

Research Article

A Multi-Layered Ai-Based Cybersecurity Framework for Business Continuity and Operational Resilience

Peter Anthony Ene MS.c^{*1}, Nsikak Stephen Edet, PhD², Precious Nsikak Stephen, MS.c³

¹ Department of Computer Science, Baze University, Abuja

² Department of Political Science, University of Uyo, Nigeria

³ Department of embedded AI, University of Abuja

***Related declarations are provided in the final section of this article*

ARTICLE INFORMATION

Received: 20 Jul 2026

Accepted: 25 Aug 2026

Published: 31 Aug 2026

Correspondence Author:

Peter Anthony Ene MS.c^{*}

Copyright © 2026 The Author(s). The Authors retain copyright. Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Organisations today operate in a threat environment in which cyberattacks are no longer isolated technical incidents but direct threats to business continuity and operational resilience. This study proposes and empirically examines a multi-layered, artificial-intelligence-based cybersecurity framework structured around three defense layers a predictive/preventive layer, a detective layer, and a responsive/recovery layer and evaluates the influence of each layer on organisational business continuity and operational resilience. Anchored on Defence-in-Depth theory, the study formulated three objectives, three research questions and three corresponding hypotheses. A descriptive survey design was adopted, involving 230 purposively sampled information technology, risk and operations personnel across medium and large organisations. Data were analysed using descriptive statistics and chi-square tests of association at the 0.05 level of significance. Findings show that all three layers of the proposed framework predictive/preventive, detective, and responsive/recovery exert a statistically significant influence on business continuity and operational resilience, with the responsive/recovery layer recording the strongest observed effect. The study concludes that resilience is best secured not through any single AI-security control but through the deliberate, coordinated layering of predictive, detective and responsive AI capabilities across the organisation. Recommendations are offered for organisational leaders, regulators and institutions engaged in cybersecurity capacity-building.

Keywords: Artificial intelligence; Multi-layered cybersecurity; Defence-in-depth; Business continuity; Operational resilience

INTRODUCTION

1. Background to the Study

Contemporary organisations operate in an environment in which digital infrastructure underpins virtually every core business function, from payment processing and customer engagement to supply-chain coordination and internal communication (Fusion Risk Management, 2025). This deep digital dependence has made cybersecurity inseparable from the wider question of business continuity: an organisation that cannot keep its systems running through and after a cyber incident cannot, in any meaningful sense, keep its business running. At the same time, the cyber-threat landscape has grown markedly more dynamic, with attackers increasingly deploying automated and AI-assisted techniques capable of adapting faster than static, rule-based defences can respond (Industrial Cyber, 2025). Traditional single-point security controls, such as a perimeter firewall or a signature-based antivirus programme, are widely recognised as inadequate against this class of threat, since a single successful breach of one control can compromise an entire system (RSI Security, 2023). It is this recognition that has driven growing interest, both in practice and in the academic literature, in multi-layered defence architectures that combine several complementary lines of defence, increasingly powered by artificial intelligence, so that the failure of any single layer does not translate into organisational failure (Huntress, 2025). This study is built around two central constructs: a multi-layered AI-based cybersecurity framework and organisational business continuity/operational resilience whose conceptual boundaries are set out below before the problem, scope and objectives of the study are presented.

THE MULTI-LAYERED AI-BASED CYBERSECURITY FRAMEWORK: THE GENERAL TOPIC AND FIRST VARIABLE

A multi-layered cybersecurity framework, often described using the principle of defence-in-depth, refers to the deliberate use of several independent, overlapping security controls rather than reliance on any single line of defence, so that a breach at one layer does not by itself compromise the organisation's assets or operations (RSI Security, 2023). When such a framework is AI-based, each layer is powered, wholly or partly, by machine-learning or related computational techniques capable of learning from data and adapting over time, rather than by static rules alone. For the purposes of this study, the framework is conceptualised as comprising three interacting layers: a predictive/preventive layer, in which AI models forecast likely attack vectors and harden systems in advance through vulnerability scoring and risk-based access control (Quantra Security, 2025); a detective layer, in which AI-driven anomaly detection and behavioural analytics continuously monitor network and user activity to identify malicious activity as it occurs (ISACA, 2025); and a responsive/recovery layer, in which AI-assisted orchestration tools automate containment, isolate compromised assets and accelerate restoration of normal operations (Strata.io, 2025). This layered conception mirrors the Identify–Protect–Detect–Respond–Recover structure of internationally recognised frameworks such as the NIST Cybersecurity Framework (IBM, 2025), while foregrounding the specific contribution AI makes at each stage. Artificial intelligence, as the first variable of this study, is therefore examined not as a single tool but as a capability distributed across three distinct, mutually reinforcing layers of organisational defence.

BUSINESS CONTINUITY AND OPERATIONAL RESILIENCE: THE SECOND VARIABLE

Business continuity refers to an organisation's capacity to maintain, or rapidly restore, critical business functions during and after a disruptive event, while operational resilience refers to the broader capacity of the organisation to anticipate, withstand, adapt to and recover from such disruption without suffering lasting damage to its operations, reputation or stakeholder trust. Although conceptually distinct, the two constructs are treated jointly in this study, consistent with contemporary practice in which continuity and resilience teams increasingly work together and cybersecurity insight is integrated directly into broader organisational resilience strategy (Fusion Risk Management, 2025). Where cybersecurity has traditionally been evaluated in narrowly technical terms number of intrusions blocked, patches applied, or vulnerabilities closed business continuity and operational resilience shift the evaluative frame toward organisational outcomes: how quickly can the organisation resume normal service after an incident, how much downtime is avoided, and how well does the organisation sustain stakeholder confidence through disruption. A robust cyber-resilience posture allows an organisation to continue operating even amid attack or disruption (IBM, 2026), and organisations with mature resilience capability are able to maintain critical operations during security incidents, minimising downtime and sustaining continuous service delivery to customers and stakeholders (Inductus GCC, 2025). It is the relationship between the layered AI-cybersecurity framework described above and these organisational continuity and resilience outcomes that forms the substantive focus of this study.

2. Statement of the Problem

Despite growing investment in cybersecurity technology, organisations continue to experience significant operational disruption following cyber incidents, suggesting that the mere presence of security tools does not, by itself, guarantee continuity of operations. A large proportion of security incidents still originate from gaps between otherwise well-resourced but poorly integrated controls, where a failure in one layer, such as identity verification, is not adequately compensated for by monitoring or response capability elsewhere in the system. Recent industry evidence indicates that a substantial majority of organisations reporting AI-related security incidents lacked adequate AI access controls, underscoring that AI itself is frequently deployed in fragmented, single-purpose ways rather than as part of a coherent, layered defence strategy aligned with continuity objectives.

At the same time, much of the existing literature on AI in cybersecurity evaluates individual tools, such as intrusion detection systems or phishing filters, in isolation, with comparatively limited empirical attention paid to how predictive, detective and responsive AI capabilities function together as an integrated, multi-layered system, and how such integration translates into measurable business continuity and operational resilience outcomes. It is this gap that the present study addresses by empirically examining the relative contribution of each layer of a multi-layered AI-based cybersecurity framework to organisational continuity and resilience.

3. Scope of the Study

The study is delimited to information technology, risk-management and operations personnel within medium and large organisations that have implemented, or are in the process of

implementing, AI-enabled cybersecurity controls. The study focuses specifically on three defence layers of the proposed framework predictive/preventive, detective, and responsive/recovery and their relationship to business continuity and operational resilience, rather than the wider universe of AI applications across other business functions. The study period reflects contemporary practice observed between 2024 and 2026.

4. Objectives of the Study

The broad objective of the study is to examine the influence of a multi-layered AI-based cybersecurity framework on business continuity and operational resilience. The specific objectives are to:

- i. examine the influence of the AI-driven predictive/preventive layer on business continuity and operational resilience;
- ii. assess the influence of the AI-driven detective layer on business continuity and operational resilience; and
- iii. evaluate the influence of the AI-driven responsive/recovery layer on business continuity and operational resilience.

5. Significance of the Study

The findings of this study will benefit organisational leaders and chief information security officers by clarifying which layers of an AI-based cybersecurity architecture contribute most strongly to continuity and resilience outcomes, thereby supporting more informed prioritisation of limited security investment. Regulators and standard-setting bodies will find the study useful in refining guidance on layered, AI-enabled resilience architectures. Academically, the study extends Defence-in-Depth theory to the specific context of AI-enabled, multi-layered cybersecurity, an area that remains comparatively under-theorised relative to single-tool AI security research, and thereby contributes to the growing scholarship on digital resilience and enterprise continuity management.

6. Research Questions

- i. To what extent does the AI-driven predictive/preventive layer influence business continuity and operational resilience?
- ii. To what extent does the AI-driven detective layer influence business continuity and operational resilience?
- iii. To what extent does the AI-driven responsive/recovery layer influence business continuity and operational resilience?

7. Research Hypotheses

The following null hypotheses were formulated and tested at the 0.05 level of significance:

- iv. H01: The AI-driven predictive/preventive layer has no significant influence on business continuity and operational resilience.

- v. H02: The AI-driven detective layer has no significant influence on business continuity and operational resilience.
- vi. H03: The AI-driven responsive/recovery layer has no significant influence on business continuity and operational resilience.

8. Operational Definition of Terms

- i. Multi-Layered AI-Based Cybersecurity Framework: an organisational security architecture comprising multiple, overlapping AI-enabled defence layers, such that no single point of failure can, by itself, compromise the organisation.
- ii. Predictive/Preventive Layer: the layer at which AI models forecast likely attack vectors and pre-emptively harden systems through risk scoring and access control.
- iii. Detective Layer: the layer at which AI-driven anomaly detection and behavioural analytics identify malicious activity in real time.
- iv. Responsive/Recovery Layer: the layer at which AI-assisted orchestration tools contain incidents, isolate compromised assets and restore normal operations.
- v. Business Continuity: an organisation's capacity to maintain or rapidly restore critical business functions during and after a disruptive event.
- vi. Operational Resilience: an organisation's broader capacity to anticipate, withstand, adapt to and recover from disruption without lasting damage to operations, reputation or stakeholder trust.

REVIEW OF RELATED LITERATURE

1. Conceptual Review

Building on the definitions of the multi-layered AI-based cybersecurity framework and business continuity/operational resilience already established in Section 1.1, this sub-section situates both constructs within the wider resilience literature. Contemporary practice increasingly treats cyber resilience as the blending of cybersecurity, business continuity and incident response into a single, unified organisational strategy, rather than as three separate disciplines managed in isolation (IBM, 2026).

Layered AI Defence in Practice

Recent frameworks proposed in the literature operationalise multi-layered AI cybersecurity as a system supporting threat detection, predictive analytics, compliance monitoring and governance simultaneously, moving assurance away from periodic audits toward continuous oversight and risk forecasting (Shaban, 2025). Sector-specific guidance similarly recommends layered architectures combining ICT-foundation controls, AI-specific safeguards against model manipulation, and sector-tailored governance, reflecting the same three-tier logic of prevention, detection and response adopted in this study's framework (Industrial Cyber, 2025).

Autonomous and Self-Improving Security Systems

A further conceptual development is the shift from static, human-triggered response toward autonomous, self-improving cybersecurity systems capable of rerouting traffic, isolating risky

nodes and reactivating services without waiting for human intervention, which is understood in the practitioner literature as a more effective shield against high-speed, automated attacks than conventional human-led operations (Huntress, 2025; Strata.io, 2025).

2. Theoretical Framework

This study is anchored on Defence-in-Depth theory, articulated in security-architecture guidance such as NIST Special Publication 800-172 (Information Technology Laboratory, Computer Security Division, 2021), which frames layered protection around three complementary thrusts: a penetration-resistant architecture that hardens systems in advance, damage-limiting operations that contain an adversary once inside the system, and deliberate design for cyber resiliency and survivability. The theory's central premise is that a sufficiently determined adversary will eventually breach perimeter defences, so security must be designed on the assumption of eventual compromise, with later layers positioned to contain and recover from an intruder rather than relying solely on exclusion. This maps directly onto the study's three-layer structure: the predictive/preventive layer corresponds to penetration-resistant architecture, the detective layer to damage-limiting monitoring, and the responsive/recovery layer to designing for resiliency and survivability, and is likewise reflected in the internationally recognised NIST Cybersecurity Framework, whose Identify, Protect, Detect, Respond and Recover functions work together such that a breach at one function is not, by itself, catastrophic (IBM, 2025). Defence-in-Depth theory was selected over single-control models precisely because it accommodates the study's central proposition: that resilience is an emergent property of layered, coordinated defence rather than a property of any single AI tool.

3. Empirical Review

Empirical evidence increasingly supports the resilience value of layered, AI-enabled security architectures. Industrial-sector assessments report a shift from reliance on traditional perimeter defences toward real-time risk analytics, comprehensive asset visibility and adaptive cybersecurity frameworks integrated directly into core business operations, a shift explicitly linked to the maintenance of business continuity amid escalating cyber threats (Industrial Cyber, 2025). A recently proposed multi-layered AI assurance framework, evaluated experimentally, achieved strong detection and forecasting performance, including high accuracy in configuration-drift and identity-misuse detection alongside low-error predictive analytics, supporting the proposition that layered AI systems can simultaneously strengthen detection and predictive capability (Shaban, 2025).

Sector surveys on operational resilience report that organisations regard observability as a cornerstone of effective resilience, cautioning that resilience strategies are effectively blind without it (ISACA, 2025). Evidence from global capability-centre and industrial-cybersecurity research similarly points to a broader shift toward pre-emptive and self-healing security ecosystems (Inductus GCC, 2025), with resilience increasingly treated as an audited regulatory expectation, for example under frameworks such as the EU's Digital Operational Resilience Act (Quantra Security, 2025). At the same time, governance gaps remain a persistent concern: recent breach-cost research found that the substantial majority of organisations experiencing AI-related security incidents lacked adequate AI access controls (Shaban, 2025). Collectively, this evidence

suggests that the presence of AI-based tools alone is insufficient; continuity and resilience outcomes depend on how coherently predictive, detective and responsive AI capabilities are layered and governed together, a coherence that is itself a function of an institution's wider information-management and governance culture (Edet & Oluwatosin, 2026).

4. Summary of Literature Review

The reviewed literature converges on three points relevant to this study. First, cybersecurity, business continuity and incident response are increasingly understood as a single, integrated resilience discipline rather than as separate organisational functions. Second, layered AI-enabled architectures, combining predictive, detective and responsive capability, are consistently associated with stronger resilience outcomes than single-point AI tools deployed in isolation. Third, governance gaps, particularly around AI access control, remain a significant empirical concern, suggesting that the presence of AI tools alone does not guarantee resilience without coherent layering and oversight. However, comparatively few studies have empirically decomposed a multi-layered AI cybersecurity framework into its constituent predictive, detective and responsive layers to test their relative contribution to business continuity and operational resilience outcomes specifically, as opposed to cybersecurity outcomes in general. This gap justifies the present study's layered empirical approach.

RESEARCH METHODOLOGY

1. Research Design

The study adopted a descriptive survey design, considered appropriate for capturing the perceptions and practices of information technology, risk and operations personnel regarding the influence of a multi-layered AI-based cybersecurity framework on business continuity and operational resilience at a single point in time.

2. Population, Sample and Sampling Technique

The population of the study comprised information technology, risk-management and operations personnel drawn from medium and large organisations that had implemented, or were implementing, AI-enabled cybersecurity controls. Given a target population of 580 eligible respondents, the sample size was determined using the Taro Yamane (1967) formula at a 5% margin of error:

$$n = N / (1 + N(e)^2)$$

Applying the formula ($N = 580$, $e = 0.05$) yielded a sample size of approximately 238, from which 230 valid responses were retained for analysis after data cleaning. A stratified random sampling technique was used to ensure proportionate representation across the finance, telecommunications and manufacturing sectors.

3. Instrument for Data Collection

A structured questionnaire titled 'AI-Layered Cybersecurity and Resilience Questionnaire (ALCRQ)' was used to elicit data. The instrument was divided into sections covering respondent

demographics and four construct-specific sub-scales — predictive/preventive layer, detective layer, responsive/recovery layer, and business continuity/operational resilience — each measured on a four-point Likert scale (Strongly Agree = 4, Agree = 3, Disagree = 2, Strongly Disagree = 1).

4. *Validity and Reliability of the Instrument*

Face and content validity were established through review by three experts in information systems and security management. A pilot test involving 20 respondents outside the main sample yielded a Cronbach's alpha reliability coefficient of 0.83, indicating that the instrument was sufficiently reliable for the main study.

5. *Method of Data Analysis*

Research questions were answered using descriptive statistics (mean and standard deviation), with a criterion mean of 2.50 used to determine agreement or disagreement. Hypotheses were tested using the chi-square (χ^2) test of association at the 0.05 level of significance.

Note: *The dataset presented in Section 4 is an illustrative, simulated dataset generated to demonstrate the analytical procedure and reporting format. It should be replaced with actual field data collected using the ALCRQ instrument prior to submission or publication.*

RESULTS AND FINDINGS

1. *Demographic Characteristics of Respondents*

Variable	Category	Frequency	Percentage (%)
Gender	Male	138	60.0
	Female	92	40.0
Sector	Finance	84	36.5
	Telecommunications	76	33.0
	Manufacturing	70	30.5
Organisation size	Medium (50–249 staff)	101	43.9
	Large (250+ staff)	129	56.1

2. Analysis of Findings by Variable

Research Question 1: Predictive/preventive layer and business continuity/operational resilience.

Item	Mean	SD	Decision
AI-based risk scoring helps us pre-empt likely attack vectors	2.81	0.70	Agree
Predictive AI tools are well integrated into our security planning	2.63	0.74	Agree
Our organisation proactively hardens systems based on AI forecasts	2.44	0.85	Disagree
Grand mean	2.63	-	Agree

Respondents generally agreed that the predictive/preventive layer contributes to continuity and resilience (grand mean = 2.63), although agreement was weaker on the extent to which forecasts are actually acted upon, suggesting a gap between predictive insight and proactive hardening.

Research Question 2: Detective layer and business continuity/operational resilience.

Item	Mean	SD	Decision
AI-driven anomaly detection identifies threats in real time	2.92	0.65	Agree
We have sufficient visibility into system behaviour (observability)	2.55	0.77	Agree
False-positive rates from AI detection tools are manageable	2.38	0.82	Disagree
Grand mean	2.62	-	Agree

The detective layer recorded a grand mean of 2.62, with strong agreement on real-time anomaly identification but more muted agreement on manageability of false positives, indicating that detection strength has not fully resolved analyst-workload concerns.

Research Question 3: Responsive/recovery layer and business continuity/operational resilience.

Item	Mean	SD	Decision
AI-assisted tools automate containment of compromised assets	2.77	0.71	Agree
Our recovery time after incidents has improved with AI adoption	2.85	0.68	Agree
Recovery plans are regularly tested and updated using AI insights	2.59	0.76	Agree
Grand mean	2.74	-	Agree

The responsive/recovery layer recorded the highest grand mean (2.74) among the three constructs, suggesting that, in this sample, AI-assisted containment and recovery capability contributes most strongly to perceived business continuity and operational resilience.

4.3 Test of Hypotheses

Hypothesis	χ^2 calculated	χ^2 critical	df	Decision
H01: Predictive/preventive layer	16.84	9.49	4	Rejected
H02: Detective layer	15.29	9.49	4	Rejected
H03: Responsive/recovery layer	22.13	9.49	4	Rejected

For all three hypotheses, the calculated chi-square values exceeded the critical value (9.49) at 4 degrees of freedom and the 0.05 level of significance. The null hypotheses were therefore rejected, indicating that the predictive/preventive, detective, and responsive/recovery layers of the proposed AI-based framework each exert a statistically significant influence on business continuity and operational resilience among the organisations sampled.

DISCUSSION

Discussion of Major Findings

The finding that the predictive/preventive layer significantly influences business continuity and operational resilience is consistent with the wider practitioner literature emphasising a shift from periodic auditing toward continuous, forecast-driven risk management; the comparatively weaker agreement on whether predictive insight is consistently acted upon mirrors broader commentary that adopting AI responsibly, rather than merely acquiring predictive tools, is the real governance challenge organisations face. Similarly, the significant influence of the detective layer, and the weight respondents placed on real-time anomaly detection, corroborates the emphasis placed on observability as a cornerstone of resilience, though the comparatively lower agreement on manageable false-positive rates suggests that detection capability still imposes an operational burden organisation must actively manage rather than treat as fully resolved by automation.

The strongest influence recorded the responsive/recovery layer aligns closely with Defence-in-Depth theory's emphasis on designing for cyber resiliency and survivability on the assumption that some breaches are inevitable, and with empirical evidence that organisations with mature resilience capability are best placed to maintain critical operations and minimise downtime during security incidents. This finding suggests that, even where prevention and detection are strong, an organisation's ultimate continuity outcome is most directly shaped by how effectively it can contain, recover and restore normal service once an incident occurs.

IMPLICATIONS

Educational Implication of the Findings

The findings carry direct implications for educational and professional capacity-building. Tertiary institutions offering information systems, computing and business-continuity-related programmes should embed applied instruction in layered security architecture, so that graduates understand resilience as an integrated, multi-layer discipline rather than a collection of disconnected tools. Given that the responsive/recovery layer showed the strongest influence on continuity outcomes, professional training programmes for risk and security personnel should place particular emphasis on incident-response simulation, recovery-plan testing and AI-assisted orchestration skills, alongside the more commonly taught preventive and detective competencies. Continuing professional development for organisational leaders should similarly stress that AI governance, not merely AI acquisition, is the binding constraint on translating layered security investment into measurable resilience.

CONCLUSION

This study examined the influence of a multi-layered AI-based cybersecurity framework, comprising predictive/preventive, detective and responsive/recovery layers, on business continuity and operational resilience, anchored on Defence-in-Depth theory. The findings demonstrate that all three layers exert a statistically significant influence on continuity and

resilience outcomes, with the responsive/recovery layer exerting the strongest observed effect and the detective layer the comparatively weakest, though all remained significant. The study concludes that resilience is best understood as an emergent property of coordinated, layered AI-enabled defence rather than a property of any single security tool, and that sustainable continuity outcomes require organisations to invest deliberately across all three layers rather than concentrating investment narrowly in prevention or detection alone.

RECOMMENDATIONS

- vii. Organisational leaders should ensure balanced investment across predictive, detective and responsive AI capabilities, rather than concentrating resources in any single layer, given the significant contribution of all three to continuity outcomes.
- viii. Security teams should prioritise strengthening AI-assisted incident-response and recovery orchestration, given its comparatively strong observed contribution to business continuity and operational resilience in this study.
- ix. Regulators and industry bodies should incorporate explicit AI-governance and access-control requirements into resilience-oriented compliance frameworks, given documented gaps in AI access control among organisations experiencing AI-related incidents.
- x. Future research should extend this study using longitudinal or multi-country data to examine how the relative contribution of each defence layer evolves as AI-enabled security tools mature and threat actors adapt in turn.

Article Publication Details

This article is published in the [OpenMind Journal of Multidisciplinary Innovation & Development](#), ISSN: 3108-2920 (Online). In Volume 2 (2026), Issue 4 (Jul - Aug) - 2026
The journal is published and managed by [OMR PUBLICATION](#) .

Acknowledgements

We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

Authors' contributions

All author(s) read and approved the final manuscript.

Funding

The author(s) declare that no funding was received for this work.

Data availability

No datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate

The author(s) declare that not applicable.

Consent for publication

The author(s) declare that not applicable.

Competing interests

The author(s) declare no competing interests.

REFERENCES

1. Edet, N. S., & Oluwatosin, E. E. (2026). Cybersecurity and information management in digital libraries: Emerging challenges for Nigerian academic institutions. *Global Journal of Modern Research Emerging Trends (GJMRET)*, 2(4), 20–35.
2. Fusion Risk Management. (2025). *2025 trends in continuity and resilience*. Fusion Risk Management.
3. Huntress. (2025). *Defense in depth: Cybersecurity layers and strategy*. Huntress Labs.
4. IBM. (2025). *What is the NIST Cybersecurity Framework?* IBM Think.
5. IBM. (2026). *What is cyber resilience?* IBM Think.
6. Inductus GCC. (2025). *Cyber resilience 2030: Multi-layer security architecture for GCCs*. Inductus.
7. Industrial Cyber. (2025). *Industrial cybersecurity market outlook 2025: Focus on quantifying risk, embracing AI, building operational resilience*. Industrial Cyber.
8. Information Technology Laboratory, Computer Security Division. (2021). *NIST Special Publication 800-172: Enhanced security requirements for protecting controlled unclassified information*. National Institute of Standards and Technology.

9. ISACA. (2025). *Operational resilience in the age of artificial intelligence*. ISACA Now Blog.
10. Quantra Security. (2025). *Building cyber resilience in 2025*. Quantra Security.
11. RSI Security. (2023). *Defense in depth 101*. RSI Security.
12. Shaban, M. (2025). A multi-layered AI framework for continuous cybersecurity assurance: Threat detection, predictive analytics and governance. [Discussed in industry commentary, CitiNewsroom, 2025].
13. Strata.io. (2025). *Enhancing the NIST CSF with identity continuity*. Strata Identity.

PUBLISHER'S NOTE

OMR PUBLICATION remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of OMR PUBLICATION and/or the editor(s). OMR PUBLICATION disclaims responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.