Cybersecurity Debt in AI-Augmented Small and Medium Enterprises: A Narrative Review of Identity Drift, Prompt Supply Chains and Recovery Readiness

[1]Paul A. Ige
[1]Department of Cyber Security, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
igepaul89@gmail.com

Received: 30-JUNE-2026; Reviewed: 25-SEPT-2026; Accepted: 30-SEPT-2026
https://dx.doi.org/10.46792/fuoyejet.v11i3.1613

REVIEW WORK

Abstract— This narrative review, which reports no new empirical data, examines cybersecurity debt in artificial intelligence (AI)-augmented small and medium enterprises (SMEs). SMEs are adopting AI tools that generate text, code, decisions and support tickets faster than their identity, assurance and recovery controls can mature, yet existing research treats SME security, AI risk, identity governance and ransomware recovery as separate topics. The objective is to integrate these strands into one management construct. Peer-reviewed studies, standards and practitioner reports published mainly between 2016 and 2026 were identified through scholarly databases and standards repositories, screened against explicit inclusion criteria and appraised for authority and relevance; 27 sources were retained. The evidence shows that credential abuse and weak authentication remain dominant breach routes, that SMEs lag larger firms in security investment and awareness, and that documented prompt injection exploits already reach business data through AI assistants. From this synthesis the review proposes a three-domain cybersecurity debt model comprising identity drift, prompt supply chains and recovery readiness, each paired with author-proposed indicators. Its contribution is an integrative construct linking AI adoption velocity, accumulated control deficiencies and recoverability, which prior studies have not connected for SMEs. In practice, SMEs should tie AI use approvals to identity inventory, prompt and plugin governance, rehearsed incident response, tested immutable backups and board-level debt reporting.

Keywords—Artificial intelligence, cyber resilience, cybersecurity debt, identity management, large language model security, OWASP, prompt injection, ransomware, small and medium enterprises, zero trust

1 INTRODUCTION

Small and medium enterprises (SMEs) increasingly depend on cloud services, software-as-a-service platforms, outsourced support and AI applications to perform work that once required larger internal teams. These same tools widen the boundary of trust. A sales assistant may connect to customer records, a code assistant may influence production software, and a help desk chatbot may handle sensitive business requests, a pattern already visible in Nigerian service settings where AI chatbots answer routine enquiries (Olasunkanmi & Adesina, 2025). For organizations with limited cybersecurity staff, the speed of adoption can exceed the speed of assurance, creating unmanaged exposure that remains invisible until an incident occurs. A similar pattern followed the rapid move to remote and cloud work during the COVID-19 pandemic, when new digital dependencies were quickly exploited by attackers (Lallie et al., 2021). Existing research addresses the relevant problems in separate streams. Studies of threats and vulnerabilities catalogue recurring technical weaknesses (Humayun et al., 2020); SME studies examine awareness, investment and practice gaps (Kabanda et al., 2018; Heidt et al., 2019; Chaudhary et al., 2023); AI security studies examine how AI both strengthens and endangers organizations (Jada & Mayayise, 2024); identity governance is framed mainly through zero trust architecture (Rose et al., 2020); and ransomware and resilience studies examine disruption and recovery (Oz et al., 2022; Alhidaifi et al., 2024). What is missing is a synthesis that connects AI adoption velocity, accumulated control deficiencies and recoverability in SMEs. In practice, these topics converge inside everyday business workflows. A weak identity process can expose an AI tool to sensitive data. A poorly governed plugin can turn a prompt into an instruction path for data leakage. A backup strategy that has not been tested can make a ransomware event a business continuity crisis. This review therefore proposes cybersecurity debt as an integrative construct for that gap.

Cybersecurity debt is used here as a practical synthesis term for accumulated, unmanaged risk created when protection, monitoring, assurance and recovery practices lag behind digital change. The term is adapted rather than newly coined. It extends technical debt, introduced by Cunningham (1992) to describe the future cost of expedient software decisions, and security debt, which software engineering research treats as the security-related subset of technical debt found in code, architecture and development practice (Rindell et al., 2019; Kruke et al., 2025). The present use differs in scope: it moves the unit of analysis from the software artefact to the SME as an operating organization, covering identities, AI workflows, vendors and recovery capability. The framing does not replace established risk management models. Rather, it gives SMEs a way to discuss security delay, inherited weakness and AI adoption in operational terms that can be tracked, prioritized and reduced.

2 LITERATURE REVIEW

2.1 OBJECTIVE OF THE REVIEW

The objective is to synthesize recent literature and

Corresponding Author
Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Ige P. A. (2026). Cybersecurity Debt in AI-Augmented Small and Medium Enterprises: A Narrative Review of Identity Drift, Prompt Supply Chains and Recovery Readiness. FUOYE Journal of Engineering and Technology (FUOYE**JET), 11(3), 418-422.**
https://dx.doi.org/10.46792/fuoyejet.v11i3.1613

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

standards on SME cybersecurity, AI security, identity governance, ransomware and cyber resilience, then organize the evidence into a concise review model. The model focuses on three visible forms of cybersecurity debt: identity drift, prompt supply chains and recovery readiness.

2.2 Background of Literature

Cybersecurity research repeatedly shows that organizations face a wide spectrum of technical and human vulnerabilities. Humayun et al. (2020) mapped cybersecurity threats and weaknesses across the literature and showed that vulnerability management, access control, malware, network security and human behavior remain recurring concerns. Studies published in this journal reach a similar conclusion from the defensive side: vulnerability assessment and penetration testing expose avoidable configuration weaknesses (Omotosho et al., 2025), and machine learning detectors can identify malicious traffic with high accuracy (Azeez et al., 2023). Both streams, however, treat weaknesses as point-in-time findings rather than as obligations that accumulate when remediation is deferred, which is the property the debt construct is designed to capture.

Research on SMEs agrees that size does not remove exposure, but it differs on the cause. Heidt et al. (2019) attribute the security divide between SMEs and large firms to resource constraints and owner-manager attitudes, whereas Kabanda et al. (2018) find that SMEs in developing countries practise security mainly in response to perceived threats and client demands rather than formal policy. Chaudhary et al. (2023) identified continuing gaps in awareness, training and preparedness, and Alshaikh (2020) argued that security culture must influence employee behavior rather than remain a policy document. Rawindaran et al. (2021) further showed that SMEs adopting machine learning security tools often lack the skills to configure and interpret them. Taken together, these findings imply that cybersecurity debt is not only a technical backlog but also a management and behavior backlog, yet none of these SME studies examines how AI adoption changes the size or shape of that backlog.

Ransomware literature shows why delayed controls are costly. Oz et al. (2022) described ransomware as an evolving threat with technical, economic and organizational dimensions. The 2026 Data Breach Investigations Report continues to link many breaches to credential abuse, human actions and ransomware patterns (Verizon, 2026). Academic and practitioner sources agree on these entry routes but differ in emphasis: surveys concentrate on malware families and defensive techniques, while practitioner data point to identity and process failures. For small organizations, a single compromised account or untested recovery process can interrupt sales, payroll, customer service and regulatory obligations at the same time.

AI expands this problem. Jada and Mayayise (2024) found that AI can strengthen organizational security through detection, automation and analysis, but it also introduces risk when governance is weak. The National Institute of Standards and Technology (NIST) presents AI risk as a socio-technical management issue involving validity, safety, security, accountability and transparency (Tabassi, 2023). The generative AI profile adds risks associated with data provenance, misuse, information integrity and human oversight (National Institute of Standards and Technology, 2024a). These frameworks are organization-neutral; they assume governance capacity that many SMEs lack and do not indicate which controls to prioritize when resources are scarce.VCyber resilience literature moves the focus from prevention alone to continuity under attack. Alhidaifi et al. (2024) reviewed strategies that include preparation, absorption, recovery and adaptation. NIST guidance on cybersecurity event recovery and incident response similarly emphasizes planning, communications, technical restoration and lessons learned (Bartock et al., 2016; Nelson et al., 2025). This stream agrees with the others on the need for preparation but is largely silent on AI-specific recovery objects such as prompts, retrieval stores and model configurations. The gap across all five streams is therefore not a lack of guidance but the absence of a single lens showing SMEs how deferred controls in identity, AI workflows and recovery compound one another.

3 METHODOLOGY

3.1 REVIEW MOTHODOLOGY

A narrative review design was chosen deliberately and does not follow a systematic protocol such as PRISMA. The topic spans peer-reviewed research, standards and practitioner incident evidence that use different vocabularies and evidence types, and AI-specific SME security studies remain scarce, so a systematic review restricted to empirical studies would exclude much of the relevant material. A narrative design allows these heterogeneous sources to be interpreted together to build a conceptual model, which is the aim of this article.

Search strategy. Searches were run in Google Scholar, ACM Digital Library, ScienceDirect, SpringerLink, Taylor & Francis Online and the FUOYE Journal of Engineering and Technology archive; standards were retrieved directly from the NIST Computer Security Resource Center and the OWASP Foundation. Search strings combined an organizational term ("small and medium enterprise" OR SME OR "small business") with a risk term (cybersecurity OR "security debt" OR "technical debt" OR ransomware OR "cyber resilience" OR "zero trust" OR "identity management") and, where relevant, an AI term ("artificial intelligence" OR "large language model" OR "prompt injection" OR "generative AI"). Reference lists of retained sources were also checked.

Inclusion, exclusion and screening. Sources were included if they (a) were published between 2016 and 2026, (b) addressed SME security, AI security, identity, ransomware, incident response or resilience, and (c) were peer-reviewed, issued by a recognized standards body, or provided a documented incident analysis. Opinion pieces, vendor marketing and sources without traceable authorship were excluded. One foundational source outside the window (Cunningham, 1992) was admitted solely to define technical debt. Screening was performed by the author in two passes, first on title and abstract and then on full text.

Quality appraisal and retained corpus. Each source was appraised for authority (peer review or standards-body status), traceability (digital object identifier or formal

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://dx.doi.org/10.4314/fuoyejet.v11i3.1613 engineering.fuoye.edu.ng/journal

publication record), recency and relevance to SMEs. Practitioner and incident reports were used to illustrate mechanisms, not as primary evidence. Because the search was exploratory and iterative, record-level hit counts were not logged. The retained corpus comprises 27 sources: 16 peer-reviewed journal articles and conference papers, eight standards and frameworks, and three practitioner or incident reports.

The synthesis was interpretive rather than statistical. Evidence was read for recurring operational problems that are likely to appear when SMEs add AI to existing cloud and identity environments. Three themes were retained because they join the literature and are observable in management practice: identity drift, prompt supply chains and recovery readiness. The value of the method is the construction of a review model that can guide risk conversation, audit scoping and future empirical research; its limitations are set out in Section 4.7.

4 RESULT AND DISCUSSION

4.1 Thematic Synthesis

The literature supports a view of cybersecurity debt as a compound condition. It grows when organizations adopt new digital capability without updating the controls that keep identity, data, software and recovery trustworthy. AI intensifies this condition because it is often embedded into work at the application layer, where business teams can deploy tools faster than security teams can inventory them. Table 1 summarizes the three domains.

Table 1. Cybersecurity debt domains for AI-augmented SMEs

Debt domain	Typical expression	Core risk	Review indicator*
Identity drift	Accounts, tokens and privileges expand without timely review.	Unauthorized access to data, tools and AI actions.	Privileged accounts and service identities reviewed within the last quarter.
Prompt supply chains	Prompts, plugins, retrieval sources and outputs are unmanaged.	Data leakage, prompt injection, poisoned context and insecure output handling.	Approved AI tools mapped to data sources, owners and logs.
Recovery readiness	Backups, incident roles and restoration steps are untested.	Extended disruption after ransomware, lockout or integrity failure.	Successful restore test for critical AI-supported processes.

*Source: Author's synthesis from reviewed literature and standards (2026). *Indicators are proposed by the author and have not been empirically validated.*

4.2 Cybersecurity Debt as a Practical Construct

Cybersecurity debt is related to technical debt, but it is broader than unfinished engineering work. It includes excessive privileges, unknown third-party integrations, weak logging, informal exception handling, missing recovery tests and security decisions that depend on individual memory. The NIST Cybersecurity Framework 2.0 supports this wider view by adding governance as a core function, placing risk oversight beside identify, protect, detect, respond and recover activities (National Institute of Standards and Technology, 2024b).

For SMEs, the usefulness of the term lies in prioritization. Management may not act on an abstract warning that AI is risky, but it can act on a debt register showing which business process uses AI, which data it reaches, which identity authorizes it, which provider hosts it, which log records it and which recovery plan restores it.

The metaphor has limits. Financial debt is denominated in a common currency, carries a known interest rate and can be summed; cybersecurity debt cannot. An unreviewed administrator account and an untested backup are not measured in comparable units, and their "interest" is probabilistic, depending on threat activity rather than a contract. The construct is therefore used here as an ordinal management tool: items can be listed, owned, dated and ranked, but they are not aggregated into a single monetary figure. Quantifying the debt would require the empirical validation proposed in Section 10.

4.3 Identity Drift

Identity drift occurs when accounts, privileges, service identities and access paths change faster than the organization can review them. AI workflows add new forms of identity pressure. A chatbot may need access to a knowledge base, a code assistant may connect to repositories, and an automation agent may trigger actions across email, customer records and ticketing tools. Each connection creates an authorization decision that can become stale.

Zero trust architecture provides a useful countermeasure because it treats access as a continuous decision based on identity, device, resource, policy and context rather than a one-time network location (Rose et al., 2020). Yet SMEs often implement zero trust unevenly. Multifactor authentication may protect email but not administrative consoles. Contractors may retain access after projects end. Service tokens may be stored without rotation. Under AI adoption, this drift becomes more serious because tools can retrieve, summarize and transmit information at machine speed. The collapse of KNP Logistics Group in the United Kingdom illustrates the cost of identity debt. In June 2023 the Akira ransomware group gained entry by guessing an employee password on an account without multifactor authentication, encrypted the firm's systems and left more than 500 lorries immobilized; the 158-year-old business could not recover and about 700 jobs were lost (Powell, 2025). No AI was involved, which is the point: AI workflows add further identities to the same weak foundations.

The following indicators are proposed by the author, informed by the reviewed literature, and have not been empirically validated; they are not drawn from the cited standards. Identity debt can be tracked through: percentage of privileged accounts reviewed in the last quarter, number of AI tools with named owners, number of service accounts without expiration, coverage of multifactor authentication, and availability of logs for AI-mediated actions. These indicators connect technical identity hygiene to business risk in a language that non-specialist leaders can use.

4.4 Prompt Supply Chains

Prompt supply chains are the linked inputs, templates, retrieval sources, plugins, model outputs, human reviews and downstream actions that make an AI workflow operate. The term is useful because a prompt is rarely just a single question. It may include hidden system instructions, retrieved documents, customer text, third-party extensions and tool permissions. A weakness at any point can alter what the model sees or what the business

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://dx.doi.org/10.4314/fuoyejet.v11i3.1613 engineering.fuoye.edu.ng/journal

does with the output.

The OWASP Top 10 for Large Language Model Applications identifies risks such as prompt injection, sensitive information disclosure, supply chain weakness, excessive agency and insecure output handling (OWASP Foundation, 2025). These risks align with the NIST AI risk framework, which emphasizes governance, mapping, measurement and management of AI risks (Tabassi, 2023). For small organizations, the immediate concern is not only advanced adversarial research. It is the ordinary practice of copying business data into public tools, connecting unreviewed plugins and accepting model-generated code without secure development review.

The risk is no longer hypothetical. In 2025 researchers disclosed EchoLeak (CVE-2025-32711), a zero-click prompt injection in Microsoft 365 Copilot in which a crafted email, once retrieved as context, caused the assistant to leak internal data without any user action (Reddy & Gujral, 2025). Many SMEs license the same productivity assistants, and the case shows how a retrieval source, an output channel and broad data permissions can combine into one exploit path.

Prompt supply chain debt can be reduced through simple controls, which, like the indicators above, are author-proposed. Organizations should maintain an inventory of AI tools, prohibit sensitive data in unapproved systems, review retrieval sources for poisoning risk, restrict plugins by business purpose, log model-assisted decisions and apply secure software development checks to generated code. The Secure Software Development Framework is relevant here because model-generated code still becomes software that must be designed, implemented, reviewed and maintained securely (Souppaya et al., 2022).

4.5 Recovery Readiness

Recovery readiness is the ability to restore trusted operations after compromise, disruption or suspected integrity failure. It is often weaker than policy suggests. Backups may exist but remain untested. Incident roles may be named but unrehearsed. Vendor contacts may be unavailable outside business hours. AI workflows add further uncertainty because organizations must know whether models, prompts, vector stores, logs and source data can be restored to a trustworthy state.

Ransomware research and incident response guidance both show that recovery is a management discipline, not a final technical step (Oz et al., 2022; Nelson et al., 2025). NIST recovery guidance calls for restoration planning, coordination, communications and testing (Bartock et al., 2016). For AI-augmented SMEs, this means backup testing should include the data sources used by AI systems, the configuration of retrieval tools, access policies and evidence needed to determine whether outputs can still be trusted. Recovery debt can be tracked with the following author-proposed measures: date of last restore test, maximum tolerable downtime for AI-supported processes, number of critical applications without immutable backups, number of vendors without incident contacts, and availability of clean administrative credentials during a lockout. These measures turn resilience into observable management work.

4.6 Governance Implications

The main governance implication is that AI approval should be tied to security debt review. A business unit seeking to adopt a tool should identify the data used, the identity that grants access, the provider, the logging path, the acceptable use limits, the recovery owner and the incident escalation route. This lightweight review is more realistic for small organizations than a large assurance program, yet it creates accountability before the tool becomes embedded. A second implication is that leaders should treat unresolved security exceptions as debt with due dates. Exceptions are sometimes necessary, but unmanaged exceptions become normal practice. A quarterly debt review can rank overdue identity reviews, unapproved AI tools, missing logs, weak backup evidence and delayed training. This rhythm connects cybersecurity culture with measurable work, supporting Alshaikh's (2020) argument that security must influence behavior.A third implication concerns future research. Empirical studies could test whether cybersecurity debt registers improve incident readiness in SMEs and whether the proposed indicators are reliable and valid. Researchers could also compare sectors where AI adoption is high but security staffing is low, such as professional services, retail, education and healthcare support businesses. Such studies would move the concept from review synthesis to validated measurement.

4.7 Limitations

Five limitations qualify the findings. First, the narrative design is not systematic, so relevant studies may have been missed and selection reflects author judgment. Second, searching, screening and appraisal were performed by a single reviewer without independent verification. Third, empirical studies of AI-specific security in SMEs are still few, so parts of the model rest on standards and practitioner evidence rather than field data. Fourth, the proposed indicators have not been tested for reliability or validity. Fifth, the review does not estimate the prevalence of any debt domain across sectors or countries, and the incident examples illustrate mechanisms rather than representative outcomes.

5 Conclusion

AI does not create an entirely separate cybersecurity problem for SMEs. It amplifies existing weaknesses in identity governance, data handling, software assurance, vendor reliance and recovery planning. This review has framed those accumulated weaknesses as cybersecurity debt so that leaders can see delayed controls as a trackable business condition rather than a vague technical concern.

The original contribution of the paper is threefold. First, it extends technical and security debt from the software artefact to the SME as an organization and applies the construct to AI adoption. Second, it proposes a three-domain cybersecurity debt model (identity drift, prompt supply chains and recovery readiness) that connects AI adoption velocity, accumulated control deficiencies and recoverability, which earlier studies treated separately. Third, it offers a starter set of author-proposed indicators that make each domain inventoriable and assignable to owners. These domains are practical because they can be inventoried, assigned to owners, tracked through

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://dx.doi.org/10.4314/fuoyejet.v11i3.1613 engineering.fuoye.edu.ng/journal

indicators and reduced through existing standards such as zero trust architecture, AI risk management, secure software development, incident response and cyber resilience guidance. SMEs should use AI adoption as a trigger to review access, data flows, tool permissions, logging and restore evidence. Doing so will not eliminate risk, but it will make security delay visible, governable and more likely to be corrected before a disruptive incident occurs.

ACKNOWLEDGMENT

No external funding was received for this manuscript. No individual or institution is acknowledged.

CONFLICT-OF-INTEREST DISCLOSURE

The author declares no financial, personal or institutional conflict of interest.

REFERENCES

Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Computing Surveys, 56*(8), 1-48. https://doi.org/10.1145/3649218

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Azeez, N. A., Odeyemi, T. O., Isiekwene, C. C., & Abidoye, A. P. (2023). Cyber attack detection in a global network using machine learning approach. *FUOYE Journal of Engineering and Technology, 8*(4). https://doi.org/10.46792/fuoyejet.v8i4.1113

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery* (NIST Special Publication 800-184). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review, 50*, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Cunningham, W. (1992). The WyCash portfolio management system. *ACM SIGPLAN OOPS Messenger, 4*(2), 29-30. https://doi.org/10.1145/157710.157715

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers, 21*(6), 1285-1305. https://doi.org/10.1007/s10796-019-09959-1

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering, 45*(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269-282. https://doi.org/10.1080/10919392.2018.1484598

Kruke, M. M., Martini, A., Cruzes, D. S., & Iovan, M. (2025). Defining security debt: A case study based on practice. In D. Pfahl, J. Gonzalez Huerta, J. Klünder, & H. Anwar (Eds.), *Product-Focused Software Process Improvement: PROFES 2024* (Lecture Notes in Computer Science, pp. 43-59). Cham: Springer. https://doi.org/10.1007/978-3-031-78386-9_4

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

National Institute of Standards and Technology. (2024a). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

National Institute of Standards and Technology. (2024b). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management* (NIST Special Publication 800-61 Revision 3). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Olasunkanmi, H. A., & Adesina, A. J. (2025). Artificial intelligence-powered chatbot for student enquiries in Nigerian tertiary education. *FUOYE Journal of Engineering and Technology, 10*(4), 595-599. https://doi.org/10.4314/fuoyejet.v10i4.4

Omotosho, O. I., Lawal, Y. P., Ogunrinola, B. I., Ajayi, O. L., Adedeji, T. A., & Akintunde, A. A. (2025). Enhancing network security using vulnerability assessment and penetration testing. *FUOYE Journal of Engineering and Technology, 10*(1), 76-83. https://doi.org/10.4314/fuoyejet.v10i1.12

OWASP Foundation. (2025). *OWASP Top 10 for Large Language Model Applications*. Wakefield, MA: OWASP Foundation. Retrieved on 30th June, 2026 from: https://owasp.org/www-project-top-10-for-large-language-model-applications/

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys, 54*(11s), 1-37. https://doi.org/10.1145/3514229

Powell, C. (2025, September 11). *One password, 700 jobs: How ransomware crippled KNP Logistics Group and what it means for the sector*. Weightmans LLP. Retrieved on 25th September, 2026 from: https://www.weightmans.com/media-centre/news/how-ransomware-crippled-knp-logistics-group/

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers, 10*(11), 150. https://doi.org/10.3390/computers10110150

Reddy, P., & Gujral, A. S. (2025). *EchoLeak: The first real-world zero-click prompt injection exploit in a production LLM system* (arXiv preprint 2509.10540). arXiv. https://doi.org/10.48550/arXiv.2509.10540

Rindell, K., Bernsmed, K., & Jaatun, M. G. (2019). Managing security in software: Or: How I learned to stop worrying and manage the security technical debt. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-8). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3339252.3340338

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-218

Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

Verizon. (2026). *2026 Data Breach Investigations Report*. New York, NY: Verizon Business. Retrieved on 30th June, 2026 from: https://www.verizon.com/business/resources/reports/dbir/

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)