prevention and financial sustainability, but these insights have limited direct application to the unique governance structures and financial flows of sports entities.

Purpose of the Study

This study aims to investigate cybersecurity measures and preventing financial mismanagement in sports organisations in Nigeria. Specifically, this study is set to:

1. Determine the impact of secure financial management software on preventing financial mismanagement in sports organisations in Nigeria.

2. Ascertain the role of access control and authentication mechanisms in preventing financial mismanagement in sports organisations in Nigeria.

Research Hypotheses

The following hypothesis were tested in the study

1. There is no significant impact of secure financial management software on preventing financial mismanagement in sports organisations in Nigeria.
2. Access control and authentication mechanisms do not significantly prevent financial mismanagement in sports organisations. in Nigeria

Methodology

This study adopts a quantitative research approach using a descriptive survey design. This research design enables the examination of the impacts of cybersecurity measures on the prevention of financial mismanagement. The population of the study comprised sports organisations in Nigeria, including national sports federations, state sports councils, professional sports clubs, and sports development agencies under the Federal Ministry of Sports Development. The respondents comprised administrative personnel directly involved in financial and information management, including sports administrators, accountants, finance officers, internal auditors, and ICT or cybersecurity officers. These respondents are considered suitable because of their roles in financial oversight and digital system management.

A multi-stage sampling technique was used to select 150 respondents for the study. Data for the study were obtained from both primary sources through the use of a structured questionnaire designed using a four-point Likert-type scale, ranging from 1 (Strongly Disagree) to 4 (Strongly Agree). The questionnaire was organised into sections measuring demographic characteristics, cybersecurity measures, and financial mismanagement prevention. The questionnaire was administered through electronic means.

Data collected was analysed using the Statistical Package for the Social Sciences (SPSS). Descriptive statistics were used to summarise respondents' characteristics. Inferential statistics of multiple regression analysis were used to test the relationship and predictive influence of cybersecurity measures on the prevention of financial mismanagement. All hypotheses were tested at a 0.05 level of significance.

Results

4.1 Demographic Data of Respondents

Figure 1: Gender Distribution of Respondents

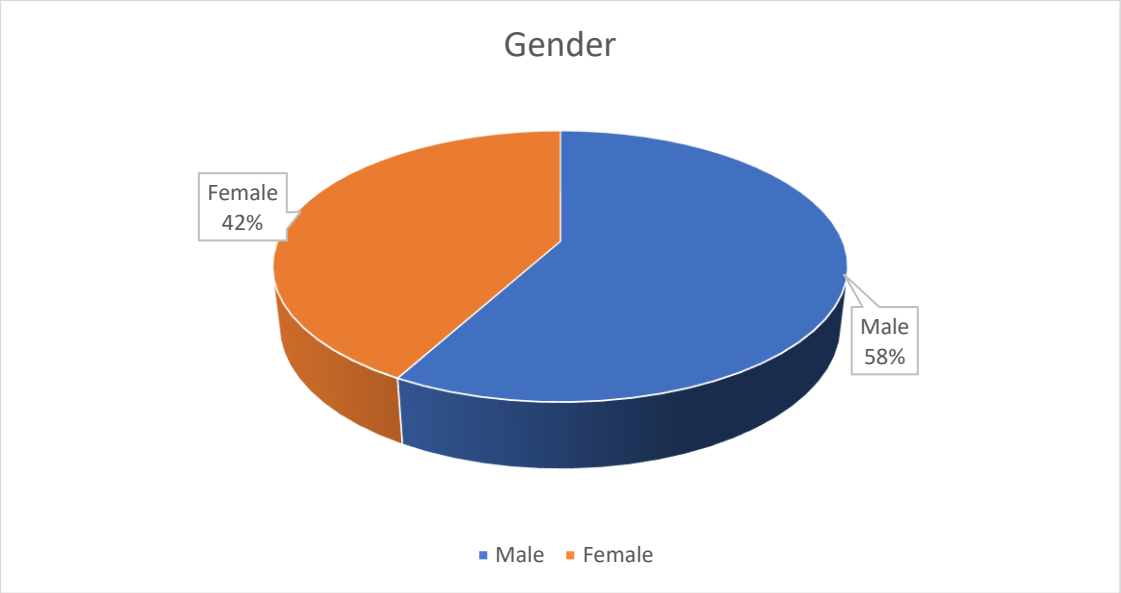

Figure 1 showed that 58% (n = 87) of the respondents are male and 42% (n = 63) of the respondents are female. It can therefore be concluded that the majority of respondents in this study are males.

Figure 2: Age Distribution of Respondents

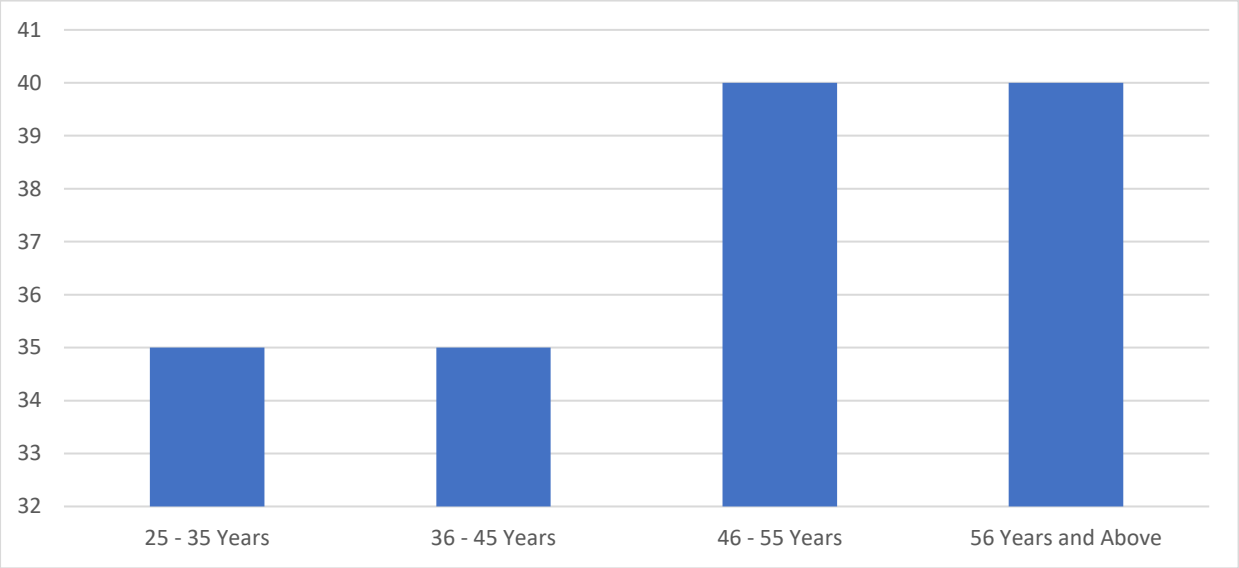

Figure 2 shows the distribution of respondents by age. It indicates that 23.3% (n = 35) of the respondents are 25 - 35 years, 23.3% (n = 35) are 36 – 45 years, and 26.7% (n = 40) are 46 – 55 years. Additionally, the table shows that 26.7% (n = 40) are 56 years and above.

Figure 3: Educational Qualification of respondents

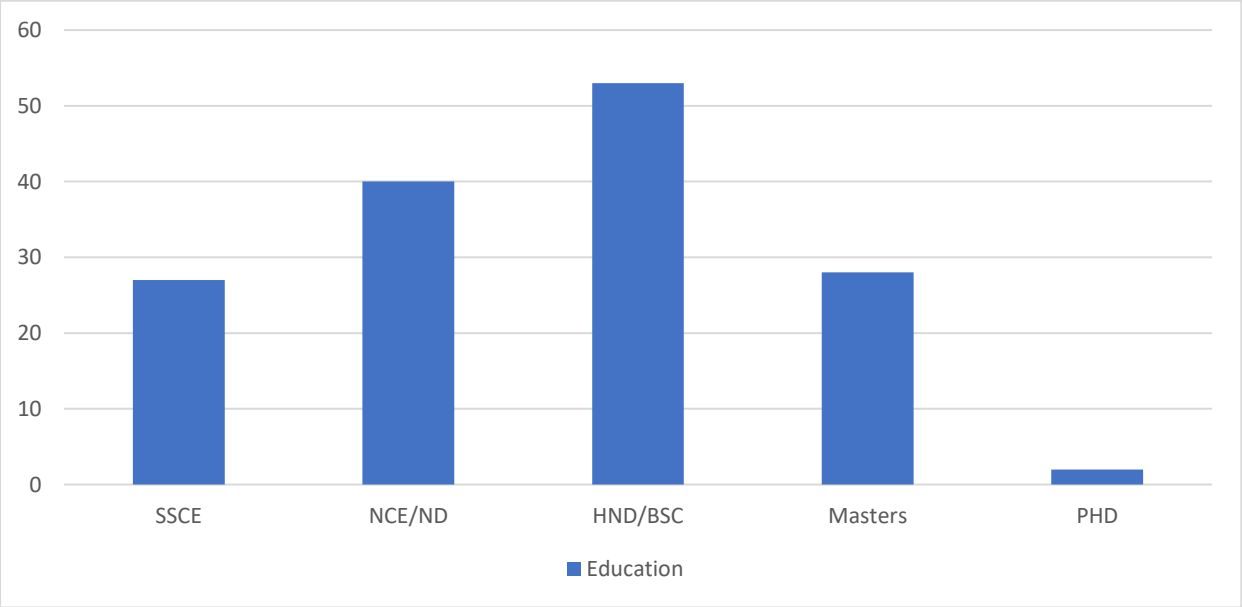

Figure 3 showed the educational qualifications of respondents sampled in this study. It reveals that 18% (n = 27) of the respondents are SSCE holders, 26.7% (n = 40) are NCE/ND holders, and 35.3% (n = 53) have HND/BSC degrees. The table also reveals that 18.7% (n = 28) of respondents are Master's holders and 1.3% (n = 2) had PHD.

Table 1: Designation of Respondents

Designation	Frequency	Percent
Sports Administrators	54	36.0
Accountants	35	23.3
Finance Officers	36	24.0
Internal Auditors	10	6.7
ICT	15	10.0
Total	**150**	**100.0**

Table one showed the designation of the respondents. Sports administrators were 36 percent, Accountants were 23.3 percent, Finance officers were 24 percent, Internal auditors were 6.7 percent, and ICT officers were 10 percent by designation respectively.

Hypothesis One: Hypothesis one state that there is no significant impact of secure financial management software on preventing financial mismanagement in sports organisations in Nigeria. To test this, the linear regression analysis was used, and the result is presented below:

Correlations

		Sec_Fin_Mgt	Fin_Mismgt
Pearson Correlation	Sec_Fin_Mgt	1.000	.510
	Fin_Mismgt	.510	1.000
Sig. (1-tailed)	Sec_Fin_Mgt	.	.000
	Fin_Mismgt	.000	.
N	Sec_Fin_Mgt	150	150
	Fin_Mismgt	150	150

The correlation table above shows a strong positive relationship between secure financial management software and financial mismanagement prevention in sports organisations, with a correlation coefficient of .510.

Model Summary

Model	R	R Square	Adjusted R-Square	Std. Error of the Estimate
1	.510[a]	.260	.255	2.55658

a. Predictors: (Constant), Sec_Fin_Mgt

From the model summary above, the value of $R^2 = 0.260$ implies that 26**%** of the variance in financial mismanagement prevention in sports organisations is explained by secure financial management software. The adjusted **R^2** is positive, suggesting that the model improves upon using the mean financial mismanagement prevention as a predictor, a sign of good model fit. The high R value also reflects strong explanatory power.

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	340.654	1	340.654	52.119	.000[b]
	Residual	967.346	148	6.536		
	Total	1308.000	149			

a. Dependent Variable: Fin_Mismgt

b. Predictors: (Constant), Sec_Fin_Mgt

From the table above, the f-value of 52.119 is significant at .000 < 0.05. This implies that there is a significant impact of secure financial management software on preventing financial mismanagement in sports organisations in Nigeria. Therefore, the null hypothesis, which stated that there is no significant impact of secure financial management software on preventing financial mismanagement in sports organisations in Nigeria, is hereby rejected.

Hypothesis Two: Access control and authentication mechanisms do not significantly prevent financial mismanagement in sports organisations in Nigeria. To test this hypothesis, the linear regression analysis was used, and the result is presented below:

Correlations

		Fin_Mismgt	Access_Control
Pearson Correlation	Fin_Mismgt	1.000	.438
	Access_Control	.438	1.000
Sig. (1-tailed)	Fin_Mismgt	.	.000
	Access_Control	.000	.
N	Fin_Mismgt	150	150
	Access_Control	150	150

The correlation table above shows a positive relationship between Access control and authentication mechanisms and financial mismanagement prevention in sports organisations in Nigeria, with a correlation coefficient of 0.438.

Model Summary

Model	R	R Square	Adjusted R-Square	Std. Error of the Estimate
1	.438[a]	.192	.187	2.67181

a. Predictors: (Constant), Inclusion

From the model summary above, the value of $R^2 = 0.192$ implies that 19.2**%** of the variance in financial mismanagement prevention in sports organisations is explained by access control and authentication mechanisms. The adjusted **R^2** is positive, suggesting that the model improves upon using the mean as a predictor, a sign of good model fit.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	251.492	1	251.492	35.230	.000[b]
	Residual	1056.508	148	7.139		
	Total	1308.000	149			

a. Dependent Variable: Fin_Mismgt

b. Predictors: (Constant), Access_Control

The ANOVA table above shows that the F value of 35.230 is significant at .000. This implies that access control and authentication mechanisms significantly prevent financial mismanagement in sports organisations in Nigeria. Thus, the null hypothesis, which states that

Access control and authentication mechanisms do not significantly prevent financial mismanagement in sports organisations, is hereby rejected.

Discussion

The first hypothesis examined whether secure financial management software significantly impacts the prevention of financial mismanagement in sports organisations in Nigeria. The regression analysis revealed a strong positive correlation ($r = .510$, $p < .05$) between secure financial management software and financial mismanagement prevention. The model explained 26% of the variance in financial mismanagement prevention ($R^2 = .260$), and the F-statistic of 52.119 was statistically significant at $p < .05$. This finding aligns with broader cybersecurity literature that emphasises the role of secure digital systems in organisational financial governance. The significant relationship observed suggests that when sports organisations implement financial management software with robust security features, such as encryption, secure data storage, automated audit trails, and transaction verification protocols, they create systematic barriers against financial irregularities.

These findings are consistent with Von Solms and Van Niekerk's (2013) conceptualisation of cybersecurity as a protective framework for organisational assets. In the sports context, where financial flows involve multiple stakeholders, including government agencies, sponsors, and international bodies, secure software systems provide standardised platforms that enhance traceability and accountability. The automated documentation and real-time monitoring capabilities of secure financial software address the deficiencies in manual record-keeping that have characterised financial scandals in Nigerian sports federations, including the cases cited in the NFF probe.

The second hypothesis investigated whether access control and authentication mechanisms significantly prevent financial mismanagement in sports organisations in Nigeria. The regression analysis revealed a positive correlation ($r = .438$, $p < .05$) between access control

mechanisms and financial mismanagement prevention. The model explained 19.2% of the variance ($R^2 = .192$), and the F-statistic of 35.230 was statistically significant at $p < .05$. These results led to the rejection of the null hypothesis, confirming that access control and authentication mechanisms significantly prevent financial mismanagement in sports organisations.

This finding underscores the importance of restricting and monitoring access to financial systems as a preventive measure against internal fraud and unauthorised transactions. Access control and authentication mechanisms, including multi-factor authentication, role-based access privileges, biometric verification, and activity logging, ensure that only authorised personnel can initiate, approve, or modify financial transactions. The findings support the argument advanced by Bada and Nurse (2019) that cyber-enabled financial crimes are often facilitated by inadequate identity verification and access management systems. By implementing robust authentication mechanisms, sports organisations can mitigate risks associated with identity theft, unauthorised system access, and business email compromise, threats that have been documented in global sports contexts and are increasingly relevant as Nigerian sports entities digitise their operations.

Conclusion and Recommendations

This study investigated cybersecurity measures on prevention of financial mismanagement in sports organisations in Nigeria, focusing specifically on secure financial management software and access control and authentication mechanisms. The empirical findings provide compelling evidence that cybersecurity measures significantly contribute to financial mismanagement prevention in sports administration contexts.

The study concludes that cybersecurity measures should not be viewed merely as technical safeguards but as strategic governance tools that systematically reduce opportunities for financial mismanagement. By creating secure digital environments for financial operations,

implementing robust authentication protocols, and establishing clear accountability trails, sports organisations can strengthen their internal control systems and build institutional capacity for financial integrity.

Based on the findings and conclusions of this study, the following recommendations are hereby made for sports organisations:

1. Sports organisations should prioritise the acquisition and implementation of secure financial management software with robust cybersecurity features, including encryption, automated audit trails, transaction verification protocols, and secure data storage.
2. Sports federations and clubs should establish and enforce strict access control and authentication protocols for all financial systems. This should include multi-factor authentication, role-based access privileges, regular password updates, and biometric verification where feasible. These mechanisms should be designed to ensure the separation of duties and prevent unauthorised access to financial systems.
3. Sports organisations should conduct periodic cybersecurity audits to assess vulnerabilities in their financial management systems and ensure that security protocols remain effective against evolving cyber threats. Software systems should be regularly updated and patched to address newly discovered security weaknesses.

References

Akanbi, T. A., Olawale, B. E., & Adesina, O. S. (2022). Cybersecurity challenges in Nigeria's digital economy: An empirical analysis. *Journal of Information Security and Applications, 68*, 103241.

Akindes, G., & Kirwin, M. (2009). Sport as international aid: Assisting development or promoting under-development in sub-Saharan Africa? In R. Levermore & A. Beacom (Eds.), *Sport and international development* (pp. 215-245). Palgrave Macmillan.

Ayo, C. K., Atinyanta, A. N., & Adebiyi, A. A. (2021). Cybersecurity awareness and fraud prevention in Nigerian financial institutions. *African Journal of Science, Technology, Innovation and Development, 13*(4), 487-496.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393-410.

Chappelet, J. L., & Mrkonjic, M. (2016). Assessing the governance of international sport federations. In *Transparency International Global Corruption Report: Sport* (pp. 61-70). Routledge.

Darby, P., Akindes, G., & Kirwin, M. (2007). Football academies and the migration of African football labor to Europe. *Journal of Sport and Social Issues, 31*(2), 143-161.

Geeraert, A. (2018). *National sports governance observer: Final report 2018*. Play the Game/Danish Institute for Sports Studies.

Geeraert, A., Mrkonjic, M., & Chappelet, J. L. (2014). A rationalist perspective on the autonomy of international sport governing bodies: Towards a pragmatic autonomy in the steering of sports. *International Journal of Sport Policy and Politics, 7*(4), 473-488.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2018). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189-220.

Parent, M. M., & Hoye, R. (2018). The impact of governance principles on sport organisations' governance practices and performance: A systematic review. *Cogent Social Sciences, 4*(1), 1503578.

Parnell, D., Widdop, P., Bond, A., & Wilson, R. (2021). COVID-19, networks and sport. *Managing Sport and Leisure, 27*(1-2), 78-84.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.