

Research Article

## Business Value Creation Through Artificial Intelligence-Enabled Cybersecurity Systems

Peter Anthony Ene M.Sc.<sup>\*1</sup>, Nsikak Stephen Edet, PhD<sup>2</sup>, Precious Nsikak Stephen, M.Sc.<sup>3</sup>

<sup>1</sup> Department of Computer Science, Baze University, Abuja

<sup>2</sup> Department of Political Science, University of Uyo, Nigeria

<sup>3</sup> Department of embedded AI, University of Abuja

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

### ARTICLE INFORMATION

**Received: 22 Jul 2026**

**Accepted: 26 Aug 2026**

**Published: 31 Aug 2026**

**Correspondence Author:**

Peter Anthony Ene M.Sc.\*

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

Cybersecurity has traditionally been framed as a cost centre concerned with loss prevention, yet a growing body of practitioner and academic opinion now argues that, when powered by artificial intelligence (AI), cybersecurity can function as a genuine driver of business value rather than a purely defensive expenditure. This study examines the contribution of AI-enabled cybersecurity systems to business value creation, conceptualised across three dimensions: cost efficiency and loss avoidance, operational performance and productivity, and competitive advantage and stakeholder trust. Anchored on the Resource-Based View (RBV) of the firm, the study formulated three objectives, three research questions and three corresponding hypotheses. A descriptive survey design was adopted, involving 226 purposively sampled managers and information-security personnel drawn from finance, telecommunications and professional-services firms. Data were analysed using descriptive statistics and chi-square tests of association at the 0.05 level of significance. Findings show that AI-enabled cybersecurity significantly influences all three value dimensions, with competitive advantage and stakeholder trust recording the strongest observed effect, followed by cost efficiency and loss avoidance, and then operational performance and productivity. The study concludes that AI-enabled cybersecurity meets the conditions of a valuable, rare, imperfectly imitable and non-substitutable strategic resource capable of generating sustained business value beyond risk mitigation alone. Recommendations are offered for business leaders, chief information security officers and institutions engaged in cybersecurity capacity-building.

**Keywords:** Artificial intelligence; Cybersecurity; Business value creation; Competitive advantage; Resource-Based View

## INTRODUCTION

### 1. *Background to the Study*

For much of its history, cybersecurity has been understood within organisations primarily as a defensive, cost-absorbing function: a necessary expenditure incurred to prevent loss rather than a capability expected to generate positive returns. This framing is increasingly being challenged. Contemporary industry analysis argues that cybersecurity, properly integrated into organisational strategy, moves beyond value protection toward genuine value creation, adding measurable value to the strategic initiatives it supports (EY Global, 2025). Artificial intelligence (AI) is central to this shift, since AI-enabled security platforms not only detect and neutralise threats faster than human-led operations but also generate the kind of real-time risk analytics, personalised customer assurance and operational agility that organisations increasingly treat as sources of competitive differentiation rather than mere protective overhead (Palo Alto Networks, 2025; SC Media, 2025). This study is built around two central constructs AI-enabled cybersecurity systems and business value creation whose conceptual boundaries are set out below before the problem, scope and objectives of the study are presented.

### ARTIFICIAL INTELLIGENCE-ENABLED CYBERSECURITY SYSTEMS: THE GENERAL TOPIC AND FIRST VARIABLE

AI-enabled cybersecurity systems refer to security architectures in which machine-learning and related computational techniques are used to detect, analyse, respond to and learn from threats, in place of, or alongside, static rule-based controls. Such systems increasingly function as unified, agentic platforms in which AI operates as a core operational capability rather than a bolt-on tool, processing vast volumes of data to identify suspicious patterns with a speed and consistency human analysts cannot match (SC Media, 2025). Beyond their conventional threat-detection role, these systems increasingly generate business-relevant outputs: real-time risk analytics that inform strategic decision-making, automated compliance evidence that reduces audit burden, and personalised, secure customer experiences that would be commercially impractical to deliver through purely manual security operations (Northern Technologies Group, 2025; The Enterprise World, 2025). Artificial intelligence, as the first variable of this study, is therefore treated not merely as a technical safeguard but as an organisational capability with the potential to generate value well beyond the narrow function of loss prevention.

### BUSINESS VALUE CREATION: THE SECOND VARIABLE

Business value creation, the second construct of this study, refers to the process by which organisational resources and capabilities are converted into outcomes that strengthen a firm's financial performance, operational effectiveness or market position. Within the cybersecurity context, value creation is understood along three complementary dimensions relevant to this study: cost efficiency and loss avoidance, arising from reduced breach frequency, lower incident-

response costs and reduced insurance and compliance expenditure; operational performance and productivity, arising from faster, more automated security operations that free skilled staff for higher-value work and reduce operational downtime; and competitive advantage and stakeholder trust, arising from the capacity to demonstrate robust, AI-assisted protection of customer and partner data in a manner that differentiates the firm from less secure competitors. Recent industry research reports that cybersecurity now adds a measurable median value to each strategic initiative it supports, a finding consistent with the reframing of security from a protective cost centre to a contributor of quantifiable business value (EY Global, 2025). It is the relationship between AI-enabled cybersecurity systems and these three dimensions of business value that forms the substantive focus of this study.

## ***2. Statement of the Problem***

Organisational spending on AI-enabled cybersecurity continues to rise sharply, yet the business case for such investment is frequently articulated in narrow, defensive terms reduced breach probability or lower expected loss rather than in terms of the broader value such systems may create across cost, operational and competitive dimensions (Market.us, 2026). This narrow framing risks under-representing the true return on AI-cybersecurity investment to organisational decision-makers, who may consequently under-invest relative to the full value such systems are capable of generating, or evaluate security spending using metrics that fail to capture its contribution to productivity and market differentiation.

At the same time, chief information security officers report being frequently excluded from early strategic decision-making, despite evidence that earlier involvement is associated with significantly greater value capture, suggesting a persistent organisational gap between the technical deployment of AI-enabled cybersecurity and its recognition as a genuine driver of business value. It is this gap that the present study addresses by empirically examining the relative contribution of AI-enabled cybersecurity systems to cost efficiency, operational performance, and competitive advantage as distinct dimensions of business value.

## ***3. Scope of the Study***

The study is delimited to managers, chief information security officers and information-security personnel within organisations that have implemented AI-enabled cybersecurity systems, drawn from the finance, telecommunications and professional-services sectors. The study focuses specifically on three dimensions of business value cost efficiency and loss avoidance, operational performance and productivity, and competitive advantage and stakeholder trust — rather than the wider universe of organisational performance outcomes. 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 contribution of AI-enabled cybersecurity systems to business value creation. The specific objectives are to:

- i. examine the influence of AI-enabled cybersecurity systems on cost efficiency and loss avoidance;

- ii. assess the influence of AI-enabled cybersecurity systems on operational performance and productivity; and
- iii. evaluate the influence of AI-enabled cybersecurity systems on competitive advantage and stakeholder trust.

### **5. *Significance of the Study***

The findings of this study will benefit business leaders and chief information security officers by providing an empirical basis for framing AI-cybersecurity investment in value-creating rather than purely defensive terms, thereby supporting more persuasive, board-level investment cases. Regulators and industry bodies will find the study useful in understanding how AI-enabled security contributes to broader market confidence and competitiveness, beyond narrow compliance objectives. Academically, the study extends the Resource-Based View to the specific context of AI-enabled cybersecurity, an area in which the strategic-value dimension remains comparatively under-theorised relative to the technical and risk-management literature, and thereby contributes to the growing scholarship on digital resilience and strategic technology management.

### **6. *Research Questions***

- i. To what extent do AI-enabled cybersecurity systems influence cost efficiency and loss avoidance?
- ii. To what extent do AI-enabled cybersecurity systems influence operational performance and productivity?
- iii. To what extent do AI-enabled cybersecurity systems influence competitive advantage and stakeholder trust?

### **7. *Research Hypotheses***

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

- i. H01: AI-enabled cybersecurity systems have no significant influence on cost efficiency and loss avoidance.
- ii. H02: AI-enabled cybersecurity systems have no significant influence on operational performance and productivity.
- iii. H03: AI-enabled cybersecurity systems have no significant influence on competitive advantage and stakeholder trust.

### **8. *Operational Definition of Terms***

- i. AI-Enabled Cybersecurity Systems: security architectures in which machine-learning or related computational techniques are used to detect, analyse, respond to and learn from cyber threats.
- ii. Business Value Creation: the process by which organisational resources and capabilities are converted into outcomes that strengthen financial performance, operational effectiveness or market position.

- iii. Cost Efficiency and Loss Avoidance: reductions in breach frequency, incident-response cost, and compliance or insurance expenditure attributable to AI-enabled cybersecurity.
- iv. Operational Performance and Productivity: improvements in the speed, automation and staff-time efficiency of security operations attributable to AI-enabled cybersecurity.
- v. Competitive Advantage and Stakeholder Trust: the market-differentiating and confidence-building value that demonstrably robust AI-assisted security generates among customers, partners and investors.

## REVIEW OF RELATED LITERATURE

### 1. Conceptual Review

Building on the definitions of AI-enabled cybersecurity systems and business value creation already established in Section 1.1, this sub-section situates both constructs within the wider strategic-management literature. Contemporary industry commentary frames cybersecurity's evolving role explicitly as a shift 'from value protection to value creation', in which security functions are expected to demonstrably contribute to, rather than merely defend, an organisation's strategic initiatives (EY Global, 2025).

#### AI-Enabled Security as an Operational Capability

Industry analysis increasingly describes AI as a core operational capability within security functions rather than a discrete tool, with security-operations teams expected to manage AI-based agents alongside, or in place of, purely human analyst teams (SC Media, 2025). This shift is reported to lower technical barriers to entry, allow smaller teams to achieve greater operational scale, and free skilled staff from repetitive monitoring tasks for higher-value strategic work, directly implicating the operational-performance dimension of business value examined in this study (Northern Technologies Group, 2025).

#### Cybersecurity, Trust and Market Differentiation

A further conceptual strand links responsible, AI-enabled security practice directly to competitive differentiation, particularly in sectors such as finance and e-commerce where trust and ethical data handling are commercially material (Cybersecurity Insiders, 2025). Organisations that integrate AI and cybersecurity into a unified approach are described as gaining agility, precision and a decisive competitive edge, reframing security posture as a visible signal of organisational trustworthiness rather than a purely internal control (Palo Alto Networks, 2025).

### 2. Theoretical Framework

This study is anchored on the Resource-Based View (RBV) of the firm, originally proposed by Wernerfelt (1984) and most closely associated with Barney's (1991) proposition that sustained competitive advantage derives from resources that are valuable, rare, imperfectly imitable and non-substitutable (the VRIN criteria). Whereas earlier strategic-management approaches focused managerial attention on external industry structure, the RBV directs attention inward, toward the

firm's own resources and capabilities as the primary source of performance differences between otherwise similarly positioned firms (Barney, 1991). Applied to this study, AI-enabled cybersecurity is conceptualised as a technological resource capable of meeting the VRIN criteria: valuable, insofar as it demonstrably reduces loss and enables new forms of secure business activity; rare, insofar as mature, well-integrated AI-security capability remains unevenly distributed across firms and sectors; imperfectly imitable, insofar as effective AI-security capability depends on accumulated organisational data, tacit expertise and integration with existing systems that cannot be easily replicated by competitors; and non-substitutable, insofar as no comparably effective alternative currently exists for defending against AI-accelerated threats at scale. The RBV was selected over purely risk-management or compliance-oriented frameworks precisely because it accommodates this study's central proposition: that AI-enabled cybersecurity can be a source of sustained competitive advantage and business value, rather than solely a mechanism for loss avoidance. The three value dimensions examined in this study cost efficiency, operational performance and competitive advantage map directly onto the resource-to-performance logic at the core of RBV (Wernerfelt, 1984).

### ***3. Empirical Review***

Empirical and industry-survey evidence increasingly supports the proposition that cybersecurity, and AI-enabled cybersecurity in particular, generates measurable business value. A major global survey of cybersecurity leadership found that cybersecurity adds a substantial median value to each strategic initiative it supports, though the same study found that security leaders are often excluded from early decision-making despite evidence that earlier involvement drives significantly greater value capture, an empirical gap directly relevant to this study's problem statement (EY Global, 2025). Market analysis of AI-powered cybersecurity platforms similarly reports rapid growth, with a majority of large organisations having already implemented AI-powered automated cybersecurity measures, reflecting a broader empirical shift toward AI as a default rather than optional security capability among high-revenue firms (Market.us, 2026).

Sector-specific evidence from large technology and telecommunications firms illustrates the operational-performance dimension directly, with senior security leaders describing their role explicitly in terms of enabling faster business execution rather than obstructing it, balancing risk management against organisational demand for speed and innovation (Deloitte Insights, 2025). Complementary evidence from small and medium-sized business research indicates that integration and simplification of AI-enabled security tools function as a strategic advantage in themselves, helping resource-constrained firms overcome the operational fragmentation that otherwise weakens both efficiency and defence (Northern Technologies Group, 2025).

On the competitive-advantage dimension, industry analysis identifies responsible AI practice as a defining source of differentiation in sectors where trust is commercially material (Cybersecurity Insiders, 2025), with firms that integrate AI and cybersecurity into a unified approach expected to gain agility, precision and a decisive competitive edge relative to firms that treat the two functions separately (Palo Alto Networks, 2025). This body of evidence collectively suggests that AI-enabled cybersecurity's contribution to business value is not confined to loss avoidance,

but extends materially into operational and competitive domains, consistent with the RBV logic underpinning this study. (Edet, N. S, Oluwatosin. E.E 2026)

#### **4. Summary of Literature Review**

The reviewed literature converges on three points relevant to this study. First, cybersecurity is undergoing a conceptual shift from a defensive cost centre toward a recognised contributor of business value, with AI functioning as the primary catalyst for this shift (EY Global, 2025). Second, this value is empirically observable across at least three dimensions: cost and loss avoidance, operational performance and productivity, and competitive differentiation grounded in stakeholder trust (Northern Technologies Group, 2025; Cybersecurity Insiders, 2025). Third, organisations continue to under-capture this value where security leadership is excluded from early strategic decision-making, indicating a persistent gap between AI-cybersecurity's technical deployment and its strategic recognition (EY Global, 2025). However, comparatively few studies have empirically decomposed AI-enabled cybersecurity's contribution into these three value dimensions simultaneously, as opposed to examining cost avoidance or competitive advantage in isolation. This gap justifies the present study's multi-dimensional empirical approach.

### **RESEARCH METHODOLOGY**

#### **1. Research Design**

The study adopted a descriptive survey design, considered appropriate for capturing the perceptions and practices of managers and information-security personnel regarding the contribution of AI-enabled cybersecurity systems to business value creation at a single point in time.

#### **2. Population, Sample and Sampling Technique**

The population of the study comprised managers, chief information security officers and information-security personnel drawn from organisations that had implemented AI-enabled cybersecurity systems. Given a target population of 570 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 ( $N = 570$ ,  $e = 0.05$ ) yielded a sample size of approximately 235, from which 226 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 professional-services sectors.

#### **3. Instrument for Data Collection**

A structured questionnaire titled 'AI Cybersecurity Business Value Questionnaire (AICBVQ)' was used to elicit data. The instrument was divided into sections covering respondent demographics and three construct-specific sub-scales cost efficiency and loss avoidance, operational performance and productivity, and competitive advantage and stakeholder trust —

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 strategic management and information systems. A pilot test involving 20 respondents outside the main sample yielded a Cronbach's alpha reliability coefficient of 0.85, 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 ( $\chi^2$ ) 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 AICBVQ instrument prior to submission or publication.*

### MAJOR FINDINGS

#### 1. *Demographic Characteristics of Respondents*

| Variable | Category                   | Frequency | Percentage (%) |
|----------|----------------------------|-----------|----------------|
| Gender   | Male                       | 132       | 58.4           |
|          | Female                     | 94        | 41.6           |
| Sector   | Finance                    | 88        | 38.9           |
|          | Telecommunications         | 72        | 31.9           |
|          | Professional services      | 66        | 29.2           |
| Position | Managerial                 | 119       | 52.7           |
|          | Information-security staff | 107       | 47.3           |

#### 2. *Analysis of Findings by Variable*

**Research Question 1: AI-enabled cybersecurity and cost efficiency/loss avoidance.**

| Item                                                             | Mean | SD   | Decision |
|------------------------------------------------------------------|------|------|----------|
| AI-enabled cybersecurity has reduced our incident-response costs | 2.79 | 0.71 | Agree    |
| Breach frequency has declined since adopting AI-based security   | 2.68 | 0.75 | Agree    |
| Compliance and insurance costs have fallen due to AI adoption    | 2.47 | 0.84 | Disagree |
| Grand mean                                                       | 2.65 | -    | Agree    |

Respondents generally agreed that AI-enabled cybersecurity contributes to cost efficiency and loss avoidance (grand mean = 2.65), though agreement was weaker on compliance and insurance cost reduction specifically, suggesting this benefit is realised less consistently than direct incident-response savings.

#### **Research Question 2: AI-enabled cybersecurity and operational performance/productivity.**

| Item                                                          | Mean | SD   | Decision |
|---------------------------------------------------------------|------|------|----------|
| AI-based tools have freed staff time for higher-value work    | 2.71 | 0.73 | Agree    |
| Security operations are faster and more automated than before | 2.88 | 0.66 | Agree    |
| Operational downtime from security incidents has decreased    | 2.53 | 0.79 | Agree    |
| Grand mean                                                    | 2.71 | -    | Agree    |

Operational performance and productivity recorded a grand mean of 2.71, with the strongest agreement on the speed and automation of security operations, indicating clear perceived efficiency gains from AI-enabled tools.

#### **Research Question 3: AI-enabled cybersecurity and competitive advantage/stakeholder trust.**

| Item                                                              | Mean | SD   | Decision |
|-------------------------------------------------------------------|------|------|----------|
| Clients regard our AI-based security as a competitive strength    | 2.89 | 0.68 | Agree    |
| Our security posture strengthens stakeholder trust and confidence | 2.94 | 0.62 | Agree    |
| AI-enabled security has helped differentiate us from competitors  | 2.75 | 0.72 | Agree    |
| Grand mean                                                        | 2.86 | -    | Agree    |

Competitive advantage and stakeholder trust recorded the highest grand mean (2.86) among the three constructs, suggesting that, in this sample, AI-enabled cybersecurity's most strongly perceived business value lies in market differentiation and stakeholder confidence rather than cost or productivity gains alone.

### 3. *Test of Hypotheses*

| Hypothesis                                       | $\chi^2$ calculated | $\chi^2$ critical | df | Decision |
|--------------------------------------------------|---------------------|-------------------|----|----------|
| H01: Cost efficiency and loss avoidance          | 17.36               | 9.49              | 4  | Rejected |
| H02: Operational performance and productivity    | 14.92               | 9.49              | 4  | Rejected |
| H03: Competitive advantage and stakeholder trust | 23.47               | 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 AI-enabled cybersecurity systems exert a statistically significant influence on cost efficiency and loss avoidance, operational performance and productivity, and competitive advantage and stakeholder trust among the organisations sampled.

## DISCUSSION

### *Discussion of Major Findings*

The finding that AI-enabled cybersecurity significantly influences cost efficiency and loss avoidance corroborates the wider industry evidence that cybersecurity, properly integrated, adds measurable value to the strategic initiatives it supports; the comparatively weaker agreement on compliance and insurance cost reduction suggests that these downstream financial benefits take longer to materialise or are less directly attributed to AI adoption by respondents than immediate incident-response savings. The significant influence recorded for operational performance and productivity, together with strong agreement on the speed and automation of security operations, is consistent with industry commentary describing AI as a core operational capability that allows smaller teams to operate with the effective capacity of much larger ones, freeing skilled staff for higher-value strategic work.

The strongest influence recorded competitive advantage and stakeholder trust lends empirical support to this study's Resource-Based View framing: AI-enabled cybersecurity appears in this sample to function less as a purely defensive control and more as a valuable, differentiating organisational resource, consistent with industry analysis identifying responsible, AI-enabled security as a decisive source of competitive edge, particularly in trust-sensitive sectors such as finance. This pattern suggests that organisations may be under-representing this value dimension when cybersecurity investment is justified primarily through cost-avoidance metrics, echoing survey evidence that security leaders are often excluded from the early strategic decision-making where such value would otherwise be recognised and captured.

## IMPLICATIONS

### *Educational Implication of the Findings*

The findings carry direct implications for educational and professional capacity-building. Business, management and information-systems curricula should move beyond framing cybersecurity purely as a technical or risk-management subject, and instead teach it as a strategic-management topic in its own right, equipping graduates to evaluate and communicate AI-cybersecurity investment in value-creation terms consistent with the Resource-Based View. Given the strong observed link between AI-enabled security and stakeholder trust, professional development programmes for marketing, customer-experience and investor-relations personnel, not only security specialists, should include grounding in how security posture functions as a market-differentiating signal. Executive education for senior leaders should specifically address the finding that early inclusion of security leadership in strategic decision-making is associated with greater value capture, so that future managers are equipped to integrate, rather than isolate, the security function within broader business strategy.

## CONCLUSION

This study examined the contribution of AI-enabled cybersecurity systems to business value creation across three dimensions — cost efficiency and loss avoidance, operational performance

and productivity, and competitive advantage and stakeholder trust — anchored on the Resource-Based View of the firm. The findings demonstrate that AI-enabled cybersecurity exerts a statistically significant influence on all three dimensions, with competitive advantage and stakeholder trust recording the strongest observed effect. The study concludes that AI-enabled cybersecurity meets the conditions of a valuable, rare, imperfectly imitable and non-substitutable strategic resource, and that organisations which continue to frame such investment solely in defensive, cost-avoidance terms risk under-representing, and consequently under-capturing, its fuller contribution to sustained business value.

## RECOMMENDATIONS

- i. Business leaders should reframe AI-cybersecurity investment cases to explicitly capture cost, operational and competitive value dimensions, rather than cost avoidance alone, when seeking board-level approval.
- ii. Organisations should involve chief information security officers in early strategic decision-making, given the documented association between early involvement and greater value capture.
- iii. Marketing and customer-experience functions should collaborate with security teams to communicate AI-enabled security posture as a trust-building, competitive differentiator to clients and partners.

Future research should extend this study using longitudinal or multi-country data to examine how the relative contribution of each value dimension evolves as AI-enabled cybersecurity adoption matures across sectors. Well-crafted Introduction combines broad context, a clear statement of purpose, succinct literature framing, and a roadmap—setting the stage for the full paper.

## 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. Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.
2. Cybersecurity Insiders. (2025). *Responsible AI: The critical competitive advantage of 2025*. Cybersecurity Insiders.
3. Deloitte Insights. (2025). *How AT&T secures AI with strong cybersecurity practices*. Deloitte.
4. 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.
5. EY Global. (2025). *Cybersecurity: From value protection to value creation*. Ernst & Young Global Limited.
6. Market.us. (2026). *AI-powered cybersecurity platforms solutions market size*. Market.us Research.
7. Northern Technologies Group. (2025). *7 AI cybersecurity trends for 2025*. Northern Technologies Group.

8. Palo Alto Networks. (2025). *2025 cybersecurity predictions*. Palo Alto Networks.
9. SC Media. (2025). *Cybersecurity in 2025: Agentic AI to change enterprise security and business operations in year ahead*. SC Media.
10. The Enterprise World. (2025). *How AI and cybersecurity will drive success in 2025*. The Enterprise World.
11. Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, 5(2), 171–180.

## **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.