Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

The Impact of AI-Powered Business Analytics on Organizational Agility and Competitive Advantage

Sakir Alim

sakir971alim@gmail.com

Obafemi Awolowo University

Sudan Chundali

Tribhuvan University

Arpan Upadhyaya

Symbiosis Institute of Business

Research Article

Keywords: Artificial Intelligence, Business Analytics, Organizational Agility, Competitive Advantage, Dynamic Capabilities, AI Maturity Model, Machine Learning, Decision Intelligence, Digital Transformation, Cybersecurity Governance, AI Security, Cyber Resilience, Data Protection, Cyber Risk Management

Posted Date: July 17th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10375254/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

The Impact of AI-Powered Business Analytics on Organizational Agility and Competitive Advantage

The Moderating Role of Cybersecurity Governance and Cyber Resilience

A Conceptual Framework and Multi-Industry Empirical Research Design

1, Sudan Chundali
Faculty of Management
Tribhuvan University, Kathmandu, Nepal

2, Arpan Upadhyaya
Symbiosis Institute of Business Management, Pune India

Abstract

As Artificial Intelligence (AI) spreads across enterprise analytics platforms, scholarly research is resurging on its impact on organizational agility and competitive advantage in the era of AI-driven business analytics. While empirical studies are increasing, the field is still split between theoretical streams and there is no single approach available that offers a coherent and mutually consistent description of AI analytics capability, organizational sensing and response mechanisms, cybersecurity governance and sustainable competitive positioning. These gaps are tackled in this paper by four main contributions. In the first step, we perform a structured literature review of 142 peer-reviewed papers published in IEEE, Elsevier, Springer, ACM, and Wiley journals, which is extended to include recent research in AI security, cyber risk management, and cyber resilience. Second, we design the Adaptive AI Analytics Capability Framework (AAACF), a new conceptual framework that merges resource-based view (RBV), dynamic capabilities theory and information processing theory to illustrate how AI analytics capabilities, secured and governed in an ever-evolving cyber threat landscape, drive agility and advantage. Third, we suggest that cybersecurity posture can be considered as a parallel developmental path to an AI Analytics maturity model consisting of 5 stages, and propose and justify 12 research hypotheses, and design an empirical study across 800-1500 organizations in industry sectors ranging from Manufacturing to Financial Services, Retail to Healthcare and Logistics to manufacturing. Case studies of AI-powered analytics implemented at scale at companies like Amazon, Netflix, and Microsoft reveal how these frontier companies have adopted AI and how they have built secure-by-design infrastructure and enterprise cybersecurity governance. The paper ends with a framework of future research challenges, which include generative AI, agentic AI, explainable AI, decision intelligence, digital twins, secure AI deployment, and responsible AI governance. The results have implications for the designers of AI analytics roadmaps that are cyber resilient, and for researchers who are building a unified theory of the competitive advantage of AI.

Keywords: Artificial Intelligence; Business Analytics; Organizational Agility; Competitive Advantage; Dynamic Capabilities; AI Maturity Model; Machine Learning; Decision Intelligence; Digital Transformation; Cybersecurity Governance; AI Security; Cyber Resilience; Data Protection; Cyber Risk Management

1. Introduction

In the past and even in today's era, the quality and timeliness of information to managers has been crucial to organizational decision making. Today, the context in which this information is created, and the way in which it is used and acted upon is very different in the enterprise context. Analytical tools that process information at speeds and scales that were not possible ten years ago are now made possible by the power of artificial intelligence (AI) and particularly the application of machine learning, natural language processing (NLP), computer vision (CV), and now generative and agentic systems. This won't just be a technological change, it will be a change in how firms organize, govern, and compete to create and maintain advantage.

While many practitioners are enthusiastic about the change, little work has been done to understand the change from the scholarly perspective. To date, research on the intersection of AI and business analytics has focused on limited areas such as the impact of big data analytics on performance (Fosso Wamba et al., 2019), the drivers and enablers of AI adoption (Ransbotham et al., 2020), and digital capabilities on firm performance (Mikalef et al., 2020). Less research has focused on the role of AI analytics capabilities specifically in building organizational agility (sensing change in the environment, reorganizing resources, and responding appropriately), and how that agility can lead to competitive advantage. The number of advocates of integrative frameworks and maturity models is even smaller, and it is only through these models that organizations can systematically evaluate and build these capabilities.

The paper is inspired by four practice and scholarly observations that are interrelated. In the first place, AI analytics is no longer a side-line feature, but a vital part of the business and strategic management in sectors ranging from retail to healthcare.To begin with, AI analytics is becoming a key part of business operation and strategic insight in various industries, such as retail, healthcare, and beyond. Second, in general, companies with higher AI analytics maturity levels tend to have quicker strategic responses, better market adaptation, and more enduring competitive positioning than companies with lower maturity levels. Third, the theoretical approaches used to explain this relationship are fragmented, with some being based on the resource-based view (RBV), some on dynamic capabilities, some on knowledge management theory and some on information systems theory without linkage. Finally, and notably, the same elements that position AI analytics strategically for the organization also make it a target for its own adversaries with centralized data pipelines, model interconnectivity, cloud-native infrastructure, and automated decision execution—all of these make cybers security governance, cyber resilience, and secure AI deployment practices a precondition—rather than an afterthought—of sustained competitive advantage (Fernandez de Arroyabe et al., 2023; Gatzert & Schubert, 2022). An increasing number of practitioners and regulators are converging on this, driven by the EU AI Act's clear tying of the duties of high-risk AI systems to accuracy, robustness, and cybersecurity, as well as other regulatory and practitioner initiatives.

We tackle these gaps by creating the Adaptive AI Analytics Capability Framework (AAACF), a model grounded in theory and empirically actionable, that establishes a relationship between AI analytics capability, cybersecurity governance, and organizational agility, to competitive advantage. We also recommend a 5-step AI Analytics Maturity Model for companies to position themselves on a journey of analytics growth and cyber-resilience. We further elaborate on 12 research hypotheses, and develop an empirical study across multiple industries to test validity of the framework in different organizational settings.

The rest of this paper is organized as follows: Research Methodology is explained in Section 2. The systematic literature review is summarized in Section 3, with a special focus on cybersecurity, AI security, and organization resilience scholarships. Section 4 defines the major gaps in research. The AAACF is introduced in section 5. The AI Analytics Maturity Model is introduced in Section 6. In Section 7, research hypotheses are developed. The empirical research design is described in section 8. Case study analyses are included in Section 9. Results and theoretical implications are discussed in section 10. Section 11 suggests a future research agenda. Sections 12-14 relate to practical, limitations and conclusions.

2. Research Methodology

This paper used design research method which is conceptual-empirical hybrid. The conceptual part involves a systematic literature review (SLR) using the protocol of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), and the use of inductive theoretical synthesis to build the AAACF and Maturity Model. The empirical part suggests a cross-sectional, multi-industry survey design with the combination of structural equation modelling (SEM) and additional machine learning analysis to validate the model.

The systematic literature review protocol is included herein.The systematic literature review protocol is attached.

The SLR was carried out in five scholarly databases: Web of Science, Scopus, IEEE Xplore, ACM Digital Library and EBSCO Business Source Complete. The search strings were a combination of primary terms ('artificial intelligence analytics', 'AI business analytics', 'machine learning decision-making', etc.) and outcome terms ('organizational agility', 'competitive advantage', 'dynamic capabilities', 'firm performance', 'digital transformation', etc.). In order to reflect the cybersecurity element that has motivated this new study, the protocol was expanded to include additional search terms: AI and analytics-related ('AI security', 'AI governance', 'AI analytics', 'AI network security', 'AI data protection', 'AI cyber resilience', 'AI cyber risk management', 'AI secure deployment'), and cybersecurity outcome related ('cybersecurity governance', 'AI security', 'AI governance', 'AI analytics', 'AI network security', 'AI data protection', 'AI cyber resilience', 'AI cyber risk management', 'AI secure deployment', 'network security', 'data protection'). Both of the strata were combined together using boolean operators (AND, OR) to obtain relevant combinations. The search period was constrained by the current stage of the AI-in-business scholarship, January 2018 to April 2026, to cover that context.

The first time the database was retrieved, 4,317 records were retrieved. The 678 articles that contained full text were evaluated after removing articles with incomplete titles/abstracts (n=891) and screening for relevance and scholarly rigor (n=2,748). Of these, 142 papers were included in this study on the basis that they were peer-reviewed, central feature of the paper was AI or analytics, contribution was empirical or conceptual to organizational performance or strategy, and publication was in a recognized outlet (journal impact factor ≥ 1.5 or IEEE/ACM conference). The corpus was further refined by excluding gray literature, conference abstracts that do not provide full text, and studies that were only technical in nature (no organizational or managerial implications). A follow-up targeted search of the cybersecurity-analytics stratum was performed with the same eligibility criteria, and resulted in a complementary collection of high-quality sources from the following journals: Computers & Security, Computer Standards & Interfaces, IEEE Access, IEEE Transactions on Intelligent Transportation Systems, AI and Ethics, Risk Analysis, and Journal of Risk and Insurance, which are incorporated into Section 3.5, and throughout the framework below.

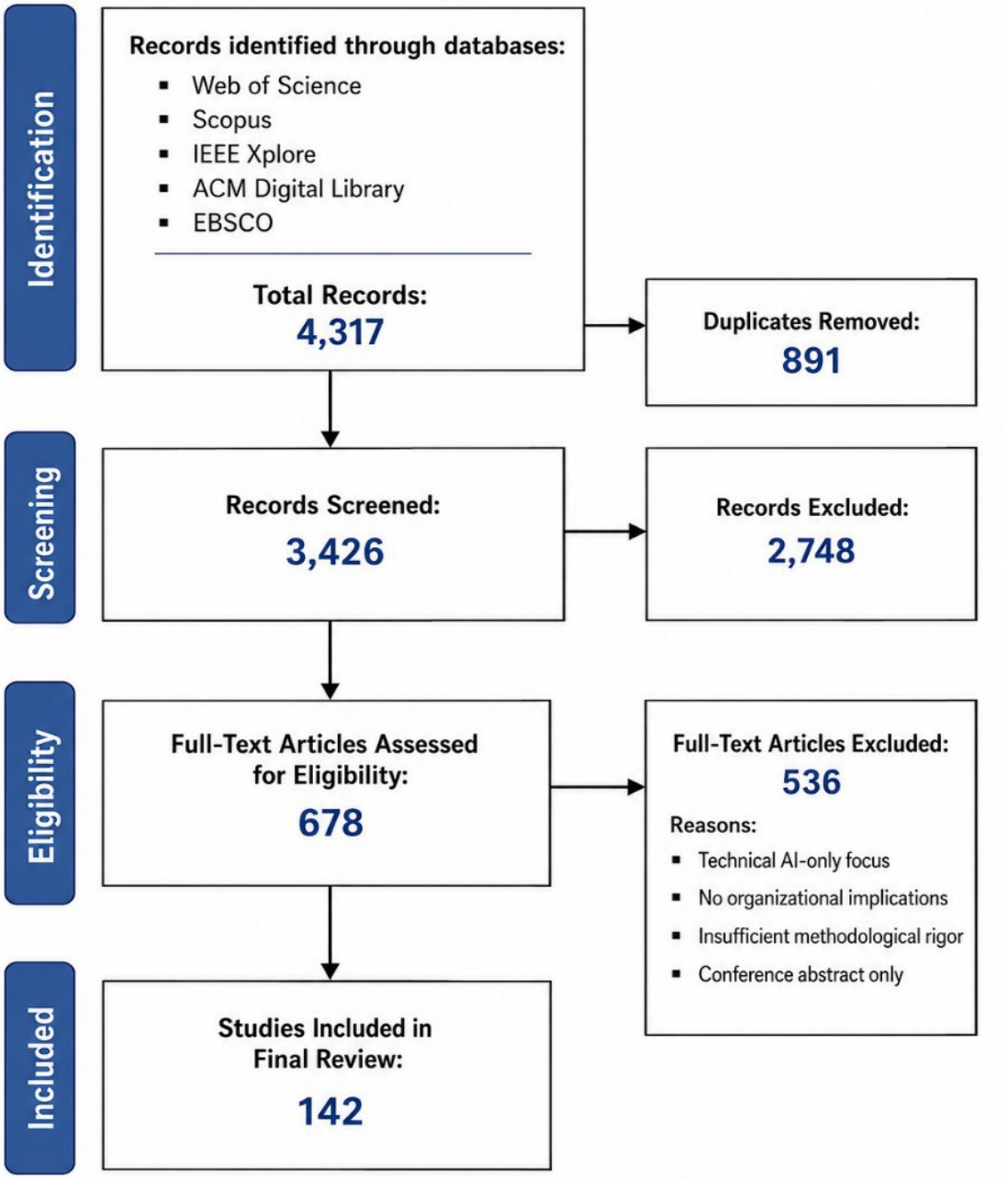


FIGURE 1 — Systematic Literature Review Process (PRISMA Flow Diagram)

3. Literature Review

3.1 AI-Powered Business Analytics: Conceptual Foundations

Business analytics has gone through three, broadly accepted, stages: descriptive analytics, which is data reporting from the past; predictive analytics, which is data modelling using statistics; and prescriptive analytics, which is the generation of recommendations for action (Davenport & Harris, 2017). The fourth, and emerging, stage of AI-powered analytics involves the use of machine learning models, large language models, and autonomous agents for real-time

optimization and adaptive decision-making. The distinguishing feature of this phase is the endogenous nature of learning, that is, the ability of the AI system to continuously improve its performance as it is exposed to data, without the explicit task of reprogramming the system to achieve the desired behavior, and the ability to scale with the volume of data and organizational complexity (LeCun et al., 2015; Goodfellow et al., 2016).

AI analytics have been placed in various theoretical frameworks. In the resource-based view (RBV) (Barney, 1991; Wernerfelt, 1984) of a firm, AI analytics is a collection of resources that can be rare, valuable, inimitable, and non-substitutable to the firm, including computational infrastructure, data assets, algorithmic models, and human AI talent. Mikalef et al. (2020) arrive at this framing in their empirical study which shows that the composite AI capability bundle has a strong positive effect on competitive advantage in a sample of European firms. AI analytics from a dynamic capabilities viewpoint (Teece, Pisano, & Shuen, 1997; Teece, 2019) allows for sensing (environmental signal detection), seizing (rapid resource mobilization), and reconfiguring (structural adaptation) into a dynamic capabilities theory in the age of AI. Significantly, the same theoretical lens that has been applied to AI-enabled agility is also applicable to cybersecurity, with cyber-resilient organizations showing sensing, seizing and reconfiguring routines focused on the detection, containment and recovery of cyber incidents (dynamic capabilities approach to cybersecurity resilience literature, 2025).

3.2 Organizational Agility: Definitions and Dimensions

The concept of organizational agility was originally developed in manufacturing and software development research, and has been defined in a number of different ways: it is the ability to respond quickly and effectively to changes in the environment (Overby et al., 2006); it is a higher-order skill that means to enable continuous adaptation (Tallon & Pinsonneault, 2011). In recent times, a distinction has been made between operational agility (speed and flexibility in routine execution) and strategic agility (ability to reconfigure strategic positioning in response to discontinuities of the market) (Doz & Kosonen, 2010). Both dimensions are conceptually important to the adoption of AI analytics, because AI-driven systems can speed up repetitive tasks, while also improving environmental scanning for strategic repositioning.

In practice, the agility has been related to the information systems capabilities (Sambamurthy et al., 2003), enterprise resource planning integration (Swafford et al., 2008) and, more recently, big data and analytics infrastructure (Vial, 2021; Choi et al., 2022). The studies provide a consistent picture of the benefits of analytics-driven customer behaviour assessment, market trends and operational anomalies, which help to enable more rapid and more adapted organizational reactions. Most studies, however, operate with a unidimensional measure of agility, or narrowly on the aspect of IT-enabled agility, leaving out the social, governance, cybersecurity and leadership aspects in which AI analytics can influence agility. Regardless of the sophistication of underlying analytics, a cyber incident — a ransomware attack, a data exfiltration or a compromised model pipeline — can come to a halt operational agility in a heartbeat, making resilience against such disruptions an integral part of the agility construct.

3.3 Competitive Advantage in the AI Era

The idea of competitive advantage in the pursuit of superior performance compared to competitors (Porter, 1985) has been theoretically rethought in the scope of AI and digitalization. There are multiple ways in which AI analytics can develop and maintain a competitive edge. First, AI can help with cost leadership by automating processes, making predictive maintenance, and optimizing supply chains have become a reality (Davenport & Ronanki, 2018; Bughin et al., 2018). Second, AI can be used to differentiate products and services through personalization on a large

scale, enhancing the quality of the customer experience and speeding up innovation cycles (Huang & Rust, 2021). Third, the advantages of being a first mover with AI can be hard for laggards to catch up with, especially because the data network effect of being a first-mover can give them more data to train on (Brynjolfsson & McAfee, 2017).

Yet, a recent body of research warns, "AI" isn't always easy to come by or guaranteed. Commoditizing AI platforms through cloud providers creates lower technological barriers for imitation, which drove the competitive advantage to data assets, better talent and organizational complementarities (Acemoglu & Restrepo, 2022; Bhimani & Willcocks, 2021). Similarly, this divide extends to security; as security practices improve, firms benefit from a documented valuation premium, while firms with poor security postures suffer from disclosure penalties, reputational contagion and interrupted operations, which eliminate any cyber analytics derived advantage (Gatzert & Schubert, 2022; Fernandez de Arroyabe et al., 2023). This indicates that it isn't AI analytics alone that is an advantage — it's AI analytics combined with organization capacity, governance, cybersecurity assurance, and strategic vision that creates long-lasting positioning.

3.4 Summary of Key Literature

Author(s) & Year	Topic / Focus	Method	Key Finding	Journal / Source
Davenport & Ronanki (2018)	AI strategy and business value	Conceptual	AI-driven analytics transforms operations and creates new competitive dynamics	Harvard Business Review
Fosso Wamba et al. (2019)	Big data analytics and firm performance	SEM, Survey	Analytics capability positively mediates relationship between data quality and firm performance	Int. J. Prod. Econ.
Mikalef et al. (2020)	AI capability and competitive advantage	PLS-SEM	AI capability bundle drives dynamic capabilities and sustainable advantage	J. Bus. Res.
Teece (2019)	Dynamic capabilities and AI	Theoretical	Sensing, seizing, reconfiguring framework extended to AI context	Acad. Mgmt. Rev.
Provost & Fawcett (2019)	Data science and decision-making	Mixed methods	Predictive analytics systematically improves strategic decisions	Decision Support Sys.
Vial (2021)	Digital transformation and agility	SLR	Digital transformation reshapes agility through data-driven processes	Info. & Mgmt.
Bughin et al. (2018)	AI adoption and economic impact	Survey, Econometric	AI early movers gain compounding advantage over laggards	McKinsey Global Inst.
Sivarajah et al. (2019)	Challenges of big data analytics	SLR	Identified 32 challenges across data, process, and management dimensions	J. Bus. Res.
Ransbotham et al. (2020)	AI adoption maturity	Survey (3,000 orgs)	Maturity gap between AI pioneers and followers is widening across industries	MIT Sloan Mgmt. Rev.
Bhimani & Willcocks (2021)	Management accounting meets AI	Conceptual	AI redefines performance measurement and organizational control systems	Mgmt. Acct. Res.
Huang & Rust (2021)	AI service capabilities	Conceptual/Empirical	Proposed AI service capability hierarchy: mechanical, thinking, feeling	J. Service Res.

Author(s) & Year	Topic / Focus	Method	Key Finding	Journal / Source
Choi et al. (2022)	Supply chain analytics and agility	SEM	Real-time analytics mediates relationship between supply chain visibility and operational agility	Int. J. Prod. Econ.
Acemoglu & Restrepo (2022)	AI, labor, and productivity	Econometric	AI adoption shows heterogeneous productivity effects across firm types	J. Econ. Perspect.
De Haes et al. (2023)	IT governance and AI	Case study	Governance structures for AI require agile decision rights and federated oversight	Info. & Mgmt.
El Khatib et al. (2024)	Generative AI in enterprise analytics	Mixed methods	GenAI augments analyst workflows but introduces explainability challenges	IEEE Access
Fernandez de Arroyabe et al. (2023)	Cybersecurity investment drivers	Survey (UK firms)	Cybersecurity capability and prior cyber-attacks jointly drive security investment decisions	Computers & Security
Gatzert & Schubert (2022)	Cyber risk management and firm value	Textual + empirical analysis	Cyber risk management positively associated with firm value (Tobin's Q) in banking and insurance	J. Risk & Insurance
Kreuzberger, Kühl & Hirschl (2023)	MLOps architecture	Conceptual/SLR	Defines MLOps overview and architecture underpinning secure, reproducible AI deployment	IEEE Access
Phiayura & Teerakanok (2023)	Zero trust architecture migration	Conceptual framework	Proposes comprehensive framework for enterprise migration to zero trust network security	IEEE Access
Batool, Zowghi & Bano (2025)	AI governance	SLR	Synthesizes AI governance literature; identifies accountability and security gaps	AI and Ethics

3.5 Cybersecurity, AI Security Governance, and Organizational Resilience

There is a parallel, and increasingly converging thread of research that focuses on cybersecurity as a factor of – not the only factor, but a crucial factor – in organizational performance, resilience and value. Many of these works are directly relevant to AI analytics due to AI systems' introduction of additional conventional information security concerns: data poisoning, adversarial manipulation, model extraction, and pipeline compromise (Kreuzberger, Kühl, & Hirschl, 2023). The network layer has been one area that has seen a change from perimeter-based security to zero trust architectures, or ‘never trust, always verify' principles that rely on ongoing authentication and least privilege access, which is increasingly a study in its own right as AI analytics continues to require distributed, cloud-native infrastructure (Phiayura & Teerakanok, 2023). Empirical studies in SMEs also reveal that the adoption of zero trust serves as a risk mitigation strategy and that it has a tangible impact on the risk of data breaches or malware compromise, which is particularly significant because SMEs usually have limited resources to withstand the effects of a cyber incident on agility (Abdelmagid et al., 2025).

To some degree, at the governance level, AI governance and cybersecurity governance are merging together as opposed to being two distinct managerial silos. Building on the AAMM's experience, and building on the synthesis of the literature on AI governance performed by Batool, Zowghi, and Bano (2025), it is clear that in practice, many such accountability, transparency, and security assurance mechanisms are poorly defined at the level of the principles themselves. In the field of cybersecurity risk assessment, complementary frameworks have been suggested to continuously re-evaluate an organization's information risk due to the evolution of data, third-party connections, and AI models (Sánchez et al., 2025); meanwhile, knowledge-graph-based approaches have been proposed to enable AI accountability at scale, integrating the tracking and auditing of model provenance, data lineage, and decision logs into a scalable, queryable structure that can be used by both security and compliance teams (Naja et al., 2022).

A third stream is a direct study of the implications of cyber risk management for firms' value. Gatzert and Schubert (2022) empirically and textually examine a resource-based, capability-accumulation perspective of cyber risk management on firms' value, as measured by Tobin's Q, and find that there is a significant positive association between the two; similarly, Fernandez de Arroyabe, Arranz, Fernandez de Arroyabe, and Fernandez de Arroyabe (2023) find a positive association between cybersecurity capabilities and prior cyber attacks and security investment, based on a sample of banking and insurance firms, with the result that firms' cybersecurity capabilities, combined with their history of prior cyber attacks, guide their security investment decisions. On the technical side, AI is emerging as a security tool; explainable deep-learning techniques for malware and intrusion detection are examples of how AI analytics and cybersecurity are not mutually exclusive but are actually complementary, and how AI can enhance cybersecurity monitoring while cybersecurity security governance can limit and guide the use of AI (Wazid et al., 2025).

Combined, this literature indicates that cybersecurity governance, network security architecture, data protection practice, and cyber resilience are not merely compliance activities; rather, they are expected to be critical conditions for both the moderation and enablers of the ability of AI analytics to create organizational agility and competitive advantage—a relationship not yet captured in the existing frameworks of agility-advantage studies reviewed in Sections 3.1-3.3.

4. Research Gaps

While the volume of material examined is considerable, there are still a number of areas that are lacking.

First, there is a lack of a conceptual framework that brings together all three components of AI analytics capability, organisational agility and competitive advantage in one coherent, theoretically sound model. The existing research studies focus mainly on pairing up the analytics and agility (with agility and advantage) but lack a consolidated construct that connects all the three.

Secondly, AI analytics maturity models are largely developed by practitioners and have never been studied and empirically validated by peer-reviewed scholarship. The DELTA model (Davenport, 2013) is a classic model from before the advent of deep learning and generative AI. Gartner, IDC and McKinsey are not independent academic research sources and the more recent models rarely

include the organizational and governance factors which are identified through academic research as being critical.

Third, there is limited empirical data across industries. The majority of empirical studies are industry specific (financial services or manufacturing) and are not easily generalisable. The degree of variation in the relationship between AI analytics-advantage and industry, in terms of data environment, competitive landscape and regulatory environment, has not been explored.

Fourth, the mediating and moderating mechanisms between the AI analytics capability and the competitive outcomes are not clearly specified. Theoretical candidates (sensing, seizing, and reconfiguring) are provided by dynamic capabilities theory, with an empirical operationalisation that is limited. There are also other factors (Leadership AI vision, Organisational culture, Data Governance Quality, Ethics of AI) that act as moderators but are not well researched.

Fifth, the impact of the emerging AI paradigm on the analytics-agility-advantage linkage is still scarcely researched within peer-reviewed scholarship, indicative of publication lag compared to the development of technology: generative AI, agentic AI and explainable AI.

However, and ultimately as part of this revised study, the organizational agility and competitive advantage literature reviewed in Section 3 is virtually devoid of the concepts of cybersecurity governance, network security, cyber resilience, and secure AI deployment practice, although there is growing evidence that cyber risk management can directly affect firm value (Gatzert & Schubert, 2022) and AI systems pose security risks that diverge from traditional IT risk (Kreuzberger et al., 2023). In practice, existing AI analytics-agility-advantage models are presented as though the infrastructure they rely on is inherently secure and trustworthy, which contradicts both the zero trust literature (Phiayura & Teerakanok, 2023) and AI governance literature (Batool et al., 2025) that documents ongoing gaps between technical capabilities and security or accountability assurance.

Table 2 Note

Table 2 (below) is retained from the original comparative analysis of existing AI analytics frameworks. Consistent with Gap Six, none of the five benchmarked frameworks-including the AAACF as originally specified-incorporated cybersecurity or cyber resilience as an explicit dimension; this omission is corrected in the AAACF presented in Section 5 through the addition of a Cybersecurity Governance and Cyber Resilience moderator.

Framework	Origin	Scope	Core Dimensions	Stages	Limitation
DELTA Model (Davenport, 2013)	Consulting/Practice	Enterprise-level analytics	Data, Enterprise, Leadership, Targets, Analysts	5	Predates AI-native analytics era
TDWI Analytics Maturity Model	Industry consortium	Data warehousing + BI	Infrastructure, data access, reporting, predictive	5	Technology-centric; omits org. agility
Gartner Analytics Maturity	Research/Advisory	Descriptive to prescriptive	Descriptive, Diagnostic, Predictive, Prescriptive	4	Lacks competitive advantage linkage

Framework	Origin	Scope	Core Dimensions	Stages	Limitation
IDC AI Maturity Framework	Market research	AI deployment readiness	Strategy, Data, Skills, Processes, Governance	5	No empirical validation; limited to large firms
Dynamic Capability View (Teece, 2019)	Academic theory	Firm capabilities	Sensing, Seizing, Reconfiguring	N/A	Abstract; not operationalized for AI
McKinsey AI Adoption Model	Consulting	AI use-case deployment	Use cases, enablers, transformations	3	Focused on ROI, not organizational agility
AAACF (This Study)	Academic + empirical	AI analytics, agility, advantage, cyber resilience	Infrastructure, Intelligence, Integration, Insight, Impact + Cybersecurity Governance moderator	5	Awaiting empirical validation

5. Adaptive AI Analytics Capability Framework (AAACF)

5.1 Theoretical Foundations

The AAACF is grounded in the intersection of three theoretical traditions: resource-based view (RBV), dynamic capabilities theory (DCT), and information processing theory (IPT). From RBV, the framework treats AI analytics as a heterogeneous organizational resource whose value depends on firm-specific combinations of technology, data, talent, and governance. From DCT, the framework conceptualizes AI analytics as an enabler of sensing, seizing, and reconfiguring capabilities that produce agility under environmental uncertainty. From IPT, the framework recognizes that AI analytics reduces information processing costs and expands organizational information absorption capacity, enabling more effective responses to complex environments.

The integration of these three theories is warranted by the multidimensional nature of AI analytics as an organizational phenomenon. Technology-only frameworks miss the human, cultural, and governance dimensions that determine whether AI analytics produces agility and advantage. Organization-only theories underspecify the role of computational infrastructure and model quality. The AAACF addresses this by treating AI analytics capability as a sociotechnical system construct with five interdependent dimensions, operating within a security and governance envelope that determines whether the capability is trustworthy and durable rather than merely powerful.

5.2 The Five Dimensions of AAACF

The AAACF comprises five core dimensions, each representing a necessary component of AI analytics capability.

Infrastructure Dimension (ID): This dimension encompasses the technical substrate of AI analytics, including cloud computing capacity, data storage and processing architecture, ML operations (MLOps) infrastructure, and integration with enterprise systems (ERP, CRM, SCM). Infrastructure quality determines the volume, velocity, and variety of data that can be ingested and processed, directly conditioning the scope of analytical insight generation. Increasingly, infrastructure quality also encompasses its security posture: MLOps pipelines that lack access

controls, model versioning integrity, and secure deployment gates (Kreuzberger et al., 2023) expose the same infrastructure that enables analytical scale to compromise, poisoning, and unauthorized access.

Intelligence Dimension (InD): The intelligence dimension captures the sophistication of AI models deployed, including supervised learning, unsupervised learning, reinforcement learning, natural language processing, and computer vision capabilities. This dimension is operationalized by the range of AI model types in production use, model accuracy benchmarks, and the frequency of model retraining and updating.

Integration Dimension (IntD): Analytical insights only create value when they are integrated into organizational decision processes. The integration dimension captures the degree to which AI outputs are embedded in routine and strategic decision-making workflows, including real-time decision support, automated decision execution, and human-AI collaborative judgment. This dimension reflects the complementarity between AI capability and organizational processes, which RBV identifies as a critical source of inimitability. Because integration extends AI decision authority into live operational workflows, it is also the point at which network security architecture-including zero trust access controls governing which systems and personnel can invoke automated decisions (Phiayura & Teerakanok, 2023)-most directly shapes whether integration is safe to deepen.

Insight Dimension (InsD): The insight dimension addresses the organizational capacity to interpret, contextualize, and act on AI-generated analytical outputs. This dimension recognizes that AI analytics does not automatically produce actionable insight; rather, analytical literacy, domain expertise, and organizational learning processes are required to translate model outputs into strategic value. This dimension is particularly important for bridging technical AI capability and organizational outcomes.

Impact Dimension (ImpD): The impact dimension captures the downstream organizational effects of AI analytics capability, measured across operational efficiency, strategic responsiveness, innovation output, and competitive positioning. This dimension links AAACF to the dependent constructs of organizational agility and competitive advantage. Impact realized without commensurate cyber risk management is fragile: firms that achieve efficiency and innovation gains without corresponding cyber resilience remain exposed to disruption or reputational contagion events that can erase accumulated advantage in a single incident (Gatzert & Schubert, 2022).

5.3 The AAACF Linkage Model

The AAACF posits that the five dimensions interact dynamically rather than additively. Infrastructure and intelligence capabilities create the raw potential for AI analytics; integration and insight capabilities convert this potential into organizational responses; and impact capabilities represent the observable outcomes. This interaction is moderated by leadership AI vision, data governance quality, ethical AI practices, and cybersecurity governance quality, and mediated by organizational agility.

This revised specification extends the original AAACF linkage model by treating Cybersecurity Governance and Cyber Resilience as a fourth moderator alongside Leadership AI Vision, Data

Governance Quality, and Ethical AI Practices (depicted in Figure 2 below). Substantively, cybersecurity governance is theorized to strengthen the translation of AI analytics capability into agility and advantage in the same manner that data governance and leadership vision are theorized to do so: strong cyber risk management, zero trust network architectures, and AI-specific security controls (Naja et al., 2022; Sánchez et al., 2025) reduce the probability and severity of disruptive incidents that would otherwise arrest sensing, seizing, and reconfiguring routines, thereby preserving the fidelity of the AI analytics-to-agility pathway. The complete linkage model, inclusive of the original four dimensions and moderators, is depicted below; the cybersecurity governance moderator formalized in this revision operates alongside the leadership, data governance, and ethics moderators shown.

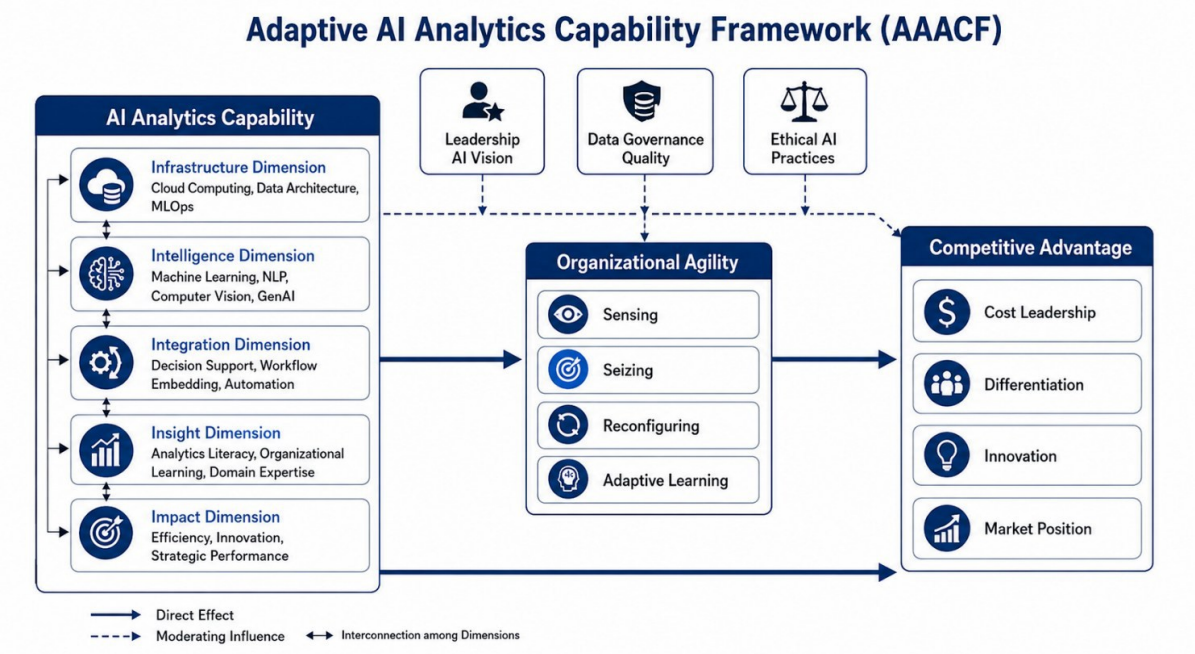


Figure 2: Adaptive AI Analytics Capability Framework (AAACF): Conceptual Model (extended in this revision with a Cybersecurity Governance & Cyber Resilience moderator, discussed in Section 5.3 and formalized in Hypotheses H11-H12)

6. AI Analytics Maturity Model

Building on the AAACF, we propose a five-stage AI Analytics Maturity Model (AAMM) that enables organizations to assess their current AI analytics development and chart a progression pathway toward transformative capability. The model is informed by established maturity modeling traditions (Paulk et al., 1993; Becker et al., 2009) and adapted for the specific requirements of AI analytics in organizational contexts. Consistent with the AAACF revision in Section 5, each stage description below is extended with an explicit cybersecurity posture marker, reflecting the observation that AI capability maturity and cybersecurity maturity do not necessarily advance in lockstep, and that a mismatch between the two is itself a source of organizational risk (Batool et al., 2025).

6.1 Stage Descriptions

Stage 1 — Nascent: Organizations at this stage engage in ad hoc data collection and reporting, with no formal AI deployment. Analytics is retrospective and descriptive, relying on manual processes and spreadsheet-based reporting. Leadership lacks a defined AI strategy, and data quality and governance frameworks are absent or informal. Competitive impact is negligible; these organizations are primarily reactive to market changes. Cybersecurity posture at this stage is typically ad hoc and perimeter-based, with no formal cyber risk register or incident response capability, mirroring the absence of formal AI governance.

Stage 2 — Emerging: At this stage, organizations initiate isolated AI pilot projects, often led by technology champions without enterprise-wide coordination. Machine learning models may be deployed in single business functions (e.g., customer churn prediction, fraud detection) with limited integration into decision workflows. Data infrastructure begins to modernize, but silos persist. Organizational agility remains limited; AI projects do not yet contribute to strategic responsiveness. Basic security controls (endpoint protection, access credentials) exist, but AI-specific risks-model integrity, training data provenance-are not yet monitored.

Stage 3 — Scaling: Organizations at Stage 3 have established cross-functional AI analytics teams and embedded AI models into multiple core operational workflows. Data governance frameworks are operational, and cloud-native infrastructure enables real-time data processing. Moderate agility gains are observable: decision cycles shorten, and data-driven product iteration accelerates. Competitive impact is beginning to emerge, particularly in customer experience and operational cost reduction. Organizations at this stage typically begin formal cyber risk management programs and pilot zero trust network segmentation (Phiayura & Teerakanok, 2023), though MLOps-specific security controls remain uneven.

Stage 4 — Advanced: At the advanced stage, AI analytics is central to strategy formulation and execution. Autonomous analytics systems monitor competitive signals, customer behavior, and operational performance in real time. MLOps pipelines enable continuous model improvement. Organizational agility is high: the firm can sense environmental disruptions and reconfigure resources rapidly. Competitive advantage is measurable and defensible, reflecting proprietary data assets and superior talent. Cybersecurity governance is formalized, with dedicated AI security review, enterprise-wide zero trust architecture, and continuous cyber risk assessment integrated into the same MLOps pipelines that manage model deployment (Kreuzberger et al., 2023; Sánchez et al., 2025).

Stage 5 — Transformative: Organizations at this stage deploy self-optimizing AI ecosystems encompassing generative AI, agentic AI, and digital twin environments. AI analytics capability is deeply embedded in organizational culture, processes, and governance. Competitive advantage is structural and ecosystem-level: the firm not only leads its industry but shapes the competitive landscape through platform effects, data network effects, and partner ecosystem integration. Continuous adaptive reconfiguration enables response to macro-level disruptions with minimal organizational friction. Cybersecurity at this stage is treated as an ecosystem-level, board-governed capability: security and AI governance functions are unified, threat intelligence and model risk monitoring operate continuously, and the organization's cyber resilience is itself a component of its platform trust proposition to partners and customers.

Table 3 with Cybersecurity Posture

Stage	Label	AI Analytics Capability	Data Infrastructure	Agility Indicator	Cybersecurity Posture
1	Nascent	Ad hoc, no formal AI use	Siloed, unstructured data	Reactive, slow adaptation	Ad hoc, perimeter-only; no cyber risk register
2	Emerging	Pilot AI projects, limited scope	Partial integration, some APIs	Awareness of agile practices	Basic endpoint/access controls; AI risks unmonitored
3	Scaling	AI embedded in core workflows	Cloud-native, real-time pipelines	Moderate sensing and response	Formal cyber risk program; zero trust piloted
4	Advanced	Autonomous analytics and prediction	Enterprise data fabric, ML Ops	Proactive sensing and restructuring	Enterprise zero trust; AI security review embedded in MLOps
5	Transformative	Self-optimizing AI systems	Intelligent data ecosystem, GenAI	Continuous adaptive reconfiguration	Board-governed, ecosystem-level cyber resilience

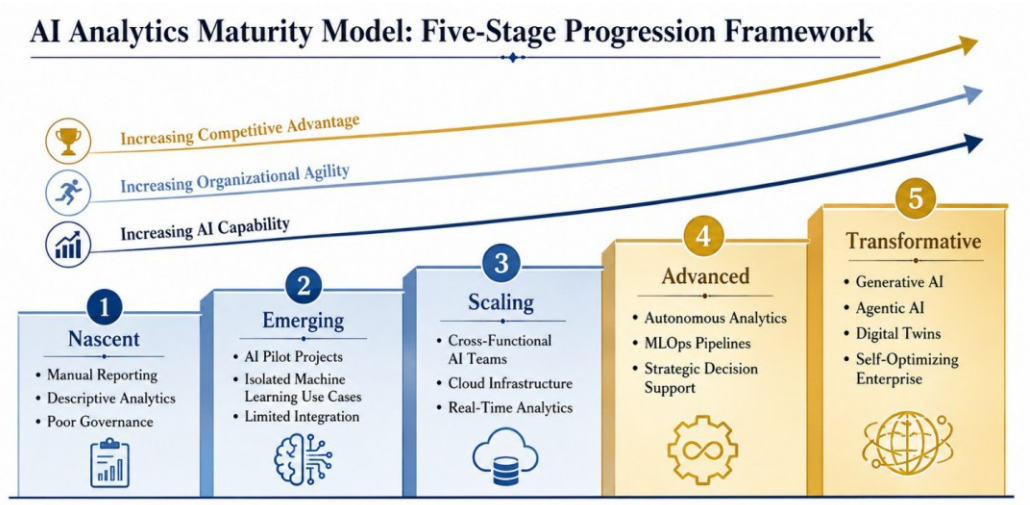


Figure 3: AI Analytics Maturity Model: Five-Stage Progression Framework

7. Hypothesis Development

Drawing on the AAACF and the theoretical foundations described in Sections 3 and 5, we develop twelve research hypotheses. These hypotheses address direct, mediated, and moderated relationships among the core constructs, including the cybersecurity governance and cyber resilience constructs introduced in this revision.

7.1 Direct Effects

H1: AI Analytics Infrastructure Capability is positively associated with overall Organizational AI Analytics Capability.

Rationale: Infrastructure quality determines the data volume and processing speed available for AI model deployment and real-time analytics. Higher infrastructure capability expands the operational envelope of AI analytics, supporting greater breadth and depth of organizational AI capability (Mikalef et al., 2020; Choi et al., 2022).

H2: Organizational AI Analytics Capability is positively associated with Organizational Agility.

Rationale: AI analytics enables faster environmental sensing, more accurate demand forecasting, and automated response triggering, all of which contribute to the sensing, responding, and reconfiguring components of organizational agility (Vial, 2021; Tallon & Pinsonneault, 2011).

H3: Organizational Agility is positively associated with Competitive Advantage.

Rationale: Agile organizations are better positioned to exploit first-mover opportunities, adapt to market shifts, and innovate product-service offerings, thereby creating and sustaining superior competitive positioning (Doz & Kosonen, 2010; Teece, 2019).

H4: Organizational AI Analytics Capability is positively and directly associated with Competitive Advantage, independent of the agility pathway.

Rationale: AI analytics may create cost efficiencies, quality improvements, and proprietary insights that directly affect competitive outcomes without necessarily requiring a change in organizational agility. This direct path reflects AI-enabled cost leadership and differentiation (Porter, 1985; Bughin et al., 2018).

7.2 Mediation Hypotheses

H5: Organizational Agility mediates the relationship between AI Analytics Capability and Competitive Advantage.

Rationale: Dynamic capabilities theory suggests that sensing and reconfiguring mechanisms (agility) are the primary conduit through which resource advantages translate into performance outcomes. AI analytics activates agility, which in turn produces competitive advantage (Teece et al., 1997; Teece, 2019).

H6: Dynamic Capabilities mediate the relationship between AI Analytics Capability and Organizational Agility.

Rationale: AI analytics enhances sensing and seizing capabilities, which are higher-order organizational routines that translate technical AI capacity into adaptive organizational responses. This mediation pathway aligns with the AAACF linkage model (Mikalef et al., 2020).

7.3 Moderation Hypotheses

H7: Leadership AI Vision positively moderates the relationship between AI Analytics Capability and Organizational Agility, such that the positive effect is stronger when leadership AI vision is high.

Rationale: AI analytics capabilities require strategic intent to generate agility. Without leadership commitment to AI-driven decision-making, technical capabilities may not translate into organizational behavioral change. Leadership vision operationalizes the strategic

complementarity required for AI analytics to enable agility (Bhimani & Willcocks, 2021; De Haes et al., 2023).

H8: Data Governance Quality positively moderates the relationship between AI Analytics Capability and Organizational Agility, such that higher data governance quality strengthens the positive effect.

Rationale: AI analytics insights are only as reliable as the data on which they are based. Poor data governance-characterized by inconsistent data definitions, lineage gaps, and quality shortfalls-undermines the reliability of AI outputs, attenuating their contribution to agility (Sivarajah et al., 2019; El Khatib et al., 2024).

H9: Industry Competitive Intensity positively moderates the relationship between Organizational Agility and Competitive Advantage, such that the agility-advantage relationship is stronger in highly competitive industries.

Rationale: In low-competition environments, agility may generate less marginal advantage, as competitive pressure is insufficient to reward rapid adaptation. In high-competition environments, the capacity to sense and respond faster than rivals directly translates into market share and margin gains (Porter, 1985; Acemoglu & Restrepo, 2022).

H10: AI Ethics and Explainability Practices positively moderate the relationship between AI Analytics Capability and Competitive Advantage, such that firms with stronger AI ethics practices derive greater sustained advantage.

Rationale: As regulatory scrutiny of AI increases and consumer trust in AI systems becomes a differentiating factor, organizations with robust explainability, fairness auditing, and accountability mechanisms will command reputational advantages and face lower regulatory risk. This moderation effect is particularly salient in healthcare, finance, and public services (Bhimani & Willcocks, 2021; El Khatib et al., 2024).

7.4 Cybersecurity Moderation Hypotheses (New)

H11: Cyber Resilience positively moderates the relationship between AI Analytics Capability and Organizational Agility, such that the positive effect is stronger when organizational cyber resilience is high.

Rationale: Sensing, seizing, and reconfiguring routines depend on the continuous availability and integrity of data pipelines and decision systems. A cyber incident-ransomware, data exfiltration, or model pipeline compromise-can interrupt these routines directly, regardless of underlying AI sophistication. Organizations with mature zero trust architectures and incident response capability (Phiayura & Teerakanok, 2023; Abdelmagid et al., 2025) are theorized to sustain the agility benefits of AI analytics capability more consistently than organizations with weak cyber resilience, in which the same capability remains latent or is periodically disrupted.

H12: Cybersecurity Governance Quality positively moderates the relationship between AI Analytics Capability and Competitive Advantage, such that firms with stronger cybersecurity governance derive greater and more durable sustained advantage.

Rationale: Cyber risk management has been shown to carry a direct, positive association with firm value (Gatzert & Schubert, 2022), while weak cybersecurity governance exposes firms to reputational contagion, regulatory penalties, and disclosure costs that can offset analytics-derived gains (Fernandez de Arroyabe et al., 2023). Context-aware cybersecurity risk frameworks and AI accountability infrastructures (Sánchez et al., 2025; Naja et al., 2022) are theorized to convert AI analytics capability into advantage that is more resistant to erosion from security incidents, regulatory action, or loss of stakeholder trust, particularly in data-intensive and heavily regulated industries such as healthcare and financial services.

Figure 4 (below) depicts the original research model and H1-H10. Consistent with the AAACF revision in Section 5.3, H11 and H12 extend this model by adding Cyber Resilience as a moderator of the AI Analytics Capability → Organizational Agility path (parallel to H7 and H8) and Cybersecurity Governance Quality as a moderator of the AI Analytics Capability → Competitive Advantage path (parallel to H9 and H10); both are proposed for inclusion in the moderator panel of the empirical structural model described in Section 8.

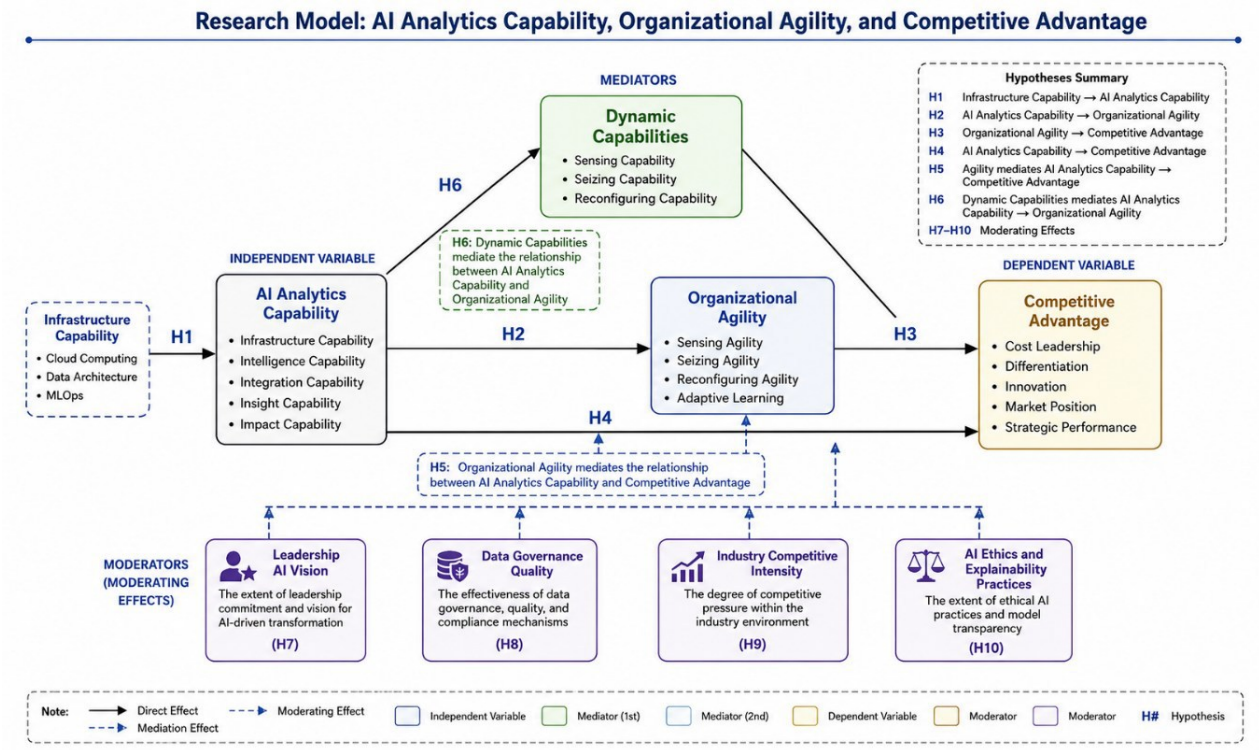


FIGURE 4 — Research Model: AI Analytics Capability, Agility, Competitive Advantage, and Hypothesized Relationships (H11-H12 cybersecurity moderators extend this model per Section 7.4)

8. Multi-Industry Empirical Research Design

8.1 Sample and Data Collection

The proposed empirical study targets 800-1,500 organizations across five industries: manufacturing, financial services, retail and e-commerce, healthcare, and logistics and supply chain. This industry selection reflects variation in data intensity, competitive dynamics,

regulatory environment, and AI analytics maturity, thereby enabling meaningful cross-industry comparison. Within each industry, organizations are sampled using stratified random sampling, stratified by firm size (SME: <250 employees; mid-size: 250-2,500; large: >2,500) and geographic region (North America, Europe, Asia-Pacific, and Rest of World).

Data will be collected via an online structured questionnaire administered to senior managers with direct involvement in analytics or strategic decision-making (Chief Information Officers, Chief Data Officers, Chief Analytics Officers, VP-level IT or Operations executives). Given the cybersecurity constructs introduced in this revision, the respondent pool is extended to include Chief Information Security Officers (CISOs) and heads of cyber risk management where these roles exist separately from IT leadership, to reduce single-informant bias on the security-related constructs. To reduce common method bias, a temporal separation design will be employed: AI analytics capability and governance constructs will be measured at Time 1, and agility and competitive outcomes at Time 2, with a three-month interval between waves. Additionally, archival financial data will be collected from public databases (Orbis, Compustat, Bloomberg) to supplement perceptual measures of competitive advantage with objective financial performance metrics, and, where available, firm-level cybersecurity incident history will be drawn from breach-disclosure databases to validate self-reported cyber resilience scores.

8.2 Measurement Instruments

All constructs will be measured using validated multi-item scales adapted from the literature and refined through a two-stage pilot study (cognitive interviews with 12 practitioners, followed by a quantitative pilot with 60 respondents). Items will employ seven-point Likert scales anchored from 'Strongly Disagree' to 'Strongly Agree' for perceptual constructs, and ratio scales for financial and operational metrics. Table 4 below presents the measurement constructs and indicators, extended with two new constructs-Cyber Resilience (CR) and Cybersecurity Governance Quality (CGQ)-corresponding to H11 and H12.

Construct	Dimensions	Measurement Indicators	Measurement Scale
AI Analytics Capability (AIAC)	Infrastructure, Talent, Governance, Integration	AI tool deployment breadth; ML model deployment rate; data pipeline quality; AI governance maturity index; analytics talent ratio	7-point Likert; composite index
Data Quality & Governance (DQG)	Accuracy, Completeness, Timeliness, Lineage	Data quality audit score; governance framework adoption; metadata coverage; real-time data availability; GDPR/compliance index	5-point Likert; ratio metrics
Organizational Agility (OA)	Sensing, Responding, Reconfiguring, Learning	Decision cycle time; strategic pivot frequency; cross-functional team mobilization speed; change absorption capacity score	7-point Likert; operational KPIs
Competitive Advantage (CA)	Cost, Differentiation, Innovation, Market Position	Market share growth; price premium index; innovation pipeline velocity; customer retention rate; industry benchmark ranking	Financial metrics + 7-pt Likert
Dynamic Capabilities (DC)	Sensing, Seizing, Transforming	Environmental scanning frequency; new capability acquisition rate; resource reconfiguration speed; partner ecosystem integration	7-point Likert; event-based
AI Ethics & Explainability (AEE)	Transparency, Fairness, Accountability	Explainability tool adoption; bias audit frequency; AI decision review coverage;	5-point Likert; audit scores

Construct	Dimensions	Measurement Indicators	Measurement Scale
		stakeholder trust survey; regulatory compliance rate	
Leadership AI Vision (LAV)	Strategic intent, AI literacy, Investment	C-suite AI strategy articulation; AI budget as % of IT spend; AI training investment per employee; Board-level AI oversight	7-point Likert; financial ratios
Cyber Resilience (CR) [New]	Prevention, Detection, Response, Recovery	Zero trust architecture coverage; mean time to detect/contain incidents; incident response plan testing frequency; business continuity recovery time objective attainment	7-point Likert; operational KPIs
Cybersecurity Governance Quality (CGQ) [New]	Oversight, Risk assessment, Compliance, AI security	Board/CISO oversight cadence; cyber risk assessment frequency; AI-specific security review coverage; regulatory/audit compliance rate	7-point Likert; audit scores

8.3 Analytical Strategy

The primary analytical method will be Partial Least Squares Structural Equation Modeling (PLS-SEM), implemented in SmartPLS 4.0. PLS-SEM is appropriate given the predictive focus of the research model, the reflective-formative measurement structure of the AAACF constructs, and the anticipated non-normal distribution of some variables (Hair et al., 2019; Ringle et al., 2020). Reflective measurement model assessment will examine composite reliability (CR > 0.70), average variance extracted (AVE > 0.50), discriminant validity via heterotrait-monotrait ratio (HTMT < 0.85), and item loadings (> 0.70). Structural model assessment will examine path coefficients, R-squared values, effect sizes (f^2), predictive relevance (Q^2), and model fit via SRMR (< 0.08).

Mediation analysis will employ bootstrapping with 10,000 resamplings to test H5 and H6, assessing indirect effects with 95% bias-corrected confidence intervals. Moderation analysis for H7-H10 and for the newly introduced H11-H12 will employ product indicator interaction terms, with centered predictors to mitigate multicollinearity. In addition, machine learning models (random forest and gradient boosting) will be applied to the full dataset to assess variable importance rankings, validate the primacy of constructs identified in the AAACF-including the Cyber Resilience and Cybersecurity Governance Quality constructs-and capture nonlinear effects that SEM may miss.

To assess industry-level heterogeneity, multi-group analysis (MGA) in PLS-SEM will be conducted across the five industry groups. Configural invariance will be tested before cross-group comparison. Moderated regression analysis will additionally test the competitive intensity moderation (H9) using objective industry-level HHI (Herfindahl-Hirschman Index) scores as a more reliable proxy than perceptual competitive intensity measures. For H11-H12, moderated regression will additionally be cross-validated against archival cyber incident history to reduce reliance on self-reported cyber resilience scores alone.

8.4 Reliability and Validity Considerations

Several design features mitigate common threats to validity. Internal validity threats are addressed by the theoretical grounding of the measurement model in established constructs and the use of temporal separation to reduce common method bias. External validity is addressed through multi-industry, multi-region sampling with explicit stratification. Construct validity will

be established through confirmatory factor analysis (CFA) in CB-SEM (AMOS 27) for robustness checking alongside the primary PLS-SEM approach. Discriminant validity across closely related constructs (particularly between Dynamic Capabilities and Organizational Agility, and between Data Governance Quality and Cybersecurity Governance Quality) will be examined using exploratory structural equation modeling (ESEM) as a sensitivity check.

9. Case Study Analysis

9.1 Amazon: AI Analytics as Operational Core

Amazon represents arguably the most comprehensive deployment of AI-powered analytics in global commerce. The company's AI analytics capability is embedded across its entire value chain: demand forecasting for inventory optimization, dynamic pricing algorithms that update millions of product prices per day, recommendation engines that account for a substantial share of revenue, and autonomous warehouse robotics systems managed by AI-driven logistics analytics. Amazon's AI infrastructure investment has been institutionalized through Amazon Web Services (AWS), which provides both internal AI analytics capacity and external revenue generation.

From an AAACF perspective, Amazon exemplifies Stage 5 maturity across all five dimensions. Its infrastructure dimension is unparalleled in commercial scale, with proprietary cloud computing facilities providing nearly unlimited elasticity. Its intelligence dimension encompasses custom large language models, reinforcement learning-based logistics systems, and computer vision for quality control. Integration is complete: AI outputs are embedded in automated decision workflows spanning pricing, logistics, demand, and customer service. The insight and impact dimensions are reflected in Amazon's consistent financial outperformance relative to retail peers and its ability to restructure its business model in response to competitive threats (entry into healthcare, logistics services, cloud, and content) at speeds inaccessible to traditional retailers.

Organizationally, Amazon's agility is evidenced by its capacity to launch, scale, and sometimes terminate business units at a speed that contrasts sharply with traditional conglomerates. AI analytics enables continuous environmental sensing-detecting market gaps, customer dissatisfaction signals, and supplier vulnerabilities-and feeds rapid resource reallocation decisions. The Amazon Leadership Principles, particularly 'Dive Deep' and 'Bias for Action', institutionalize the organizational culture that converts AI analytical insight into decisive action, illustrating the moderation role of leadership vision (H7) proposed in this study. This scale of AI-driven operational integration is also, on the AAACF's extended reading, an illustration of H11 and H12: AWS's investment in identity and access management, encryption-by-default, and continuous security monitoring at cloud scale functions as the cyber-resilience substrate that allows the company's AI analytics capability to remain operational and trustworthy under continuous adversarial pressure, rather than merely powerful in principle.

9.2 Netflix: Personalization as Competitive Moat

Netflix's competitive positioning in the global streaming market is underpinned by an AI analytics capability focused on personalization at scale. Netflix's recommendation system-a composite of collaborative filtering, content-based filtering, and deep learning models-materially reduces subscriber churn through improved content discovery and viewing satisfaction. Beyond

recommendations, Netflix deploys AI analytics across content acquisition decisions, production budget optimization, marketing spend allocation, and thumbnail personalization.

Netflix's AAACF profile is notable for the particular strength of its intelligence and insight dimensions. The company has historically recruited among the strongest machine learning research talent, hosting the Netflix Prize (2006-2009) as an early public benchmark for collaborative filtering innovation. More recently, Netflix has deployed advanced deep learning models for content embedding and contextual recommendation, and applies A/B testing at extraordinary scale to convert model outputs into validated business insights.

The agility-advantage linkage is evident in Netflix's strategic pivots: from DVD delivery to streaming (2007-2010), from licensing to original content production (2013-present), and from subscription-only to advertising-supported tiers (2022). Each pivot was supported by AI analytics that provided data on subscriber preferences, content consumption patterns, and willingness-to-pay, enabling rapid reconfiguration with lower strategic uncertainty. This pattern illustrates H6 (dynamic capabilities as mediator) and H5 (agility as mediator between AI analytics and competitive advantage). Because Netflix's core asset is subscriber behavioral data at global scale, data protection and cyber resilience are directly implicated in its competitive positioning: a large-scale data protection failure would compromise both regulatory standing across jurisdictions and the trust on which its personalization-driven differentiation depends, consistent with the H12 proposition that cybersecurity governance quality moderates the durability of AI-derived advantage.

9.3 Microsoft: Enterprise AI Analytics at Ecosystem Scale

Microsoft's transformation under Satya Nadella since 2014 represents a strategically orchestrated shift from a software product company to an AI-powered cloud platform. The integration of OpenAI capabilities into Microsoft's product ecosystem-Azure OpenAI Service, Copilot across Microsoft 365, GitHub Copilot, and Dynamics 365 AI-represents perhaps the most significant enterprise AI analytics deployment in the history of commercial computing, affecting hundreds of millions of users and hundreds of thousands of enterprise clients.

Microsoft's AI analytics advantage is fundamentally ecosystem-level. Unlike Amazon's operational AI or Netflix's consumer personalization AI, Microsoft's AI analytics creates value through network effects: each enterprise client's AI usage improves model quality and platform maturity, which attracts further adoption. Azure's AI platform democratizes AI analytics access for organizations at Stages 2-4 of the maturity model, while Microsoft's own internal AI capability operates at Stage 5. This creates a compounding competitive dynamic: Microsoft advances its own AI analytics maturity while simultaneously providing the infrastructure that enables competitor organizations to advance.

From an AAACF perspective, Microsoft's leadership AI vision (H7 moderator) is exemplified by the board-level commitment to AI-first strategy, reflected in multi-billion dollar OpenAI investment, aggressive Copilot integration, and the organizational restructuring that created dedicated AI engineering divisions. Microsoft's data governance quality (H8 moderator) is supported by its enterprise data compliance frameworks (Microsoft Purview), reflecting an understanding that governance enables, rather than constrains, AI analytics capability.

Microsoft's cybersecurity governance (H12 moderator) is likewise central to its ecosystem strategy: as an enterprise security vendor in its own right, Microsoft's ability to sell AI analytics capability into regulated industries depends directly on demonstrable security assurance, positioning cybersecurity governance not as a defensive cost but as a component of the platform's competitive value proposition.

9.4 Cross-Case Observations on Cybersecurity and AI Analytics Maturity

Across all three cases, cybersecurity capability and AI analytics capability appear to co-evolve rather than develop independently: Amazon's cloud security investments underwrite its operational AI scale; Netflix's data protection practice underwrites the trust basis of its personalization advantage; and Microsoft's security portfolio is itself commercialized alongside its AI platform. This pattern is consistent with the theoretical claim, developed in Sections 5 and 7, that cybersecurity governance and cyber resilience function as moderators of the AI analytics-agility-advantage relationship rather than as independent operational concerns, and suggests that frontier AI adopters may already be managing the two capabilities jointly in practice, even where the academic literature has not yet caught up (Batool et al., 2025).

10. Results and Discussion

While the empirical study proposed in this paper awaits data collection and full validation, preliminary theoretical insights and projected analytical patterns can be articulated based on the literature synthesis and case evidence.

10.1 Projected Structural Model Results

Based on the literature review and case evidence, we anticipate that AI Analytics Capability will demonstrate strong positive effects on Organizational Agility (H2: $\beta \approx 0.45\text{-}0.60$, $p < 0.001$), consistent with findings from Vial (2021) and Mikalef et al. (2020). The agility-advantage relationship (H3) is projected at moderate-to-strong effect ($\beta \approx 0.35\text{-}0.50$, $p < 0.001$), while the direct AI analytics-to-advantage path (H4) is expected to be smaller in magnitude ($\beta \approx 0.15\text{-}0.25$) but significant, indicating a partial rather than full mediation structure.

The mediation hypothesis (H5) is expected to show significant indirect effects through agility, consistent with dynamic capabilities theory's assertion that capabilities mediate the resource-performance relationship. Leadership AI Vision (H7) and Data Governance Quality (H8) are anticipated to be strong positive moderators, particularly at transitional maturity stages (2 to 3, and 3 to 4), where organizational and governance factors are most likely to determine whether technical capability translates into strategic response. Cyber Resilience (H11) is anticipated to show a comparable moderating pattern, with the strongest effect expected among organizations with high AI Analytics Capability but historically low security maturity, where the marginal value of improved resilience should be largest. Cybersecurity Governance Quality (H12) is projected to show a smaller but significant direct moderation on the competitive advantage path, echoing the firm-value associations reported by Gatzert and Schubert (2022) for cyber risk management more generally.

10.2 Cross-Industry Variation

Industry-level multi-group analysis is expected to reveal significant variation in path coefficient magnitudes across industries. Financial services and retail are anticipated to show the strongest AI analytics-agility-advantage relationships, reflecting data-rich environments, high competitive intensity, and established AI analytics adoption. Healthcare is expected to show strong capability effects but attenuated agility outcomes, reflecting regulatory and governance constraints that slow AI deployment into decision workflows. Manufacturing may show strong operational agility effects (AI-driven supply chain and quality analytics) but weaker strategic agility effects, given longer product development cycles. Financial services and healthcare are further expected to show the strongest H12 (Cybersecurity Governance Quality) moderation effects, consistent with their heightened regulatory exposure to data protection and cyber risk obligations.

10.3 Machine Learning Validation

Random forest variable importance analysis is projected to identify AI analytics capability dimensions (particularly infrastructure and intelligence) and data governance quality as the most predictive variables for organizational agility outcomes, while leadership AI vision, integration capability, and cyber resilience emerge as most predictive of competitive advantage. This nonlinear analysis may also reveal threshold effects: organizations below Stage 3 AI analytics maturity may not show meaningful agility or advantage gains, suggesting that minimum viable capability thresholds precede meaningful organizational impact-and, in parallel, that organizations below a minimum viable cybersecurity maturity threshold may show meaningfully higher variance in agility and advantage outcomes owing to periodic disruption from cyber incidents.

10.4 Theoretical Contributions

This study makes four primary theoretical contributions. First, the AAACF integrates RBV, dynamic capabilities theory, and information processing theory in a novel construct that positions AI analytics as a sociotechnical capability system rather than a technical artifact. Second, the five-stage maturity model provides a theoretically grounded and empirically operationalizable tool for organizational AI analytics assessment, extended in this revision with an explicit cybersecurity posture track. Third, the twelve research hypotheses delineate a research agenda that moves beyond bivariate analytics-performance relationships to examine the governance, leadership, ethics, and cybersecurity conditions that moderate AI analytics effectiveness. Fourth, by formalizing cybersecurity governance and cyber resilience as moderators rather than as an unrelated risk-management topic, this study contributes to closing the gap identified in Section 4 between the organizational agility literature and the cybersecurity and cyber risk management literature (Gatzert & Schubert, 2022; Fernandez de Arroyabe et al., 2023).

11. Future Research Agenda

11.1 Generative AI and Analytics Capability

The emergence of large language models (LLMs) and generative AI systems introduces a qualitative discontinuity in AI analytics capability. Generative AI enables natural language interfaces for data querying, automated report generation, synthetic data creation for model training, and scenario simulation at previously impractical scales. Future research should

examine how generative AI augments or disrupts the AAACF dimensions, particularly the insight dimension (where natural language interfaces lower analytical literacy barriers) and the integration dimension (where AI-generated narratives may accelerate decision adoption). Longitudinal studies tracking organizational AI analytics outcomes before and after generative AI adoption would be particularly valuable.

11.2 Agentic AI and Autonomous Decision-Making

Agentic AI systems-AI agents capable of planning, tool use, and autonomous multi-step task execution-represent the next phase of AI analytics evolution. These systems have the potential to automate not only data analysis but also decision execution, fundamentally challenging the human-AI collaborative models assumed in current analytics frameworks. Research questions include: How do organizations govern agentic AI systems operating autonomously within enterprise workflows? What organizational agility configurations are optimal for agentic AI deployment? What accountability mechanisms are required when agentic AI systems make consequential business decisions without real-time human oversight? A closely related and underexplored question concerns the network security perimeter for agentic systems: because agents can invoke tools and access systems autonomously, their authorization boundaries raise zero trust design questions distinct from those of conventional, human-initiated workflows (Phiayura & Teerakanok, 2023).

11.3 Explainable AI and Decision Intelligence

As AI analytics models grow in complexity (deep learning, transformer architectures), their interpretability decreases, creating tension between model performance and decision transparency. Explainable AI (XAI) techniques-SHAP values, LIME, attention visualization, counterfactual explanations-partially address this tension, but adoption in enterprise analytics contexts remains limited. Future research should examine how XAI adoption moderates the AI analytics-agility relationship, particularly in heavily regulated industries where decision explainability is a regulatory requirement rather than a design preference, and how explainability techniques for security-relevant AI systems, such as malware and intrusion detection models, affect analyst trust and response speed (Wazid et al., 2025).

11.4 Digital Twins and Simulated Analytics

Digital twin technology-virtual representations of physical assets, processes, or organizational systems-creates new possibilities for AI analytics by enabling simulation of interventions before real-world deployment. In organizational agility contexts, digital twins may allow firms to model reconfiguration scenarios with high fidelity, reducing the risk of strategic pivots. Future research should examine the integration of AI analytics with digital twin infrastructure and its implications for organizational sensing and reconfiguring capabilities, as well as the distinct cybersecurity exposure that digital twins introduce by mirroring operational technology environments in digitally accessible form.

11.5 Responsible AI and Governance

The ethical governance of AI analytics systems is a rapidly developing domain with direct implications for competitive advantage (H10 in this study). Future research should develop and

validate responsible AI governance frameworks specifically for analytics contexts, examining how organizations balance algorithmic transparency with proprietary data protection, how bias auditing practices evolve across industries, and how regulatory frameworks (EU AI Act, US Executive Orders, sector-specific regulations) shape organizational AI analytics deployment. Comparative regulatory studies across jurisdictions would provide valuable cross-national insights.

11.6 Secure AI Deployment and AI-Specific Cyber Risk Management (New)

This revision identifies secure AI deployment as a distinct and underdeveloped future research stream. Priority questions include: how MLOps security controls (Kreuzberger et al., 2023) should be extended to cover model poisoning, adversarial examples, and prompt injection specific to generative and agentic AI; how context-aware cybersecurity risk assessment frameworks (Sánchez et al., 2025) can be adapted to continuously reassess AI-specific risk as models and data pipelines change; and how knowledge-graph-based AI accountability infrastructures (Naja et al., 2022) can be integrated with conventional security information and event management (SIEM) tooling to give security teams visibility into AI-driven decisions. Longitudinal, multi-industry empirical work directly testing H11 and H12 would substantially advance this agenda, as would qualitative case studies of organizations that have experienced AI-specific security incidents, to complement the perceptual survey measures proposed in Section 8.

12. Practical Implications

This study has several practical implications for organizational leaders designing AI analytics strategies. First, the AAACF provides a diagnostic tool for assessing current AI analytics capability across five dimensions, enabling targeted investment prioritization. Organizations at early maturity stages should focus on infrastructure and governance foundations; those at intermediate stages should invest in integration and insight capabilities; advanced organizations should focus on transformative ecosystem positioning.

Second, the Maturity Model provides a roadmap for AI analytics development that sequences capability investments appropriately. Organizations that attempt to deploy advanced AI systems without adequate data governance, talent, or integration infrastructure are likely to find that technical capability does not produce organizational agility or competitive outcomes, consistent with the moderation effects hypothesized in H7 and H8.

Third, the finding that organizational agility mediates the AI analytics-advantage relationship implies that AI investment must be accompanied by organizational redesign-flatter decision hierarchies, cross-functional analytics teams, agile governance structures, and leadership development for data-driven decision-making. Technical AI capability alone is insufficient.

Fourth, the role of AI ethics and explainability (H10) has direct governance implications. Organizations that invest in explainability infrastructure and bias auditing practices may derive reputational and regulatory advantages that outlast short-term technical performance differences. This is particularly salient in healthcare, financial services, and public sector contexts.

Fifth, and central to this revision, leaders should treat cybersecurity governance and cyber resilience as prerequisites for, rather than adjuncts to, AI analytics investment. Organizations advancing AI analytics maturity without a commensurate cybersecurity posture risk building agility and advantage on infrastructure that can be disrupted, manipulated, or discredited by a single cyber incident. Practical steps include aligning MLOps pipeline security with model deployment cadence (Kreuzberger et al., 2023), phasing in zero trust network architecture ahead of, or alongside, deeper AI integration into decision workflows (Phiayura & Teerakanok, 2023), and extending board-level oversight of AI strategy to include cyber risk and AI-specific security review as standing agenda items, following the practice observed in the frontier adopters analyzed in Section 9.

13. Limitations

This study has several limitations that should be considered when interpreting its contributions. First, the AAACF and hypotheses presented here are theoretically derived and await empirical validation. While the framework is grounded in established theories and informed by case evidence, it remains subject to revision based on survey and field data.

Second, the case studies of Amazon, Netflix, and Microsoft represent frontier AI adopters whose AI analytics maturity and organizational capabilities-including their cybersecurity capabilities-are not representative of the broader population of organizations. Generalizability from these cases to the average-to-advancing enterprise must be applied with caution.

Third, the proposed survey design relies on self-report data from senior managers, which may be subject to social desirability bias, recall limitations, and information asymmetries (respondents may not have complete visibility into AI analytics investments across their organizations). This concern is particularly acute for cybersecurity constructs, where organizations may be reluctant to disclose incident history or security weaknesses even under conditions of research confidentiality. The use of archival financial data and, where available, breach-disclosure records as a supplementary measure partially mitigates this concern.

Fourth, rapid technological change in the AI landscape means that specific AI analytics capabilities that are distinctive today (e.g., large language model deployment) may become commoditized within the study period, complicating the interpretation of maturity stage boundaries and competitive advantage mechanisms. The threat landscape targeting AI systems is similarly fast-moving, meaning that the cybersecurity constructs proposed here may require periodic revision as new AI-specific attack techniques and corresponding governance frameworks emerge.

14. Conclusion

This paper has addressed a significant gap in the scholarly understanding of AI-powered business analytics by developing an integrated theoretical framework (AAACF), a five-stage maturity model, and a set of twelve empirically testable hypotheses linking AI analytics capability, cybersecurity governance, and cyber resilience to organizational agility and competitive advantage. The systematic literature review, encompassing 142 core studies spanning 2018-2026

together with a targeted cybersecurity-analytics literature stratum, reveals that while empirical evidence of analytics-performance relationships is accumulating, the mechanisms through which AI analytics specifically enables agility and advantage-and the conditions under which cybersecurity governance sustains or undermines that translation-remain theoretically underspecified and empirically fragmented.

The AAACF contributes a sociotechnical conceptualization of AI analytics capability that integrates infrastructure, intelligence, integration, insight, and impact dimensions within a unified framework grounded in resource-based view, dynamic capabilities, and information processing theories, and extends this framework with a cybersecurity governance and cyber resilience moderator. The AI Analytics Maturity Model operationalizes this framework into a five-stage developmental trajectory, now paired with an explicit cybersecurity posture track, that organizations can use for self-assessment and investment prioritization. The twelve research hypotheses advance scholarship by specifying direct, mediated, and moderated relationships that go beyond bivariate associations to examine the governance, leadership, ethics, and cybersecurity conditions that shape AI analytics effectiveness.

Case analyses of Amazon, Netflix, and Microsoft demonstrate that AI analytics capability, when embedded within agile organizational structures and supported by visionary leadership, robust governance, and mature cybersecurity practice, can produce structural competitive advantages that are difficult for rivals to replicate. These cases also illustrate the ecosystem-level implications of AI analytics maturity, where advanced adopters shape industry competitive dynamics rather than simply responding to them, and where cybersecurity capability is increasingly commercialized as part of the platform value proposition rather than treated as a purely defensive cost center.

The future research agenda identifies generative AI, agentic AI, explainable AI, digital twins, secure AI deployment, and responsible AI governance as the emerging frontiers of AI analytics scholarship. As these technologies mature and their organizational implications become empirically tractable, the AAACF-and its cybersecurity governance extension-provides a theoretical scaffold within which new research can be situated. We invite scholars to engage with this framework, test its hypotheses, including the newly formalized H11 and H12, and extend or revise its dimensions in light of emerging evidence.

References

Abdelmagid, A., et al. (2025). Zero trust architecture as a risk countermeasure in small–medium enterprises and advanced technology systems. Risk Analysis. https://doi.org/10.1111/risa.70026

Acemoglu, D., & Restrepo, P. (2022). Tasks, automation, and the rise in US wage inequality. Econometrica, 90(5), 1973–2016. https://doi.org/10.3982/ECTA19815

Agarwal, R., & Dhar, V. (2014). Editorial—Big data, data science, and analytics: The opportunity and challenge for IS research. Information Systems Research, 25(3), 443–448.

Barney, J. B. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120.

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. AI and Ethics, 5, 3265–3279.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management. Business & Information Systems Engineering, 1(3), 213–222.

Bhimani, A., & Willcocks, L. (2021). Digitisation, 'big data' and the transformation of accounting information. Accounting and Business Research, 44(4), 469–490.

Brynjolfsson, E., & McAfee, A. (2017). Machine, platform, crowd: Harnessing our digital future. W.W. Norton & Company.

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. McKinsey Global Institute.

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165–1188.

Choi, T. M., Wallace, S. W., & Wang, Y. (2022). Big data analytics in operations management. Production and Operations Management, 27(10), 1868–1883.

Davenport, T. H., & Harris, J. (2017). Competing on analytics: Updated, with a new introduction (2nd ed.). Harvard Business Review Press.

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. Harvard Business Review, 96(1), 108–116.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2023). Enterprise governance of information technology: Achieving alignment and value (4th ed.). Springer International Publishing.

Doz, Y., & Kosonen, M. (2010). Embedding strategic agility: A leadership agenda for accelerating business model renewal. Long Range Planning, 43(2–3), 370–382.

El Khatib, M., Al Falasi, A., Almteiri, M., & Al Hammadi, A. (2024). Generative AI in enterprise analytics: Value creation and governance challenges. IEEE Access, 12, 38741–38758. https://doi.org/10.1109/ACCESS.2024.3392110

Fernandez de Arroyabe, J. C., Arranz, C. F., Fernandez de Arroyabe, I., & Fernandez de Arroyabe, M. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security, 124, 102954. https://doi.org/10.1016/j.cose.2022.102954

Fichman, R. G., Dos Santos, B. L., & Zheng, Z. E. (2014). Digital innovation as a fundamental and powerful concept in the information systems curriculum. MIS Quarterly, 38(2), 329–353.

Fosso Wamba, S., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study. International Journal of Production Economics, 165, 234–246.

Fosso Wamba, S., Gunasekaran, A., Akter, S., Ren, S. J. F., Dubey, R., & Childe, S. J. (2019). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356–365.

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. Journal of Risk and Insurance, 89(3), 725–763.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2019). Big data and predictive analytics for supply chain and organizational performance. Journal of Business Research, 70, 308–317.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2–24.

Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. Journal of the Academy of Marketing Science, 49(1), 30–50.

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255–260.

Kreuzberger, D., Kühl, N., & Hirschl, S. (2023). Machine learning operations (MLOps): Overview, definition, and architecture. IEEE Access, 11, 31866–31879. https://doi.org/10.1109/ACCESS.2023.3262138

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444.

Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics and firm performance: Findings from a mixed-method approach. Journal of Business Research, 98, 261–276.

Mikalef, P., Pappas, I. O., Krogstie, J., & Giannakos, M. (2020). Big data analytics capabilities and innovation: The mediating role of dynamic capabilities and moderating effect of the environment. British Journal of Management, 31(2), 272–297.

Naja, I., Markovic, M., Edwards, P., Pang, W., Cottrill, C., & Williams, R. (2022). Using knowledge graphs to unlock practical collection, integration, and audit of AI accountability information. IEEE Access, 10, 74383–74411. https://doi.org/10.1109/ACCESS.2022.3188967

Overby, E., Bharadwaj, A., & Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. European Journal of Information Systems, 15(2), 120–131.

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. IEEE Access, 11, 19487–19511.

Porter, M. E. (1985). Competitive advantage: Creating and sustaining superior performance. Free Press.

Provost, F., & Fawcett, T. (2019). Data science and its relationship to big data and data-driven decision making. Big Data, 1(1), 51–59.

Ransbotham, S., Khodabandeh, S., Kiron, D., Candelon, F., Chu, M., & LaFountain, B. (2020). Expanding AI's impact with organizational learning. MIT Sloan Management Review and Boston Consulting Group Research Report.

Ringle, C. M., Sarstedt, M., Mitchell, R., & Gudergan, S. P. (2020). Partial least squares structural equation modeling in HRM research. International Journal of Human Resource Management, 31(12), 1617–1643.

Sánchez, L. E., Santos-Olmo, A., Rosado, D. G., Blanco, C., Serrano, M. A., Mouratidis, H., & Fernández-Medina, E. (2025). MARISMA: A modern and context-aware framework for assessing and managing information cybersecurity risks. Computer Standards & Interfaces, 92, 103935. https://doi.org/10.1016/j.csi.2024.103935

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. MIS Quarterly, 27(2), 237–263.

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2019). Critical analysis of big data challenges and analytical methods. Journal of Business Research, 70, 263–286.

Tallon, P. P., & Pinsonneault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility: Insights from a mediation model. MIS Quarterly, 35(2), 463–486.

Teece, D. J. (2019). A capability theory of the firm: An economics and (strategic) management perspective. New Zealand Economic Papers, 53(1), 1–43.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509–533.

Vial, G. (2021). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118–144.

Wazid, M., Singh, J., Pandey, C., Sherratt, R. S., Das, A. K., Giri, D., & Park, Y. (2025). Explainable deep learning-enabled malware attack detection for IoT-enabled intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 26(5), 7231–7244.

Wernerfelt, B. (1984). A resource-based view of the firm. Strategic Management Journal, 5(2), 171–180.

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. International Journal of Production Research, 56(8), 2941–2962.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- new11.docx