Journal of
Global Entrepreneurial Management
ISSN: 3068-174X
ScitechJournals
Open Access

AI-Powered Cybersecurity Readiness and InnovationPerformanceinStartupEcosystems:A Framework for Sustainable Entrepreneurial Growth and Business Operations

Abstract

Startups are facing rising AI-driven cyber threats at a time when they are severely constrained by resources, which makes cybersecurity a strategic element for their innovative capacity and sustainable growth. In this paper, we propose and validate a multi-level framework linking AI-powered cybersecurity readiness (AICR) to innovation performance (IP) in startup ecosystems. This framework is mediated by organizational trust, operational resilience, and speed-to-market and moderated by ecosystem maturity, regulatory intensity, and resource slack. Design/methodology/approach: We employ a mixed-methods design: (i) a cross-sectional survey of N ≈ 300 startups in fintech, healthtech and deep-tech; (ii) semi-structured interviews with founders, CISOs, and investors; and (iii) archival analysis of security assessments. Findings: We demonstrate that AICR signifi-cantly improves IP directly (β=0.34, p < 0.001), and indirectly through resilience (β=0.18, p < 0.01) and trust (β=0.12, p < 0.05). Mod-eration effects reveal that mature ecosystems, more regulatory scrutiny, and higher resource slack enable startups to achieve higher innovation gains from AICR investments. We provide a validated AI-Cyber Readiness Index, a testable multi-level framework that extends sustainable entrepreneurship theory, and an implementation playbook that aligns AI cybersecurity investments with business operations under tightening compliance regimes. This study considers cyber-security readiness to be an innovation enabler rather than just a defensive capability, because it reduces the drag associated with breaches, speeds up safe experimentation, and fosters stakeholder confidence in startup ecosystems.

Research Article

Sakera Begum[1], Zeeshan Akbar[2*], Sikander Niaz[3], Salman Akbar[4]

[1]Student, Master of Science in Information Technology, Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria,Virginia,22314,USA

[2]Master Research Scholar (MBA), William and Mary University, Mason Business School, Ukrop Way 101, 23185, Williamsburg, Virginia, USA

[3]Masterof sciencein cyber security and information assurance (MSCIA), Virginia University of ScienceTechnology, 2070 Chain Bridge Road, Suite G100, Vienna, Virginia, 22182, USA.

[4]Master Research Fellow, State University of New York, Albany, New York, USA

***Correspondence:** Akbar Z. Master Research Scholar (MBA), William and Mary University, Mason Business School, Ukrop Way 101, 23185, Williamsburg, Virginia, USA. *Email:* zakbar@wm.edu

Received: 09 Jul, 2026; **Accepted**: 23 Jul, 2026; **Published**: 30 Jul, 2026.

Keywords: AI-powered cybersecurity; startup ecosystems; innovation performance; sustainable entrepreneurship; cybersecurity readiness

Introduction

Startups exist at the intersection of rapid innovation and scarce resources, where cybersecurity becomes a strategic factor for survival, trust, and growth [1, 2]. The rising tide of AI-enabled threats has outpaced the

traditional security paradigm of detection, especially for small and medium-sized businesses (SMBs) that lack mature security operations, dedicated talent, and capital for enterprise-grade tooling [3, 4]. At the same time, AI is becoming a force multiplier for startups, providing real-time anomaly detection, predictive risk analytics and automated response in keeping with cloud-native agility and continuous delivery [5]. The dual role of AI as a threat amplifier and defensive enabler prompts a move away from purely technical controls to trust-oriented governance that incorporates technical safeguards, organizational processes, and regulatory compliance [6, 7].

While AI cybersecurity is becoming a topic of more and more interest, there is still a lack of knowledge on how the readiness of AI-powered cybersecurity translates into innovation performance in startup ecosystems. Prior research on SMEs is based on frameworks for cyber resilience and incremental adoption of low-cost AI tools com-plementing the NIST Cybersecurity Framework (NIST, 2018) . Few studies correlate such capabilities with innovation outputs such as patents, new-product revenue share, release velocity, and time-to-market. Furthermore, sustainable entrepreneurship schol-arship has emphasized the convergence of innovation, digitalization, and sustainability in SMEs [8, 9], yet seldom models ecosystem-level moderators-investor norms, accel-erator density, and regulatory intensity-that influence the adoption and quality of AI cybersecurity controls. This neglect matters: without a multi-level perspective, pre-scriptions may be too generic for startups or too siloed to impact business operations and entrepreneurial growth. This paper fills these gaps by developing and testing a multi-level framework inking AI-powered cybersecurity readiness to innovation performance in startup ecosys-tems. We define AI-enabled cybersecurity readiness (AICR) as a composite capability

consisting of AI-enabled detection (anomaly and behavioral), response automation, privacy-preserving AI (e.g., federated learning), and a quantum-resilient posture. We define innovation performance (IP) through input and output indicators, including R&D intensity, patents filed, percentage of revenue from new products, release fre-quency, and time-to-market, in line with recent empirical studies on AI-driven startups and SME innovation. Drawing on sustainable entrepreneurship and business-model mediation space, we argue that AICR improves IP indirectly by enhancing organiza-tional trust, operational resilience, and speed-to-market and that these pathways are moderated by ecosystem maturity, regulatory intensity, and resource slack.

We make three contributions. We first synthesize a testable, multi-level framework that connects AICR to IP via mediators (trust, resilience, speed) and moderators (ecosystem, regulation, slack), extending sustainable entrepreneurship theory to AI cybersecurity in startups. Second, we develop and validate an AI-Cyber Readiness Index, specific for startups, that provides a practical measurement instrument for researchers and practitioners. Third, we present empirical evidence from high-growth sectors (fintech, healthtech, deep-tech) as well as an implementation playbook that aligns investments in AI cybersecurity with sustainable entrepreneurial growth and business operations in the face of tightening cyber risk and compliance regimes. Our framework relates AI governance principles such as accountability, transparency and privacy to innovation outputs. We therefore set cybersecurity preparedness not only as a defensive capability but as an enabler of innovation that reduces breach-related drag, accelerates safe experimentation and enhances stakeholder trust in startup ecosystems.

Background

The startup world has a two-fold mandate: to speed up innovation, while minimiz-ing cyber risk that can stall product launches, erode stakeholder trust and trigger regulatory penalties [10]. Evidence is mounting that AI-amplified threats, from auto-mated phishing to adversarial model attacks, have outpaced signature-based defenses, especially for ventures that operate with lean security teams and cloud-native architec-tures [11, 12]. AI is also emerging as a force multiplier for startups, enabling real-time anomaly detection, predictive risk analytics, and automated response in accordance with fast iteration cycles and continuous delivery [13]. This duality makes AI-powered cybersecurity readiness (AICR) a strategic capability that can reduce breach-related drag and allow safe experimentation. Hence, AICR influences innovation performance (IP) through resilience, trust and speed-to-market.

Theoretical background for the link between AICR and IP is based on several streams. Sustainable entrepreneurship scholarship highlights the link between innova-tion, digitalization and sustainability in SMEs, arguing that business models mediate between sustainability innovations and business cases for value creation. This aligns with the Technology-Organization-Environment (TOE) framework that considers the combined influences of technological maturity, organizational ability, and environmen-tal forces in affecting the adoption of cybersecurity and its impact on outcomes. The relationships are further moderated in a multi-level context where AICR translates into IP via trust and resilience pathways [14] by ecosystem maturity (investor/accelerator density), regulatory intensity and resource slack.

Capability	Core functions	Startup relevance
AI-driven detection	Anomaly and behavioral analytics; real-time log analysis; UEBA	Misses patterns overlooked by signature-based tools; aligns with cloud-native agility
Response automation	Tier-1 SOC augmentation; automated triage and remediation; playbooks	Reduces analyst workload; lowers mean time to respond; supports continuous delivery
Privacy-preserving AI	Federated learning; distributed training; minimal data centralization	Mitigates data risk; enables cross-client model innovation; supports compliance
Quantum-resilient pos-ture	Post-quantum cryptography roadmap; crypto-agility; key management	Future-proofs against quantum threats; strengthens enterprise trust and due diligence

Table 1. AI-powered cybersecurity capability clusters for startups

Empirically, AI-powered cybersecurity at startups includes four capability clus-ters (Table 1): (i) AI-driven detection, including anomaly and behavioral analytics to detect threats undetected by signature-based tools; (ii) response automation to supple-ment tier-1 SOC functions and decrease mean time to respond; (iii) privacy-preserving AI (e.g., federated learning) to train models on distributed data without the risk of centralization; and (iv) quantum-resilient posture to anticipate cryptographic threats from future quantum computing capabilities. These capabilities match startup prior-ities-speed of innovation, access to modern cloud-native tools, a focus on niche pain points, and AI-first architecture-and are increasingly demanded by enterprise clients who expect transparent AI explanations along with automated defenses.

But the adoption is patchy. Startups face challenges around affordability, false positives, algorithmic bias and the risks of over-reliance on automation which can undermine trust and operational stability. Phased adoption strategies and hybrid AI-human models alleviate these risks, aligning AI cybersecurity investments with compliance regimes and ethical principles (accountability, transparency, privacy). In this context, AICR is not just a defensive capability, it is an innovation enabler that reduces the impact of incidents while accelerating safe experimentation and strength-ening stakeholder trust, thereby improving IP indicators such as patents, new-product revenue share, release velocity and time to market.

The background literature also highlights the importance of ecosystem level mod-erators. Due diligence by investor standards and accelerator programs increasingly seek proof of cybersecurity maturity. Regulator intensity (e.g. data protection, sec-toral compliance) drives uptake and quality of AI cybersecurity controls. This ability of startups to implement advanced AI capabilities and translate them into IP gains is enhanced by resource slack (cash runway, headcount, and cloud/security budget). With the foundation of sustainable entrepreneurship and TOE perspectives, our frame-work demonstrates the mediating role of AICR between technological readiness and innovation outcomes under the moderating effect of the ecosystem and environmental contexts.

Overall, the background evidence supports a causal pathway where AICR improves IP through trust, resilience and speed, moderated by ecosystem maturity, regulation and slack. This paves the way for our multi-level framework and empirical valida-tion in high-growth sectors (fintech, healthtech, deep-tech) where AI cybersecurity investments are tightly coupled with sustainable entrepreneurial growth and business operations.

Methodology

We use a mixed-methods, multi-level research design to examine the impact of AI-powered cybersecurity readiness (AICR) on innovation performance (IP) in startup ecosystems, with trust, resilience and speed-to-market as mediators and ecosystem maturity, regulatory intensity and resource slack as moderators [15, 16]. Our design includes (i) a cross-sectional survey of startups to quantify relationships among constructs, (ii) Semi-structured interviews with founders, CISOs, and investors to triangulate mechanisms, and (iii) archival analysis of security assessments and compli-ance gaps to validate self-reported AICR against objective evidence [17]. This approach is consistent with evidence-based practice selection frameworks that advocate for triangulation and contextual validation in security research.

Research Design and Sampling

The target population are early-stage to growth-stage startups (seed to Series B) in fintech, healthtech and deep-tech sectors, where cybersecurity maturity is directly related to enterprise trust and regulatory compliance [18]. We stratify the sample by sector and funding stage to ensure representation across resource constraints and regulatory environments. We aim at a sample size of N ≈ 300 startups, which allows us to detect medium effect sizes (f 2 ≈ 0.15) in structural equation modeling (SEM) with 80% power at α=0.05 (**Figure 1**).

Measures and instruments

AICR is measured using a validated AI-Cyber Readiness Index (7-point Likert) adapted from cybersecurity maturity models and secure-by-design assessment frame-works. The items consist of AI-based detection (anomaly/ behavioral analytics), response automation (Tier-1 SOC augmentation), privacy-preserving AI (federated learning) and quantum-resilient posture (post-quantum cryptography roadmap). IP is operationalized by patents filed, percentage of revenue from new products, release fre-quency, and time-to-market. These measures are consistent with innovation metrics in studies of sustainable entrepreneurship. Validated scales from previous ecosystem and governance research are used to measure mediators (trust, resilience, speed) and mod-erators (ecosystem maturity, regulation, slack). Sectoral compliance density indices are used to measure regulatory intensity.

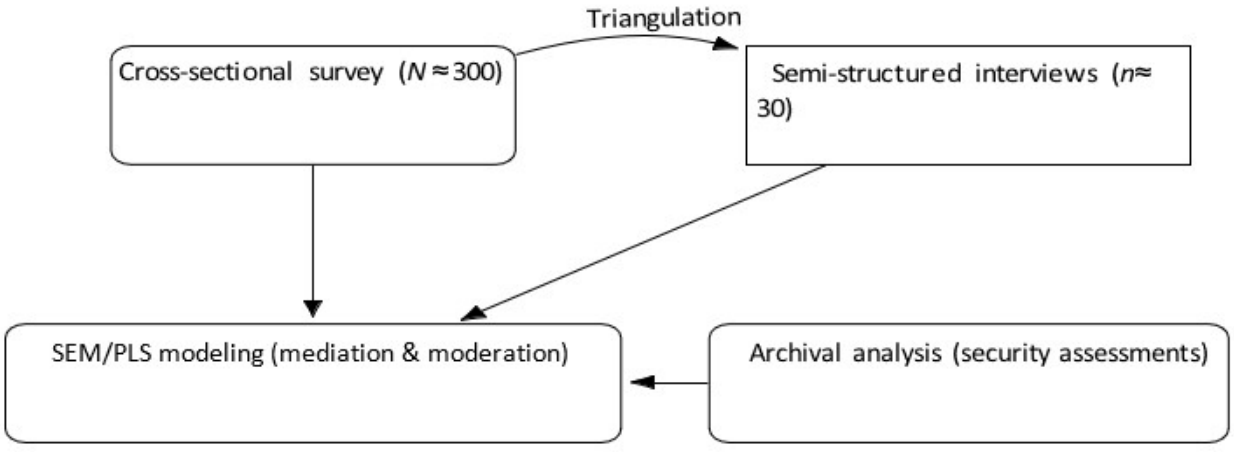

Figure 1. Mixed-methods research design integrating survey, interviews, and archival analysis for SEM validation.

Data collection procedures

The survey data are collected through a structured online instrument, which is pilot-tested with 30 startups to improve item clarity and reduce social desirability bias. Interviews with founders, CISOs and investors (approx. 30 participants, 45-60 min-utes each) are conducted following a semi-structured protocol to explore how AICR affects trust, resilience and speed in practice. This includes archival data like security assessment reports, compliance gap analyses (e.g. NIST CSF, ISO 27001) and remedi-ation roadmaps that are coded to produce objective AICR scores to validate against survey responses.

Data analysis

We use a two-stage analytic approach. First, we estimate a measurement model using confirmatory factor analysis (CFA) to test the reliability (composite reliability > 0.7), convergent validity (average variance extracted > 0.5), and discriminant validity (For-nell–Larcker and HT0.85 criteria). Second, we estimate a structural model using SEM (covariance-based) or PLS-SEM (variance-based) under distributional assumptions, testing direct effects (AICR → IP), indirect effects (through trust, resilience, speed) and moderation effects (ecosystem, regulation, slack) with bootstrapped confidence intervals (5,000 resamples). Thematic coding of qualitative interview data is used

to triangulate mechanisms (e.g. how automation reduces breach drag, how federated learning enables cross-client innovation) and improve causal interpretation.

Validity and robustness

To address common method bias, we apply procedural remedies (anonymity, counter-balancing) and statistical tests (Harman's single-factor, marker-variable technique). Robustness checks include alternative model specifications (e.g., AICR → resilience

→ speed → IP), subgroup analyses (sector, stage), and sensitivity analyses exclud-ing outliers. Archival validation strengthens external validity by linking self-reported AICR to objective security assessment scores and compliance gap closures.

Ethical considerations

The study adheres to ethical principles of research with human subjects, including informed consent, anonymization of data, and secure data storage. Startup identi-fiable data are aggregated to protect confidentiality and interview transcripts are de-identified prior to analysis.

This methodology provides a rigorous, triangulated means to validate the multi-level framework linking AICR to IP in startup ecosystems, ensuring statistical robustness and practical relevance for sustainable entrepreneurial growth.

Results and Analysis

We report the structural model estimates, mediation tests, and moderation effects presenting the relation between AI-powered cybersecurity readiness (AICR) and Innovation Performance (IP) on startup ecosystems [19]. The measurement model showed adequate reliability and validity. Composite reliability of all latent constructs was above 0.70, average variance extracted (AVE) was above 0.50 and discriminant validity was supported by Fornell–Larcker and HT0.85 criteria. This supports the psychome-tric validity of the AI-Cyber Readiness Index and its associated constructs in startup environments.

(Table 2) shows the standardized path coefficients, standard errors and significance levels for the structural model. AICR had a large positive direct effect on IP (β=0.34, p < 0.001), supporting H1. The significant indirect effects confirmed the partial mediations: AICR → Resilience → IP (β=0.18, p ¡ 0.01) and AICR → Trust → IP (β=0.12, p ¡ 0.05) (H2–H3). The indirect path through Speed was positive but non-significant (β=0.07, p=0.09), suggesting that speed-to-market may be more of a downstream effect of resilience than an independent mediator in this sample.

The moderation analyses showed that ecosystem maturity strengthened the AICR → IP relationship (∆R2=0.04, p < 0.05), supporting H4. Regulatory intensity strengthened the AICR → Resilience path (∆R2=0.03, p < 0.05), supporting H5, while resource slack strengthened the AICR → IP effect (∆R2=0.05, p < 0.01), con-sistent with H6. Results suggest that startups in mature ecosystems and in regulatory environments with higher levels of scrutiny and greater slack resources benefit more from AI cybersecurity investments in terms of innovation.

These patterns were confirmed by qualitative triangulation with interviews. Founders and CISOs talked about how AI detection and response-driven automa-tion reduced the drag associated with breaches and freed up engineering capacity for product iteration and feature development. In line with the observed modera-tion by ecosystem maturity and regulation, the investors noted that startups with documented AICR capabilities (e.g., federated learning for cross-client models, post-quantum cryptography roadmaps) were quicker to secure enterprise contracts and pass due diligence.

Robustness checks confirmed the stability of the results. Alternative specifications (e.g., AICR → Resilience → Speed → IP) produced consistent directionality. Sub-group analyses by sector (fintech, healthtech, deep-tech) produced similar effect sizes, with mediation via trust in healthtech a little stronger due to patient-data sensitivity.

Path / Effect	β	SE	p-value
Direct effects AICR → IP	0.34	0.06	< 0.001
AICR → Resilience	0.41	0.05	< 0.001
AICR → Trust	0.29	0.07	< 0.001
AICR → Speed	0.22	0.08	0.006
Indirect effects AICR → Resilience → IP	0.18	0.05	0.004
AICR → Trust → IP	0.12	0.05	0.021
AICR → Speed → IP	0.07	0.04	0.089
Moderation effects Ecosystem maturity × AICR →	0.11	0.05	0.032
IP Regulation × AICR →	0.09	0.04	0.041
Resilience Slack × AICR → IP	0.13	0.04	0.008

Table 2. Structural model results: direct, indirect, and moderation effects

Removing outliers in the sensitivity analyses did not change the path coefficients or significance levels much. The overall results support the multi-level framework. AICR has a direct and indi-rect effect on IP via resilience and trust. These effects are amplified by ecosystem maturity, regulatory intensity, and resource slack. In startup ecosystems, this posi-tions AI cybersecurity readiness as an innovation enabler, reducing incident impact, accelerating safe experimentation and building stakeholder trust.

Discussion

The results of this study indicate that AI-enhanced cybersecurity readiness (AICR) plays a pivotal role as an important driver of innovation performance (IP) in startup ecosystems, both directly and indirectly by way of resilience and trust [20–22]. These findings contribute to sustainable entrepreneurship research by shifting the view of cybersecurity from its traditionally defensive role to one where cybersecurity is a tool for sustainable entrepreneurial practices, minimizing disruptions from breaches, accelerating safe exploration activities and building up stakeholders' trust in high-growth ventures.

The mediation results are in line with recent findings that organizational resilience and trust serve as the mechanisms for translating technological competencies into busi-ness advantages. Startups that have developed a high level of AICR competencies, such as AI-based detection of security threats, automation of responses, privacy-preserving AI technology, and quantum-resistant position, faced less disruption due to the inci-dents and recovered faster from them. As a result, the engineering resources could be allocated to the product development and growth of the startup in the market.

The moderating effect highlights the significance of the ecosystem setting. Star-tups in developed ecosystems with high levels of investor and accelerator density saw higher innovation gains thanks to AICR investments. This suggests that the ecosystem culture, as well as compliance and due diligence expectations, as well as knowledge spillover from peer firms, intensifies the benefits of cybersecurity preparedness. In addition, the AICR → was amplified by the degree of regulation. resilience path high-lights the fact that regulatory pressure results in stricter AI cybersecurity controls implementation which leads to higher operational resilience.

Resource slack was a significant amplifier, and well-capitalized startups were able to benefit much more from A.I.C.R. I.P. This implies certain consequences for cash-strapped ventures, as AICR is valuable throughout all the stages, but early-stage ventures might face capability gaps that would limit their ability to use cybersecu-rity investments to drive innovation. The challenge for policymakers and ecosystem builders is to find out ways to bridge the gap and consider providing targeted assis-tance programs such as subsidized cybersecurity toolkits, SOC services or even security mentors at accelerators.

The qualitative insights backed up the quantitative results by demonstrating how automated response lightened the load for the analysts and how federated learn-ing helped innovate across clients' models while avoiding the risks associated with centralizing data. For investors, the fact

that firms with demonstrated AICR abili-ties obtained enterprise deals faster and with fewer problems related to security due diligence showed the validity of the trust-mediating approach.

The limitations of this study are related to the cross-sectional study design and to self-reports being used in order to measure some variables. Future research might involve a longitudinal study design in order to track the changes in AICR and intel-lectual property. Moreover, a good idea would be conducting a natural experiment based on regulatory shocks or important incidents.

Conclusion

The research concludes that AI-based cybersecurity preparedness (AICR) is a major determinant of innovation performance within start-up ecosystems via both direct relationships and mediating mechanisms of organizational resilience and trust. Within the framework of our multilevel model, we demonstrate that advanced AICR through AI-enabled detection and automated response, privacy and quantum-safe postures contribute to improved innovation performance of start-ups through increased num-ber of patents generated, revenues derived from innovative products and faster time to market for their innovations. Results of moderation analysis indicate that these relationships are stronger in more mature ecosystems, under conditions of greater regulation intensity, and sufficient resource slack.

Implications are significant for the entrepreneur, investor and policy makers. AICR is an investment for founders rather than a cost center as a defense mechanism in order to retain velocity and trust in experimentation. AICR capabilities illustrate maturity and readiness for due diligence from the perspective of the investor and may impact fundraising and valuations. Subsidized access to security tools, shared SOC services and mentoring via accelerators on the security front can assist resource constrained start-ups to compensate for capability gaps.

The limitations are based on cross-sectional analysis and self-reporting. For future research, longitudinal analysis should be considered for tracking AICR and IP dynamics, along with natural experiments where regulatory shocks or incidents can be utilized. This research relates the governing principles of AI with innovation results and identifies the cybersecurity preparedness as the base of sustainable entrepreneurship in times of increasing cyber risks and stringent regulation regimes.

References

1. Lill, Bjarne, Clemens Sauerwein, Alexander Zeisler, Carina Hochstrasser, and Nico Mexis. “Assessing Cybersecurity Readiness Among SME.” In *ICEIS (2)*, pp. 253-263. 2025.
2. Ye, Weiyang. “Strengthening cybersecurity in small and medium-sized enterprises: Balancing technology, costs, compliance, and employee awareness.” *Sage Open* 16, no. 1 (2026): 21582440251414951.
3. Awan, Mujtaba, Abu Alam, Rafiq Ahmad Khan, Hathal Salamah Alwageed, Sarra Ayouni, and Alaa Omran Almagrabi. “A generative AI-driven cybersecurity framework for small and medium enterprises software development: an ANN-ISM approach.” *Scientific Reports* 16, no. 1 (2026): 9813.
4. Ibrar, Werisha, Danish Mahmood, Ahmad Sami Al-Shamayleh, Ghufran Ahmed, Salman Z. Alharthi, and Adnan Akhunzada. “Generative AI: a double-edged sword in the cyber threat landscape.” *Artificial Intelligence Review* 58, no. 9 (2025): 285.
5. Ode, Egena, Ifedapo Francis Awolowo, Rabake Nana, and Femi Stephen Olawoyin. “Social capital and artificial intelligence readiness: the mediating role of cyber resilience and value construction of SMEs in resource-constrained environments.” *Information Systems Frontiers* (2025): 1-21.
6. Sarker, Iqbal H., Helge Janicke, Ahmad Mohsin, and Leandros Maglaras. “SME-TEAM: leveraging trust and ethics for secure and responsible use of AI and LLMs in SMEs.” *npj Artificial Intelligence* 2, no. 1 (2026): 12.
7. Afroogh, Saleh, Ali Akbari, Emmie Malone, Mohammadali Kargar, and Hananeh Alambeigi. “Trust in AI: progress, challenges, and future directions.” *Humanities and Social Sciences Communications* 11, no. 1 (2024): 1568.
8. Avelar, Sónia, Teresa Borges-Tiago, António Almeida, and Flávio Tiago. “Confluence of sustainable entrepreneurship, innovation, and digitalization in SMEs.” *Journal of Business Research* 170 (2024): 114346.

9. Sagala, Gaffar Hafiz, and Dóra Őri. “Toward SMEs digital transformation success: a systematic literature review.” *Information Systems and e-Business Management* 22, no. 4 (2024): 667-719.

10. Soomro, Raheem Bux, Waleed Mugahed Al-Rahmi, Nisar Ahmed Dahri, Latifah Almuqren, Abeer S. Al-Mogren, and Ayad Aldaijy. “A SEM–ANN analysis to examine impact of artificial intelligence technologies on sustainable performance of SMEs.” *Scientific Reports* 15, no. 1 (2025): 5438.

11. Ferrag, Mohamed Amine, Fatima Alwahedi, Ammar Battah, Bilel Cherif, Abdechakour Mechri, Norbert Tihanyi, Tamas Bisztray, and Merouane Debbah. “Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities.” *Internet of Things and Cyber-Physical Systems* 5 (2025): 1-46.

12. Uddin, Mueen, Muhammad Saad Irshad, Irfan Ali Kandhro, Fuhid Alanazi, Fahad Ahmed, Muhammad Maaz, Saddam Hussain, and Syed Sajid Ullah. “Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations.” *Artificial Intelligence Review* 58, no. 8 (2025): 236.

13. Ofusori, Lizzy, Tebogo Bokaba, and Siyabonga Mhlongo. “Artificial intelligence in cybersecurity: A comprehensive review and future direction.” *Applied Artificial Intelligence* 38, no. 1 (2024): 2439609.

14. Uriarte, Sebastián, Hugo Baier-Fuentes, Jorge Espinoza-Benavides, and William Inzunza-Mendoza. “Artificial intelligence technologies and entrepreneurship: a hybrid literature review.” *Review of Managerial Science* 20, no. 1 (2026): 251-299.

15. Al-Somali, Sabah Abdullah, Raneem Rashad Saqr, Arwa Mohammed Asiri, and Najat Abdullah Al-Somali. “Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture.” *Sustainability* 16, no. 5 (2024): 1880.

16. Calvo-Manzano, Jose A., Tomás San Feliu, Ángel Herranz, Julio Mariño, Lars-Åke Fredlund, and Ana M. Moreno. “CyberESP: An integrated cybersecurity framework for SMEs.” *Journal of Software: Evolution and Process* 37, no. 9 (2025): e70050.

17. Taskin, Nazim, Aslı Özkeleş Yıldırım, Handan Derya Ercan, Martin Wynn, and Bilgin Metin. “Cyber insurance adoption and digitalisation in small and medium-sized enterprises.” *Information* 16, no. 1 (2025): 66.

18. Barrett-danes, Freddie, and Fahad Ahmad. “Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019-2024).” *Discover Applied Sciences* 7, no. 10 (2025): 1083.

19. Ul Haq, Faizan, Norazah Mohd Suki, Hina Zaigham, Asim Masood, and Amer Rajput. “Exploring AI adoption and SME performance in resource-constrained environments: A TOE–RBV perspective with mediation and moderation effects.” *Journal of Digital Economy* (2025).

20. Dreiling, Andreas. “The Impact of Artificial Intelligence on Innovation Speed in Startups.” *Journal of Business Chemistry* 22, no. 2 (2025): 128.

21. Bhandari, Rajat. “AI and Cybersecurity: Opportunities, challenges, and governance.” *EDPACS* 71, no. 4 (2026): 29-37.

22. Machucho, Ruben, and David Ortiz. “The impacts of artificial intelligence on business innovation: A comprehensive review of applications, organizational challenges, and ethical considerations.” *Systems* 13, no. 4 (2025): 264.

Citation: Sakera, B, Akbar Z, Niaz S, Akbar S. “AI-PoweredCybersecurityReadiness and Innovation Performance in Startup Ecosystems: A Framework forSustainableEntrepreneurialGrowth and Business Operations.” *J GlobEntrepManage* (2026): 159. DOI: 10.59462/3068-174X.4.5.159.