American Impact Review

Theoretical Article

Digital Resilience in Small and Medium Enterprises: Aligning IT Infrastructure, Cybersecurity, and Operational Performance

Maksim Tumakov[1*], Renata Blazhko[2], Timur Vasilev[3], and Aleksei Panov[4]

[1] *DefenScope;* [2] *Moscow Institute of Physics and Technology (MIPT);* [3] *Paybis;* [4] *MSD.*

[*] Corresponding author

OPEN ACCESS

Citation:
Maksim Tumakov et al. (2026). Digital Resilience in Small and Medium Enterprises: Aligning IT Infrastructure, Cybersecurity, and Operational Performance. *Am. Impact Rev.*
10.66308/air.e2026046

Received: May 12, 2026
Accepted: May 24, 2026
Published: May 25, 2026

DOI:
10.66308/air.e2026046

ISSN: 3071-124X

Abstract

Small and medium enterprises increasingly depend on digital technologies for coordination, customer interaction, data access, and operational continuity. However, technology adoption alone does not guarantee resilience or improved performance. Many SMEs remain exposed to cyber incidents, fragmented IT systems, weak security routines, and limited recovery capacity. This conceptual paper develops a model for future empirical testing by explaining how IT infrastructure capability and cybersecurity capability can improve operational performance when they are embedded in daily operational routines. Operational embedding refers to the integration of technology and security practices into critical workflows, recovery priorities, and continuity responsibilities. Drawing on recent literature published between 2021 and 2026 and selected foundational theory, the study argues that digital resilience should be understood as an organizational capability that enables SMEs to anticipate disruptions, absorb shocks, adapt processes, and recover operations. The proposed model positions IT infrastructure as the technical foundation, cybersecurity as the protection and recovery layer, operational embedding as the condition that strengthens their effect, and digital resilience as a partial mediator between capabilities and operational performance. Operational performance is captured through downtime reduction, continuity, response speed, productivity, and service quality.

Keywords: Digital resilience, Small and medium enterprises, IT infrastructure, Cybersecurity, Operational performance

1. Introduction

Small and medium enterprises have become increasingly dependent on digital systems for everyday operations. Cloud platforms, online communication tools, customer databases, digital payment systems, remote work tools, and social media channels now shape how many SMEs produce, sell, coordinate, and respond to market changes. This dependence creates opportunities for efficiency and flexibility, but it also increases exposure to digital disruption.

The central problem is that SMEs often digitalize without building the organizational capacity needed to remain stable under stress. A firm may adopt cloud tools, e-commerce platforms, or digital communication channels, but still lack reliable backup routines, cybersecurity awareness, incident response processes, or clear responsibility for digital continuity. In this situation, digitalization can increase both capability and vulnerability.

Recent studies show that digital technologies can support SME resilience, but their effects are not automatic. Digital transformation strengthens resilience when it is connected with learning, innovation, leadership, agility,

and dynamic capabilities. Cybersecurity studies add another important point: SMEs need not only prevention, but also detection, response, recovery, and continuity planning. This means that digital resilience is not only a technology issue. It is an operational embedding issue.

This article is built on a simple argument: digital resilience in SMEs emerges when IT infrastructure, cybersecurity practices, and operational routines work together as one system. IT infrastructure provides the technical base, cybersecurity protects and restores that base, and operational embedding ensures that digital resources support the actual processes through which the firm creates value.

The purpose of this article is to develop a conceptual model explaining how operational embedding among IT infrastructure, cybersecurity, and daily routines can strengthen digital resilience and improve operational performance in SMEs.

1.1. Theoretical Background

The theoretical foundation of the article combines dynamic capabilities, strategic alignment, and organizational resilience. Dynamic capabilities theory explains how firms integrate, build, and reconfigure resources when environments change. This is relevant because digital resilience requires SMEs to use IT and cybersecurity resources not only for routine efficiency, but also for adaptation and recovery. Teece, Pisano, and Shuen (1997) introduced dynamic capabilities as a way to explain how firms renew their resource base, while Teece (2007) later clarified the microfoundations of sensing, seizing, and transforming. These ideas support the view that digital resilience is a capability rather than a technology possession.

The article also draws from strategic alignment literature, especially the idea that information technology creates value when it is connected with business strategy, organizational infrastructure, and processes. Venkatraman, Henderson, and Oldach (1993) describe continuous strategic alignment as a way to exploit IT capabilities for competitive success. However, this article does not use the broad term business-IT alignment as its main construct. Instead, it uses the narrower term **operational embedding**. Operational embedding refers to the degree to which IT infrastructure and cybersecurity practices are built into the everyday routines, recovery priorities, and continuity needs of SMEs.

Finally, organizational resilience literature provides the capability-based logic for anticipation, coping, adaptation, and recovery. Duchek (2020) conceptualizes organizational resilience as a capability that develops through phases before, during, and after adversity. This temporal view is important for the present article because digital resilience also unfolds over time: SMEs prepare before disruption, absorb and respond during disruption, and learn after disruption. The model therefore treats digital resilience as a formative process rather than as a single reflective attitude or perception.

1.2. Literature Review

The literature on SME digital resilience has developed across several related but still partly separated research streams. One stream examines how digital transformation helps small firms survive disruption. Another focuses on IT and digital capabilities as resources that support performance. A third stream studies cybersecurity and cyber resilience in SMEs. A fourth stream connects business continuity, operational resilience, and performance. This article brings these streams together and argues that their common mechanism is operational embedding: digital resources improve performance when they are integrated with cybersecurity routines and operational priorities.

1.2.1. Digital Transformation and SME Resilience

Recent research increasingly treats digital transformation as a source of resilience for SMEs. During crises, digital technologies can help small firms maintain communication with customers, reorganize delivery channels, coordinate employees, access data remotely, and adapt business models. Khurana, Dutta, and Singh Ghura (2022) show that resilience can emerge as a second-order dynamic capability when SMEs use digital transformation to sense changes, seize opportunities, and transform business activities within an entrepreneurial ecosystem. Ashiru, Nakpodia, and You (2022) similarly show that emerging digital communication technologies can support SME resilience by helping firms respond to disruption and maintain relationships with stakeholders. This view is important because it moves the discussion beyond technology adoption and toward the organizational capacity to reconfigure resources under uncertainty.

Empirical studies also show that the value of digitalization depends on how deeply and broadly it is embedded in the firm. Sinha, Raby, and Salari (2025) examine digitalization scope and depth in SMEs during crisis conditions and suggest that digitalization has nuanced effects on resilience rather than a simple linear effect. This supports the idea that more digitalization is not always better by itself. What matters is whether digital tools are used in ways that fit the firm's context, capabilities, and operational needs.

Other studies connect digital transformation with learning and innovation. Awad and Martín-Rojas (2024) argue that digital transformation strengthens organizational resilience through organizational learning and innovation. Similarly, Martín-Rojas, Garrido-Moreno, and García-Morales (2026) identify digital technologies, transformational leadership, and innovation as important drivers of organizational resilience in SMEs. These studies suggest that resilience is not produced by digital tools alone. Digital tools become valuable when they trigger learning, support innovation, and help the organization adapt its routines.

This literature provides the first foundation for the present article: digital transformation can strengthen SME resilience, but only when digital resources are translated into organizational capabilities. Therefore, the article treats digital resilience as a capability built through use, operational embedding, and adaptation rather than as a direct consequence of technology ownership.

1.2.2. IT Infrastructure and Digital Capabilities

A second stream of literature focuses on IT capabilities and digital capabilities. These studies are useful because they explain why technology investments do not automatically produce performance improvements. Trieu et al. (2023) show that IT capabilities can support organizational ambidexterity and resilience, which then contribute to SME performance. This finding is central for the present article because it positions IT as an enabling capability rather than as a direct performance variable.

Li, Tong, Wei, and Yang (2022) provide a similar argument in the context of digital technology-enabled dynamic capabilities. Their study shows that digitalization capabilities influence firm performance through agility-related mechanisms. This implies that the value of digital resources is mediated by the firm's ability to adjust operations and respond to market changes. For SMEs, this is especially relevant because limited resources make it difficult to gain value from technology unless it directly supports operational adaptation.

Yu, Wang, and Moon (2022) connect digital transformation capability with operational performance and conceptualize digital transformation capability through sensing, organizing, and restructuring. This is useful for the present model because these three dimensions correspond closely to the logic of digital resilience: firms must sense disruptions, organize resources, and restructure processes. IT infrastructure therefore matters not only as hardware, software, or connectivity, but as the technical base that enables data access, coordination, process visibility, and recovery.

From this stream, the article derives the second foundation: IT infrastructure capability is necessary but

insufficient. It becomes strategically meaningful when it supports operational continuity, flexibility, and recovery. This is why the central model does not place IT infrastructure as a direct route to performance. Instead, it positions IT infrastructure as one part of a broader digital resilience system.

1.2.3. Cybersecurity Capability and Cyber Resilience in SMEs

A third stream of literature highlights cybersecurity as a resilience issue. SMEs are often more vulnerable to cyber risks because they have limited budgets, informal security procedures, low cybersecurity awareness, and weaker access to specialized expertise. Hoppe, Gatzert, and Gruner (2021) show that cyber risk management in SMEs requires attention not only to technical controls but also to risk culture, awareness, and managerial practices. This supports the view that cybersecurity should be integrated into general management rather than treated as an isolated IT function.

Cybersecurity resilience research makes this argument even stronger. Fernandez de Arroyabe et al. (2023) examine cybersecurity resilience in SMEs and focus on the ability to handle, recover from, and adapt to cyber incidents. Their approach is directly relevant to the present article because it defines cybersecurity in resilience terms: the question is not only whether the firm can prevent attacks, but whether it can continue and recover when disruption occurs.

Armenia et al. (2021) study cyber risk evaluation and cybersecurity investment in SMEs through dynamic simulation. Their work shows that security investment decisions involve trade-offs and that SMEs need decision support to understand risk, cost, and resilience outcomes. Song and Park (2024) extend this discussion by examining policy scenarios for strengthening SME cybersecurity resilience, emphasizing the role of support mechanisms, incentives, and recovery after incidents. Neri and Niccolini (2025) add a qualitative perspective by showing that cyber-organizational resilience in SMEs depends on remediation capacity, adaptive capacity, awareness, resources, and business continuity practices.

This stream provides the third foundation for the model: cybersecurity capability is not only a protective layer, but also a recovery and adaptation capability. In the context of SMEs, cybersecurity contributes to digital resilience when it is connected with backups, access control, monitoring, incident response, employee behavior, and recovery priorities.

1.2.4. Business Continuity, Operational Resilience, and Performance

The fourth stream connects resilience with operational continuity and performance. Business continuity management research is useful because it translates resilience into practical organizational routines. De Matteis, Elia, and Del Vecchio (2023) discuss business continuity management and organizational resilience from an SME perspective, showing that SMEs need continuity practices that match their resource constraints and operational realities. Awang Ali, Hanafiah, and Mogindol (2023) integrate business continuity management practices, organizational resilience, and performance in an SME framework. Their review suggests that preparedness, management support, external requirements, and embedded continuity practices are important for SME resilience.

Galaitsi et al. (2023) clarify the distinction between business continuity management, operational resilience, and organizational resilience. This distinction helps position the present article. Business continuity management focuses on maintaining critical activities during disruption. Operational resilience focuses on the capacity to continue delivering important services or outputs under stress. Organizational resilience is broader and includes adaptation, learning, and transformation. Digital resilience in SMEs can therefore be understood as the digital layer connecting these three ideas.

The performance dimension is also important. He et al. (2022) show that digital transformation can contribute

to organizational resilience and performance, while Li et al. (2022) show that digital capabilities affect performance through agility. These findings support the idea that operational performance should not be treated only as financial output. In the SME context, operational performance includes process continuity, lower downtime, delivery reliability, productivity, service quality, response speed, and flexibility.

This stream provides the fourth foundation: digital resilience matters because it translates digital and cybersecurity capabilities into operational outcomes. The article therefore defines operational performance as the firm's ability to maintain stable and effective operations under both normal and disruptive conditions.

1.2.5. Synthesis: Operational Embedding as the Missing Mechanism

Taken together, these streams suggest that digital resilience in SMEs cannot be explained by one factor alone. Digital transformation research shows the importance of digital tools, learning, innovation, and adaptation. IT capability research shows that technological resources need organizational mechanisms to influence performance. Cybersecurity research shows that digital risk management must include prevention, response, and recovery. Business continuity research shows that resilience must be embedded in operational routines.

The missing mechanism connecting these streams is operational embedding. Operational embedding means that IT infrastructure, cybersecurity practices, and operational routines are designed and managed in relation to one another. For example, a backup system contributes to resilience only if it protects the data required by critical processes and if employees know how recovery should occur. Access control contributes to resilience only if it protects operational systems without blocking necessary work. Cloud tools contribute to resilience only if they improve continuity, coordination, and recovery rather than creating new unmanaged dependencies.

The gap is that prior studies usually capture only part of this configuration. Khurana et al. (2022) and Awad and Martín-Rojas (2024) emphasize digital transformation and resilience, but cybersecurity is not their central mechanism. Fernandez de Arroyabe et al. (2023) and Armenia et al. (2021) focus on cybersecurity resilience and investment, but operational performance is less developed. Awang Ali et al. (2023) and De Matteis et al. (2023) connect continuity and resilience, but do not fully integrate IT infrastructure and cybersecurity capability. This article therefore does not claim that previous literature already proves the full integrated hypothesis. It uses the gap between these streams to build a new conceptual model.

This synthesis leads to the core position of the article: SMEs improve operational performance through digital resilience when IT infrastructure capability and cybersecurity capability are embedded in daily operational routines. The article therefore defends an operational-embedding view of digital resilience rather than a technology-adoption view.

Central Hypothesis to Be Discussed and Defended

Central hypothesis: In digitally dependent SMEs, IT infrastructure capability and cybersecurity capability improve operational performance primarily when they are embedded in daily operational routines; this relationship is partially mediated by digital resilience and conditioned by firm size, digital maturity, industry risk, and resource availability.

This hypothesis is deliberately written as one integrated claim rather than as a list of separate H1/H2 statements. It allows the article to defend one original idea: SMEs do not become resilient simply because they adopt digital tools or cybersecurity controls. They become resilient when digital infrastructure, security practices, and operational routines reinforce each other.

The hypothesis is also falsifiable. It would be weakened if IT infrastructure and cybersecurity capability improved operational performance regardless of operational embedding, if digital resilience did not explain any part of the relationship, or if boundary conditions such as firm size, digital maturity, industry exposure,

and resource constraints did not change the strength of the proposed effects.

The hypothesis draws on several streams of recent research. Studies on digital transformation and SME resilience show that digital technologies can support adaptation and continuity, especially when they are embedded in learning and innovation processes. Studies on IT capabilities show that technological resources affect performance through organizational capabilities rather than through direct technological possession. Cybersecurity research shows that SMEs require prevention, response, and recovery capacity. Business continuity and operational resilience research then connects these capabilities with continuity, flexibility, and performance.

2. Method

This article uses a conceptual research design supported by a structured literature selection procedure. The aim is to build a defensible conceptual model from DOI-verified studies and foundational theory, not to claim exhaustive systematic review coverage. This design is suitable for the present study because the research problem is integrative: digital transformation, IT infrastructure capability, cybersecurity capability, business continuity, and operational performance are usually examined in separate streams.

The recent literature review focuses on peer-reviewed studies published from 2021 to 2026 that examine at least one of the following areas: digital resilience in SMEs, digital transformation and organizational resilience, IT or digital capabilities and performance, cybersecurity resilience in SMEs, cyber risk management, business continuity management, and operational resilience. Theoretical foundations published before 2021 were included only when they were necessary for defining core concepts, such as dynamic capabilities, strategic alignment, and organizational resilience.

The search was conducted through Crossref, Google Scholar, ScienceDirect, SpringerLink, Emerald, Taylor & Francis, SAGE Journals, Wiley Online Library, and MDPI. The main search strings were: ”SME digital resilience”, ”digital transformation SME resilience”, ”IT capabilities organizational resilience SMEs”, ”cybersecurity resilience SMEs”, ”cyber risk management SMEs”, ”business continuity management SMEs resilience performance”, and ”digital transformation capability operational performance”.

Table 1. Structured Literature Selection Log

Selection step	Working count	Procedure	Working output
Search pool	62 candidate records	Keyword searches and backward/forward checking across publisher pages and Crossref metadata.	Initial candidate pool from recent SME, IT capability, cybersecurity, resilience, and performance literature.
Relevance filter	39 records retained	Removal of non-peer-reviewed items, weakly related items, reports without article status, and records without verifiable DOI.	Peer-reviewed DOI-bearing studies retained for full metadata checking.
Conceptual fit	27 records assessed	Assessment of fit with the article’s constructs: IT infrastructure capability, cybersecurity capability, operational embedding, digital resilience, and operational performance.	Studies grouped into thematic streams rather than summarized individually.
Final synthesis set	22 sources included	Final inclusion required direct conceptual relevance and DOI verification through doi.org, publisher pages, or Crossref.	18 recent DOI-verified studies plus 4 DOI-verified foundational theory sources.

The five records excluded at the conceptual fit step were removed because they were redundant with included studies, lacked SME-specific scope, or addressed resilience without a clear connection to IT infrastructure, cybersecurity, or operational performance. The counts in Table 1 document the working selection log for this draft. They should be updated if the database search is rerun before submission.

The analysis followed a thematic synthesis approach. The selected studies were grouped into five themes:

digital transformation and SME resilience; IT and digital capabilities; cybersecurity and cyber resilience; business continuity, operational resilience, and performance; and operational embedding as a synthesis mechanism. The aim was not to summarize every article separately, but to identify the mechanism that connects the themes into one coherent model.

Conceptual Variables and Measurement Logic

$$\text{ITC}_i = \phi_1\text{Reliability}_i + \phi_2\text{Integration}_i + \phi_3\text{DataAccess}_i + \phi_4\text{CloudUse}_i + \phi_5\text{Connectivity}_i + \phi_6\text{Scalability}_i$$

$$\text{CSC}_i = \gamma_1\text{Backups}_i + \gamma_2\text{AccessControl}_i + \gamma_3\text{Monitoring}_i + \gamma_4\text{IncidentResponse}_i + \gamma_5\text{Awareness}_i + \gamma_6\text{RecoveryPlanning}_i$$

$$\text{OE}_i = \delta_1\text{ProcessLink}_i + \delta_2\text{ContinuityPlanning}_i + \delta_3\text{RecoveryPriority}_i + \delta_4\text{RoleClarity}_i$$

If this article is later converted into an empirical study, the central hypothesis can be tested through survey indicators. The constructs are defined as composites because the article is interested in capability configurations rather than isolated single-item perceptions.

Here, **ITC** captures the technical base of digital operations, **CSC** captures prevention-response-recovery capability, and **OE** captures whether technology and security routines are embedded in daily operational work.

Formula-Based Model

$$\text{DR} = f(\text{ITC}, \text{CSC}, \text{OE}, \text{ITC} \times \text{OE}, \text{CSC} \times \text{OE})$$
$$\text{OP} = f(\text{DR}, \text{ITC}, \text{CSC}, \text{OE}, \text{Controls})$$

$$\text{DR}_i = \alpha_0 + \alpha_1\text{ITC}_i + \alpha_2\text{CSC}_i + \alpha_3\text{OE}_i + \alpha_4(\text{ITC}_i \times \text{OE}_i) + \alpha_5(\text{CSC}_i \times \text{OE}_i) + \alpha_6\text{Controls}_i + \varepsilon_i$$
$$\text{OP}_i = \beta_0 + \beta_1\text{DR}_i + \beta_2\text{ITC}_i + \beta_3\text{CSC}_i + \beta_4\text{OE}_i + \beta_5\text{Controls}_i + \mu_i$$

$$\text{IE}_{\text{ITC}} = (\alpha_1 + \alpha_4\text{OE}_i) \times \beta_1$$
$$\text{IE}_{\text{CSC}} = (\alpha_2 + \alpha_5\text{OE}_i) \times \beta_1$$

$$\text{DRI}_i = w_1\text{Anticipation}_i + w_2\text{Absorption}_i + w_3\text{Adaptation}_i + w_4\text{Recovery}_i + w_5\text{Learning}_i$$

The conceptual relationship is treated as a moderated partial mediation model. Digital resilience is the main mechanism linking IT and cybersecurity capabilities to operational performance, but direct effects are retained because IT infrastructure and cybersecurity can also influence performance without passing fully through resilience.

Where **DR** means digital resilience, **ITC** means IT infrastructure capability, **CSC** means cybersecurity capability, **OE** means operational embedding, and **OP** means operational performance.

If survey data are collected, the model can be written more formally:

The model expects positive signs for $\alpha1$, $\alpha2$, $\alpha3$, $\alpha4$, $\alpha5$, and $\beta1$. The direct coefficients $\beta2$ and $\beta3$ are retained to test partial mediation rather than assuming that digital resilience fully explains operational performance.

The indirect effects can be discussed as conditional indirect effects:

Digital resilience should be treated as a formative composite rather than a reflective scale because anticipation, absorption, adaptation, recovery, and learning are process dimensions that jointly form resilience. They are not interchangeable reflections of a single attitude.

For future empirical work, this measurement logic favors PLS-SEM or composite-based modeling over a purely reflective CB-SEM specification.

Table 2. Thematic Synthesis of the Reviewed Literature

Literature stream	Representative sources	Main insight	Implication for the model
Digital transformation and SME resilience	Khurana et al. (2022); Awad and Martín-Rojas (2024); Sinha et al. (2025); Martín-Rojas et al. (2026)	Digital technologies can support SME resilience, but their effects depend on learning, innovation, digital depth, and contextual use.	Digital resilience should be treated as an organizational capability, not as simple technology adoption.
IT infrastructure and digital capabilities	Trieu et al. (2023); Li et al. (2022); Yu et al. (2022); He et al. (2022)	IT and digital capabilities improve performance through intermediate organizational mechanisms such as agility, ambidexterity, transformation capability, and resilience.	IT infrastructure capability is modeled as an antecedent of digital resilience and also retained as a possible direct contributor to operational performance.
Cybersecurity capability and cyber resilience	Hoppe et al. (2021); Armenia et al. (2021); Fernandez de Arroyabe et al. (2023); Neri and Niccolini (2025); Song and Park (2024)	Cybersecurity in SMEs is not only prevention; it includes risk awareness, investment decisions, response capacity, recovery, and adaptation after incidents.	Cybersecurity capability is modeled as a resilience-building capability rather than a purely technical control.
Business continuity, operational resilience, and performance	Awang Ali et al. (2023); De Matteis et al. (2023); Galaitsi et al. (2023)	Continuity practices, operational flexibility, preparedness, and recovery routines translate resilience into operational and managerial outcomes.	Operational performance is defined through continuity, recovery speed, service quality, flexibility, productivity, and cost avoidance.
Foundational management theory	Teece et al. (1997); Teece (2007); Venkatraman et al. (1993); Duchek (2020)	Dynamic capabilities, strategic alignment, and resilience theory explain why resources matter only when they are reconfigured and connected with organizational processes.	The model is framed as a management capability model rather than as a technical cybersecurity model.

The complete DOI-verified source details are reported in the reference list rather than in the body of the article, which keeps the main table focused on analytical synthesis.

3. Conceptual Development and Proposed Model

The reviewed literature suggests four analytical findings. First, digital technologies support resilience when they improve coordination, access to information, communication with customers, process flexibility, and the ability to reconfigure operations. However, digitalization alone is insufficient. Its value depends on how technologies are embedded in routines, learning, and decision-making.

Second, cybersecurity should be treated as a resilience capability rather than as a narrow technical control. For SMEs, cybersecurity includes risk awareness, access management, backups, monitoring, incident response, recovery capacity, and employee behavior. These practices reduce the probability of disruption and improve the firm's ability to continue operations after an incident.

Third, the link between digital resources and operational performance is partly indirect and partly direct. IT infrastructure and cybersecurity may improve performance directly by reducing downtime or improving

process reliability, but their stronger strategic contribution appears when they are embedded in operational routines and converted into digital resilience.

Fourth, digital resilience can be positioned as the central mechanism that converts technical and security resources into operational value. In this article, digital resilience means the SME's ability to anticipate digital disruptions, absorb shocks, adapt operational routines, recover critical processes, and learn from incidents. This mechanism is expected to be stronger in firms with higher digital maturity, adequate resources, and greater exposure to digital operational risks.

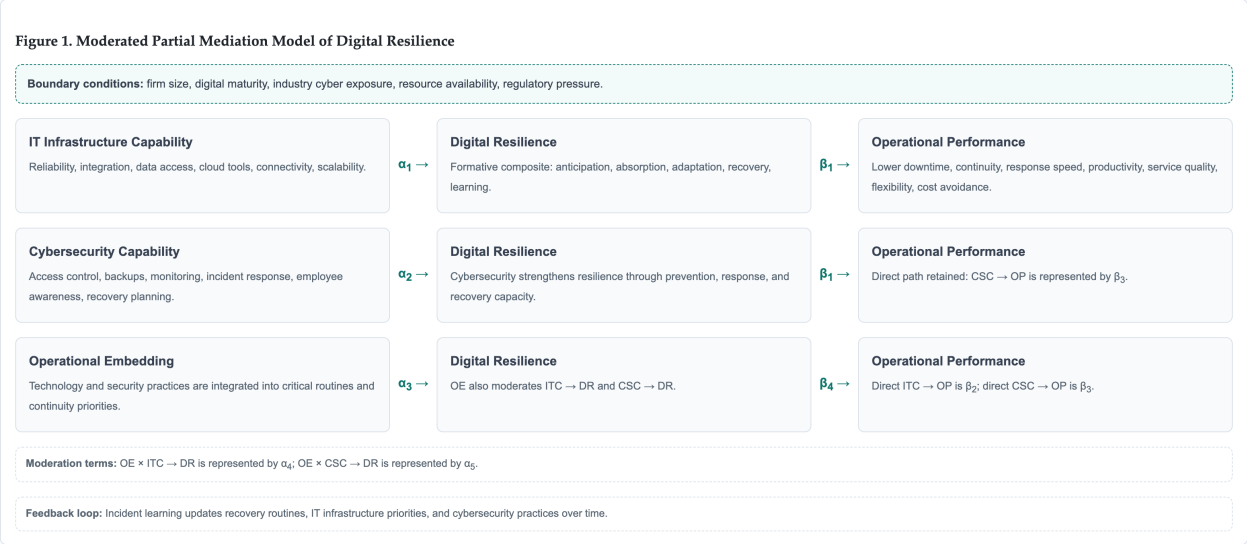

Figure 1. Moderated Partial Mediation Model of Digital Resilience

The diagram presents operational embedding as both a direct antecedent of digital resilience and a moderator of the ITC to DR and CSC to DR paths. The retained direct paths from ITC, CSC, and OE to OP reflect the partial mediation logic of the model.

Feedback loop: Incident learning updates recovery routines, IT infrastructure priorities, and cybersecurity practices over time.

Formal Interpretation of the Central Hypothesis

$$\begin{aligned}
\partial DR/\partial ITC &= \alpha_{1} + \alpha_{4}\mathrm{OE} > 0 \\
\partial DR/\partial CSC &= \alpha_{2} + \alpha_{5}\mathrm{OE} > 0
\end{aligned}$$

$$\begin{aligned}
\partial OP/\partial DR &= \beta_1 > 0 \\
\mathrm{TE}_{\mathrm{ITC}} &= \beta_2 + [(\alpha_1 + \alpha_4 \mathrm{OE}) \times \beta_1] \\
\mathrm{TE}_{\mathrm{CSC}} &= \beta_3 + [(\alpha_2 + \alpha_5 \mathrm{OE}) \times \beta_1]
\end{aligned}$$

$$\mathrm{BoundaryEffect} = h(\mathrm{FirmSize}, \mathrm{DigitalMaturity}, \mathrm{IndustryRisk}, \mathrm{ResourceAvailability}, \mathrm{RegulatoryPressure})$$

$$\text{ExpectedLoss}_i = P(\text{CyberIncident}_i) \times \text{OperationalLoss}_i$$
$$\text{NetResilienceValue}_i = \Delta ExpectedLoss_i + \Delta OperationalContinuity_i - \text{DigitalSecurityCost}_i$$

The central hypothesis can be expressed as a set of expected inequalities. These expressions make the argument testable without fragmenting the paper into a long list of conventional H1/H2 statements.

The first expression means that IT infrastructure capability should strengthen digital resilience, especially when operational embedding is high. The second expression means that cybersecurity capability should strengthen digital resilience, again more strongly when cybersecurity routines are embedded in operational work.

These expressions clarify that the model assumes partial mediation. IT infrastructure and cybersecurity capability may affect operational performance directly, but part of their total effect is expected to pass through digital resilience.

The boundary condition expression means that the strength of the model is not assumed to be universal. The expected effects should be weaker when SMEs have very low resources, low digital dependency, or formal security routines that are not connected with operations.

The final expression adds the business management logic of the article. Digital resilience has economic value when it reduces expected operational loss, improves continuity, and justifies the cost of IT and cybersecurity investments. In this expression, ΔExpectedLoss < 0 indicates loss reduction attributable to digital resilience.

4. Discussion

The finding that digitalization is insufficient by itself refines recent SME digital transformation literature. Khurana et al. (2022), Awad and Martín-Rojas (2024), and Martín-Rojas et al. (2026) show that digital technologies can strengthen resilience, but the present article clarifies the managerial condition under which this is most likely to occur: digital tools need to be embedded in operational routines. This shifts the discussion from adoption to use, from possession to capability, and from technology availability to continuity value.

The finding that cybersecurity should be treated as a resilience capability extends cyber risk management research in SMEs. Hoppe et al. (2021), Armenia et al. (2021), Fernandez de Arroyabe et al. (2023), and Neri and Niccolini (2025) show that cybersecurity is not limited to technical prevention. The present model adds that cybersecurity creates business value when it is linked to recovery priorities, employee behavior, and critical process continuity. This is why operational embedding is positioned as a moderator rather than as a simple background condition.

The finding that digital resilience partially mediates the relationship between capabilities and performance reconciles IT capability and operational performance studies. Trieu et al. (2023), Li et al. (2022), and Yu et al. (2022) suggest that digital and IT capabilities can influence performance through organizational mechanisms such as ambidexterity, agility, and transformation capability. The present article keeps direct ITC and CSC paths to performance in the model, but argues that a meaningful part of their performance effect is transmitted through digital resilience.

The proposed model has boundary conditions. Operational embedding may not improve performance when micro firms lack basic resources, when employees have insufficient digital skills, when the industry has low digital dependency, or when regulatory constraints create security routines that are formal but not operationally useful. This boundary logic is consistent with Sinha et al. (2025), who show that digitalization depth and scope can have nuanced rather than linear effects, and with Khurana et al. (2022), who position resilience

in SMEs as a dynamic capability shaped by resource reconfiguration under crisis conditions. Conversely, the proposed effects should be stronger in SMEs with higher digital maturity, greater dependence on digital transactions, stronger exposure to cyber risk, and clearer continuity priorities.

The model also has an economic implication for a business management journal. Cybersecurity and IT investment should not be evaluated only as technical expenditure. They should be evaluated as mechanisms for avoiding downtime, reducing expected loss, protecting revenue continuity, and maintaining customer service. This connects the model with cost-benefit reasoning in SME cyber risk management and makes the article relevant to managers who must justify limited digital and security budgets.

5. Conclusion

This article contributes an operational-embedding view of digital resilience in SMEs. Its central claim is that IT infrastructure capability and cybersecurity capability improve operational performance most strongly when they are embedded in daily routines and continuity priorities. Digital resilience is therefore not treated as a general attitude toward disruption, but as a formative capability built through anticipation, absorption, adaptation, recovery, and learning.

The article also clarifies the role of digital resilience as a partial mediator rather than as the only path from technology to performance. This is important because SMEs may gain some direct operational benefits from IT infrastructure and cybersecurity, but their more durable performance benefits depend on whether these resources help the firm continue, recover, and adapt during disruption.

The main limitation is that the article develops a conceptual model rather than testing it with survey or case data. Future research should test the moderated partial mediation model empirically, compare micro, small, and medium-sized firms, and examine whether the model behaves differently across industries with different levels of digital dependency and cyber exposure.

6. Suggestions

SME managers should begin by mapping critical operations and identifying the digital systems that each operation depends on. This helps managers see which processes would be most affected by system failure, cyber incidents, data loss, or communication breakdowns.

Second, cybersecurity practices should be connected with business continuity priorities. Backups, access control, incident response, employee awareness, and recovery planning should be designed around critical operations rather than treated as isolated technical tasks.

Third, SMEs should use simple operational indicators to monitor digital resilience. Useful indicators include downtime, recovery time, backup reliability, number of incidents, response speed, process interruptions, and service continuity.

Fourth, SME managers should connect digital resilience to financial reasoning. Even simple estimates of downtime cost, expected loss from incidents, recovery cost, and lost sales can help justify investments in backups, security awareness, access control, and continuity planning.

Future research can test the proposed model through survey data, compare SMEs across sectors, study micro firms separately from medium-sized enterprises, and examine how digital resilience develops over time after actual disruptions.

References

1. All DOIs in this working list were checked through doi.org, publisher pages, or Crossref metadata during preparation. The list includes 18 recent studies for the review corpus and 4 foundational theory sources needed for conceptual grounding.

2. Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems, 147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

3. Ashiru, F., Nakpodia, F., & You, J. J. (2022). Adapting emerging digital communication technologies for resilience: Evidence from Nigerian SMEs. *Annals of Operations Research, 327*(2), 795-823. https://doi.org/10.1007/s10479-022-05049-9

4. Awad, J. A. R., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship, 13*, 69. https://doi.org/10.1186/s13731-024-00405-4

5. Awang Ali, Q. S., Hanafiah, M. H., & Mogindol, S. H. (2023). Systematic literature review of Business Continuity Management practices: Integrating organisational resilience and performance in SMEs BCM framework. *International Journal of Disaster Risk Reduction, 99*, 104135. https://doi.org/10.1016/j.ijdrr.2023.104135

6. De Matteis, J., Elia, G., & Del Vecchio, P. (2023). Business continuity management and organizational resilience: A small and medium enterprises perspective. *Journal of Contingencies and Crisis Management, 31*(4), 670-682. https://doi.org/10.1111/1468-5973.12470

7. Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research, 13*(1), 215-246. https://doi.org/10.1007/s40685-019-0085-7

8. Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (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

9. Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. A. (2023). Cybersecurity resilience in SMEs: A machine learning approach. *Journal of Computer Information Systems, 64*(6), 711-727. https://doi.org/10.1080/08874417.2023.2248925

10. Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. *International Journal of Disaster Risk Science, 14*(5), 713-721. https://doi.org/10.1007/s13753-023-00494-x

11. He, Z., Huang, H., Choi, H., & Bilgihan, A. (2022). Building organizational resilience with digital transformation. *Journal of Service Management, 34*(1), 147-171. https://doi.org/10.1108/JOSM-06-2021-0216

12. Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: Insights from industry surveys. *The Journal of Risk Finance, 22*(3/4), 240-260. https://doi.org/10.1108/JRF-02-2020-0024

13. Khurana, I., Dutta, D. K., & Singh Ghura, A. (2022). SMEs and digital transformation during a crisis: The emergence of resilience as a second-order dynamic capability in an entrepreneurial ecosystem. *Journal of Business Research, 150*, 623-641. https://doi.org/10.1016/j.jbusres.2022.06.048

14. Li, L., Tong, Y., Wei, L., & Yang, S. (2022). Digital technology-enabled dynamic capabilities and their impacts on firm performance: Evidence from the COVID-19 pandemic. *Information & Management, 59*(8), 103689. https://doi.org/10.1016/j.im.2022.103689

15. Martín-Rojas, R., Garrido-Moreno, A., & García-Morales, V. J. (2026). Building organizational resilience in SMEs: The key role of digital technologies, transformational leadership, and innovation. *Review of Managerial Science*. https://doi.org/10.1007/s11846-025-00965-z

16. Neri, M., & Niccolini, F. (2025). On the path to cyber organizational resilience: Shedding light on the context of SMEs. *International Journal of Organizational Analysis, 33*(12), 105-131. https://doi.org/10.1108/IJOA-06-2024-4572

17. Sinha, K. K., Raby, S., & Salari, T. (2025). Exploring the scope and depth of digitalisation in times of crisis: Implications for SME resilience. *International Small Business Journal: Researching Entrepreneurship, 43*(3), 219-245. https://doi.org/10.1177/02662426241293000

18. Song, J., & Park, M. J. (2024). A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises. *Information Development*. https://doi.org/10.1177/02666669241252996

19. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. *Strategic Management Journal, 28*(13), 1319-1350. https://doi.org/10.1002/smj.640

20. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

21. Trieu, H. D. X., Nguyen, P. V., Nguyen, T. T. M., Vu, H. T. M., & Tran, K. T. (2023). Information technology capabilities and organizational ambidexterity facilitating organizational resilience and firm performance of SMEs. *Asia Pacific Management Review, 28*(4), 544-555. https://doi.org/10.1016/j.apmrv.2023.03.004

22. Venkatraman, N., Henderson, J. C., & Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. *European Management Journal, 11*(2), 139-149. https://doi.org/10.1016/0263-2373(93)90037-I

23. Yu, J., Wang, J., & Moon, T. (2022). Influence of digital transformation capability on operational performance. *Sustainability, 14*(13), 7909. https://doi.org/10.3390/su14137909