

Evaluating Cybersecurity Emergency Response Team Practices in Nigeria: Insights from National and Sectoral Cybersecurity Experts

Frank Torhile Hemen^{1*}, Steve Bassey²

¹Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

²Visiting Research Fellow-Centre for Cyberspace study studies, Nasarawa state university, Keffi, Nigeria

*Correspondence to: Frank Torhile Hemen, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria, E-mail: frank4tor@gmail.com

Received: July 28, 2026; Manuscript No: JETA-26-8727; Editor Assigned: August 07, 2026; PreQc No: JETA-26-8727 (PQ); Reviewed: August 19, 2026; Revised: August 24, 2026; Manuscript No: JETA-26-8727 (R); Published: October 27, 2026

Citation: Hemen FT, Bassey S (2026). Evaluating Cybersecurity Emergency Response Team Practices in Nigeria: Insights from National and Sectoral Cybersecurity Experts. J. Emerg. Trends Artif. Intell. Vol.1 Iss.1, October (2026), pp:27-39.

Copyright: © 2026 Frank Torhile Hemen, Steve Bassey. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

ABSTRACT

Cybersecurity Emergency Response Teams (CERTs) play a critical role in strengthening national cyber resilience through coordinated incident detection, analysis, response, recovery, and cyber threat intelligence. Despite Nigeria's growing investment in national cybersecurity institutions, empirical evidence regarding the operational maturity of its Cybersecurity Emergency Response Teams remains limited. This study evaluated the operational maturity of CERT practices in Nigeria using a convergent mixed-methods research design. Data were collected from 21 purposively selected participants comprising personnel from the Nigeria Computer Emergency Response Team (ngCERT), sectoral CERT representatives, constituency organizations, and international cybersecurity experts. Semi-structured interviews, structured capability assessment instruments, and document analysis were employed to generate qualitative and quantitative evidence. Qualitative data were analysed using Framework Analysis, while quantitative capability assessments were analysed using descriptive statistics. The evaluation was guided by ISO/IEC 27035:2023, the NIST Computer Security Incident Handling Guide (SP 800-61 Revision 3), and the FIRST CSIRT Services Framework.

The findings indicate that Nigerian CERTs demonstrate moderate operational maturity in incident detection, triage, and coordination but exhibit comparatively lower capability in proactive threat hunting, cyber threat intelligence integration, malware analysis, and post-incident organizational learning. Fragmented institutional coordination, limited information sharing, shortages of experienced cybersecurity professionals, inadequate funding, and insufficient technological infrastructure were identified as major constraints affecting operational effectiveness. The study further reveals that although Nigeria has established important institutional mechanisms for cybersecurity incident response, significant improvements in governance, workforce development, collaborative information sharing, and continuous capability improvement are necessary to achieve alignment with international best practices.

The study contributes to cybersecurity governance literature by providing an empirical evaluation of CERT operational maturity in Nigeria using internationally recognized incident response frameworks. The findings provide evidence-based recommendations for strengthening national cyber resilience, improving institutional coordination, and enhancing cybersecurity incident response capabilities across critical sectors.

Keywords: Cybersecurity Emergency Response Team; CERT; CSIRT; Operational Maturity; Incident Response; Cyber Resilience; Nigeria; Mixed Methods

INTRODUCTION

The rapid expansion of digital technologies has transformed the global socio-economic landscape by increasing dependence on interconnected information systems, cloud computing, artificial intelligence (AI), mobile technologies, and critical digital infrastructure. Governments, financial institutions, telecommunications providers, healthcare systems, and private enterprises increasingly rely on digital platforms to deliver essential services. While digital transformation has accelerated innovation and economic development, it has also significantly

expanded the cyber threat landscape. Cyberattacks such as ransomware, phishing, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), supply chain compromises, insider attacks, and business email compromise (BEC) have become more frequent, sophisticated, and disruptive, posing substantial risks to national security, economic stability, and public trust [1,2].

Globally, cybercrime has evolved into one of the most significant threats to digital economies, prompting governments and organizations to strengthen their

cybersecurity governance frameworks. Contemporary cybersecurity strategies increasingly emphasize cyber resilience rather than traditional perimeter defence, recognizing that cyber incidents cannot be completely prevented but can be effectively managed through coordinated preparedness, rapid detection, efficient response, timely recovery, and continuous organizational learning. Consequently, Cybersecurity Emergency Response Teams (CERTs), also known as Computer Security Incident Response Teams (CSIRTs), have become indispensable institutional mechanisms for coordinating responses to cybersecurity incidents and supporting national cyber resilience [3,4,5].

CERTs serve as specialized entities responsible for coordinating incident detection, analysis, containment, eradication, recovery, vulnerability management, threat intelligence sharing, digital forensics, cybersecurity awareness, and stakeholder collaboration. Beyond technical incident handling, mature CERTs facilitate strategic coordination among governments, regulatory agencies, private organizations, academia, and international cybersecurity communities. International frameworks such as the FIRST CSIRT Services Framework, ISO/IEC 27035:2023, and the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (SP 800-61 Revision 3) provide guidance for developing standardized, repeatable, and effective incident response capabilities that enhance organizational and national cyber resilience [3,4,5].

Several countries have established mature national CERT ecosystems that integrate operational response with cybersecurity governance and public-private collaboration. For example, the United States Cybersecurity and Infrastructure Security Agency (CISA), the Malaysian Computer Emergency Response Team (MyCERT), and other national CERTs have demonstrated the value of structured incident response processes, coordinated threat intelligence sharing, and continuous capability development in strengthening national preparedness against cyber threats. These international experiences illustrate that effective CERT operations depend not only on advanced technical infrastructure but also on clear governance arrangements, sustainable funding, skilled personnel, robust legal frameworks, and trusted collaboration among stakeholders.

Nigeria has experienced rapid growth in digital connectivity over the past decade, driven by expanding internet penetration, financial technology innovations, electronic commerce, digital government initiatives, and increasing adoption of cloud-based services. These developments have supported economic growth and digital inclusion but have simultaneously increased exposure to cyber threats targeting government institutions, financial systems, telecommunications infrastructure, businesses, and individual users. Phishing campaigns, ransomware attacks, identity theft, financial fraud, and attacks against critical information infrastructure continue to present significant challenges to national cybersecurity.

In response to these threats, Nigeria has introduced several institutional and policy measures aimed at strengthening national cybersecurity. The establishment of the Nigeria

Computer Emergency Response Team (ngCERT), alongside sector-specific incident response capabilities within banking, telecommunications, and government institutions, represents an important milestone in the country's cybersecurity governance framework [6,7,8,9]. In addition, regulatory agencies such as the National Information Technology Development Agency (NITDA), the Nigerian Communications Commission (NCC), and the Central Bank of Nigeria (CBN) have developed policies and sectoral guidelines to improve cybersecurity preparedness, incident reporting, and risk management [8,9,10].

Despite these initiatives, recurring cyber incidents continue to expose limitations in Nigeria's incident response capabilities. Reports from practitioners and policymakers suggest persistent challenges relating to fragmented coordination among CERTs, limited information sharing, inadequate technical infrastructure, shortages of skilled cybersecurity professionals, insufficient funding, and inconsistent implementation of internationally recognized incident response standards [2,11,12]. These constraints have implications for the timely detection, containment, and recovery of cybersecurity incidents, particularly within critical national information infrastructure.

Although cybersecurity has received increasing scholarly attention in Nigeria, much of the existing literature focuses on cybercrime, cybersecurity awareness, digital forensics, information security management, or national cybersecurity policy. Comparatively little empirical research has examined how CERTs operate in practice, how their operational maturity compares with international best practices, and what organizational and institutional factors influence their effectiveness. Furthermore, studies evaluating Nigerian CERTs using internationally recognized incident response frameworks remain limited. This lack of empirical evidence constrains efforts to strengthen incident response governance and develop evidence-based cybersecurity policies.

Against this background, this study evaluates Cybersecurity Emergency Response Team practices in Nigeria by drawing on perspectives from national CERT personnel, sectoral CERT representatives, constituency organizations, and international cybersecurity experts. The study integrates qualitative evidence from semi-structured interviews with quantitative capability assessments and documentary evidence to provide a comprehensive evaluation of current CERT practices. The evaluation is guided by three internationally recognized frameworks: ISO/IEC 27035:2023, the NIST Computer Security Incident Handling Guide (SP 800-61 Revision 3), and the FIRST CSIRT Services Framework.

These complementary frameworks provide benchmarks for assessing incident management processes, organizational preparedness, service maturity, and continuous improvement.

Specifically, the study addresses the following research questions:

What are the current operational practices of Cybersecurity Emergency Response Teams in Nigeria?
What organizational, technical, and institutional challenges affect CERT operations?

How effective are current CERT practices in mitigating and responding to cybersecurity incidents?

The findings are expected to contribute to both scholarship and practice. From an academic perspective, the study expands the limited empirical literature on CERT effectiveness in developing countries by providing an evidence-based assessment of Nigeria's incident response ecosystem. From a practical perspective, the findings provide policymakers, regulators, cybersecurity practitioners, and organizational leaders with insights that can inform improvements in governance, institutional coordination, workforce development, cyber threat intelligence, and operational capability. By identifying strengths, weaknesses, and opportunities for improvement, the study contributes to ongoing efforts to strengthen Nigeria's national cyber resilience and enhance the protection of critical information infrastructure.

LITERATURE REVIEW

Cybersecurity Emergency Response Teams and National Cyber Resilience

Cybersecurity Emergency Response Teams (CERTs), also referred to as Computer Security Incident Response Teams (CSIRTs), constitute the operational backbone of national cybersecurity incident management. Their responsibilities have expanded beyond traditional incident handling to include threat intelligence dissemination, vulnerability coordination, digital forensics, cyber threat analysis, stakeholder communication, and capacity building. Modern CERTs therefore function as technical, organizational, and strategic coordination centres that strengthen national cyber resilience.

International standards increasingly emphasise structured incident response as a prerequisite for effective cybersecurity governance. ISO/IEC 27035 provides guidance for the governance and management of information security incidents, while the NIST Computer Security Incident Handling Guide (SP 800-61 Revision 3) defines an incident response lifecycle encompassing preparation, detection and analysis, containment, eradication and recovery, and post-incident improvement. Similarly, the FIRST CSIRT Services Framework outlines the core operational services expected of mature incident response teams, including incident management, vulnerability management, situational awareness, and knowledge transfer. Together, these frameworks provide internationally recognised benchmarks for evaluating CERT maturity and operational effectiveness.

Research consistently shows that organisations implementing structured incident response frameworks experience improved coordination, faster recovery, and greater organisational resilience. Nevertheless, implementation remains uneven, particularly in developing countries where financial, technical, institutional, and human resource constraints limit operational maturity.

Current Perspectives on CERT Effectiveness

Recent literature demonstrates a shift in cybersecurity research from evaluating technical controls alone toward examining organisational capability, collaboration, governance, and resilience. Contemporary studies argue that CERT effectiveness depends on the interaction of technology, institutional arrangements, organisational culture, workforce competence, and external partnerships rather than on technical infrastructure alone.

A systematic literature review by Kassim, Li, and Arief highlighted that although national CSIRTs increasingly rely on public data, open-source intelligence (OSINT), and freely available analytical tools, empirical evidence explaining how these resources are integrated into operational practice remains fragmented [13]. The authors concluded that considerably more empirical investigations are required to understand how national CERTs actually perform incident response activities and utilise available intelligence resources.

Similarly, research on cybersecurity incident management has shown that many organisations attempt to align their practices with ISO/IEC 27035 but continue to encounter significant implementation challenges. These include inadequate post-incident learning, inconsistent documentation, weak organisational communication, and insufficient integration of lessons learned into future incident response planning. Such findings suggest that adopting international standards alone does not guarantee operational maturity; organisational capacity and governance are equally important determinants of effectiveness.

Another important dimension concerns cyber-threat information sharing. Mkuzangwe and Khan argued that effective information sharing among CERTs remains constrained by inconsistent adoption of common standards and interoperability mechanisms [14]. They observed that fragmented information-sharing practices reduce collective situational awareness and limit coordinated responses to emerging cyber threats. Their review reinforces the importance of trusted collaboration among organisational, sectoral, and national CERTs.

Cybersecurity Coordination in Nigeria

Nigeria has progressively strengthened its cybersecurity governance architecture through the establishment of the Nigeria Computer Emergency Response Team (ngCERT), sectoral CSIRTs, and the implementation of the National Cybersecurity Policy and Strategy [6,7]. These initiatives reflect increasing recognition of cybersecurity as a national security and economic development priority.

However, existing Nigerian literature suggests that institutional development has progressed more rapidly than operational evaluation. Ikuero's review of cybersecurity coordination in Nigeria found that while national structures for cybersecurity governance have been established, challenges remain regarding implementation, stakeholder coordination, public awareness, and institutional collaboration [6,11]. The review identified the establishment of ngCERT and sectoral

CSIRTs as significant milestones but emphasised the need for stronger operational coordination and continuous institutional development.

Similarly, studies examining Nigeria's broader cybersecurity framework indicate that although important legislative and policy reforms have been introduced, persistent gaps remain in incident disclosure practices, regulatory harmonisation, institutional coordination, and implementation capacity. These limitations reduce the effectiveness of national cybersecurity governance despite continued policy development.

The operational profile published by ngCERT demonstrates that the national CERT provides incident triage, coordination, technical assistance, vulnerability management, and communication with domestic and international stakeholders [7]. While these documented services indicate alignment with internationally recognised CERT functions, publicly available documentation provides limited empirical evidence regarding the effectiveness, maturity, and stakeholder perceptions of these services in practice. coordination, knowledge transfer, situational awareness, and quality management. Unlike purely technical frameworks, FIRST explicitly recognises collaboration and service maturity as key indicators of CERT effectiveness. Collectively, these frameworks provide complementary perspectives for evaluating operational capability, governance, organisational maturity, and stakeholder collaboration within Nigeria's CERT ecosystem.

Operational Maturity as a Framework for CERT Evaluation

Operational maturity has emerged as an important concept for evaluating the effectiveness of cybersecurity incident response capabilities. Unlike assessments that focus exclusively on technical performance, operational maturity considers the extent to which governance structures, organizational processes, human resources, technologies, collaboration mechanisms, and continuous improvement processes function together to support effective incident management.

A mature CERT demonstrates the ability to detect incidents rapidly, analyse threats accurately, coordinate responses efficiently, recover affected systems promptly, and systematically capture lessons learned for future improvement. Operational maturity therefore reflects not only technical competence but also institutional readiness and organizational resilience.

International evaluation models consistently identify several dimensions of CERT maturity:

- governance and leadership;
- incident management processes;
- technical capability;
- cyber threat intelligence;
- stakeholder collaboration;
- workforce competence;
- post-incident learning and continual improvement.

These dimensions form the conceptual basis for evaluating the operational maturity of Nigerian CERTs in this study.

International Standards Guiding CERT Operations

International standards provide structured guidance for developing and evaluating incident response capability.

ISO/IEC 27035:2023

ISO/IEC 27035 establishes principles and processes for information security incident management [4]. It emphasizes preparation, detection, reporting, assessment, response, recovery, and continual improvement. The standard also highlights the importance of clearly defined roles and responsibilities, incident communication procedures, documentation, and organizational learning.

NIST SP 800-61 Revision 3

The NIST Computer Security Incident Handling Guide provides practical guidance for establishing and managing incident response capabilities [15]. Revision 3 aligns incident response with the NIST Cybersecurity Framework (CSF) 2.0 and emphasizes governance, risk management, cyber resilience, coordinated response, and continuous capability improvement. The framework encourages organizations to integrate incident response into broader enterprise cybersecurity governance rather than treating it solely as a technical function.

FIRST CSIRT Services Framework

The FIRST CSIRT Services Framework identifies the core services expected of mature CERTs [16]. These include incident management, vulnerability management, situational awareness, knowledge transfer, coordination, trusted information sharing, and security quality management. Unlike technical standards that focus primarily on incident handling procedures, the FIRST framework provides a comprehensive operational model for evaluating organizational capability and service maturity.

The integration of these three frameworks provides a robust basis for assessing CERT operational maturity across strategic, organizational, technical, and collaborative dimension.

Cyber Threat Intelligence and Collaborative Incident Response

Cyber threat intelligence (CTI) has become one of the defining characteristics of mature incident response capability [5,17]. Modern CERTs increasingly rely on intelligence-driven approaches that integrate technical indicators, contextual information, and collaborative knowledge sharing to improve preparedness and response effectiveness.

Effective CTI enables organizations to identify emerging attack campaigns, detect vulnerabilities before exploitation, anticipate adversary behaviour, and prioritize defensive actions. However, successful intelligence sharing depends on trust, standardized reporting mechanisms, legal protections, and strong institutional relationships among stakeholders.

Several studies have shown that weak information-sharing cultures, fragmented governance arrangements, and concerns regarding confidentiality or reputational damage often reduce the effectiveness of national cybersecurity ecosystems [2,12].

Consequently, strengthening trusted collaboration has become a central objective of cybersecurity governance worldwide.

Cybersecurity Governance and CERT Development in Nigeria

Nigeria has made significant progress in strengthening its cybersecurity governance framework through the establishment of the Nigeria Computer Emergency Response Team (ngCERT), sector-specific CERTs, national cybersecurity policies, and institutional partnerships [6,7]. These developments have improved national awareness, incident coordination, and stakeholder engagement.

Despite these achievements, available evidence indicates that Nigerian CERTs continue to experience institutional and operational constraints. Recurring challenges include fragmented coordination among stakeholders, inconsistent incident reporting practices, shortages of experienced cybersecurity professionals, funding limitations, and inadequate access to advanced threat intelligence capabilities [2,11,12]. These factors affect the overall maturity and effectiveness of incident response activities.

Although existing Nigerian studies have examined cybercrime, cybersecurity awareness, digital forensics, and legal or policy issues, relatively few have evaluated the operational maturity of CERTs using internationally recognized assessment frameworks or integrated perspectives from multiple stakeholder groups.

Theoretical and Conceptual Foundation

This study is anchored on two complementary theoretical perspectives and three internationally recognized operational frameworks.

Socio-Technical Systems Theory

Socio-Technical Systems Theory argues that organizational performance is determined by the interaction between technological systems and social structures [14]. Applied to cybersecurity incident response, the theory suggests that effective CERT operations depend not only on technical infrastructure but also on governance, organizational culture, workforce competence, communication, and stakeholder collaboration.

Cyber Deterrence Theory

Cyber Deterrence Theory proposes that organizations reduce the likelihood and impact of cyberattacks by increasing the perceived costs and reducing the expected benefits available to malicious actors [18]. Effective incident detection, rapid containment, coordinated response, and resilient recovery contribute to deterrence by denial, making attacks less likely to succeed.

Operational Evaluation Framework

The study integrates three complementary operational frameworks:

- ISO/IEC 27035:2023, which provides guidance for information security incident management and continual improvement [3,4,5].
- NIST SP 800-61 Revision 3, which defines the incident response lifecycle and aligns incident handling with organizational cybersecurity governance.
- FIRST CSIRT Services Framework Version 2.1, which specifies the operational services and maturity characteristics expected of effective CERTs.
- The integration of these frameworks provides a comprehensive basis for evaluating operational maturity across governance, incident management, collaboration, technical capability, and organizational learning.

exclusively for academic research purposes and handled in accordance with accepted research ethics principles.

MATERIALS AND METHODS

Research Design

This study adopted a convergent mixed-methods research design to evaluate the operational maturity of Cybersecurity Emergency Response Teams (CERTs) in Nigeria [13]. A mixed-methods approach was considered appropriate because the evaluation of CERT effectiveness requires both quantitative measurement of operational capability and qualitative exploration of governance structures, organizational processes, stakeholder collaboration, and operational experiences. By integrating numerical capability assessments with rich qualitative evidence, the study provides a comprehensive understanding of CERT practices that would not be achievable through a single-method approach.

The convergent mixed-methods design enabled qualitative and quantitative data to be collected concurrently, analysed independently, and integrated during interpretation. This design enhances methodological triangulation, improves the credibility of findings, and allows convergence or divergence between different data sources to be identified. Such integration is particularly valuable when evaluating complex socio-technical systems such as national cybersecurity incident response.

The study is descriptive and evaluative in nature. Rather than testing causal relationships, it assesses the operational maturity of Nigerian CERTs against internationally recognised benchmarks. The evaluation criteria were derived from three complementary frameworks:

- ISO/IEC 27035:2023 (Information Security Incident Management)
- NIST Special Publication 800-61 Revision 3 (Computer Security Incident Handling)
- FIRST CSIRT Services Framework Version 2.1

These frameworks collectively informed the assessment of governance, preparedness, incident detection, response coordination, recovery, cyber threat intelligence, workforce capability, stakeholder collaboration, and continual improvement.

Study Population

The study population comprised organisations and professionals directly involved in cybersecurity incident response and governance within Nigeria. Participants were selected from institutions possessing practical responsibility for

cybersecurity operations, incident management, policy implementation, and cyber resilience.

The target population consisted of four stakeholder categories:

Stakeholder Group	Role
Nigeria Computer Emergency Response Team (ngCERT)	National incident coordination and cyber resilience
Sectoral CERTs	Incident response within banking, telecommunications, government and critical sectors
Constituency Organisations	Organisations interacting with CERTs during incident reporting and response
International Cybersecurity Experts	Independent perspectives on global CERT best practices Including multiple stakeholder groups allowed the study to capture diverse operational experiences and reduce institutional bias

Sampling Technique and Sample Size

Because the study focused on specialised cybersecurity professionals with extensive operational experience, purposive sampling was employed as the primary sampling strategy. Participants were selected based on demonstrated expertise in cybersecurity governance, digital forensics, incident response, cyber threat intelligence, vulnerability management, and national cybersecurity policy.

To identify additional participants with specialised knowledge that might not be readily accessible through formal organisational structures, snowball sampling was subsequently applied. Initial participants recommended other experts who met the inclusion criteria and possessed substantial operational experience.

A total of 21 participants were included:

Participant Category	Number	Percentage
ngCERT Personnel	4	19.00%
Sectoral CERT Representatives	6	28.60%
Constituency Organisations	8	38.10%
International Cybersecurity Experts	3	14.30%
Total	31	100.00%

Although relatively small, the sample size is appropriate for qualitative and mixed-methods research involving highly specialised expert participants. The emphasis of the study is analytical depth and operational insight rather than statistical generalisation.

- incident handling practices;
- organisational collaboration;
- cyber threat intelligence;
- workforce capability;
- institutional challenges;
- perceptions of operational effectiveness.

Data Collection Methods

Three complementary methods were employed.

Semi-Structured Interviews

Semi-structured interviews constituted the primary source of qualitative evidence. An interview guide containing standardised open-ended questions was developed from the three international incident response frameworks.

The interviews explored:

- governance arrangements;
- operational procedures;

The semi-structured format provided consistency while allowing participants to elaborate on practical experiences.

Structured Capability Assessment

A structured capability assessment instrument was designed using maturity indicators derived from ISO/IEC 27035:2023, NIST SP 800-61 Revision 3, and the FIRST CSIRT Services Framework.

Participants assessed operational capability across several dimensions using a five-point Likert maturity scale, where:

Score	Interpretation
1	Very Low Capability
2	Low Capability
3	Moderate Capability

4	High Capability
5	Very High Capability

Capability dimensions included:

- Governance
- Preparedness
- Detection and Analysis
- Containment and Recovery
- Threat Intelligence
- Collaboration
- Workforce Capability
- Post-Incident Learning

Document Analysis

To enhance methodological triangulation, documentary evidence was reviewed. Documents included:

- National cybersecurity policies
- Incident response procedures
- Regulatory guidelines
- CERT operational manuals
- Public advisories
- Strategic plans
- Institutional reports.

Document analysis enabled comparison between official procedures and participant experiences.

Data Analysis

Qualitative Analysis

Qualitative data were analysed using Framework Analysis, which is well suited to policy-oriented and applied research. The analysis followed five stages:

- Familiarisation with interview transcripts.
- Development of an analytical framework based on the research objectives and international standards.
- Systematic coding of qualitative data.
- Charting coded information into thematic matrices.
- Interpretation of patterns and relationships.
- The analytical framework remained sufficiently flexible to allow inductive themes to emerge.

Quantitative Analysis

Quantitative capability assessment data were analysed using descriptive statistics.

The following statistical measures were computed:

- frequencies
- percentages
- means
- capability maturity scores.

The quantitative findings were subsequently compared with qualitative evidence during triangulation.

Integration of Mixed-Methods Findings

A defining feature of the convergent design was the integration of qualitative and quantitative evidence. Integration occurred by:

- comparing interview narratives with capability assessment scores;
- validating emerging themes using documentary evidence;
- identifying areas of convergence and divergence.

This strengthened the robustness of the findings and enhanced confidence in the study's conclusions.

Trustworthiness and Research Quality

Several procedures enhanced methodological rigour.

Credibility

- Triangulation of interviews, surveys, and documents.
- Multiple stakeholder perspectives.
- International evaluation frameworks.

Dependability

- Standardised interview protocol.
- Consistent coding procedures.
- Transparent analytical framework.

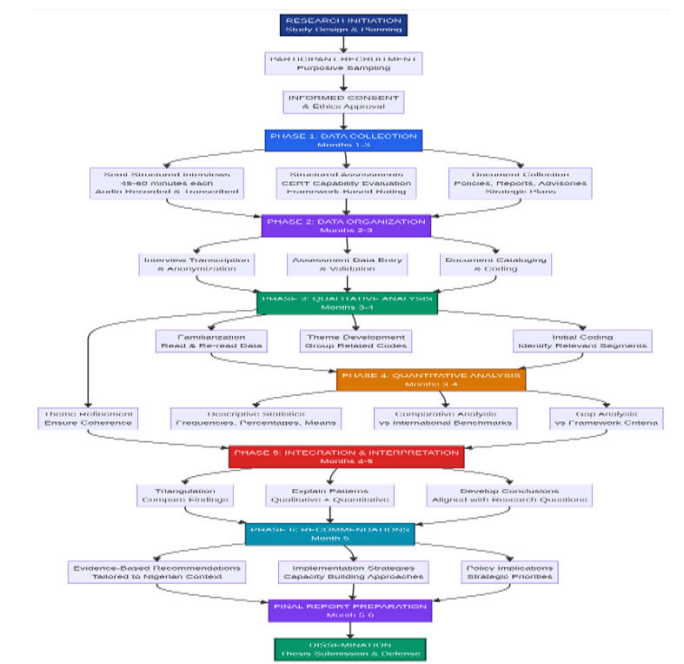
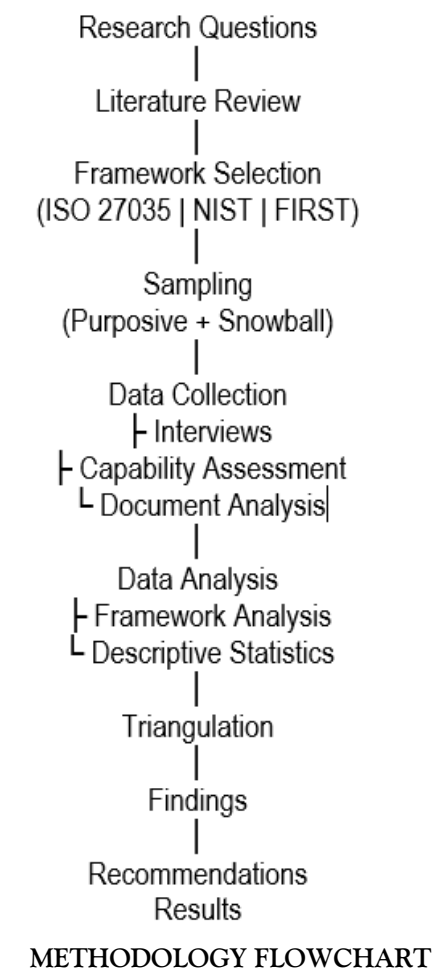
Confirmability

- Systematic documentation of analytical decisions.
- Evidence-based interpretation.
- Audit trail of coding procedures.

Transferability

Although context-specific, the methodological framework may be adapted for evaluating CERTs in other developing countries.

Proposed Methodology Workflow Figure



Research Methodology Flowchart showing the six phases of research execution from initiation through dissemination.

RESULTS

Respondent Characteristics

Twenty-one cybersecurity professionals participated in the study. The participants represented four stakeholder groups comprising personnel from the Nigeria Computer Emergency Response Team (ngCERT), sectoral CERTs, constituency organizations, and international cybersecurity experts. Their diverse professional backgrounds provided multiple perspectives on the operational practices and maturity of CERTs in Nigeria.

Category	Frequency	Percentage (%)	Average Years of Experience
ngCERT Personnel	4	19	8.5
Sectoral CERT Representatives	6	28.6	7.2
Constituency Organizations	8	38.1	6.4
International Experts	3	14.3	12
Total	21	100	8.1

Table 1: Participants Distribution

The respondents possessed substantial professional experience in cybersecurity incident management, cyber defence, digital forensics, information security governance, and cybersecurity policy implementation. Their combined expertise provided an appropriate basis for evaluating the operational maturity of Nigerian CERTs.

Operational Maturity Assessment

Capability assessment results indicate that Nigeria's CERT ecosystem demonstrates moderate operational maturity overall. Participants consistently acknowledged notable progress in preparedness, incident detection, and coordination, while identifying important gaps in advanced technical capabilities, cyber threat intelligence, and post-incident learning

Capability Dimension	Maturity Level	Interpretation
Governance	Moderate	Institutional structures established but coordination requires strengthening
Preparedness	High	Policies, plans, and awareness programmes largely operational

Incident Detection	High	Effective monitoring and incident identification mechanisms
Incident Coordination	Moderate-High	Coordination exists but remains fragmented across sectors
Threat Intelligence	Moderate	Intelligence capability developing but limited integration
Digital Forensics	Moderate	Available but constrained by skills and resources
Malware Analysis	Moderate	Limited advanced analytical capability
Recovery and Lessons Learned	Moderate	Improvement processes inconsistent
Continuous Improvement	Moderate	Need for structured capability development

Table 2: Operational Capability Assessment

Overall, respondents perceived Nigeria's CERT ecosystem as operationally functional but not yet fully aligned with international best practices.

Strengths of Current CERT Practices

Analysis of interview data identified several recurring strengths.

Institutional Development

Participants consistently recognised that the establishment of ngCERT and sector-specific CERTs has significantly strengthened national cybersecurity coordination. The existence of dedicated incident response institutions has improved reporting mechanisms, coordination during incidents, and stakeholder awareness.

Incident Detection and Response

Most participants indicated that incident detection and initial response activities have improved considerably compared with previous years. Standard operating procedures for incident reporting and coordination are increasingly institutionalised, particularly within highly regulated sectors.

Stakeholder Awareness

Respondents acknowledged increased cybersecurity awareness among government agencies, financial institutions, telecommunications providers, and selected critical infrastructure operators. Awareness programmes, advisories, and coordinated outreach were viewed as important contributions to national cyber resilience.

Major Operational Challenges

Despite these strengths, participants identified several persistent constraints.

Fragmented Institutional Coordination

The most frequently reported challenge concerned coordination among government institutions, sectoral CERTs, regulators, and private-sector organizations. Participants observed that overlapping institutional mandates, inconsistent reporting channels, and varying operational procedures

sometimes delayed coordinated responses to significant cyber incidents.

Workforce Capacity

Respondents highlighted shortages of experienced cybersecurity professionals, particularly in specialist areas such as digital forensics, malware reverse engineering, cyber threat intelligence, and incident coordination. Limited opportunities for advanced training and professional certification were perceived as major barriers to improving operational maturity.

Resource Constraints

Many participants reported that limited financial resources, outdated technological infrastructure, and insufficient investment in advanced cybersecurity tools constrained CERT operations. These resource limitations affected threat intelligence, automation, digital forensic capability, and continuous improvement initiatives.

Information Sharing

Although information sharing has improved, participants noted that organizations remain hesitant to disclose cyber incidents because of concerns about confidentiality, reputational impact, and regulatory consequences. These concerns reduce collective situational awareness and hinder collaborative incident response.

Comparative Capability Analysis

A comparison of the assessed capability dimensions indicates clear variation across operational functions.

- Preparedness 3.5 out of 5.0
- Detection 3.2
- Recovery,cont 2.8
- Continuous Improvement 2.1

Comparative Operational Capability Across CERT Functions

The illustrates that preparedness and detection represent the strongest areas of performance, while cyber threat intelligence, advanced technical analysis, and continuous improvement remain comparatively weaker. These patterns are consistent with participants' qualitative accounts and documentary evidence.

Integration of Qualitative and Quantitative Findings

The convergent mixed-methods design enabled triangulation of interview evidence, capability assessments, and documentary analysis. Across all three sources, several consistent themes emerged:

- Nigeria has established a functional institutional framework for cybersecurity incident response.
- Preparedness and incident detection are comparatively mature.
- Coordination mechanisms have improved but remain uneven across sectors.
- Threat intelligence, advanced malware analysis, and digital forensics require further development.

Sustainable workforce development, improved governance, and stronger information sharing are essential to enhance operational maturity.

The convergence of qualitative and quantitative findings strengthens confidence in the overall conclusion that the Nigerian CERT ecosystem has established a solid institutional foundation but has not yet achieved the level of operational maturity reflected in leading international CERT models.

RECOMMENDATION

Overview of Findings

This study evaluated the operational maturity of Cybersecurity Emergency Response Team (CERT) practices in Nigeria using a convergent mixed-methods approach guided by internationally recognised incident response frameworks. The findings indicate that Nigeria has established a functional institutional foundation for cybersecurity incident response through the Nigeria Computer Emergency Response Team (ngCERT) and selected sectoral CERTs. Participants consistently recognised improvements in incident preparedness, detection, coordination, and cybersecurity awareness, suggesting that significant progress has been achieved in developing a national cybersecurity governance architecture. However, the results also demonstrate that the operational maturity of the Nigerian CERT ecosystem remains moderate, with notable weaknesses in cyber threat intelligence integration, advanced malware analysis, digital forensics, post-incident organisational learning, and continuous capability improvement. These findings directly address the study's research questions by showing that while operational structures are in place, important organisational and technical challenges continue to limit overall effectiveness.

Current Operational Practices of Nigerian CERTs

The first research question sought to evaluate the current operational practices of Cybersecurity Emergency Response Teams in Nigeria. The findings indicate that Nigerian CERTs have adopted many of the core operational functions expected of contemporary incident response organisations, including incident reporting, triage, technical coordination, stakeholder communication, vulnerability notification, and awareness

activities. Participants observed that these functions have become increasingly structured, particularly within highly regulated sectors such as banking and telecommunications.

The capability assessment further indicates that preparedness and incident detection represent the strongest dimensions of current practice. This suggests that investments in policy development, institutional structures, awareness programmes, and basic incident response processes have produced measurable improvements in national cybersecurity preparedness. Nevertheless, the assessment also demonstrates that higher-level capabilities including proactive threat hunting, cyber threat intelligence integration, advanced malware analysis, digital forensic capability, and systematic post-incident review remain comparatively underdeveloped. This imbalance indicates that current operational practices continue to emphasise reactive incident response rather than intelligence-driven and resilience-oriented cybersecurity management.

Organisational and Institutional Challenges

The second research question examined the challenges affecting CERT operations. The findings reveal that organisational and institutional factors exert a substantial influence on operational effectiveness. Participants consistently identified fragmented inter-agency coordination, inconsistent information sharing, shortages of experienced cybersecurity professionals, inadequate funding, and limited technological resources as the principal barriers to effective incident response.

These findings reinforce the understanding that cybersecurity capability is not determined solely by technical infrastructure. Rather, effective incident response depends upon governance arrangements that promote coordination, accountability, and timely information exchange across multiple stakeholders. Although Nigeria has established several institutions responsible for cybersecurity governance, participants indicated that overlapping responsibilities and inconsistent operational procedures sometimes reduce the efficiency of coordinated incident response.

Workforce development emerged as another critical challenge. Respondents highlighted persistent shortages of specialised expertise in cyber threat intelligence, malware reverse engineering, digital forensics, and advanced incident analysis. This suggests that sustainable investment in professional training, certification, mentoring, and retention strategies is essential for strengthening national incident response capability. The findings further indicate that technological investments alone are unlikely to achieve substantial improvements without corresponding investments in human capital and institutional capacity.

Operational Effectiveness of Nigerian CERTs

The third research question evaluated the effectiveness of current CERT practices in mitigating and responding to cybersecurity incidents. The findings demonstrate that Nigerian CERTs have established a credible operational foundation capable of supporting national incident response activities. Participants acknowledged improvements in incident

coordination, technical support, stakeholder engagement, and cybersecurity awareness compared with previous years.

However, effectiveness varied considerably across operational dimensions. Capabilities associated with preparedness and initial incident response received relatively stronger assessments, whereas proactive cyber threat intelligence, advanced analytical capability, and organisational learning received comparatively lower ratings. This pattern indicates that Nigerian CERTs have developed essential operational functions but have not yet achieved the level of maturity associated with leading international CERT organisations.

Importantly, participants emphasised that operational effectiveness should not be evaluated solely by the number of incidents handled or technical services delivered. Rather, effective CERT operations require continuous adaptation to an evolving threat environment through structured governance, collaborative information sharing, workforce development, technological innovation, and systematic post-incident learning. The findings therefore support the view that operational maturity is a multidimensional construct encompassing technical, organisational, institutional, and collaborative capabilities.

Theoretical Contributions

The study contributes to the literature on cybersecurity governance by demonstrating the usefulness of an operational maturity perspective for evaluating CERT effectiveness within developing digital economies. Whereas many previous studies have focused on cybercrime trends, legal frameworks, or cybersecurity awareness, this research adopts a multidimensional evaluation framework integrating governance, organisational capability, technical competence, workforce development, stakeholder collaboration, and continuous improvement.

A further contribution lies in the integration of qualitative interviews, capability assessments, and documentary analysis. This convergent mixed-methods approach provides a richer understanding of operational capability than studies relying exclusively on surveys or document reviews. By combining multiple sources of evidence, the study demonstrates how technical performance, governance arrangements, and organisational processes interact to shape the effectiveness of national incident response systems.

Practical and Policy Implications

The findings have several implications for policymakers, regulators, and cybersecurity practitioners.

For government institutions, the results highlight the importance of strengthening institutional coordination among ngCERT, sectoral CERTs, law enforcement agencies, and operators of Critical National Information Infrastructure [6,19]. Harmonised governance arrangements, standardised reporting procedures, and trusted information-sharing mechanisms would improve national situational awareness and support coordinated responses to large-scale cyber incidents [20,21].

For CERT organisations, the findings indicate that future investments should prioritise cyber threat intelligence integration, advanced digital forensics, malware analysis, proactive threat hunting, and structured post-incident review [3,4,5]. These capabilities are essential for progressing from reactive incident handling to intelligence-driven cybersecurity operations [22,23].

For private organisations and critical infrastructure operators, stronger collaboration with national and sectoral CERTs, timely incident reporting, participation in information-sharing initiatives, and alignment with recognised incident response standards will contribute to improved organisational and national cyber resilience.

DISCUSSION

Overall, the discussion demonstrates that Nigeria has made significant progress in establishing institutional mechanisms for cybersecurity incident response. Nevertheless, the operational maturity of the national CERT ecosystem remains at an intermediate stage of development. Future improvements require coordinated investments in governance, workforce capability, cyber threat intelligence, advanced technical capacity, collaborative information sharing, and continuous organisational learning. Addressing these priorities will not only strengthen the effectiveness of Nigerian CERTs but also enhance national cyber resilience and provide a stronger foundation for protecting critical digital infrastructure against increasingly sophisticated cyber threats.

CONCLUSION

Cybersecurity incident response has become an indispensable component of national security, digital governance, and economic resilience in an era characterised by increasingly sophisticated cyber threats. This study evaluated the operational maturity of Cybersecurity Emergency Response Team (CERT) practices in Nigeria using a convergent mixed-methods design informed by ISO/IEC 27035:2023, NIST Special Publication 800-61 Revision 3, and the FIRST CSIRT Services Framework Version 2.1. By integrating qualitative interviews, structured capability assessments, and documentary analysis, the study provides one of the most comprehensive empirical assessments of Nigeria's CERT ecosystem to date.

The findings indicate that Nigeria has established an important institutional foundation for cybersecurity incident response through the Nigeria Computer Emergency Response Team (ngCERT) and selected sector-specific CERTs. Progress is evident in incident preparedness, detection, coordination, and stakeholder awareness, demonstrating the positive impact of national cybersecurity policies and institutional reforms. These achievements represent important milestones in strengthening the country's cyber resilience.

Nevertheless, the study also demonstrates that the operational maturity of the Nigerian CERT ecosystem remains at an intermediate stage of development. Significant capability gaps persist in cyber threat intelligence integration, advanced malware analysis, digital forensics, proactive threat hunting,

post-incident organisational learning, and continuous capability improvement. Furthermore, fragmented institutional coordination, limited information sharing, shortages of highly skilled cybersecurity professionals, and resource constraints continue to reduce operational effectiveness.

Overall, the findings demonstrate that strengthening Nigeria's cybersecurity incident response capability requires a balanced strategy integrating governance reform, technical capability enhancement, workforce development, collaborative intelligence sharing, sustainable investment, and continuous organisational learning. Such an approach will not only improve CERT effectiveness but also strengthen national cyber resilience, enhance the protection of critical information infrastructure, and support sustainable digital transformation.

Finally, this study contributes to cybersecurity governance literature by providing an empirically grounded operational maturity assessment of CERT practices in a developing digital economy. The proposed evaluation framework offers a practical model that may be adapted by other countries seeking to strengthen national incident response capabilities and benchmark their CERT operations against internationally recognised standards.

PRACTICAL IMPLICATIONS

Implications for Government

The findings underscore the need for stronger institutional coordination among ngCERT, sectoral CERTs, regulatory agencies, law enforcement organisations, and operators of Critical National Information Infrastructure (CNII). Government should prioritise the harmonisation of cybersecurity governance structures, establish standardised national incident reporting mechanisms, strengthen public-private partnerships, and expand investment in advanced cybersecurity infrastructure. Continued alignment with international incident response standards will further improve national cyber resilience.

Implications for ngCERT

As the national cybersecurity coordination body, ngCERT should continue transitioning from predominantly reactive incident handling towards intelligence-driven cybersecurity operations. This includes strengthening cyber threat intelligence capabilities, expanding digital forensic laboratories, improving malware analysis, institutionalising post-incident reviews, and integrating automation technologies such as Security Orchestration, Automation and Response (SOAR) and Extended Detection and Response (XDR). Investment in continuous professional development and international collaboration should remain strategic priorities.

Implications for Sectoral CERTs

Sectoral CERTs should strengthen alignment with internationally recognised frameworks by institutionalising structured incident response procedures, conducting regular cyber exercises, enhancing vulnerability management processes,

and participating actively in trusted information-sharing communities. Greater collaboration with ngCERT and cross-sector coordination mechanisms will improve collective preparedness and response effectiveness.

Implications for Organisations

Public and private organisations interacting with CERTs should strengthen internal cybersecurity governance, establish formal incident reporting procedures, participate in cyber threat intelligence sharing initiatives, and integrate internationally recognised incident response standards into organisational cybersecurity programmes. Timely incident reporting, collaborative learning, and organisational preparedness will improve both institutional resilience and national cybersecurity capability.

Policy Recommendations

Based on the findings, the following strategic actions are recommended:

- Develop a national CERT maturity assessment framework aligned with ISO/IEC 27035, NIST SP 800-61 Revision 3, and the FIRST CSIRT Services Framework.
- Establish a secure national cyber threat intelligence exchange platform connecting ngCERT, sectoral CERTs, regulators, and critical infrastructure operators.
- Increase investment in specialised workforce development through professional certification, postgraduate education, and international technical exchanges.
- Institutionalise periodic national cyber resilience exercises involving government agencies, critical infrastructure providers, academia, and industry.
- Strengthen legal and regulatory mechanisms that encourage trusted information sharing while protecting organisational confidentiality and sensitive operational data.
- Introduce performance measurement indicators for evaluating operational maturity and continual improvement within national and sectoral CERTs.

Study Limitations

Several limitations should be considered when interpreting the findings.

First, the study employed purposive and snowball sampling involving twenty-one experienced cybersecurity professionals. Although participants represented key stakeholder groups with substantial expertise, the relatively small sample limits the statistical generalisability of the findings.

Second, the capability assessment relied partly on participants' professional judgements and organisational experiences. While triangulation with interviews and documentary evidence enhanced credibility, some responses may reflect subjective institutional perspectives.

Third, the study focused primarily on ngCERT and selected sectoral CERTs. Consequently, the findings may not fully represent every cybersecurity incident response capability operating within Nigeria.

Finally, cybersecurity is characterised by rapid technological and organisational change. Emerging technologies, evolving threat actors, and ongoing policy reforms may alter CERT operational maturity over time, necessitating periodic reassessment.

FUTURE RESEARCH

The present study provides several opportunities for future investigation.

Longitudinal studies should examine how CERT operational maturity evolves following policy reforms, technological investments, and institutional capacity-building initiatives. Such research would provide valuable evidence regarding the sustainability of cybersecurity governance improvements.

Comparative studies involving multiple African countries would facilitate regional benchmarking and identify transferable governance practices for strengthening national cyber resilience across developing digital economies.

Future research should also employ larger quantitative datasets and advanced statistical techniques to examine relationships among governance quality, workforce capability, cyber threat intelligence, stakeholder collaboration, and operational effectiveness.

Emerging technologies including artificial intelligence, machine learning, generative AI, SOAR, XDR, and autonomous cyber defence also warrant investigation to determine how they influence incident response capability, organisational resilience, and CERT operational maturity.

Finally, future evaluations should investigate the perspectives of policymakers, law enforcement agencies, critical infrastructure operators, and private-sector organisations to develop a more comprehensive understanding of the broader cybersecurity governance ecosystem.

ETHICAL CONSIDERATIONS

Ethical principles were observed throughout the study.

Participants:

- received detailed information about the research;
- provided informed consent;
- participated voluntarily;
- retained the right to withdraw without penalty.

Confidentiality was maintained by anonymising interview transcripts and reporting findings in aggregated form. Data were stored securely and used exclusively for academic purposes.

ACKNOWLEDGEMENTS

The author expresses sincere appreciation to all cybersecurity professionals, CERT personnel, sectoral representatives, constituency organizations, and international experts who voluntarily participated in this study. Their professional insights and practical experiences provided the empirical foundation for this research.

CONFLICT OF INTEREST

The author declares that there are no competing financial or non-financial interests that could have influenced the conduct or reporting of this research.

Data Availability Statement

The qualitative interview data generated during this study are not publicly available because they contain information that could compromise participant confidentiality. Aggregated data supporting the findings are available from the corresponding author upon reasonable request and subject to ethical considerations.

REFERENCES

1. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024.
2. INTERPOL. African cyber threat assessment report 2024.
3. FIRST. CSIRT Roles and Competences (Addendum Version 0.9).
4. International Organization for Standardization. ISO/IEC 27035:2023 Information security, cybersecurity and privacy protection Guidance on managing information security incidents.
5. Nelson A, Rekhi S, Souppaya M, Scarfone K. Incident response recommendations and considerations for cybersecurity risk management. NIST special publication. 2025 Apr;800.
6. Office of the National Security Adviser. National Cybersecurity Policy and Strategy.
7. Nigeria Computer Emergency Response Team. National Cybersecurity Advisories and Incident Response Publications.
8. Central Bank of Nigeria. (2022). Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions
9. Nigerian Communications Commission. Annual Cybersecurity Report.
10. National Information Technology Development Agency. National Digital Economy and Cybersecurity Initiatives.
11. CSEAN. Cybersecurity society of Africa threat assessment.
12. Kincl, T., Čech, P., & Novotný, V. Human factors in cybersecurity incident management. *Cybersecurity and Human Factors*, 12(3), 234–251.
13. Kassim SR, Li S, Arief B. The Use of Public Data and Free Tools in National CSIRTs' Operational Practices: A Systematic Literature Review. *arXiv preprint arXiv:2306.07988*. 2023.
14. Malatji M, Marnewick A, von Solms S. Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*. 2020;95:101846.
15. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0.
16. Forum of Incident Response and Security Team. Team Types Within the Context of Services Frameworks (Version 1.1).
17. Forum of Incident Response and Security Teams. CSIRT Services Framework (Version 2.1).
18. Cybersecurity and Infrastructure Security Agency. Cybersecurity Performance Goals.
19. Cybersecurity and Infrastructure Security Agency. Cybersecurity Incident and Vulnerability Response Playbooks.
20. Carnegie Mellon University Software Engineering Institute. CERT Division Overview.
21. BakerHostetler. 2024 data security incident response report.
22. Frisby, R. Global cybersecurity exposure assessment. *Password Managers*.
23. Makoshi, A. Cybersecurity challenges in Nigeria's financial sector. *African Journal of Information Security*, 4(1), 78–95.