ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Integrating Cybersecurity into Data Management: A Unified Framework for Office Data Security

Ifeyinwa Nkemdilim Obiokafor[1*], Blessing Nwamaka Iduh[2]

[1]Lecturer, Department of Computing Sciences, Cybersecurity Programme, Admiralty University of Nigeria.

[2]Lecturer, Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria.

***Corresponding Author**

DOI: https://doi.org/10.51583/IJLTEMAS.2026.15020000151

Received: 07 March 2026; Accepted: 12 March 2026; Published: 27 March 20266

ABSTRACT

The accelerated rate of digitization within the context of the office environment has seen organizational dependence on digital information systems escalate concurrently with an increased threat profile for cybersecurity breaches. This current study seeks to investigate the integration of active cybersecurity controls within the context of organizational data management to improve the security posture for data confidentiality, integrity, and availability. To this end, a mixed-methods research design was utilized to investigate this problem, incorporating a systematic review of existing literature and a quantitative survey of 150 mid- to large-scale organizations. The results highlight a significant disparity between the implementation of individual cybersecurity tools and the development of an overarching cybersecurity framework. The results demonstrate that organizations that implement an integrated data management system, incorporating end-to-end encryption, multi-factor authentication, rigorous administrative controls, cybersecurity training for staff, and effective data governance practices, are significantly less likely to experience data breaches when compared to organizations that implement a disjointed approach to cybersecurity. Additionally, this study recognizes organizational security awareness culture as a key influencer on cybersecurity posture, as employee awareness has a direct influence on the efficacy of cybersecurity controls and the mitigation of cybersecurity threats. As such, this study proposes a Unified Office Data Security Management (ODSM) framework that incorporates a holistic approach to cybersecurity controls to protect organizational data. The proposed framework provides a guide for organizations to improve cybersecurity governance, organizational resilience, and sustainability.

Keywords: Cybersecurity, Data Management, Office Data Security, Data Governance, Encryption, Security Awareness.

INTRODUCTION

The modern environment of the office space has witnessed an important evolution, transitioning from the paper-based filing system to an environment that is dynamic, computer-centric, and evolving. While the move towards cloud computing, collaboration, and virtual working has significantly enhanced the efficiency and connectivity of the management of data in an organization, the parallel move towards an expanded attack surface has positioned the organization's data as the primary target for the sophisticated array of cyber threats. While the integrity, confidentiality, and availability of the organization's sensitive information, including intellectual property, financial information, and employee information, remain at risk [4], the role of cybersecurity must now be understood as an integral part of the management of the organization's office space. While the traditional approach to the management of the organization's office space, which frequently neglected the role of security measures, has failed to address the sophisticated array of cyber threats, the financial consequences of data breach, including the cost of regulatory actions, remediation, and business

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

disruption, remain important considerations, along with the parallel move towards the negative consequences of reputation that may impact the organization's clients [12]. Therefore, the contemporary move towards the management of the organization's office space must now address the issue of the management of the organization's data in an environment that is complex, sophisticated, and adversarial.

Despite the increased recognition of the threats, there is a significant gap between having the tools to effectively deal with the threats and having a comprehensive organization-wide strategy that integrates cybersecurity into the data management lifecycle effectively. Many organizations invest heavily in the best available technology, including firewalls and intrusion detection systems, but tend to underestimate the significance of the human factor and the role of administrative policy [10], [11]. This is because the human factor is the least predictable and most commonly exploited threat surface.

As a result, the need to bridge this gap is the driving force behind this research. The main aim of this paper is to examine and articulate a framework for the integration of robust cybersecurity tools into the core of office data management practices. The research seeks to move beyond the singular focus of cybersecurity tools and delve into the synergy between cybersecurity tools, administrative policy, and organizational culture.

The paper is organized as follows: the introduction is followed by Section II, which is a detailed literature review of existing cybersecurity models, their suitability and how it relates to the management of data. Section III outlines the mixed-methods approach used in the study, followed by Section IV, which outlines the results and examines the correlation between the integrated security frameworks and the reduction of data breach incidents. Sections V to VII discuss the implications of the study, the proposed ODSM model, and the conclusion, respectively.

LITERATURE REVIEW

This section is a comprehensive literature review of all relevant literature related to the subject of cybersecurity in office data management. The literature is categorized under three main themes, namely, the changing cyber threat landscape for office data, the traditional triad of technical, administrative, and physical controls, and the identified gap with regards to integrated frameworks and human factors.

The Evolving Cyber Threat Landscape for Office Data

The digitalization of office work has significantly altered the threat landscape for office data. Initial research focused on defense strategies against external threats such as computer viruses and worms [15], [21]. Current research, however, reveals a shift towards a more targeted and insider form of cyber threats. Phishing and social engineering attacks have been identified as the main entry points for data breaches, indicating a targeted exploitation of the office worker's inherent nature of trusting their colleagues and the organization, as well as their lack of awareness with regards to cybersecurity best practices [8], [9], [16]. Studies by [2] consistently show that over 80% of all data breaches have a human element, highlighting the office worker's workstation as a key front in office data defense. Additionally, the increasing popularity of cloud services and remote work has eliminated the traditional network boundary, creating new and complex challenges with regards to data sovereignty, as well as the security of office data accessed via unsecured networks by remote office workers [18]. Ransomware, once a generic threat, has evolved into a targeted and disruptive threat, wherein essential data management systems are compromised, thereby impacting an organization's integrity and ability to conduct business as usual [1], [7].

Foundational Cybersecurity Measures: The Triad of Technical, Administrative, and Physical Controls

Literature reviews that there are three main types of cybersecurity measures:

Technical Controls: This refers to the technological mechanisms put in place to ensure the security of the data. There is substantial research evidence proving the efficacy of various forms of technical security mechanisms. For instance, data encryption, both at rest and in transit, is deemed a hard requirement for

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

ensuring the confidentiality of the data [20]. Another example is the efficacy of Multi-factor Authentication (MFA) in reducing the possibility of unauthorized access due to stolen credentials, as confirmed through various research studies [14]. Finally, Access Control Models, including Role-Based Access Control (RBAC), play a vital role in ensuring the principle of least privilege, thereby limiting the potential damage from both external breaches and insider threats [5] - [6]

Administrative Controls: These include the overall policies, procedures, and governance structures in place that affect security. Studies have strongly correlated the presence of strong administrative controls with successful security initiatives. Among the more important of these are the Data Governance Frameworks that address data ownership, classification, and handling practices [17]. Training and security awareness programs are consistently cited as one of the key factors in the successful implementation of security initiatives. As [13] point out, effective training must go beyond the simple compliance focus of annual training programs and instill the overall "security mindset" in employees. Incident Response and Disaster Recovery Planning are well-established areas of administrative controls aimed at minimizing the overall downtime and data loss in the event of a security breach [1].

Physical Controls: Though less emphasized in the digital age, physical controls represent one of the more basic aspects of overall security. Unauthorized physical access to servers and computer stations can bypass even the most advanced technical security measures. As such, they represent an integral aspect of overall security [3].

The Integration Gap and the Primacy of the Human Factor

A critical analysis of the research in the field reveals a notable gap in the body of knowledge, with a lack of studies on the integration of the different controls in a unified and manageable manner, particularly in the context of the office environment. Organizations are also faced with the problem of a "siloed" approach to security, where the different technical tools are not fully integrated with the organizational policies and procedures [7], leading to complexities in the management of the security environment, which in turn act as a barrier to the management of the data. Furthermore, one of the notable findings in the most recent studies in the field is the emphasis on the importance of the role of the human element in the management of the security environment. For example, the study presented in [11] highlights the fact that the most important factor in the management of the security environment, in the context of the threat of social engineering, is the "security culture" of the organization, or the attitudes and perceptions of the employees towards the organization's security.

Synthesis and Research Positioning

To summarize, the study of the related works gives a sound understanding of individual cybersecurity threats and controls. As has been well-established, the solution to the problem of cybersecurity is a combination of the technical, administrative, and physical. However, the research is wanting in providing a comprehensive model that seamlessly incorporates these concepts, particularly in the context of the management of office data in a distributed manner. The tendency to view the issue of cybersecurity in a purely technological context, divorced from the process of data management and organizational culture, is a critical threat. The purpose of this paper is to attempt to fill this lacuna in the literature by addressing the issue of integration. Expanding on the well-established knowledge of individual controls and the increasingly acknowledged significance of security culture, the following sections of this paper will empirically examine the synergy between these concepts and propose a unified model of Office Data Security Management (ODSM) that bridges the gap between policy, technology, and people.

RESEARCH METHODOLOGY

This study made use of a mixed-methods approach, which is considered to be an effective tool for ensuring that all aspects of a particular issue are sufficiently investigated. This is because it combined two research paradigms, which ensured that, through triangulation, the study produced valid and reliable results. This is

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

supported by the fact that, through mixed-methods research, it is possible to have an explanation for how and why something happens, which is usually lacking when quantitative research is used alone [3].

Research Design

The study was conducted through two phases, which, though they took place sequentially, were interconnected:

Phase 1: Qualitative Preliminary Study: This study made use of a systematic review, which helped to create an initial comprehension of the vital variables, as well as existing models, and refine the research tool for Phase 2.

Phase 2: Quantitative Core Study: This study made use of a cross-sectional survey, which was conducted on sampled organizations to collect data on the issue under investigation.

The data from both phases were integrated during the analysis and interpretation stage to develop a comprehensive understanding of the research problem.

Data Collection Methods

Phase 1: Systematic Literature Review: A systematic literature review was carried out following the guidelines provided in reference [19]. The review process covered peer-reviewed journals, conference publications, and essential industry publications within the time frame of 2018 to 2023. The key terms used in this process included “cyber security framework,” “data governance,” “security culture,” “office data management,” and “human factor in cyber security.” The data collection process was carried out using the IEEE Xplore, ACM Digital Library, and Scopus database tools. This process helped identify 72 key publications, which led to the construction of the survey tool and helped identify the key constructs to be measured in the survey process.

Phase 2: Quantitative Survey

A quantitative survey design was used, where a structured online survey tool was used to collect data from the target population, who are IT managers, data security experts, and CEOs, in medium to large-scale organizations with a strength of 100 to 5,000 employees, operating in different industries in the Southeast region of Nigeria.

Instrument Development: The instrument is designed on the constructs that were identified in the literature review. The instrument is divided into four major sections:

- Demographics: Organization size, sector, and role.
- Technical and Administrative Controls: This consists of questions pertaining to the extent to which different controls have been implemented in the organization, such as the extent to which encryption and MFA have been implemented, the frequency of security training provided to employees, data classification policy, and many more.
- Security Culture: This was designed on the Human Factor in Cyber (HFC) Security model.
- Security Outcomes: Questions pertaining to the number of security incidents the organization has faced in the last 12 months, such as data breach incidents, ransomware, and many more.
- Sampling Strategy and Data Collection: Purposive sampling strategy is used in this study. This approach is based on the assumption that the respondents who have in-depth knowledge about the data security practices followed in the organization will be able to provide reliable information. This survey is circulated among the professionals through professional networking sites such as LinkedIn, WhatsApp, Telegram, and many more. A total of 187 responses were collected. After data cleaning and validation, the remaining responses were 150, and the sample size is 80.2% of the response collected.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Data Analysis Techniques

The data collected using the questionnaire method will be analyzed using IBM SPSS Statistics, version 28.

Quantitative Data Analysis:

Descriptive Statistics: Frequency, Means, and Standard Deviations will be used to analyze the demographic details and the extent of implementation of the various security practices.

Inferential Statistics: To test the research hypotheses, several techniques will be used, such as:

- **Correlation Analysis (Pearson's r):** Used to examine the relationships between the implementation of integrated security frameworks, strength of security culture, and the number of security incidents.
- **Multiple Regression Analysis**: Was used to establish the predictive capacity of technical controls, administrative controls, and security culture in reducing the number of data breach cases. Using this analysis, the most important factors that predict the effectiveness of data security could be established.
- **Independent Samples t-test:** Was used to compare the results of the security measures between organizations that had an established, integrated data security model and those that did not.

Qualitative Data Integration: The results obtained from the systematic literature review were used to interpret the results obtained from the analysis. For instance, the results obtained from the qualitative analysis on the reasons for the failure of administrative controls could have been used to explain the results obtained from the regression analysis.

Ethical Considerations

The study was conducted with the highest level of ethical consideration. For instance, the participants were first presented with an informed consent form that explained the purpose of the study, the voluntary nature of the participation, and the confidentiality of the information they provided. Moreover, the information provided was anonymous, which meant that no personally identifiable information was collected. Using the mixed method approach, the researchers were able to conduct an in-depth analysis of the factors that promote the effectiveness of the security measures in the management of office data.

FINDINGS

The empirical findings of the quantitative survey, structured to address the core research objectives. The results are organized to first describe the sample characteristics, then detail the implementation levels of cybersecurity measures, and finally, present the analytical results examining the relationships between these measures and security outcomes. This structured presentation enables a comprehensive understanding of how integrated cybersecurity practices influence organizational data security performance.

Descriptive Statistics of the Sample

The final sample of 150 organizations represented a diverse cross-section of industries, including Financial Services (22%), Healthcare (18%), Technology (25%), Professional Services (20%), and Manufacturing (15%). In terms of size, 34% were mid-sized (100-500 employees), 42% were large (501-2000 employees), and 24% were enterprise-level (2001-5000 employees). The primary respondents were IT Security Managers (45%), Data Protection Officers (25%), C-level executives (15%), and other IT leads (15%).

Implementation Levels of Cybersecurity Measures

The survey assessed the adoption rate of various technical and administrative controls on a 5-point Likert scale (1=Not Implemented, 5=Fully Implemented).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Technical Controls: The implementation of core technical controls was generally high, though with significant variation:

- Data Encryption (at-rest & in-transit): Mean = 4.45 (SD = 0.82)
- Multi-factor Authentication (MFA): Mean = 4.20 (SD = 1.05)
- Role-Based Access Control (RBAC): Mean = 3.95 (SD = 1.18)
- Automated Security Auditing/Logging: Mean = 3.70 (SD = 1.30)

Administrative Controls and Security Culture: The implementation of administrative measures showed greater disparity:

- Formal Data Governance Policy: Mean = 3.90 (SD = 1.25)
- Regular (Bi-annual or more) Security Training**:** Mean = 3.40 (SD = 1.45)
- Measured Security Culture Score: Mean = 3.15 (SD = 1.15)

A notable finding was that only 38% of organizations reported having a fully integrated framework where technical controls were explicitly mapped to and supported by formal administrative policies.

Analytical Results: Correlations and Predictive Power

The impact of these measures, correlation and regression analyses was conducted. Correlation with Security Incident Reduction: A strong, statistically significant negative correlation was found between the implementation of an integrated framework and the number of self-reported security incidents ($r = -0.68$, $p < .001$). This indicates that as the level of integration increases, the number of security incidents decreases. Furthermore, the Security Culture Score also showed a significant negative correlation with security incidents ($r = -0.72$, $p < .001$), suggesting it may be an even stronger mitigating factor. Regression Analysis: A multiple linear regression was performed to predict the reduction in security incidents based on three predictor variables: (1) Composite Technical Control Score, (2) Composite Administrative Control Score, and (3) Security Culture Score. The regression model was statistically significant, $F(3, 146) = 42.35$, $p < .001$, and accounted for 62% of the variance in security incident reduction ($R^2 = .62$).

The coefficients, as shown in Table 1, reveal the relative influence of each factor:

TABLE I: Regression Coefficients for Predictors of Security Incident Reduction

Predictor Variable	Unstandardized Coefficient (B)	Standard Error	Standardized Coefficient (β)	t-value	p-value
(Constant)	5.12	0.45		11.38	<.001
Technical Controls	-0.25	0.08	-0.21	-3.13	.002
Administrative Controls	-0.31	0.09	-0.26	-3.44	<.001
Security Culture	**-0.49**	**0.07**	**-0.48**	**-7.00**	**<.001**

Dependent Variable: Reduction in Security Incidents

The analysis indicates that while both technical and administrative controls are significant predictors ($p < .01$), the Security Culture Score ($\beta = -0.48$, $p < .001$) is the most substantial unique predictor of a reduction in security incidents.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Comparative Analysis: The Impact of an Integrated Framework

An independent-samples t-test was conducted to compare the security outcomes for organizations with and without a formally documented, integrated security and data management framework. The results were striking:

- Organizations with an integrated framework (n=57) reported a mean of 1.2 security incidents per year.
- Organizations without an integrated framework (n=93) reported a mean of 3.8 security incidents per year.

This difference, 2.6 incidents, was statistically significant, $t(148) = 6.78$, $p < .001$. This provides strong empirical evidence that a holistic, integrated approach is far more effective than deploying measures in isolation.

In summary, the findings robustly demonstrate that:

- The integration of cybersecurity measures into data management is not widespread.
- Both technical and administrative controls are necessary, but the strength of an organization's security culture is the most powerful predictor of positive security outcomes.
- Organizations employing a unified framework experience significantly fewer security incident.

Unified Office Data Security Management (ODSM) Framework

Unified Office Data Security Management (ODSM), framework, is designed to ensure the security of organizational data throughout the data lifecycle, from the time of data creation to the time of data archiving or deletion. ODSM is a comprehensive framework that ensures the security of organizational data while considering the technical aspects of security management as well as the governance aspects that focus on the role of human behavior [1], [20]. ODSM framework is fashioned on the recognition that data security breaches do not only result from technical errors but often from human actions, policies, and governance. Thus, the ODSM framework is based on the integration of technical security management, human behavior, and institutional policies [15].

Components of the Unified Office Data Security Management (ODSM)
Data Governance and Policy Framework: This is the component that outlines the institutional policies that cover the process of data creation, access, and security.

Data security management under this component includes the following aspects: data classification policies that cover data classified as public, internal, confidential, or restricted; data ownership and data stewardship; adherence to institutional regulations that cover ISO 27001 and data privacy regulations that cover the EU's GDPR; access control policies; and data retention and deletion.

As a result, the Data Governance and Policy Framework ensure the establishment of a data governance structure that ensures data security [21].

Data Lifecycle Security Management: This is the component that ensures the security of data at every stage of the data lifecycle [15][9]. The stages of protection and the security controls that cover the data lifecycle include the following:

- Data Creation: Data classification, secure templates
- Data Storage: encryption, access control
- Data Processing: secure applications, audit logs
- Data Sharing: secure email, file protection

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

- Data Archiving: secure backup systems
- Data Disposal: secure deletion and destruction

Technical Security Infrastructure: This component focuses on technology-based security controls. The key technologies include data encryption, multi-factor authentication, endpoint security solutions, secure cloud storage solutions, data loss prevention solutions, network firewalls, intrusion detection systems, and backup and disaster recovery solutions. These technologies, in aggregate, offer security against cyber-attacks, insider attacks, and data breaches [9], [12].

Behavioral and Human-Centered Security Controls: The workforce is both the main vulnerability and main security asset in terms of office data security. The mitigation strategies include cybersecurity awareness programs, phishing simulation programs, acceptable use policy programs, promotion of a culture of password security, insider threat awareness programs, and role-based security responsibilities. The collective effect of these strategies is to build a security-conscious workforce that actively contributes to data security in an organization [9].

Monitoring, Auditing, and Incident Response: Data security monitoring ensures that all security policies are functioning optimally. This is a proactive strategy that includes real-time security monitoring, security audit and compliance checks, incident response programs, digital forensics programs, and post-incident review programs. This strategy helps in the early detection of security threats and quick response to security incidents to contain them before they get out of hand.

Business Continuity and Data Sustainability: ODSM ensures business continuity through its automated backup systems, disaster recovery programs, redundant data storage systems, business continuity programs, and business resilience tests. This ensures that an organization will always continue to operate even in the event of a security incident or system failure.

ODSM Implementation Model

The implementation of *ODSM* framework in an organization involves a strategic five-step model:

- Assessment Phase: This phase involves assessing an organization's current data security level and risks involved.
- Policy Development Phase: This phase sees the development of policies in an organization.
- Technology Deployment Phase: This phase involves deploying technology in an organization.
- Capacity Building Phase: This phase sees a culture of security awareness among employees in an organization.
- Continuous Improvement Phase: This phase involves monitoring performance and conducting audits to improve policies.

The adoption of the Unified ODSM framework ensures a holistic approach to data security in an organization. The implementation of the Unified ODSM framework in an organization ensures the protection of enterprise data from security risks such as data breach and insider threat attacks.

The implementation of the Unified ODSM framework in an organization ensures compliance with relevant laws. The implementation of the Unified ODSM framework in an organization ensures a culture of cybersecurity among employees. The implementation of the Unified ODSM framework in an organization ensures sustainability.

DISCUSSION

This paper investigated the integration of cybersecurity measures into office data management and to identify the key factors that lead to its effectiveness. The findings provided robust, empirical evidence that moves the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

discourse beyond theoretical best practices into actionable, data-driven insights. This section interprets these results, discusses their broader implications, states the conclusions, and proposes recommendations for both practitioners and future research.

DISCUSSION OF THE FINDINGS

The findings of the study substantiate several core propositions in the cybersecurity literature while arriving at a more refined comprehension of the interrelations of these propositions.

1) The Paramount Importance of Security Culture: The most prominent finding was the preeminence of security culture (β = -0.48) over other variables in the mitigation of security incidents. This observation supports the earlier propositions in the cybersecurity literature [11]-[12]. It shows that the most advanced technical security measures (for example, encryption, multi-factor authentication) can be easily circumvented by one employee who is tricked by a phishing attack owing to inadequate security culture. A good security culture is the ultimate security solution that can improve the efficacy of all other security controls, transforming them from mere compliance-driven rules to a way of life in the organization.

2) The Synergy of an Integrated Framework: The negative correlation between integrated frameworks and security incidents was found to be statistically significant (t-test), with a correlation coefficient of (r= -0.68). This clearly establishes the significance of synergy and its practical applicability. The adoption of a fragmented security approach, whereby the IT department implements solutions independently of organizational policy, will inevitably create unnecessary complexities. For example, the implementation of a robust RBAC solution will be relevant to the extent to which organizational policy has addressed issues of data ownership and user roles. The integrated approach eliminates these complexities by providing a complete solution that combines the human, administrative, and technical dimensions of security.

3) The Foundational Role of Administrative Controls: Although security culture was found to be the most important variable, the regression analysis revealed the significance of administrative controls to the security function (β = -0.26). These further underlines the fact that security culture cannot be developed independently and must be developed through appropriate administrative controls [17], [21].

Implications for Practice and Theory

Practical Implications*:* For the organization, the implications are as follows:

- Reassess Security Investments: Management should reassess investments and priorities towards those endeavors that enhance the organization's human capital and cultural development, such as ongoing security training and awareness campaigns, as opposed to new software solutions.
- Adopt a Holistic Model: The search for the elusive security "silver bullet" is a waste of time and resources. Organizations should prioritize the development of a cohesive framework, such as the proposed Office Data Security Management (ODSM) model, that explicitly integrates all three aspects: technology, policy, and people.
- Measure What Matters: Organizations must also develop a means of measuring and benchmarking security culture via surveys and assessments.

Theoretical Contributions: The current research contributes to the theoretical body of knowledge as follows:

- Quantitative Validation: The current research provides quantitative validation of the importance of security culture and integrated frameworks from a theoretical perspective.
- Quantification of Factors: The current research also provides a means of quantifying the relative importance of a myriad of factors in the determination of security outcomes.
- Office Data Security Management (ODSM) Model: The current research also provides a tangible means of testing the effectiveness of a proposed Office Data Security Management (ODSM) model.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

CONCLUSIONS

In conclusion, the current research has sought to prove the following: that office data management in the digital age is inextricably tied to cybersecurity; that cybersecurity is not merely a product of accumulated technologies; and that the best means of protecting an organization from the threat of data breaches is a culture of shared responsibility for cybersecurity, supported by a cohesive framework that seeks to integrate all aspects of the organization towards a common end: data protection.

LIMITATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

The present study has several limitations, which outline the scope for future research. Firstly, the study's reliance on self-reported data for security breaches could have led to some bias. Secondly, the study's focus on medium and large firms could limit the generalizability of the study's findings to very small firms and to diverse cultural settings.

Taking the above limitations into consideration, the following recommendations are made for future research:

1) Longitudinal studies could be conducted to track the organizations over time to assess the impact of the integrated framework on the organizations' security culture.
2) Future studies could focus on conducting research to determine if the relative weightage of technical, administrative, and cultural factors varies significantly between highly regulated industries such as the health and finance sectors compared to other industries.
3) Qualitative studies could also be conducted to determine the managerial and leadership factors that are most likely to impact the organizations' security culture.
4) Future studies could focus on validating the ODSM model by conducting the same in diverse organizational settings and assessing the components of the model for their practical utility.

By addressing these avenues, the academic and professional communities can continue to build upon the findings of this study to develop ever more effective strategies for securing our most vital digital assets.

REFERENCES

1. Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49(C), 424–438.
2. Brandao, P. R. (2025). Cyber Threat Intelligence with Symmetry for Zero-Trust Security. Computer Science and Mathematics. https://doi.org/10.20944/preprints202508.0059.v1
3. Creswell, J. W., & Clark, V. L. P. (2018). Qualitative inquiry and research design (Fourth edition). SAGE.
4. He, M., & Chen, Y. (2025). Personal data protection in China: Progress, challenges and prospects in the age of big data and AI. Telecommunications Policy, 49(10), 103076. https://doi.org/10.1016/j.telpol.2025.103076
5. Marquis, Y. A. (2024). From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts. Journal of Engineering Research and Reports, 26(5), 138–154. https://doi.org/10.9734/jerr/2024/v26i51141
6. Mehra, T. (2024). The Critical Role of Role-Based Access Control (RBAC) in securing backup, recovery, and storage systems. International Journal of Science and Research Archive, 13(1), 1192–1194. https://doi.org/10.30574/ijsra.2024.13.1.1733
7. Merlo, T. R., Fard, F., & Hawamdeh, S. (2025). Cloud Computing's Impact on the Digital Transformation of the Enterprise: A Mixed-Methods Approach. Sustainability, 17(13), 5755. https://doi.org/10.3390/su17135755
8. Obiokafor, I. N. (2023). Approaches to a secure, sustainable, and diversified Nigerian economy in a cashless society. World Journal of Advanced Research and Reviews, 20(2), Article 2. https://doi.org/10.30574/wjarr.2023.20.2.2266

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

9. Obiokafor, I. N., Ajonuma, M. E., & Aguboshim, F. C. (2025). Integrating Privacy by Design (PbD) in the system development life cycle for enhanced data protection. World Journal of Advanced Research and Reviews, 26(1), 1233–1240. https://doi.org/10.30574/wjarr.2025.26.1.0538
10. Obiokafor, I. N., & Mbonu, O. (2025). The intersection of digital policy and cybersecurity: Implications for sustainable development. World Journal of Advanced Engineering Technology and Sciences, 14(3), 077–085. https://doi.org/10.30574/wjaets.2025.14.3.0094
11. Oluremi, D., Vallabhaneni, R., Lallie, H., & Guglielmo, M. C. (2025). Abstract on Human Factors in Cybersecurity: Social Engineering and Insider Threats.
12. Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. International Journal of Information Management, 74, 102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719
13. Puhakainen, P., & Siponen, M. (2021). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly, 34(4), 757-778.
14. Rabzelj, M., & Sedlar, U. (2025). Beyond the Leak: Analyzing the Real-World Exploitation of Stolen Credentials Using Honeypots. Sensors, 25(12), 3676. https://doi.org/10.3390/s25123676
15. Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. Journal of Industrial Information Integration, 36, 100520. https://doi.org/10.1016/j.jii.2023.100520
16. Sonar, O., Anvekar, N., & Hebbalkar, S. (2025). Phishing and Social Engineering: Analyzing Human Vulnerability. 8(4).
17. Vararean-Cochisa, D., & Crisan, E.-L. (2025). The digital transformation of the construction industry: A review. IIM Ranchi Journal of Management Studies, 4(1), 3–16. https://doi.org/10.1108/IRJMS-04-2024-0035
18. Verma, S. (2025). Cybersecurity compliance in the age of remote work: Challenges and solutions. World Journal of Advanced Engineering Technology and Sciences, 15(1), 1112–1120. https://doi.org/10.30574/wjaets.2025.15.1.0286
19. Webster, J., & Watson, R. T. (2002). Analyzing The Past to Prepare For The Future: Writing A Literature Review. 26(2), xiii–xxiii.
20. Yee, C. K., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT in Education, 8(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021
21. Obiokafor, I. N., Onwuka, U. P., Okoye, O. M., & Ameke, B. C. (2025). Strategies for data protection and privacy in administrative information systems. ANSPOLY Journal of Advanced Research in Science & Technology (AJARST), 2(2), 66–77