Balancing Digital Transformation, Organizational Agility, and Cyber Resilience:A Multi-Case Study of Post-Pandemic Financial SMEs

Authors

Abiodun Okunola, Abi Cit, James Claer

Date; November 3, 2026

Abstract

The post-pandemic period has confronted financial small and medium enterprises (SMEs) with a trilemma: accelerating digital transformation while preserving organizational agility and strengthening cyber resilience under severe resource constraints. Although prior research has separately examined digitalization and agility or cybersecurity maturity, no integrated framework explains how these three imperatives interact within resource-limited financial SMEs. This study addresses that gap through a multi-case design involving twelve financial SMEs across three regulatory jurisdictions, combining semi-structured interviews with documentary analysis of cyber-incident and digital-investment records. A fuzzy-set qualitative comparative analysis (fsQCA) identified configurations of digital capability, agile governance, and cyber-resilience practices associated with superior performance outcomes. The integrated framework achieved 89.4% coverage of high-performing cases, with agile decision rights and foundational (production-oriented) digital infrastructure emerging as the strongest conditions, consistent with large-scale evidence that production technologies outperform consumption technologies in predicting SME agility . The study concludes that cyber resilience is not a constraint on digital transformation but a complementary capability that, when paired with agility, enables sustainable post-pandemic recovery. Practitioners receive an actionable configuration roadmap; policymakers receive guidance on modular, scale-appropriate security frameworks.

Keywords: digital transformation, organizational agility, cyber resilience, financial SMEs, post-pandemic recovery

1. Introduction

1.1 Background

The COVID-19 pandemic functioned as an unplanned natural experiment in organizational digitalization. Faced with mobility restrictions and disrupted supply chains, enterprises worldwide compressed years of planned technology adoption into months, expanding remote-work infrastructure, e-commerce channels, and cloud-based operations . For small and medium enterprises (SMEs), this acceleration was both a lifeline and a stress test. Recent large-scale evidence from 491,636 SME technology-adoption records demonstrates that digital transformation remains a critical driver of organizational agility in the post-pandemic era, yet the measurement of agility and its predictors remains underexplored at scale .

Financial SMEs occupy a particularly exposed position within this landscape. They handle high-value transactions and sensitive customer data, making them attractive targets for financially motivated cybercriminals, yet they typically lack the financial, technical, and human capacity to adopt comprehensive international cybersecurity standards such as NIST CSF or ISO/IEC 27001 . The ISC2 expert practitioner literature confirms that financial services are among the most targeted sectors, with small and midsize businesses facing ransomware, infostealer malware, and social-engineering campaigns that exploit precisely the resource gaps these firms possess . Consequently, the post-pandemic financial SME must simultaneously pursue three objectives that are often treated as competing: digital transformation for competitiveness, organizational agility for responsiveness, and cyber resilience for survival.

1.2 Problem Statement

Existing scholarship has produced valuable but fragmented insights. On one hand, machine-learning studies have established that production-oriented technologies (automation, digital infrastructure) predict organizational agility more strongly than customer-facing consumption technologies . On the other, cybersecurity research has developed resilience frameworks tailored to resource-constrained FinTech SMEs, demonstrating that adaptive risk management practices significantly enhance cyber resilience . Separately, studies of digital resilience in FinTech have examined dynamic capabilities after security failures but relied on small, homogeneous samples that limit generalizability .

What remains missing is an integrated account of how digital transformation, organizational agility, and cyber resilience operate jointly in post-pandemic financial SMEs. Three specific gaps persist. First, no study has modeled the *configurational* relationships among these three constructs—that is, how they combine rather than compete. Second, existing frameworks either assume large-firm resources or, when adapted for SMEs, treat cybersecurity as a standalone compliance exercise rather than as an enabler of agile digital operations. Third, the empirical base for financial SMEs specifically remains thin, with most digital-transformation research focusing on manufacturing or general SME populations . The unsolved issue, therefore, is the absence of a

validated, empirically grounded framework that specifies which combinations of digital, agile, and cyber-resilience practices distinguish high-performing financial SMEs from their peers in the post-pandemic environment.

1.3 Objectives of the Study

General objective: To develop and validate an integrated framework explaining how digital transformation, organizational agility, and cyber resilience jointly shape the post-pandemic performance of financial SMEs.

Specific objectives:

1. To identify the configurations of digital-transformation practices, agile governance mechanisms, and cyber-resilience capabilities associated with superior performance in financial SMEs.
2. To design a configurational framework that integrates these three imperatives and is implementable under resource constraints.
3. To validate the framework through multi-case comparison across financial SMEs in diverse regulatory contexts.

1.4 Research Questions

1. Which combinations of digital-transformation, organizational-agility, and cyber-resilience conditions are sufficient for high performance among post-pandemic financial SMEs?
2. How does the proposed integrated framework account for performance differences that separate digitalization-only or cybersecurity-only explanations cannot capture?
3. What implementation barriers and enabling factors shape the adoption of integrated digital-agility-resilience practices in resource-constrained financial SMEs?

1.5 Significance of the Study

For practitioners and administrators: The study provides financial SME leaders with a configuration roadmap rather than a generic maturity model. It identifies which combinations of practices—particularly foundational digital infrastructure, distributed decision rights, and adaptive incident-response routines—are associated with high performance, enabling prioritized investment under budget constraints.

For policymakers and regulators: The findings inform the design of modular, scale-appropriate cybersecurity frameworks. Rather than mandating compliance regimes designed for large institutions, regulators can support the specific configurations that empirical evidence links to resilience and agility in smaller financial firms.

For academic literature: The study extends the Technology-Organization-Environment and dynamic-capability perspectives by introducing a configurational logic that treats cyber resilience as complementary to, rather than constraining, digital transformation. It also contributes rare empirical evidence on financial SMEs specifically.

For future researchers: The framework and case protocol provide a replicable template for comparative research across regulatory jurisdictions and SME sub-sectors.

1.6 Scope and Limitations

The study focuses on financial SMEs (defined as firms with fewer than 250 employees and annual turnover below EUR 50 million, consistent with the European Commission definition) operating in retail banking, payments, lending, and insurance intermediation. The temporal scope is the post-pandemic period from 2022 to 2025. Geographically, the study draws on cases from three jurisdictions selected for regulatory variation: a Eurozone member state, a Southeast Asian emerging economy, and a Gulf Cooperation Council country. Excluded from scope are large financial institutions, pure cryptocurrency firms, and SMEs that ceased operations during the pandemic.

Three limitations are acknowledged upfront. First, the multi-case design prioritizes analytical generalization over statistical generalization; findings characterize configurations rather than population parameters. Second, retrospective interview data may be subject to recall bias, mitigated through documentary triangulation. Third, the study does not measure long-term performance outcomes beyond the observation window.

2. Literature Review

2.1 Conceptual Review

Digital transformation in the SME context refers to the integration of digital technologies across business functions, fundamentally altering value delivery and operational processes . For financial SMEs, digital transformation encompasses core-system modernization, digital customer onboarding, automated compliance workflows, and cloud-based service delivery. The post-pandemic literature emphasizes that transformation is not merely technological adoption but organizational reconfiguration around digital capabilities.

Organizational agility denotes a firm‘s capacity to sense and respond rapidly to environmental changes through flexible resource allocation and decision-making structures. Recent machine-learning evidence distinguishes between production technologies (automation, digital infrastructure) and consumption technologies (customer-facing platforms), finding that the former

more strongly predict agility outcomes . This distinction is consequential for resource-constrained SMEs that must choose where to invest first.

Cyber resilience extends beyond prevention to encompass the capacity to anticipate, withstand, recover from, and adapt to cyber incidents. In financial SME contexts, resilience is increasingly framed as a dynamic capability rather than a static set of controls. Research on Nairobi FinTech SMEs demonstrates that adaptive risk-management practices—integrated governance, technical controls, operational processes, and human capabilities—significantly enhance cyber resilience, even under resource constraints . The practitioner literature reinforces that small financial institutions face the same threat actors as large ones, but with fewer buffers, making resilience architecture a strategic rather than technical concern .

2.2 Theoretical Framework

This study draws on three complementary theoretical lenses.

Dynamic Capabilities Theory provides the overarching logic. Originally articulated to explain how firms integrate, build, and reconfigure internal and external competences to address rapidly changing environments, the theory is particularly apt for the post-pandemic financial SME context. Digital transformation, organizational agility, and cyber resilience can each be understood as dynamic capabilities—or as components of a higher-order capability for managing digital-environmental turbulence. The study extends this perspective by examining how these capabilities combine configurationaly rather than operating in isolation.

Technology-Organization-Environment (TOE) Framework supplies the contextual dimension. TOE posits that technology adoption is shaped by technological attributes, organizational characteristics, and environmental conditions. For financial SMEs, the environmental dimension includes regulatory pressure (e.g., DORA in the EU, NIS2 transposition) and threat-landscape intensity . The framework helps explain why identical digital investments may yield different resilience outcomes across regulatory contexts.

Prospect Theory informs the interpretation of decision-making under risk. Financial SME leaders facing cyber threats and digital-competition pressures make choices under uncertainty, often weighting losses more heavily than equivalent gains. This lens helps explain why some firms prioritize defensive cybersecurity investments over transformative digital projects—or, conversely, why some underinvest in resilience while pursuing growth. The study uses prospect theory not as a predictive model but as an interpretive resource for understanding strategic trade-offs.

2.3 Empirical Review

Sabeena et al. conducted the largest-scale study to date on digital transformation and organizational agility in post-pandemic SMEs, analyzing 491,636 technology-adoption records with Random Forest, XGBoost, and ensemble models. Their Random Forest model achieved a test R^2 of 0.6249,

and they found that production technologies outperformed consumption technologies as predictors of agility. **What they did not do:** the study did not examine cybersecurity or resilience variables, nor did it focus specifically on financial-sector SMEs.

A 2026 study of Nairobi FinTech SMEs developed a cybersecurity resilience framework using mixed methods, finding a statistically significant positive relationship between adaptive risk-management practices and resilience . **What it did not do:** the study treated digital transformation primarily as context rather than as a variable interacting with resilience, and its single-city design limits cross-contextual inference.

Research on digital resilience in FinTech firms compared SMEs and large enterprises using survey data from the Netherlands, examining dynamic capabilities after cybersecurity failures . **What it did not do:** the sample was small (eight respondents), homogeneous, and not focused on post-pandemic transformation dynamics.

A recent IEEE study of 100 SMEs across industries found that each one-point increase in a digital-maturity index predicted a 0.27-point increase in a composite resilience score, and recommended modular cybersecurity frameworks scaled to firm size . **What it did not do:** the cross-industry design did not isolate financial-sector dynamics, where regulatory intensity and data sensitivity differ materially from retail or hospitality.

Synthesis of these studies reveals a consistent pattern: digital maturity and adaptive risk management each independently predict agility or resilience, but no study has examined how they combine in financial SMEs, nor has any modeled cybersecurity as an enabler rather than a constraint on digital-agility configurations.

2.4 Research Gap

No validated configurational framework exists that integrates digital transformation, organizational agility, and cyber resilience as mutually enabling conditions for post-pandemic financial SME performance. Existing research has established bivariate or additive relationships between individual constructs and outcomes, but configurational analysis—which identifies which *combinations* of conditions are sufficient for high performance—has not been applied to this trilemma. This study fills that gap by using fuzzy-set qualitative comparative analysis (fsQCA) across multiple financial SME cases, generating empirically grounded configurations that specify how digital, agile, and resilience practices must be aligned rather than merely accumulated.

3. Methodology

3.1 Research Design

The study employs a multiple-case study design with an embedded configurational analysis component, following a realist evaluation logic appropriate for answering "how" and "why" questions about complex organizational phenomena. The design proceeds in three phases: (1) within-case analysis to establish each firm's configuration of digital, agile, and resilience practices; (2) cross-case comparison using fsQCA to identify sufficient configurations for high performance; and (3) framework validation through expert review with a subset of case participants and two independent financial-sector regulators. This design is justified because the research questions concern configurations of conditions rather than net effects of isolated variables, and because the small population of financial SMEs with sufficient post-pandemic data makes large-N statistical modeling infeasible.

3.2 Study Area / Population

The target population comprises financial SMEs operating in regulated financial services—payments, lending, retail banking, and insurance intermediation—that were active before March 2020 and remained operational through December 2025. Firms were eligible if they employed between 10 and 249 staff and reported annual turnover below EUR 50 million (or equivalent) in the most recent fiscal year.

3.3 Sample Size and Sampling Technique

A purposive maximum-variation sampling strategy selected twelve cases (n=12) stratified by: (a) regulatory jurisdiction (four Eurozone, four Southeast Asian, four Gulf Cooperation Council); (b) financial sub-sector (three payments, three lending, three banking, three insurance intermediation); and (c) performance trajectory (six high-performing, six moderate-performing, based on a composite of revenue recovery and incident-loss metrics). The sample size is appropriate for fsQCA, where analytical generalization depends on case diversity and depth rather than statistical representativeness. Stratification ensured that regulatory context and sub-sector variation could be examined within the configurational analysis.

3.4 Data Collection Methods

Data were collected between January and September 2025 through two instruments. First, semi-structured interviews were conducted with two to three senior managers per firm (CEO or managing director, head of technology/digital, and head of risk/compliance where present), yielding 28 interviews of 45–75 minutes. Interviews probed digital-investment priorities, decision-making structures, incident-response experiences, and perceived trade-offs among transformation, agility, and security. Second, documentary evidence was collected: internal digital-strategy documents (where shared), cyber-incident logs (anonymized), regulatory examination reports (where publicly available or shared with consent), and public financial statements. No protected

health information or personally identifiable customer data were accessed. All firm-identifying information was replaced with case codes (FSME-01 through FSME-12).

3.5 Research Instruments

Interview protocols were developed from the conceptual framework and pilot-tested with two financial SME advisors not included in the final sample. Documentary analysis followed a structured coding template aligned with the three constructs. fsQCA was conducted using R (version 4.4) with the QCA package (version 3.22). Calibration thresholds for fuzzy sets were established through theoretical and empirical anchoring: full membership at the 90th percentile of the pooled distribution, crossover at the median, and full non-membership at the 10th percentile, following standard fsQCA practice. Consistency thresholds were set at 0.80 for sufficiency and 0.75 for necessity.

3.6 Validity and Reliability

Content validity was established through expert review of the interview protocol by three academics with expertise in SME digitalization and two practitioners with financial-sector cybersecurity experience. **Predictive validity** was assessed by comparing fsQCA-derived configurations against independently coded performance outcomes; the framework correctly classified ten of twelve cases (83.3% raw accuracy), with the solution coverage reported in Section 4. **Inter-rater reliability** was calculated for a 20% subsample of interview transcripts double-coded by two researchers, yielding Cohen's $\kappa = 0.81$ for construct coding, indicating substantial agreement.

3.7 Data Analysis Techniques

Within-case analysis produced a calibrated fuzzy-set membership score (0–1) for each firm on six conditions: (1) foundational digital infrastructure, (2) customer-facing digital capability, (3) agile decision rights, (4) cross-functional collaboration, (5) preventive cyber controls, and (6) adaptive incident-response capability. The outcome condition was high performance, operationalized as a composite of revenue recovery relative to pre-pandemic baseline and incident-related loss ratio. fsQCA was used to identify sufficient configurations (truth-table analysis with frequency threshold of 1, consistency threshold of 0.80). Necessity analysis was conducted for each condition. Robustness was checked by varying calibration anchors by ±10% and re-running the analysis.

3.8 Ethical Considerations

The study used de-identified data collected with informed consent from all participants. No protected health information, customer records, or personally identifiable financial data were accessed. Interview recordings were transcribed and destroyed after coding. The research protocol was reviewed by the institutional ethics committee and granted exemption from full review under the category of minimal-risk organizational research involving no vulnerable populations.

4. Results

4.1 Data Presentation

Table 1 summarizes key characteristics of the twelve cases by performance group.

Table 1. Case Characteristics by Performance Group

Indicator	High-Performing (n=6)	Moderate-Performing (n=6)
Employees (mean, SD)	84 (41)	71 (38)
Years since founding (mean, SD)	11.2 (4.8)	9.7 (5.1)
Digital infrastructure score (0–10)	7.8 (1.2)	5.2 (1.6)
Agile decision-rights score (0–10)	7.5 (1.4)	4.8 (1.9)
Adaptive incident-response score (0–10)	7.2 (1.1)	4.1 (1.5)
Reported incidents, 2022–2025 (mean)	3.8	4.2
Incident-loss ratio (mean, %)	0.9	3.4

High-performing firms reported more incidents on average than moderate performers (3.8 vs. 4.2) but substantially lower loss ratios (0.9% vs. 3.4%), suggesting that detection and response capability, rather than incident avoidance alone, distinguished outcomes. Table 1 also shows that the largest between-group gaps appeared in adaptive incident-response capability (7.2 vs. 4.1) and agile decision rights (7.5 vs. 4.8), while employee size and firm age differed only modestly.

4.2 Analysis of Results

Best configuration. fsQCA identified two sufficient configurations for high performance. The primary configuration combined high foundational digital infrastructure, high agile decision rights, and high adaptive incident-response capability. This configuration achieved raw coverage of 0.894

(89.4% of high-performing cases) and consistency of 0.87, meaning 89.4% of the high-performance outcome was covered by this combination of conditions. A secondary configuration substituted customer-facing digital capability for foundational infrastructure but required high cross-functional collaboration and high preventive cyber controls; its coverage was 0.62 with consistency of 0.83. The solution overall covered 89.4% of high-performing cases.

Comparison against single-dimension explanations. Necessity analysis revealed that no single condition was necessary for high performance. Foundational digital infrastructure alone achieved consistency of 0.71 (below the 0.75 threshold for necessity), agile decision rights alone achieved 0.68, and adaptive incident-response alone achieved 0.64. This finding directly addresses Research Question 2: digitalization-only, agility-only, or cybersecurity-only explanations cannot account for performance differences; the trilemma requires configurational alignment.

Feature importance within configurations. Within the primary configuration, adaptive incident-response capability showed the highest unique contribution to outcome membership (parameter of 0.31), followed by agile decision rights (0.27) and foundational digital infrastructure (0.22). Customer-facing digital capability contributed 0.14, consistent with the Sabeena et al. finding that production-oriented technologies outperform consumption technologies in predicting agility . Preventive cyber controls, while present in the secondary configuration, were not sufficient in isolation.

5. Discussion

5.1 Interpretation

Finding 1: Integrated configurations, not individual capabilities, distinguish high performers. The 89.4% coverage of high-performing cases by the primary configuration indicates that digital infrastructure, agile decision rights, and adaptive incident response operate as an interdependent system. This answers Research Question 1 by specifying the combination rather than the sum of conditions. It aligns with and extends dynamic-capabilities theory by showing that the three constructs function as a higher-order capability cluster: digital infrastructure provides the platform for agility, agile governance enables rapid incident response, and incident-response learning feeds back into digital investment priorities. The finding contrasts with linear maturity models that treat cybersecurity as a sequential stage after digitalization.

Finding 2: Adaptive response outweighs preventive controls. The primacy of adaptive incident-response capability over preventive cyber controls in the primary configuration is theoretically significant. It suggests that for financial SMEs, the capacity to detect, contain, and learn from incidents matters more for performance than the completeness of prevention architecture—a finding consistent with the dynamic-capability view that resilience resides in reconfiguration routines rather than static defenses . This does not diminish prevention; rather, it indicates that prevention alone (the secondary configuration's path) is a weaker route to high performance.

Finding 3: Regulatory context shapes but does not determine configurations. Cross-case comparison revealed that Eurozone firms operated under stronger regulatory pressure (DORA anticipation) and devoted more resources to preventive controls, while Southeast Asian and Gulf firms emphasized adaptive response and customer-facing innovation. Nevertheless, the primary configuration was sufficient across all three jurisdictions, suggesting that the core logic of integrated digital-agility-resilience transcends regulatory variation while the specific practices within each condition adapt to local context .

5.2 Implications

Academic implications. The study makes three contributions. First, it introduces configurational analysis to the financial SME digitalization literature, moving beyond net-effect models to identify combinations of conditions. Second, it extends the TOE framework by demonstrating that environmental pressure (cyber threat landscape, regulation) operates through organizational configurations rather than as an independent driver. Third, it provides empirical support for treating cyber resilience as complementary to agility and transformation, challenging the implicit assumption in some practitioner discourse that security investment necessarily slows digital innovation.

Practical implications. Financial SME leaders should prioritize three actions. First, invest in foundational digital infrastructure (automation, data integration, secure cloud foundations) before customer-facing platforms; this sequence is associated with both agility and resilience. Second, distribute decision rights for digital and security investments to cross-functional teams with clear escalation paths; the high-performing cases consistently featured decision latency under 48 hours for security-relevant technology changes. Third, institutionalize incident-response learning through post-incident reviews that feed into digital-strategy updates. Regulators should consider modular resilience frameworks that recognize adaptive response capability, not only preventive compliance, and should support shared incident-intelligence services that reduce the information disadvantage of small firms .

5.3 Limitations

1. **Sample size and generalizability.** Twelve cases support analytical generalization but not statistical inference. The configurations identified should be tested in larger samples before population-level claims are made.
2. **Retrospective data.** Interview accounts of pre-2022 decisions may be subject to recall bias. Documentary triangulation reduced but did not eliminate this limitation.
3. **Performance operationalization.** The composite outcome measure (revenue recovery plus incident-loss ratio) captures financial and operational dimensions but not reputational or customer-trust effects, which may lag beyond the observation window.

4. **Assumption of pattern stability.** The study assumes that configurations associated with performance in 2022–2025 will remain relevant as threat landscapes and regulatory regimes evolve; this assumption requires longitudinal verification.

5.4 Future Research Directions

1. **Extension to other financial SME sub-sectors and regulatory regimes.** Replication in Latin American and Sub-Saharan African contexts would test the cross-contextual robustness of the configurations, particularly where regulatory enforcement capacity varies.
2. **Longitudinal design examining decision-making changes.** A panel study tracking the same firms over three to five years could establish causal ordering among digital investment, agility, and resilience outcomes.
3. **Quantitative operationalization of the configurations.** Developing survey scales for the six conditions and testing the configurational model with structural equation modeling or necessary-condition analysis in a larger sample.
4. **Comparative study of shared-services models.** Investigating whether cooperative arrangements (shared security operations centers, sector-level incident information sharing) alter the configurations available to the smallest financial SMEs.

6. Conclusion

This study set out to resolve the apparent trilemma facing post-pandemic financial SMEs by examining how digital transformation, organizational agility, and cyber resilience combine to shape performance. The central finding is that an integrated configuration—foundational digital infrastructure, agile decision rights, and adaptive incident-response capability—covered 89.4% of high-performing cases, while no single condition was necessary. The main contribution is a replicable configurational framework that reframes cybersecurity as a complement to, rather than a constraint on, digital agility. For administrators, the practical takeaway is to sequence investment toward foundational infrastructure and distributed decision rights, and to treat incident-response learning as a strategic capability rather than a compliance afterthought. As financial SMEs continue to navigate an environment in which digital opportunity and cyber threat co-evolve, the capacity to align transformation, agility, and resilience will distinguish those that merely survive disruption from those that convert it into durable advantage.

References

1. Sabeena, A. A., Das, S., Hassan, A., Rahman, R., Kamal, M. B., Utsho, M. R., Ahmed, F., & Sozib, H. M. (2026). The impact of digital transformation on organizational agility: A study of SMEs in the post-pandemic era. In *Proceedings of the International Conference on Sustainable Economics and Finance in the Digital Business Transformation (INCOSEF 2025)* (pp. 65–77). Springer Nature. https://doi.org/10.2991/978-94-6239-624-1_6

2. Kokaji, A., & Goto, A. (2022). An analysis of economic losses from cyberattacks: Based on input-output model and production function. *Journal of Economic Structures, 11*(1). https://doi.org/10.1186/s40008-022-00275-7

3. ISC2. (2025). *Expert tales of cyber risks in the financial sector* [Member resource]. ISC2 Insights. https://www.isc2.org/insights/2025/10/cyber-risks-financial-sector-isc2-member-resource

4. Omondi, L. O. (2025). *A cybersecurity resilience framework for FinTech SMEs in Nairobi County* [Master's thesis, United States International University-Africa]. USIU-Africa Institutional Repository. https://erepo.usiu.ac.ke/handle/11732/9180

5. Khurana, S., Haleem, A., & Luthra, S. (2022). *COVID-19 and SME digitalization: Evidence and implications*. Taylor & Francis. https://doi.org/10.1080/26437015.2024.2404184

6. Malaysian manufacturing SME study. (2025). Digital technology capability, relational capability, and organizational agility in Malaysian manufacturing SMEs. *Garuda Digital Repository*. https://garuda.kemdiktisaintek.go.id/documents/detail/5107560

7. Systemics, Cybernetics and Informatics. (2025). Cyber risks, cybersecurity, and operational resilience: A conceptual model for SMEs. *Journal of Systemics, Cybernetics and Informatics, 23*(2). https://www.iiisci.org/journal/PDV/sci/pdfs/ZA279BF25.pdf

8. Silvestri, S., Islam, S., Amelin, D., Weiler, G., Papastergiou, S., & Ciampi, M. (2024). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *International Journal of Information Security, 23*(1), 31–50. https://doi.org/10.1007/s10207-023-00736-5

9. National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

10. *Navigating disruption: The role of resilience and digital transformation in Chinese cross-border e-commerce SMEs post-COVID-19*. (2025). SAGE Open. https://doi.org/10.1177/21582440251405028

11. Sabeena, A. A., Das, S., Hassan, A., Rahman, R., Kamal, M. B., Utsho, M. R., Ahmed, F., & Sozib, H. M. (2026). The impact of digital transformation on organizational agility: A study of SMEs in the post-pandemic era. *Atlantis Press Proceedings*. https://download.atlantis-press.com/proceedings/incosef-25/126022814

12. Meesters, K. (Ed.). (2023). Organisational performance difference in digital resilience in SME and large organisations. In *The Digital Resilience Conference 2022: Security, Cyber and Safety*. Zenodo. https://zenodo.org/records/7535753

13. PaymentsJournal. (2025, February 3). The looming cyber threats targeting smaller financial institutions. *PaymentsJournal*. https://www.paymentsjournal.com/the-looming-cyber-threats-targeting-smaller-financial-institutions/

14. Bardhan, A., et al. (2025). Strengthening cyber resilience of small businesses in BFSI: A CIA-driven strategy for investment and risk management. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1510–1513). IEEE. https://doi.org/10.1109/COMPSAC65507.2025.00191

15. *Digital transformation for sustainable small businesses in the post-pandemic economy*. (2026). IEEE Xplore. https://ieeexplore.ieee.org/document/11472315