ANUK COLLEGE OF PRIVATE SECTOR Accounting Journal

VOL. 2 NO. 3 OCTOBER, 2025

A Publication of College of Private Sector Accounting
ANAN University Kwall, Plateau State, Nigeria.

Published October, 2025.

Web Address: https://www.anukpsaj.com, Email: anukpsaj@gmail.com

Printed by:
MUSSAB Printers,
NB, 9 Muri road by gwari road, Kaduna State, Nigeria.
Phone contact: 07038776658,
Email: meetsuleiman009@gmail.com

Structure of Manuscript

Manuscripts must be typed on A size paper with 12 font size (Times New Roman), not more than 15 pages, double-spaced, and in English. The file name should include the corresponding author's name and a keyword from the title.

Sequence of Manuscript

I. Title page
II. Abstract (150-250 words)
III. Keywords (3-5)
IV. Introduction
V. Literature Review
VI. Methodology
VII. Results and Discussion
VIII. Conclusion and Recommendations
IX. References (APA 7th Edition)
X. Appendices (if necessary)
XI. Author Biographies (optional)

Plagiarism Policy

ANUK is committed to maintaining high standards through an indept peer-review process with sound ethical policies. Any infringements of professional ethical codes, such as plagiarism; including self-plagiarism, fraudulent use of data, are seriously frowned at by the journal with zero tolerance.

ANUK implements the Code of Conduct of the Committee on Publication Ethics (COPE), and uses the COPE Flowcharts for Resolving cases of suspected plagiarism or any publication misconduct.

In order to avoid plagiarism cases with the ANUK, the following guidelines must be strictly adhered to by authors:

Authors should ensure that they have written entirely original works, and if authors have used the work and/or words of others that this has been appropriately cited or quoted.

An author should not, in general, publish manuscripts describing essentially the same research in more than one journal or primary publication. Submitting the same manuscript to more than one journal concurrently constitutes unethical publishing behavior and is unacceptable.

Proper acknowledgment of the work of others must always be adhered to. Authors should cite publications that have been influential in determining the nature of the reported work.

Editorial Team

TABLE OF CONTENT

TABLE OF CONTENT

EFFECT OF CYBERSECURITY INCIDENT PREPAREDNESS ON THE EFFICACY OF DIGITAL FORENSIC INVESTIGATIONS IN NIGERIAN FINANCIAL INSTITUTIONS

ADEGBEMI TITILAYO ADESOLA

SUNDAY MLANGA

GANIYU A. MUSTAPHA

ABSTRACT

Cybersecurity preparedness in Nigerian financial institutions faces persistent challenges from evolving cyber threats, inadequate infrastructure, and human-factor vulnerabilities that undermine the effectiveness of digital forensic investigations. This study investigates the effect of incident response planning, cybersecurity awareness and training, infrastructure investment, threat monitoring capability, and communication and coordination mechanisms on the efficacy of digital forensic investigations across banks, fintech firms, and insurance companies in Nigeria. The sample consisted of 120 cybersecurity and digital forensic professionals. Using a quantitative survey design and multiple linear regression, the study examines the influence of the five preparedness dimensions on forensic investigation outcomes. The findings reveal that all five factors significantly enhance forensic efficacy, collectively improving the speed, accuracy, and legal defensibility of digital investigations ($p < 0.05$). Incident response planning emerged as the strongest predictor ($\beta = 0.328$), followed by cybersecurity awareness and training ($\beta = 0.290$), threat monitoring capability ($\beta = 0.267$), infrastructure investment ($\beta = 0.246$), and communication and coordination mechanisms ($\beta = 0.218$). Grounded in the Forensic Readiness Model and Socio-Technical Systems Theory, the study recommends institutionalizing structured incident response frameworks, conducting regular cybersecurity training, and investing in forensic infrastructure and real-time monitoring to enhance cyber resilience and digital forensic capacity in Nigeria's financial sector.

Key words: Communication Coordination Mechanism, Cybersecurity Awareness and Training, Incident Response Planning, Infrastructure Investment, Threat Monitoring Capability

1.0 Introduction

The efficacy of digital forensic investigations has become a pivotal issue in global cybersecurity as cybercrimes escalate in frequency and complexity. Financial institutions, in particular, face persistent threats such as data breaches, identity theft, ransomware, and complex financial fraud schemes. Achieving high levels of forensic efficacy reflected in accuracy, timeliness, evidence integrity, and admissibility has therefore become essential for effective incident response, regulatory compliance, legal enforcement, and organizational resilience. Recent scholarship highlights the contribution of advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) to this goal. By improving threat detection and classification, AI and ML significantly enhance the speed and precision of forensic investigations, enabling faster responses to cyber incidents and reducing exposure to risk (Fakiha, 2023). Global institutions including INTERPOL and the FBI advocate embedding digital forensics within national and corporate cybersecurity strategies. For example, the FBI's Cyber Division integrates cyber incident readiness with forensic analysis to identify and prosecute cybercriminals swiftly. Similarly, financial regulators in countries such as the U.S., UK, and Australia have introduced cyber incident preparedness policies to ensure effective forensic tracking of breaches (Hassan et al., 2024; Serketzis et al., 2019).

Across Africa, the growing sophistication of digital crimes exposes weaknesses in traditional security measures, underscoring the need for robust

cybersecurity frameworks, especially in rapidly urbanising regions like Smart Cities (Ahmad et al., 2024). Although South Africa is among the continent's most advanced economies, persistent gaps remain in countering complex threats (Gcaza & Von Solms, 2017). A systematic, collaborative model of cybersecurity information sharing enabling diverse stakeholders to exchange actionable threat intelligence has been proposed to bolster national resilience (Mutemwa et al., 2017).

In Nigeria, the efficacy of digital forensic investigations is constrained by rising cyber threats, including phishing, malware, and unauthorised access, as financial institutions digitise their operations. Despite the cybersecurity framework of the Central Bank of Nigeria (CBN), recent high-profile cyberattacks reveal systemic weaknesses. While some institutions have established response teams and forensic units, their effectiveness is limited by inadequate infrastructure, slow response times, insufficiently trained staff, and poor documentation practices. Progress has been made in adopting advanced security technologies and staff training, yet stronger regulatory frameworks and greater customer-awareness initiatives remain necessary (Reis et al., 2024).

Linking cybersecurity incident preparedness to the efficacy of digital forensic investigations is increasingly emphasised in contemporary research. Proactive measures such as threat identification, detailed response plans, and continuous training can improve the precision, timeliness, and reliability of forensic outcomes (Serketzis et al., 2019). Conversely, insufficient preparedness often results in delayed action, compromised evidence, and failed investigations (Hassan et al., 2024; Sabillon et al., 2017). However, empirical studies in Nigeria rarely examine how preparedness directly shapes investigative outcomes. Most research either focuses on cybersecurity awareness or digital forensic techniques in isolation. Conceptually, little is known about how elements of preparedness including infrastructure, human resource readiness, and procedural frameworks interact to influence forensic results. Empirically, studies remain largely qualitative, lacking data-driven models to measure these relationships. Practically, Nigerian financial institutions still grapple with poor documentation of cyber incidents, uncoordinated responses, and weak evidence management, undermining the objectives of forensic investigations. This study seeks to bridge these gaps by empirically examining how cybersecurity incident preparedness affects the efficacy of digital forensic investigations in Nigerian financial institutions. Specifically, it aims to evaluate the effect of incident response planning on forensic efficacy; assess the influence of cybersecurity awareness and employee training on investigative outcomes; determine the impact of cybersecurity infrastructure investment on forensic capacity; examine the effect of threat detection and monitoring capabilities on forensic investigations; and analyse the role of communication and coordination mechanisms in enhancing forensic investigation effectiveness. Accordingly, the study tests the following null hypotheses:

H_o1: Incident response planning has no significant effect on the efficacy of digital forensic investigations in Nigerian financial institutions.

H_o2: Cybersecurity awareness and training have no significant effect on the efficacy of digital forensic investigations.

H_o3: Investment in cybersecurity infrastructure does not significantly affect the efficacy of digital forensic investigations.

H_o4: Threat detection and monitoring capabilities do not significantly influence the efficacy of digital forensic investigations.

H_o5: Communication and coordination mechanisms during cyber incidents do not significantly affect forensic investigation outcomes.

2.0 Literature Review

2.1.1 Digital Forensic Investigations

Digital forensic investigations involve systematically identifying, collecting, analysing, and preserving electronic evidence for legal, policy, or disciplinary purposes, following strict protocols to ensure evidence integrity and admissibility (Raghavan, 2012). This includes network, mobile, and cloud forensics, each requiring specialised skills. Their effectiveness depends on organisational preparedness trained staff, forensic tools, and standard procedures for evidence handling (Allah Rakha, 2024). Timely access to unaltered data, secure chain of custody, and proper documentation support incident attribution and legal outcomes (Mohammed et al., 2016). Poorly executed processes risk evidence exclusion and weaken deterrence (Ay, 2020). In Nigeria, many financial institutions lack in-house forensic capacity or rely on ad hoc approaches, undermining investigation quality (Mustapha & Sinha, 2024). Strengthening processes is vital for cyber accountability and a resilient financial system.

2.1.2 Incident Response Planning

Incident response planning creates structured processes to detect, manage, and recover from cyber incidents, ensuring timely, coordinated responses and preserving evidence (Nelson et al., 2025). Plans typically define roles, communication, and escalation paths. Effective planning accelerates threat containment and systematic evidence collection, crucial for legal and post-incident analysis (Werlinger et al., 2010). Without it, organisations risk inconsistent responses, evidence loss, and delays (Okoye et al., 2024). In Nigeria, weak frameworks compromise investigations and cyber resilience (Dawodu et al., 2023).

2.1.2.1 Cybersecurity Awareness and Training

Awareness and training educate employees on threats, preventive behaviours, and responses to reduce human error the weakest cybersecurity link (Zhang et al., 2021). Effective programs improve evidence preservation and prompt reporting, promoting a culture of forensic readiness (Sabillon et al., 2019; Nasir, 2023). In Nigeria, training is inconsistent, lacking standard curricula and stakeholder engagement, hampering incident reporting and traceability (Nwachukwu & Hassan, 2023). Consistent, role-specific training strengthens preparedness and outcomes.

2.1.2.2 Investment in Cybersecurity Infrastructure

Cybersecurity infrastructure investments firewalls, IDS, SIEM, and encryption support defence and forensic readiness (Arpilleda, 2023). Robust tools enable real-time detection, evidence capture, and automated responses, essential for accuracy and legal admissibility (Zaman & Mazinani, 2023). Poor investment leads to blind spots and incomplete forensic trails. While Tier-1 Nigerian banks invest significantly, smaller institutions face gaps impacting efficacy (Balogun & Eze, 2023). Budget prioritisation is key for resilience.

2.1.2.3 Threat Detection and Monitoring

Continuous monitoring identifies unusual activities or breaches, shaping the speed and accuracy of responses (Sankaram et al., 2024). Early detection allows prompt capture of volatile data and preserves evidence (Camacho, 2024). Automated systems like SIEM correlate logs and detect attack patterns, aiding post-incident forensics (Adeoye & Nnaji, 2022). Nigerian institutions vary widely; outdated systems hinder real-time detection, weakening readiness.

2.1.2.4 Communication and Coordination Mechanisms

Communication and coordination protocols govern how information is shared and actions synchronised during incidents, internally and with external stakeholders (Vakilinia et al., 2017). Efficient coordination contextualises evidence for legal use; poor communication causes mishandling, conflicting actions, and delays (Saeed et al., 2023). In Nigeria, unclear policies and silos impede management and evidence sharing. Cross-functional frameworks and drills enhance forensic processes.

2.2 Empirical Studies

Empirical studies highlight how cybersecurity incident preparedness strongly influences the efficacy of digital forensic investigations in financial institutions. Pang et al. (2020) and Adebayo (2021) show that structured incident response planning improves investigation speed and quality. Pang et al. (2020) found Singaporean banks with documented frameworks achieved a 35% faster forensic turnaround, while Adebayo (2021) reported fewer than 30% of Nigerian banks had formal strategies, exposing a preparedness gap undermining evidence preservation. Cybersecurity awareness also shapes outcomes. Olajide and Ume (2022) found Nigerian institutions with regular training recorded higher forensic success, while Salifu et al. (2021) linked evidence mishandling to poorly trained staff, compromising integrity and admissibility. Yet most studies lack clear definitions of "effective training" or standardized metrics for forensic performance.

Infrastructure investment further enables forensic capacity. Mthimunye and Tolla (2020) showed that SIEMs and encrypted logging improve evidence retrieval in South Africa. Ogundipe (2021) confirmed this in Nigeria but noted limited generalizability from a single-bank study, underscoring the need for broader research.

Real-time threat detection enhances responsiveness. Liu and Zhao (2019) found early detection enables proactive forensic action, whereas Musa and Adewole (2023) reported Nigerian banks still use outdated tools, delaying response and missing investigative opportunities. Few studies quantify these delays or examine causal relationships statistically. Effective communication mechanisms are equally critical. Johnson et al. (2022) showed structured interdepartmental communication reduces redundancy and confusion during cyber crises, improving documentation and handovers. Bello (2022) reported 46% of Nigerian institutions lacked coordination among IT, legal, and risk teams, impeding timely forensic engagement and diminishing outcomes. Collectively, these findings affirm the multifaceted link between preparedness variables and forensic efficacy but reveal persistent gaps in Nigeria, including minimal use of inferential methods and lack of integrated models examining these dimensions. Addressing these gaps could guide data-driven improvements to cybersecurity and digital forensic frameworks in Nigerian financial institutions.

Theoretical Framework

This study applies the Forensic Readiness Model and Socio-Technical Systems Theory to explain how preparedness influences forensic efficacy. The Forensic Readiness Model (Tan, 2001) stresses proactive integration of planning, training, and infrastructure for swift, accurate responses. In Nigeria, it underscores embedding forensic thinking in cybersecurity frameworks to reduce delays and protect evidence. The Socio-Technical Systems Theory (Trist & Emery, 1951) highlights the interplay between social (skills, communication) and technical (tools, processes) systems. It shows that advanced detection tools are ineffective without trained staff and

coordination. Together, these theories justify focusing on incident response planning, cybersecurity awareness, infrastructure investment, threat detection, and communication mechanisms as key variables enhancing the efficacy of digital forensic investigations.

Methodology

This study adopts a quantitative research design using a cross-sectional survey to investigate the relationship between cybersecurity incident preparedness and the efficacy of digital forensic investigations in Nigerian financial institutions. A cross-sectional design is appropriate as it enables the collection of data at a single point in time to analyse relationships among variables without manipulation (Kerlinger & Lee, 2000). The research is also anchored on a positivist philosophy, which emphasizes objective measurement, empirical observation, and statistical testing of hypotheses (Creswell, 2018). By examining the influence of cybersecurity preparedness dimensions on digital forensic efficacy, the study applies a scientific approach consistent with prior work on information security governance and incident management (Nguyen & Kim, 2021; Adeoye & Ibeh, 2023).

The population comprised 150 cybersecurity and digital forensic professionals across licensed Nigerian financial institutions, including commercial banks, microfinance institutions, fintech companies, and insurance firms. The target group consisted of cybersecurity analysts, IT auditors, incident responders, and forensic investigators drawn purposively from cybersecurity units, forensic teams, and IT risk departments. A total of 120 personnel were selected to ensure that respondents possessed the necessary expertise and experience relevant to the research objectives (Ali-Momoh et al., 2024; Oladipo & Adeyemi, 2022).

Primary data were collected through a structured questionnaire designed to capture demographic information, measures of cybersecurity preparedness, and indicators of forensic investigation effectiveness. The instrument employed a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5) to measure respondents' perceptions and experiences. To ensure clarity, validity, and reliability, the questionnaire was pre-tested with a small sample of professionals before large-scale administration (Onifade & Yusuf, 2021).

Data were analysed using the Statistical Package for Social Sciences (SPSS). Descriptive statistics such as means and standard deviations were used to summarize the demographic profile and variable distributions. Regression analysis was employed to test the hypothesized relationships between cybersecurity preparedness and the efficacy of digital forensic investigations. Model estimation was carried out to assess the significance and strength of the independent variables (Nguyen & Kim, 2021).

Consistent with prior studies (Okoye & Eze, 2020; Bello & Hassan, 2022), the conceptual model specifies the Efficacy of Digital Forensic Investigations (DFE) as the dependent variable, directly influenced by five dimensions of cybersecurity incident preparedness: Incident Response Planning (IRP), Cybersecurity Awareness and Training (CAT), Infrastructure Investment (INF), Threat Monitoring Capability (TMC), and Communication and Coordination Mechanisms (CCM). The model is expressed as:

The model is expressed as: $\mathbf{EDFI = \beta_0 + \beta_1 IRP + \beta_2 CAT + \beta_3 INF + \beta_4 TMC + \beta_5 CCM + \varepsilon}$ Where: **DFE** = Efficacy of Digital Forensic Investigations, **IRP** = Incident Response Planning, **CAT** = Cybersecurity Awareness and Training, **INF** = Infrastructure Investment, **TMC** = Threat Monitoring Capability, **CCM** = Communication and Coordination Mechanisms, β_0 = Intercept, $\beta_1 ... \beta_5$ = Coefficients of the independent variables, ε = Error term

4.0 Result and Discussion

This section presents the results of the study, including the description of variables, normality test and correlation analysis. The section also contains regression results.

Table 1: Descriptive Statistics

Variables	Minimum	Maximum	Mean	Std. Deviation
Incident Response Planning	2.50	5.00	4.02	0.58
Cybersecurity Awareness & Training	2.10	5.00	3.76	0.70
Infrastructure Investment	2.00	5.00	3.91	0.66
Threat Monitoring Capability	2.30	5.00	3.85	0.69
Communication & Coordination Mechanism	1.80	5.00	3.73	0.73

Source: output of SPSS

These results show that, on average, institutions are relatively well-prepared across all cybersecurity preparedness dimensions, with incident response planning scoring the highest. Minimum and maximum scores reflect the lowest and highest Likert-scale responses recorded for the items under each variable. This inference is based on mean scores above the mid-point (3.0) on the 5-point Likert scale, indicating moderate to high preparedness

Table 4: Regression Coefficients

Variables	Unstandardized B	Std. Error	Beta	t	Sig.
(Constant)	-0.003	0.120	—	-0.613	0.521
Incident Response Planning (IRP)	0.328	0.062		5.290	0.000**
Cybersecurity Awareness & Training	0.290	0.067	—	4.330	0.000**
Infrastructure Investment	0.246	0.059	—	4.170	0.000**
Threat Monitoring Capability	0.267	0.063	—	4.240	0.000**
Communication & Coordination	0.218	0.068	—	3.210	0.001**

Source: SPSS Version 23 Output, 2025

The regression analysis revealed that all five cybersecurity preparedness factors significantly enhance the efficacy of digital forensic investigations in Nigerian financial institutions ($p < 0.05$). Incident Response Planning (IRP) demonstrated the strongest effect ($B = 0.328$, $t = 5.290$, $p = 0.000$), followed closely by Cybersecurity Awareness & Training ($B = 0.290$, $t = 4.330$, $p = 0.000$) and Threat Monitoring Capability ($B = 0.267$, $t = 4.240$, $p = 0.000$). Infrastructure Investment ($B = 0.246$, $t = 4.170$, $p = 0.000$) and Communication & Coordination ($B = 0.218$, $t = 3.210$, $p = 0.001$) also showed significant, though comparatively weaker, positive impacts. These findings confirm that comprehensive cybersecurity preparation, particularly robust response planning, staff training, and threat detection systems substantially improve forensic investigation outcomes. While the study shows relatively good preparedness on average, significant gaps remain across institutions especially in infrastructure, training, and coordination. The high mean scores reflect the better-performing institutions, but variability indicates many are still underprepared. The results support rejecting all null hypotheses, highlighting the critical need for Nigerian financial institutions to strengthen these preparedness dimensions to combat cyber threats effectively.

Discussion of Findings

This study investigated the effect of various components of cybersecurity incident preparedness on the efficacy of digital forensic investigations in Nigerian financial institutions. The findings offer critical insights into how each preparedness element contributes to enhancing investigative effectiveness, providing both theoretical reinforcement and empirical clarity.

Incident Response Planning emerged as the most influential predictor of digital forensic efficacy. This confirms earlier findings by (Werlinger et al., 2010) which emphasized the importance of structured, pre-defined procedures in ensuring rapid and effective responses to security incidents. The strong influence of this variable aligns with the Forensic Readiness Model, which stresses the value of upfront planning in ensuring digital evidence is quickly secured and preserved for investigations.

Cybersecurity Awareness and Training also showed a significant and positive impact, consistent with (Hodhod et al., 2023), who argued that internal personnel capacity and organizational knowledge are vital for effective forensic readiness. Awareness programs empower staff to identify suspicious activity and understand reporting protocols key inputs

to successful forensic analysis. This reinforces the Socio-Technical Systems Theory, which advocates for a balance between technical systems and human capacity.

Infrastructure Investment demonstrated a strong positive relationship with forensic investigation efficacy. The result supports the findings of (Kloosterman et al., 2015), who noted that the availability of up-to-date technology and tools such as secure servers, logging mechanisms, and forensic toolkits enhances the quality and speed of investigations. It also highlights the critical role of financial commitment in sustaining cybersecurity frameworks.

Threat Detection Capabilities were found to significantly influence forensic efficacy, reaffirming global evidence presented by Liu and Zhao (2019). Institutions with stronger monitoring systems can detect intrusions earlier, which aids in collecting timely and accurate digital traces. In the Nigerian context, this finding suggests a pressing need for continuous investment in threat intelligence and real-time monitoring systems.

Communication and Coordination Mechanisms had a statistically significant, though slightly weaker, effect compared to other variables. Nevertheless, this result validates (Cataldo et al., 2007; Okhuysen and Bechky, 2009) who emphasized the often-overlooked role of cross-functional collaboration in successful incident resolution and evidence preservation. Inter-departmental coordination and clarity in chain-of-custody procedures can make or break a forensic investigation.

Collectively, these findings align with both the Forensic Readiness Model and the Socio-Technical Systems Theory, underlining the importance of integrating technical infrastructure with organizational culture and preparedness strategies. The rejection of all null hypotheses (H_{01}–H_{05}) further confirms that each cybersecurity preparedness dimension significantly enhances digital forensic investigation outcomes in Nigerian financial institutions.

5.0 Conclusion and Recommendations

This study examined how cybersecurity incident preparedness influences the efficacy of digital forensic investigations in Nigerian financial institutions. Results show that preparedness components incident response planning, training and awareness, infrastructure investment, threat monitoring, and communication positively impact forensic effectiveness.

Incident response planning and training emerged as the strongest factors, emphasizing the importance of structured strategies and human capacity in achieving accurate, timely, and admissible investigations. The findings affirm the Forensic Readiness Model and Socio-Technical Systems Theory, highlighting the synergy of people, processes, and technology in combating cybercrime. Based on the findings, the following recommendations are proposed:

1. Strengthen Institutional Incident Response Frameworks Financial institutions should develop and regularly update detailed incident response plans that define roles, escalation procedures, and evidence preservation protocols. Simulation exercises should be conducted routinely to assess preparedness, with oversight from internal IT units and regulators such as the Central Bank of Nigeria (CBN) and the Nigeria Deposit Insurance Corporation (NDIC).
2. Institutionalize Cybersecurity Training and Awareness Mandatory quarterly cybersecurity training programs should be implemented across all staff levels to enhance awareness of emerging threats, early warning signs, and evidence handling best practices. These programs should be managed by HR departments in collaboration with professional bodies like the Chartered Institute of Bankers of Nigeria (CIBN) and monitored through training evaluations and phishing simulations.
3. Invest in Modern Cybersecurity and Forensic Infrastructure Financial institutions should allocate dedicated budgets for acquiring and maintaining digital forensic tools, intrusion detection systems (IDS), and Security Information and Event Management (SIEM) platforms. These tools will support real-time data collection and evidence preservation. Executive leadership should ensure regular infrastructure audits and performance evaluations are conducted.
4. Implement Real-Time Threat Detection and Monitoring Mechanisms Institutions should deploy AI-enabled threat detection systems and establish 24/7 Security Operations Centers (SOCs) to monitor and respond to incidents promptly. Trained analysts should be available to assess alerts and trigger forensic protocols. Effectiveness should be tracked through performance indicators such as alert logs, response times, and resolution rates.
5. Establish Structured Communication and Coordination Protocols A centralized incident response team should be formed, comprising members from IT, Legal, Risk, and Compliance departments, to ensure seamless coordination during cyber events. Post-incident debriefs and communication effectiveness reviews should be institutionalized to continuously improve response strategies and enhance overall investigative outcomes.

REFERENCES

Ahmad, I., Akagha, O., Anyanwu, A., Dawodu, S., Ejairu, E., & Onwusinkwue, S. (2024). Cybersecurity challenges in smart cities: A case review of African metropolises. *Computer Science & IT Research Journal*, *5*(2), 254–269. https://doi.org/10.51594/csitrj.v5i2.756

Aksoy, C. (2024). BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS. *letme Ekonomi ve Yönetim Ara t rmalar Dergisi*, *7*(1), 96–110. https://doi.org/10.33416/baybem.1374001

Allah Rakha, N. (2024). Cybercrime and the Law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Arpilleda, J. (2023). Cybersecurity in the Smart Grid: Vulnerabilities, Threats, and Countermeasures. *International Journal of Advanced Research in Science, Communication and Technology*, 743–750. https://doi.org/10.48175/ijarsct-12364

Ay, O. (2020). Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*(1), 1–8. https://doi.org/10.24966/flis-733x/100045

Badsha, S., Vakilinia, I., & Sengupta, S. (2019). *Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense*. 0708–0714. https://doi.org/10.1109/ccwc.2019.8666477

Bhoyar, L., Mehar, P., & Chavali, K. (2024). An overview of DNA degradation and its implications in forensic caseworks. *Egyptian Journal of Forensic Sciences*, *14*(1). https://doi.org/10.1186/s41935-024-00389-y

Blanco, C., Santos-Olmo, A., & Sánchez, L. E. (2024). QISS: Quantum-Enhanced Sustainable Security Incident Handling in the IoT. *Information*, *15*(4), 181. https://doi.org/10.3390/info15040181

Budowle, B., Chakraborty, R., & Murch, R. (2005). Microbial forensics: the next forensic challenge. *International Journal of Legal Medicine*, *119*(6), 317–330. https://doi.org/10.1007/s00414-005-0535-y

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75

Cataldo, M., Herbsleb, J. D., Bass, L., & Bass, M. (2007). *On Coordination Mechanisms in Global Software Development*. 71–80. https://doi.org/10.1109/icgse.2007.33

Dawodu, S., Akindote, O., Adegbite, A., Omotosho, A., & Ewuga, S. (2023). Cybersecurity risk assessment in banking: Methodologies and best practices. *Computer Science & IT Research Journal*, *4*(3), 220–243. https://doi.org/10.51594/csitrj.v4i3.659

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, *134*, 103435.https://doi.org/10.1016/j.cose.2023.103435

Esposito, M., Roccuzzo, S., Zuccarello, P., Sessa, F., Cocimano, G., & Salerno, M. (2023). Advances in Technologies in Crime Scene Investigation. *Diagnostics*, *13*(20), 3169. https://doi.org/10.3390/diagnostics13203169

Et Al, N. K. (2023). AI in Cybersecurity: Threat Detection and Response with Machine Learning. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(3), 38–46. https://doi.org/10.52783/tjjpt.v44.i3.237

Fakiha, B. (2023). Enhancing cyber forensics with AI and Machine Learning: A study on automated threat analysis and classification. *International Journal of Safety and Security Engineering*, *13*(4), 701–707. https://doi.org/10.18280/ijsse.130412

Galinec, D., & Steingartner, W. (2017). *Combining cybersecurity and cyber defense to achieve cyberresilience*. 87–93.https://doi.org/10.1109/informatics.2017.8327227

Gcaza, N., & Von Solms, R. (2017). A Strategy for a Cybersecurity Culture: A South African Perspective. *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, *80*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems*, *12*(5), 165. https://doi.org/10.3390/systems12050165

Hassan, A., Oladeinde, M., Abrahams, T., Abdul, A., Ewuga, S., & Dawodu, S. (2024). Cybersecurity in banking: A global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41–59. https://doi.org/10.51594/csitrj.v5i1.701

Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics*, *12*(17), 3544.

https://doi.org/10.3390/electronics12173544

I Alghamdi, M. (2021). *Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities*. intechopen. https://doi.org/10.5772/intechopen.94452

Kaur, H., Kumar Thakur, R., Kumar Reddy, K. V., Paul, T., Sanjaiy Sl, D., Mahato, J., & Naveen, K. (2024). Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review. *E3S Web of Conferences*, *556*, 01006. https://doi.org/10.1051/e3sconf/202455601006

Klein, T., & Romano, G. (2025). Optimizing Cybersecurity Incident Response via Adaptive Reinforcement Learning. *Journal of Advances in Engineering and Technology*, *2*(1). https://doi.org/10.62177/jaet.v2i1.212

Kloosterman, A., Van Der Steen, M., Koper, C., Van Asten, A., Geradts, Z., Van Eijk, E., Mapes, A., Van Den Berg, J., & Verheij, S. (2015). The interface between forensic science and technology: how technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *370*(1674), 20140264. https://doi.org/10.1098/rstb.2014.0264

Macdermott, A., Shi, Q., & Baker, T. (2018). *Iot Forensics: Challenges for the Ioa Era*. 1–5. https://doi.org/10.1109/ntms.2018.8328748

Miracle, N. O. (2024). The Importance of Network Security in Protecting Sensitive Data and Information. *International Journal of Research and Innovation in Applied Science*, *9*(6), 259–270. https://doi.org/10.51584/ijrias.2024.906024

Mohammed, H., Li, F., & Clarke, N. (2016). An automated approach for digital forensic analysis of heterogeneous big data. *Journal of Digital Forensics, Security and Law*, *11*(2). https://doi.org/10.15394/jdfsl.2016.1384

Mungo, JamaineDr. (2023). Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. *Journal of Cyber Security Technology*, *8*(2), 71–119.https://doi.org/10.1080/23742917.2023.2244210

Mustapha, A., & Sinha, A. (2024). Cyberfraud in the Nigerian Banking Sector: The Techniques and Preventive Measures. *International Journal of Innovative Science and Research Technology (IJISRT)*, 171–179. https://doi.org/10.38124/ijisrt/ijisrt24aug395

Mutemwa, M., Mkhonto, N., & Mtsweni, J. (2017). *Developing a cyber threat intelligence sharing platform for South African organisations*, *9*, 1–6. https://doi.org/10.1109/ictas.2017.7920657

Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2023). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems*, *33*(2), 200–220. https://doi.org/10.1080/0960085x.2023.2257168

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management:* National institute of standards technology.https://doi.org/10.6028/nist.sp.800-61r3

Okoye, C., Usman, F., Mhlongo, N., Odeyemi, O., Nwankwo, E., & Ike, C. (2024). Accelerating SME growth in the African context: Harnessing FinTech, AI, and cybersecurity for economic prosperity. *International Journal of Science and Research Archive*, *11*(1), 2477–2486. https://doi.org/10.30574/ijsra.2024.11.1.0231

Olaniyi, O. O., Oladoyinbo, T. O., Alao, A. I., Olaniyi, F. G., & Omogoroye, O. O. (2024). CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 31–49. https://doi.org/10.9734/jerr/2024/v26i61160

Ortiz-Garcés, I., Sánchez-Viteri, S., Govea, J., & Villegas-Ch, W. (2024). CyberEduPlatform: an educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence. *PeerJ. Computer Science*, *10*, e2041. https://doi.org/10.7717/peerj-cs.2041

Peruch, M., Buffon, M., Jakovski, Z., Spiliopoulou, C., Addobbati, R., Franzin, M., Magni, P. A., & D'Errico, S. (2024). Comparative Toxicological Analyses of Traditional Matrices and Blow Fly Larvae in Four Cases of Highly Decomposed Human Cadavers. *Insects*, *15*(7), 500. https://doi.org/10.3390/insects15070500

Raghavan, S. (2012). Digital forensic research: current state of the art. *CSI Transactions on ICT*, *1*(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

Ramakrishnan, S., & Chittibala, D. R. (2024). Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024. *International Journal of Computing and Engineering*, *5*(2), 36–44. https://doi.org/10.47941/ijce.1754

Raza, S. A., Tahira, K., & Shaikh, M. (2023). Cryptocurrency Investigations in Digital Forensics: Contemporary Challenges and Methodological Advances. *Information Dynamics and Applications*, *2*(3), 126–134.

https://doi.org/10.56578/ida020302

Reis, O., Obi, O., Oliha, J., & Osasona, F. (2024). Cybersecurity dynamics in Nigerian banking: Trends and strategies review. *Computer Science & IT Research Journal*, *5*(2), 336–364 https://doi.org/10.51594/csitrj.v5i2.761

Rich, M. S., & Aiken, M. P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sciences*, *4*(1), 110–151. https://doi.org/10.3390/forensicsci4010008

Sabillon, R., Serra-Ruiz, J., Mora, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program. *Journal of Cases on Information Technology*, *21*(3), 26–39. https://doi.org/10.4018/jcit.2019070102

Saeed, S., Almuhaideb, A. M., Suayyid, S. A., Al-Ghamdi, M. S., & Al-Muhaisen, H. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

Sankaram, M., Roopesh, M., Rasetti, S., & Nishat, N. (2024). A COMPREHENSIVE REVIEW OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN ENHANCING CYBERSECURITY THREAT DETECTION AND RESPONSE MECHANISMS. *GLOBAL MAINSTREAM JOURNAL*, *3*(5), 1–14. https://doi.org/10.62304/jbedpm.v3i05.180

Saravanan, V., Santhosh, K., Tripathi, K., P, N., & Vidyasri, P. (2025). AI-Driven Cybersecurity: Enhancing Threat Detection and Mitigation with Deep Learning. *International Journal of Computational and Experimental Science and Engineering*, *11*(2). https://doi.org/10.22399/ijcesen.1358

Sauzier, G., Van Bronswijk, W., & Lewis, S. W. (2021). Chemometrics in forensic science: approaches and applications. *The Analyst*, *146*(8), 2415–2448. https://doi.org/10.1039/d1an00082a

Sendjaja, T., Irwandi, I., Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. *International Journal of Science and Society*, *6*(1), 1008–1019. https://doi.org/10.54783/ijsoc.v6i1.1098

Serketzis, N., Baltatzis, D., Pangalos, G., Katos, V., & Ilioudis, C. (2019). Improving forensic triage efficiency through cyber threat intelligence. *Future Internet*, *11*(7), 162. https://doi.org/10.3390/fi11070162

Tolossa, D. (2023). IMPORTANCE OF CYBERSECURITY AWARENESS TRAINING FOR EMPLOYEES IN BUSINESS. *VIDYA - A JOURNAL OF GUJARAT UNIVERSITY*, *2*(2), 104–107. https://doi.org/10.47413/vidya.v2i2.206

Vakilinia, I., Sengupta, S., & Tosh, D. K. (2017). *Privacy-preserving cybersecurityinformation exchange mechanism*. *41*, 1–7. https://doi.org/10.23919/spects.2017.8046783

Werlinger, R., Muldner, K., Beznosov, K., & Hawkey, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, *18*(1), 26–42. https://doi.org/10.1108/09685221011035241

Xiao, J., Xu, Q., & Li, S. (2019). Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation. *IEEE Access*, *7*, 55432–55442. https://doi.org/10.1109/access.2019.2913648

Zaman, D., & Mazinani, M. (2023). Cybersecurity in Smart Grids: Protecting Critical Infrastructure from Cyber Attacks. *SHIFRA*, *2023*, 86–94. https://doi.org/10.70470/shifra/2023/010

Zangana, H. M., Omar, M., & Mohammed, D. (2024). *Introduction to Artificial Intelligence in Cybersecurity and Forensic Science* (pp. 1–24).igiglobal. https://doi.org/10.4018/979-8-3373-0588-2.ch001

Zhang, Z. (Justin), Abdous, M., Li, W., & He, W. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*, *121*(3), 613–636. https://doi.org/10.1108/imds-08-2020-0462