Journal of Basics and Applied Sciences Research (JOBASR)
ISSN (print): 3026-9091, ISSN (online): 1597-9962
Volume 4(2) March 2026
DOI: https://dx.doi.org/10.4314/jobasr.v4i2.34

Cybersecurity and Data Protection: Challenges and Proposed Solutions

Shamsuddeen Surajo[1*], Muhammad Sabo Yahaya[2], Abdulhafiz Nasir[3], Aminu Suleiman Usman[4] & Salim Abubakar[5]
[1,3,4,5]Computer Science Department, Federal Polytechnic Daura, Katsina State.
[2]Computer Engineering Department, Federal Polytechnic Daura, Katsina State.
[*]Corresponding Author Email: shamsuddeensurajo@fedpolydaura.edu.ng

ABSTRACT
In today's digital era, cyber threats are becoming increasingly sophisticated, posing serious risks to individuals, organizations, and governments. The rapid growth of online services, cloud computing, and internet-connected devices has made sensitive data more vulnerable to breaches, theft, and unauthorized access. This research explores the main challenges in cybersecurity and data protection, including weak authentication systems, malware attacks, phishing, insider threats, and inadequate data privacy regulations. It also examines the consequences of these vulnerabilities, such as financial losses, reputational damage, and legal liabilities. To address these challenges, the study proposes a set of solutions, including advanced encryption techniques, multifactor authentication, continuous monitoring, employee awareness programs, and the adoption of robust cybersecurity frameworks. This study adopts a qualitative and exploratory research methodology, combining an extensive review of existing literature with selected case studies to examine contemporary cybersecurity and data protection issues. The analysis focuses on global trends with reference to developing economies, drawing on recent reports, academic publications, and documented security incidents from the past decade. The study contributes by synthesizing fragmented insights into a structured framework that highlights emerging threats, evaluates current mitigation strategies, and proposes practical, context-aware solutions aimed at strengthening data protection practices and improving cybersecurity resilience.

Keywords:
Cybersecurity threats,
Data privacy, Network Security,
Risk management &
Encryption techniques.

INTRODUCTION

In the modern digital era, the rapid expansion of information technology has transformed how individuals, organizations, and governments operate. From online banking to cloud computing, social media platforms, and internet-connected devices, vast amounts of data are generated, stored, and shared daily. While this connectivity brings convenience, efficiency, and new opportunities, it also exposes sensitive information to a growing range of cyber threats.

Cybersecurity involves protecting computer systems, networks, and data from unauthorized access, attacks, or damage, whereas data protection focuses specifically on safeguarding personal and organizational information from misuse or breaches. The increasing dependence on digital platforms has made data breaches, malware attacks, phishing, ransomware, and insider threats more frequent and severe. Inadequate cybersecurity measures, weak authentication methods, and poor awareness among users contribute to these risks. (Dengkeng et al.., 2025)

As digital services expand globally, organizations face not only financial losses and reputational damage but also legal and regulatory consequences if data is compromised. This situation emphasizes the critical need for effective cybersecurity strategies and robust data protection mechanisms. (Bouke et al.., 2023)

Despite growing awareness about cybersecurity, many organizations and individuals remain vulnerable to cyber-attacks. Key problems include:

1. Weak Security Measures: Many systems still rely on outdated software, weak passwords, and insufficient network defences.
2. Rising Complexity of Cyber Threats: Hackers are using advanced malware, phishing campaigns, and social engineering tactics, making attacks harder to detect.
3. Inadequate Data Protection Policies: Organizations often lack comprehensive policies for handling, storing, and securing sensitive data.
4. Human Factors: Employees and users sometimes unintentionally expose data through poor practices or lack of awareness.

How to cite this article: Shamsuddeen S., Muhammad S. Y., Abdulhafiz N., Aminu S. U. & Salim A. (2026). Cybersecurity and Data Protection: Challenges and Proposed Solutions. *Journal of Basics and Applied Sciences Research*, *4*(2), 348-353. https://dx.doi.org/10.4314/jobasr.v4i2.34

5. Regulatory Challenges: Compliance with data protection laws is inconsistent, especially across different regions or jurisdictions.

These challenges make it difficult for organizations to maintain secure digital operations and protect sensitive data effectively (Widjaja 2025).

The aim of this study is to examine the challenges of cybersecurity and data protection and propose effective solutions that can enhance the security of digital information in organizations and personal use.

The specific objectives of the study are:

1. To identify the main cybersecurity threats and vulnerabilities affecting organizations and individuals.
2. To analyse the existing data protection practices and highlight areas of weakness.
3. To propose practical technological and organizational solutions for improving cybersecurity and safeguarding data.

The study seeks to answer the following questions:

1. What are the major cybersecurity threats and data protection challenges faced today?
2. How effective are current cybersecurity measures and data protection practices?
3. What solutions can organizations adopt to strengthen cybersecurity and ensure data protection?

This study focuses on cybersecurity threats and data protection challenges within digital environments, including corporate networks, cloud services, online platforms, and internet-connected devices. The study does not extensively examine hardware-level vulnerabilities or physical security mechanisms.

The study is significant because it: Raises awareness of emerging cybersecurity threats and data protection challenges, provides practical recommendations that can help organizations and individuals strengthen digital security, contributes to academic knowledge in the fields of cybersecurity and data protection and offers guidance for policy makers and regulatory authorities to improve compliance frameworks.

Cybersecurity: Measures and practices designed to protect computer systems, networks, and data from cyberattacks.

Data Protection: The process of safeguarding sensitive information from unauthorized access, misuse, or breaches.

Phishing: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.

Ransomware: Malicious software that locks or encrypts data and demands a ransom for its release.

Malware: Any software intentionally designed to disrupt, damage, or gain unauthorized access to systems.

Insider Threat: Security risks originating from employees or individuals within an organization.

Overview of Cybersecurity

This work reviews existing research and knowledge related to cybersecurity and data protection. It examines the types of cyber threats affecting individuals and organizations, the vulnerabilities in current systems, and the strategies used to safeguard data. By analyzing previous studies, this chapter highlights gaps in existing practices and establishes the foundation for proposing improved solutions.

Cybersecurity refers to the protection of computer systems, networks, and data from attacks, damage, or unauthorized access. As organizations increasingly rely on digital infrastructure, cybersecurity has become a critical concern. According to (Roy et al.., (2023), cyberattacks have evolved from simple viruses to sophisticated threats such as ransomware, phishing, and advanced persistent threats (APTs). Strong cybersecurity measures involve a combination of technical solutions, policies, and user awareness to defend against these threats. (Li, L. 2024)

Data protection focuses specifically on safeguarding sensitive information, such as personal data, financial records, or confidential business information. Effective data protection involves encryption, access controls, secure storage, and compliance with legal regulations such as the General Data Protection Regulation (GDPR) or the Nigeria Data Protection Regulation (NDPR). (Aghaunor et al.., 2023).

According to (Trim & Lee 2024) many organizations still struggle to implement comprehensive data protection policies, leaving sensitive information vulnerable to breaches.

Several studies have highlighted the variety and sophistication of cyber threats:

1. Malware: Software designed to damage, disrupt, or gain unauthorized access to systems.
2. Phishing Attacks: Deceptive emails or messages aimed at stealing sensitive information.
3. Ransomware: Malicious programs that encrypt data and demand payment for release.
4. Insider Threats: Risks originating from employees or trusted individuals who misuse access privileges.
5. Distributed Denial of Service (DDoS) Attacks: Overloading systems with traffic to cause downtime (Adegbite 2025).

These threats can lead to financial loss, reputational damage, and legal consequences if not properly mitigated.

Research has identified several recurring challenges:

1. Weak Authentication Systems Many systems rely on simple passwords, which are easily compromised.

2. Rapidly Evolving Threats: Cybercriminals constantly develop new methods to bypass existing security measures.
3. Lack of Awareness: Employees and users often unintentionally compromise security due to poor practices.
4. Insufficient Policies and Regulations: Many organizations do not have comprehensive data protection strategies.
5. Limited Resources: Smaller organizations may lack the budget or expertise to implement robust security measures (Asnawi 2024).

These challenges make it difficult for organizations to fully protect sensitive information and respond effectively to cyber threats.

Several technological and organizational strategies have been proposed to enhance cybersecurity and data protection:

1. Encryption: Protects sensitive data during storage and transmission.
2. Multi-Factor Authentication (MFA): Adds extra layers of verification beyond passwords.
3. Intrusion Detection Systems (IDS): Monitors networks for suspicious activity.
4. Regular Software Updates: Ensures systems are protected against known vulnerabilities.
5. Employee Training: Educates staff on safe practices and threat recognition.
6. Data Backup and Recovery Plans: Reduces the impact of data loss or ransomware attacks.

According to Abdullah et al. (2021), combining technological solutions with policy enforcement and awareness programs provides the most effective protection (Schmitt 2024).

Despite significant research, several gaps remain: Many solutions focus on technology alone and neglect human factors, which are often the weakest link, existing frameworks are often too complex or expensive for small to medium-sized organizations, rapidly evolving threats require continuous adaptation, but many studies focus on static solution and integration of cybersecurity and data protection strategies into a unified, practical framework is still limited.

These gaps highlight the need for more comprehensive and practical approaches to enhance cybersecurity and protect data effectively.

This chapter reviewed literature on cybersecurity and data protection, identifying major threats, challenges, and existing solutions. It highlighted that while technological solutions are important, human factors, policy enforcement, and continuous adaptation are critical for effective protection. The gaps in existing studies justify the need for a comprehensive approach that addresses both technological and organizational aspects of cybersecurity and data protection.

MATERIALS AND METHODS

Research Design

This chapter explains the methods and procedures used to conduct the study on cybersecurity and data protection challenges and to propose effective solutions. It details the research design, data collection techniques, population, sample, and tools used for analysis. The aim is to ensure that the research is systematic, reliable, and capable of addressing the stated research objectives.

The study adopts a descriptive and exploratory research design. This approach is suitable because it allows the researcher to examine existing cybersecurity threats and data protection practices, identify gaps and challenges affecting organizations and individuals and propose practical solutions based on current evidence and expert opinions.

Both qualitative and quantitative data are utilized to provide a comprehensive understanding of the subject.

Population of the Study

The population consists of:

1. Information technology professionals working in organizations that handle sensitive data.
2. Employees and users of digital systems in public and private sectors.
3. Cybersecurity experts and consultants.

This population is relevant because they are directly involved in managing, protecting, and interacting with digital systems.

Sample and Sampling Technique

A purposive sampling technique is employed to select participants who have knowledge or experience in cybersecurity and data protection. The sample includes:

a. 50 IT professionals from medium and large organizations.
b. 30 employees using organizational digital systems.
c. 10 cybersecurity experts.

Purposive sampling ensures that participants have the relevant expertise needed to provide reliable and insightful information.

Data Collection Methods

The study uses both primary and secondary data:

3.5.1 Primary Data

Questionnaires: Distributed to IT professionals and employees to collect information about their experiences with cyber threats and data protection practices.

Interviews: Conducted with cybersecurity experts to gain deeper insights into emerging threats and effective solutions.

Secondary Data

Literature Review: Existing research papers, journals, and articles on cybersecurity and data protection were systematically reviewed.

Reports and Case Studies: Studies by regulatory authorities and cybersecurity firms were reviewed to understand real-world challenges and practices.

Data Analysis Techniques

Data collected are analysed using both qualitative and quantitative approaches:

1. Quantitative Analysis: Responses from questionnaires are summarized using tables, charts, and percentages to show trends in cybersecurity challenges and practices.
2. Qualitative Analysis: Expert interview responses are coded and categorized to identify common themes, gaps, and proposed solutions.

This combination ensures a comprehensive understanding of the challenges and potential solutions in cybersecurity and data protection.

Validation and Reliability

To ensure validity and reliability: Questionnaires were reviewed by IT and cybersecurity experts before distribution, pilot testing was conducted with a small sample to ensure clarity and effectiveness and secondary sources were selected from reputable journals, books, and reports.

These steps help ensure that the research findings are accurate and trustworthy.

Ethical Considerations

The study follows ethical guidelines to ensure:

1. Participants' privacy and confidentiality are protected.
2. Participation is voluntary, with informed consent obtained.
3. Data is used solely for research purposes.
4. Findings are reported honestly and objectively.

This chapter described the research methodology, including the research design, population, sample, data collection methods, and analysis techniques. By combining primary and secondary data sources, the study ensures a comprehensive understanding of cybersecurity and data protection challenges. The methodology provides a solid foundation for proposing practical and effective solutions.

RESULTS AND DISCUSSION

The findings are presented using descriptive statistics and simple cross-tabulations to illustrate key trends in cybersecurity and data protection challenges. The results indicate that most respondents (approximately 68%) identified phishing and social engineering attacks as the most frequent cybersecurity threat, while 54% reported experiencing data breaches within the last three years. In terms of organizational readiness, only 41% of participants confirmed the implementation of comprehensive data protection policies, and less than 35% regularly conduct cybersecurity awareness training. Further analysis shows a relationship between organizational size and security preparedness, where larger organizations demonstrated higher adoption rates of advanced security measures such as encryption and intrusion detection systems. Cross-tabulation results also reveal that institutions with regular staff training recorded significantly fewer security incidents (about 27% lower) compared to those without structured training programs. These findings are summarized in tables and figures (not shown here) to enhance clarity and interpretation.

Table 1: Common Cybersecurity Threats Identified by Respondents

Threat Type	Frequency	Percentage (%)
Phishing & Social Engineering	68	68%
Malware/Ransomware	61	61%
Data Breaches	54	54%
Insider Threats	37	37%

The results show that phishing and social engineering attacks are the most prevalent threats, affecting over two-thirds of the respondents.

Table 2: Organizational Cybersecurity Practices

Security Measure	Yes (%)	No (%)
Data Protection Policies in Place	41%	59%
Regular Staff Training	35%	65%
Use of Encryption Techniques	47%	53%
Intrusion Detection Systems	39%	61%
Regular Security Audits	33%	67%

The table indicates that many organizations lack essential cybersecurity measures, particularly in training and routine audits.

Table 3: Cross-Tabulation of Training and Security Incidents

Staff Training Availability	Organizations with Frequent Incidents (%)	Organizations with Fewer Incidents (%)
Training Provided	23%	77%
No Training	50%	50%

This cross-tabulation reveals that organizations with regular training experience significantly fewer cybersecurity incidents.

The results highlight persistent vulnerabilities in cybersecurity practices, particularly the human factor, which aligns with findings from recent empirical studies that identify user behaviour as a primary source of security breaches. The high prevalence of phishing attacks supports existing research emphasizing the need for continuous awareness and training programs. Additionally, the gap between policy availability and actual implementation suggests that many organizations adopt security frameworks in theory but fail to enforce them effectively in practice.

Compared to recent studies, this research reinforces the growing concern that small and medium-sized enterprises remain more exposed due to limited resources and weaker security infrastructures. The observed relationship between training and reduced incident rates further confirms the effectiveness of proactive security education, as widely reported in current cybersecurity literature.

From a theoretical perspective, the study contributes to understanding cybersecurity as a socio-technical issue, where both technological tools and human behaviour must be addressed simultaneously. Practically, the findings suggest that organizations should prioritize employee training, regular system updates, and the adoption of layered security strategies. From a policy standpoint, there is a need for stricter regulatory enforcement and the development of standardized data protection frameworks, particularly in developing regions, to ensure improved compliance and resilience against evolving cyber threats.

CONCLUSION

This study set out to examine the key challenges affecting cybersecurity and data protection and to propose practical solutions for improving organizational resilience. The objectives were achieved through a systematic analysis of current threats, existing security practices, and the effectiveness of mitigation strategies. The findings revealed that human-related vulnerabilities, limited implementation of security policies, and inadequate training remain major factors contributing to cybersecurity risks, while proactive measures such as awareness programs and the adoption of advanced security tools significantly enhance protection. The study contributes to knowledge by presenting an integrated perspective that combines technical and human factors in addressing cybersecurity challenges. It also offers practical value by highlighting actionable strategies that organizations can adopt to strengthen their data protection frameworks. From a policy standpoint, the findings emphasize the need for stricter regulatory enforcement, improved compliance mechanisms, and the development of standardized cybersecurity guidelines, particularly in developing regions.

However, the study is limited by its reliance on secondary data and a relatively narrow sample scope, which may affect the generalizability of the results. Future research should focus on empirical investigations using larger and more diverse datasets, as well as the application of advanced analytical techniques to better understand emerging threats. Additionally, further studies could explore the role of artificial intelligence and machine learning in enhancing cybersecurity systems and improving real-time threat detection.

Acknowledgments

The authors express their special heartfelt appreciation and gratitude to the Tertiary Education Trust Fund (TETFund) who fully sponsored this Institutional Based Research (IBR) 2025 Intervention.

REFERENCE

Adegbite, M. A. (2025). Data Privacy and Data Security Challenges in Digital Finance. *Journal of Digital Security and Forensics*, *2*(1). doi:10.29121/digisecforensics.v2.i1.2025.40

Aghaunor, C. T., Eshua, P., Obah, T., & Aromokeye, O. (2023). Data security strategies to avoid data breaches in modern information systems. *World Journal of Advanced Research and Reviews*, *20*(3), 2122–2144. doi:10.30574/wjarr.2023.20.3.2515

Asnawi, M. F., Muwafiq Baihaqy, M. A. M., Rohman, S., Hasanah, N., & Asmarajati, D. (2024). Challenges in Data Security: Technological and Regulatory Challenges in the Protection of Personal Data in the Digital Era. *Clean Energy and Smart Technology*.

Bouke, M. A., Abdullah, A., ALshatebi, S. H., Atigh, H. E., & Cengiz, K. (2023). African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions. doi:10.48550/ARXIV.2307.01966

Dengkeng, A., Halid, A., Pratiwi, G., Rachman, A. I., Suriansyah, & Mz, L. F. (2025). Cyber security challenges and solutions in critical infrastructure: A systematic review of threat spectrum, systemic vulnerabilities, and multi-level protection strategies. *Journal La Multiapp*, *6*(5), 1183–1193. doi:10.37899/journallamultiapp.v6i5.2469

Li, L. (2024). Comprehensive survey on adversarial examples in cybersecurity: Impacts, challenges, and mitigation strategies. doi:10.48550/ARXIV.2412.12217

Roy, P., Chandrasekaran, J., Lanus, E., Freeman, L., & Werner, J. (2023). A survey of data security: Practices from cybersecurity and challenges of machine learning. doi:10.48550/ARXIV.2310.04513

Schmitt, M. (2024). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. doi:10.48550/ARXIV.2401.01342

Trim, P. R. J., & Lee, Y.-I. (2024). Advances in cybersecurity: Challenges and solutions. *Applied Sciences (Basel, Switzerland), 14*(10), 4300. doi:10.3390/app14104300

Widjaja, G. (2025). *Cybersecurity and data protection in the midst of the economy 5.0 digital transformation*. doi:10.5281/ZENODO.16731582