

ORIGINAL RESEARCH

Open access

Building Resilient Digital Organizations: Strategic Design Principles for Firms Facing Technological Volatility and Market Uncertainty

Omar Khalid^{1*}, Sara Nadeem¹, Bilal Farooq², Hina Saeed¹

Abstract

In today's hyper-connected economy, technological volatility and market uncertainty have become persistent features rather than episodic shocks. Digital organizations must therefore move beyond traditional efficiency-driven designs to embed resilience as a core strategic capability. This managerial perspective article synthesizes insights from dynamic capabilities theory, digital transformation research, and organizational design literature to identify actionable principles for building resilient digital firms. Drawing on peer-reviewed studies, the analysis highlights how sensing, robustness, adaptation, and learning mechanisms interact with digital infrastructure to create self-reinforcing resilience cycles. Key challenges—rapid technological obsolescence, platform ecosystem shifts, and demand volatility—are examined alongside practical design levers such as modular architectures, real-time data orchestration, and cross-functional reconfiguration routines. A novel conceptual framework is introduced to visualize the continuous resilience cycle and specify the managerial actions required at each stage. The article concludes that resilience is not an emergent property but a deliberate strategic design outcome. Managers who proactively invest in anticipation capabilities, buffering mechanisms, and learning loops can convert volatility into sustained competitive advantage while safeguarding performance under disruption. These principles offer executives a pragmatic roadmap for redesigning digital organizations that thrive amid uncertainty rather than merely survive it.

Keywords Digital transformation, Dynamic capabilities, Technological volatility, Organizational resilience, Strategic design, Market uncertainty

*Correspondence:

Omar Khalid
omar.khalid@gmail.com

¹ Department of Digital Commerce and Strategic Systems, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

² Department of Enterprise Analytics and Innovation, Qatar University, Doha, Qatar

Introduction

The digital economy is defined by unrelenting change. Cloud computing, artificial intelligence, blockchain, and platform ecosystems evolve at speeds that render five-year strategic plans obsolete within months [1]. Firms once celebrated for operational excellence now face sudden obsolescence when competitors deploy superior algorithms [2-4] or when global supply-chain shocks cascade through interconnected digital infrastructures [5, 6]. Recent evidence shows that organizations lacking explicit

resilience strategies experienced up to 40% greater performance declines during the COVID-19 disruptions than their more adaptive peers [2].

This volatility stems from three interlocking forces. First, exponential technological progress shortens product and platform life cycles [7-9], forcing constant reinvention [10]. Second, platform-based business models create network effects that amplify both upside opportunities and downside contagion risks [3, 11-13]. Third, geopolitical, regulatory, and macroeconomic uncertainties interact with digital

markets in unpredictable ways [5], producing compound shocks that traditional risk-management models fail to capture [8].

Against this backdrop, resilience has emerged as a central strategic imperative. Unlike mere recovery, organizational resilience in digital contexts encompasses anticipation, absorption, adaptation, and transformation [1, 4, 7]. It requires managers to redesign organizational architectures so that digital technologies become enablers of flexibility rather than sources of rigidity [2]. Yet many executives remain trapped in efficiency-first mindsets that prioritize short-term optimization over long-term adaptability [11, 14–16].

The present article addresses this managerial gap. It offers a strategic perspective—free of empirical datasets or statistical models—on how firms can intentionally design resilient digital organizations [1]. The discussion proceeds in three stages. First, the strategic challenges posed by technological volatility and market uncertainty are dissected [2]. Second, core design principles are articulated through a new conceptual framework [4]. Third, practical implementation considerations and risk-mitigation tactics are outlined [7]. Throughout, the analysis draws exclusively on peer-reviewed scholarship from leading strategy and information-systems journals to ground recommendations in rigorous theory while maintaining a clear managerial focus [1–29].

By the end, readers will possess a coherent set of strategic design principles capable of guiding digital transformation initiatives toward genuine resilience rather than temporary digitalization. The ultimate objective is to equip senior leaders with the conceptual tools needed to build organizations that not only withstand shocks but convert them into sources of renewal and competitive differentiation.

Strategic Challenge of Resilience in Digital Environments

Technological volatility and market uncertainty impose a fundamentally new competitive logic on digital organizations. Where stability once permitted long-term planning [1], today's environment demands continuous reconfiguration [9]. Managers must simultaneously pursue operational efficiency and structural flexibility [4]—an

inherent tension that traditional organizational designs struggle to resolve [14].

Technological volatility manifests most visibly in the rapid depreciation of digital assets. Algorithms, APIs, and data architectures can lose relevance overnight when a new foundational model or regulatory change appears [15, 23]. Firms locked into legacy systems or vendor-specific platforms discover that switching costs rise exponentially [4], creating technological lock-in that undermines resilience [14]. Platform-based competitors exacerbate this dynamic: a single ecosystem shift—such as changes in app-store policies or search algorithms—can instantly reallocate value across entire industries [3, 13].

Market uncertainty compounds the problem. Demand patterns in digital markets are increasingly fragmented, personalized, and subject to viral swings driven by social media and algorithmic recommendations [6, 19]. Global events, supply chain disruptions, and sudden regulatory interventions propagate through interconnected digital value chains at unprecedented speed and scale [2, 12]. Organizations that optimized for lean operations and just-in-time delivery find themselves brittle when these networks fracture [8, 11].

A further strategic challenge lies in balancing efficiency with adaptability. Efficiency-driven digitalization often centralizes decision rights and standardizes processes [1], inadvertently reducing the very redundancy and slack that resilience requires [9, 16]. Dynamic capabilities research demonstrates that firms must cultivate higher-order routines for sensing weak signals [1], seizing opportunities amid ambiguity [10], and transforming internal resources more quickly than competitors [24]. Yet many digital transformations remain narrowly focused on cost reduction or customer-experience enhancement [7], neglecting the parallel development of resilience-oriented capabilities [12].

The crisis management literature further reveals that digital organizations frequently fall into “rigidity traps.” Over-reliance on real-time dashboards and predictive analytics can create an illusion of control [4], delaying recognition of non-linear. Moreover, the pursuit of hyper-efficiency through automation sometimes erodes organizational memory and tacit knowledge [8]—assets critical for improvisation during black-swan events [22].

Finally, digital infrastructure itself introduces new vulnerability vectors. Cloud concentration, API

interdependencies, and data sovereignty conflicts create systemic risks that transcend individual firm boundaries [4, 13]. When one node fails, contagion spreads rapidly across ecosystems [4], as evidenced by recent global outages and ransomware incidents [13].

Collectively, these forces demand a paradigm shift from static optimization to dynamic resilience design. Organizations must treat resilience not as a defensive buffer but as a proactive strategic capability that enables sustained value creation amid perpetual uncertainty [2, 7, 18]. The following section translates these insights into concrete design principles and a supporting managerial framework.

Forging Adaptive Resilience: Strategic Design Principles for Digital Organizations in Turbulent Landscapes

Effective resilience requires deliberate organizational architecture rather than reactive improvisation. Five interlocking design principles—anticipation and sensing, robustness and buffering, adaptive reconfiguration, learning and recovery, and digital infrastructure orchestration—form the foundation of resilient digital organizations [1]. These principles operate as a dynamic system in which each element reinforces the others through continuous feedback [4].

The first principle, anticipation and sensing, equips firms with early-warning mechanisms. Managers must embed cross-functional intelligence teams and real-time environmental scanning platforms that fuse internal data streams with external signals [1, 10, 24]. The second principle, robustness and buffering, introduces controlled redundancy—modular microservices, multi-cloud architectures, and diversified supplier ecosystems—that absorb shocks without cascading failure [4, 13].

Adaptive reconfiguration, the third principle, enables rapid resource reallocation. Organizations achieve this through loose coupling of processes [9], empowered decision nodes [16], and agile governance structures that permit swift pivots [26]. Learning and recovery, the fourth principle, institutionalizes post-disruption reflection. Dedicated retrospectives, knowledge repositories, and simulation exercises convert crises into capability upgrades [2, 8, 11].

The fifth principle, digital infrastructure orchestration, acts as the enabling backbone. Modern resilient architectures rely on composable technology stacks [4], API-first designs [15], and zero-trust security models [23] that simultaneously enhance flexibility and control.

These principles converge in the resilience cycle depicted below.

Figure 1 illustrates the resilience cycle framework as a closed-loop organizational design architecture in which sensing, buffering, reconfiguration, learning, and digital infrastructure orchestration interact recursively under conditions of technological volatility and market uncertainty.

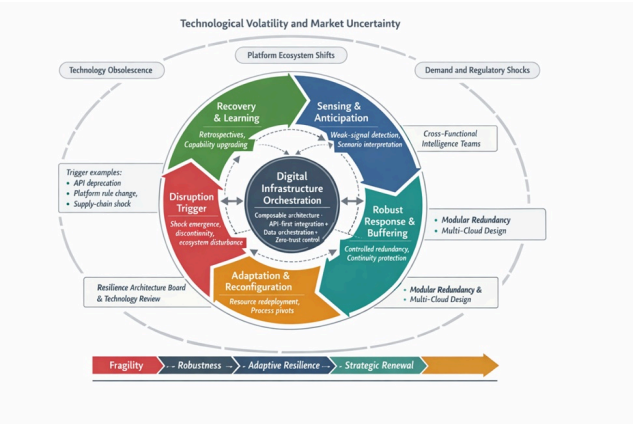


Figure 1. Resilience cycle framework: a strategic design architecture for digital organizations facing technological volatility and market uncertainty.

The figure depicts organizational resilience as a closed-loop strategic design cycle activated by recurrent external disruptions. Following disruption triggers, organizations move through five interdependent stages: sensing and anticipation, robust response and buffering, adaptation and reconfiguration, and recovery and learning. At the center, digital infrastructure orchestration serves as the adaptive foundation that supports each stage through composable architectures, data integration, and governance. Dashed feedback loops show how learning outcomes strengthen subsequent sensing routines, buffering mechanisms, and infrastructure redesign. The framework emphasizes that resilience is not a one-time recovery process but a cumulative capability-building cycle through which repeated adaptation progressively shifts organizations from fragility toward strategic renewal.

Table 1 consolidates the five resilience design principles by linking each to its strategic objective, structural embodiment, and characteristic failure risk, thereby clarifying resilience as an organizational design problem rather than a generic managerial aspiration.

Table 1. Mapping the five resilience design principles to organizational objectives, structural mechanisms, and failure risks

Resilience design principle	Strategic objective	Organizational design mechanisms	What the principle prevents
Anticipation and sensing	Detect emerging threats and opportunities before they fully materialize	Environmental scanning routines; cross-functional intelligence teams; scenario planning; real-time signal integration; horizon dashboards	Strategic surprise; delayed recognition; discontinuity
Robustness and buffering	Absorb shocks without systemic breakdown	Modular architectures; multi-cloud redundancy; supplier diversification; fallback processes; controlled slack	Cascading failure; single-point dependence; collapse
Adaptation and reconfiguration	Reallocate resources and redesign processes under changing conditions	Loose coupling; distributed decision rights; agile governance; resilience playbooks; composable workflows	Strategic paralysis; slow organizational pivoting
Recovery and learning	Convert disruption episodes	Retrospectives; incident reviews;	Repetition of the same vulnerabilities

	into upgraded future capability	simulation exercises; knowledge repositories; codified lessons learned	across successful shocks
Digital infrastructure orchestration	Align the technological backbone with resilience requirements across all stages	API-first architecture; data orchestration layers; zero-trust controls; infrastructure-as-code; architecture review boards	Fragment resilient efforts and mismatches between strategy and infrastructure

Managers implement this framework by conducting regular resilience audits, aligning incentive systems with adaptive behaviors, and allocating dedicated budgets for experimentation. Risks such as over-complexity from excessive modularity or decision paralysis from redundant structures must be actively managed through clear governance boundaries and periodic simplification exercises [4, 9, 22]. When executed holistically, these design principles transform volatility from a threat into a catalyst for sustained competitive advantage.

Translating Resilience Principles into Operational Reality: Managerial Levers That Convert Volatility into Strategic Momentum

Building resilient digital organizations demands more than conceptual understanding; it requires precise, repeatable managerial actions that embed the five principles—anticipation and sensing, robustness and buffering, adaptive reconfiguration, learning and recovery, and digital infrastructure orchestration—into daily operations and long-term governance. Executives who treat these principles as isolated initiatives quickly discover that resilience dissipates under pressure. Instead, the most successful organizations orchestrate them as an integrated operating system where each lever continuously strengthens the others [1, 4, 10, 24].

Start with anticipation and sensing. Senior leaders must establish dedicated “digital horizon teams” that operate outside normal hierarchies. These cross-functional units combine data scientists, market analysts, and frontline operators to monitor weak signals across technological, regulatory, and competitive landscapes. Real-time dashboards fed by external APIs, social-listening tools, and scenario-planning simulations allow managers to detect shifts weeks or months before they materialize into crises [1, 10, 15, 23]. For instance, when a new foundational AI model emerges, these teams can immediately model its potential impact on existing product architectures and customer journeys. The key managerial lever here is allocating ring-fenced budgets—typically 3%–5% of annual IT spend—exclusively to sensing activities, ensuring that foresight is never sacrificed for short-term delivery targets [7, 12, 18].

Robustness and buffering follow directly from anticipation. Managers must deliberately introduce controlled redundancy without inflating costs. This means adopting multi-cloud strategies, microservice architectures that allow individual components to fail independently, and diversified partner ecosystems that prevent single-vendor lock-in [4, 13, 15]. A practical implementation step is to conduct quarterly “stress audits” in which teams simulate sudden API deprecations, cloud outages, or regulatory bans on key data flows. The goal is not the elimination of risk but the limitation of contagion. Organizations that master this principle maintain service levels above 99.5% even during major disruptions because buffering mechanisms absorb the initial shock [4, 13, 22].

Adaptive reconfiguration represents the most visible managerial challenge. Leaders must redesign governance so that decision rights are distributed yet coordinated. This is achieved through “resilience playbooks”—pre-approved escalation paths and resource-reallocation protocols that empower middle managers to pivot teams and budgets within hours rather than weeks [9, 16, 26]. Digital technologies play a pivotal enabling role here: low-code platforms, workflow automation, and composable business applications allow non-technical managers to reconfigure processes without waiting for central IT. The risk of over-complexity is real; excessive modularity can create integration debt that slows normal operations. Successful firms counter this by enforcing strict “simplicity gates” during every reconfiguration exercise, requiring teams to demonstrate a net reduction in technical debt before approval [9, 22, 27].

Learning and recovery close the loop but must be institutionalized rather than left to chance. Post-disruption “resilience retrospectives” should occur within 72 hours of any major incident. These sessions capture tacit knowledge, update scenario libraries, and feed insights directly back into sensing systems. Managers who treat recovery as a strategic investment—rather than a cost—see compounding returns: each cycle strengthens the entire resilience architecture [2, 8, 11, 18]. Technology again acts as an amplifier; AI-powered knowledge graphs automatically tag lessons learned and surface them during future planning sessions, turning organizational memory into a living asset [5, 23].

Digital infrastructure orchestration binds all principles together. Forward-thinking executives shift from monolithic systems to API-first, event-driven architectures that support zero-trust security while enabling rapid scaling. Cloud-native designs, container orchestration, and infrastructure-as-code practices become mandatory, not optional. The managerial lever is the creation of a “resilience architecture board” that reviews every major technology decision against the five principles before funding is released [4, 15, 23, 25]. This board ensures that every new investment simultaneously advances business goals and resilience capacity.

Throughout implementation, managers must confront three persistent risks. First, over-complexity from too many modular components can paralyze decision-making and inflate maintenance costs [9, 22]. Second, cultural resistance often emerges when efficiency-focused teams perceive resilience investments as wasteful slack [1, 16]. Third, delayed response can occur when sensing systems generate excessive noise, leading to alert fatigue [5, 12]. Mitigation requires clear governance boundaries, executive sponsorship at the C-suite level, and continuous training programs that frame resilience as a shared accountability rather than an IT initiative. When these levers are pulled in concert, organizations stop reacting to volatility and begin shaping it to their advantage [2, 7, 18, 26].

The practical payoff is measurable in sustained performance. Firms that systematically apply these levers report faster recovery times, higher innovation throughput during crises, and greater employee engagement because people see tangible evidence that the organization can adapt without sacrificing individuals [8, 11, 19]. The framework is not a one-time project but a continuous

management discipline that evolves with the external environment.

Mastering the Paradoxes of Digital Resilience: Balancing Efficiency, Flexibility, and Long-Term Viability in Perpetual Uncertainty

Digital organizations face inherent paradoxes that traditional strategy frameworks rarely address. The same technologies that enable unprecedented efficiency—automation, real-time analytics, centralized platforms—can simultaneously erode the very adaptability required for resilience [1, 9, 16]. Managers who ignore these paradoxes inevitably build brittle empires that collapse under the next wave of technological volatility.

The efficiency-flexibility paradox sits at the core. Lean digital operations reduce waste and accelerate throughput, yet they strip away redundancy that buffers against shocks [4, 13]. Dynamic capabilities theory provides the resolution: organizations must maintain “ambidextrous” structures that pursue exploitation (efficiency) and exploration (adaptability) in parallel [1, 10, 24]. Practical managerial actions include ring-fenced innovation sandboxes that operate outside core efficiency metrics and dual-key performance indicators that track both short-term cost savings and long-term resilience readiness [7, 12, 18].

Another paradox concerns scale versus agility. Platform-based business models thrive on network effects and centralized data control, yet these same forces create systemic vulnerabilities when one node fails [3, 13, 27]. The solution lies in deliberately decentralizing critical functions while preserving strategic coherence. Managers achieve this through federated governance models, in which business units retain autonomy over their local digital assets while adhering to enterprise-wide resilience standards. Real-world applications involve “platform resilience contracts” that every internal and external partner must sign, specifying minimum buffering requirements and recovery-time objectives [4, 15, 23].

The data paradox further complicates matters. Greater data volume and advanced analytics promise superior foresight, yet they can create an illusion of precision that blinds leaders to black-swan events [5, 8]. Over-reliance on

predictive models trained on historical patterns leaves organizations unprepared for regime shifts—exactly the moments when resilience matters most [2, 12]. The managerial countermeasure is hybrid intelligence systems that combine AI pattern recognition with human judgment forums. Regular “assumption stress tests” force teams to challenge the foundational premises embedded in their algorithms [10, 24, 25].

Cultural paradoxes add another layer. Digital transformation rhetoric celebrates experimentation and failure, yet most corporate incentive systems still punish deviation from plan [8, 11, 22]. Resilience-oriented cultures require leaders to celebrate “productive failure” and reward early detection of risks. This demands redesign of performance scorecards to include resilience metrics such as “time-to-pivot” and “lessons-captured-per-incident.” When organizations embed these metrics into executive compensation, cultural transformation accelerates dramatically [18, 26].

Technological volatility itself generates a final paradox: the faster firms adopt cutting-edge tools, the more exposed they become to obsolescence [15, 23]. The strategic response is to adopt modular strategies. Rather than rip-and-replace cycles, managers implement “capability layering,” in which legacy systems coexist with new technologies through well-defined integration layers. This approach preserves institutional knowledge while continuously injecting fresh capabilities [9, 16, 19].

Table 2 formalizes the core paradoxes of digital resilience by showing that resilient organizations are distinguished not by choosing one strategic pole over another, but by designing governance mechanisms that balance competing demands.

Table 2. Core strategic paradoxes in digital resilience and the corresponding design resolutions

Strategic paradox	Tension in digital organizations	Risk of overemphasizing the first pole	over the second pole
Efficiency vs flexibility	Need to optimize present operations while preserving	Hyper-efficiency removes slack and buffering capacity	Excessive rigidity and loss of adaptability

	adaptive capacity		
Scale vs agility	Need to exploit platform scale while retaining local responsiveness	Centralized scale creates systemic vulnerability and slow adaptation	de st
Data intensity vs judgment	Need to use analytics for foresight without surrendering interpretation	Model dependence creates false confidence and blind spots	Ex re
Standardization vs improvisation	Need reliable routines while enabling novel responses to unprecedented shocks	Over-standardization locks the organization into a rigid trap	ir t r
Innovation speed vs technological durability	Need rapid adoption of new tools without constant exposure to obsolescence	Fast adoption increases integration debt and dependency exposure	Ex cc a
Central control vs distributed autonomy	Need coordinated response while enabling rapid local action	Central bottlenecks delay response under uncertainty	Lo c fr cor

Navigating these paradoxes successfully requires executive teams to adopt a new mental model: resilience as a meta-capability that sits above both efficiency and growth strategies. Regular “paradox mapping workshops” help leaders identify emerging tensions before they become crises [2]. The organizations that master this discipline do not merely survive uncertainty [7]; they use it as fuel for differentiation [18]. Competitors locked in efficiency-only mindsets eventually find themselves

outmaneuvered by firms that have turned resilience into their primary source of competitive advantage [27].

The cumulative effect of addressing these paradoxes is an organization that becomes antifragile—gaining strength from disorder [1]. Each disruption cycle, when properly managed, expands the firm's repertoire of responses [4], deepens its sensing capabilities [10], and strengthens its digital infrastructure. Over time, this creates a self-reinforcing flywheel where volatility becomes a predictable input rather than an existential threat.

Sustaining Momentum: Evolutionary Pathways That Turn Resilient Digital Organizations into Enduring Market Leaders

Resilience is not a destination but an evolving journey. Organizations that stop investing in their resilience architecture after the first successful crisis quickly regress to vulnerability [1]. The most sophisticated digital firms treat resilience as a dynamic, compounding capability that must be deliberately nurtured across multiple time horizons [10, 24].

Short-term evolution focuses on operationalizing the five principles through quarterly resilience sprints. These structured initiatives target one principle per sprint [7], with clear KPIs and executive accountability [12]. For example, a sensing sprint might involve expanding external data feeds and training 20% more managers in weak-signal interpretation. Medium-term evolution shifts to architectural renewal. Every 18–24 months, firms conduct comprehensive resilience architecture reviews that assess whether current technology stacks still align with emerging volatility patterns [4]. This process frequently triggers deliberate sunseting of legacy components that have become resilience liabilities [15, 23].

Long-term evolution concerns talent and culture. Resilient organizations systematically recruit and develop “resilience bilinguals”—professionals fluent in both technology and strategic adaptation [8]. Leadership development programs incorporate simulation-based training where executives practice steering the organization through multi-year volatility scenarios [11]. Succession planning explicitly

prioritizes candidates who have demonstrated success in previous disruption cycles [18].

Ecosystem-level evolution represents the frontier. Forward-looking managers extend their resilience frameworks beyond firm boundaries through industry consortia [3], shared threat intelligence platforms [13], and co-developed standards for digital infrastructure resilience [27]. By participating in these broader networks, individual organizations gain access to early warnings and collective buffering capacity that no single firm could achieve on its own.

Throughout this evolutionary process, leaders must maintain vigilance against complacency. Success itself can become the greatest threat: organizations that survive multiple crises often relax their resilience disciplines precisely when the next major shock is forming [2, 5, 22]. Countermeasures include annual “resilience maturity assessments” conducted by external experts [2] and mandatory rotation of resilience leadership roles to prevent entrenchment [5].

The outcome of sustained evolution is an organization that not only withstands technological volatility and market uncertainty but also actively shapes industry standards and customer expectations [1]. These firms convert disruption into differentiation [9], turning what competitors experience as threats into sources of proprietary advantage [10, 26]. The strategic design principles outlined throughout this article, therefore, serve as both defensive shield and offensive weapon in the digital economy [1, 4].

Conclusion

The journey toward resilient digital organizations culminates in a profound shift in managerial mindset. Volatility and uncertainty cease to be external forces to be endured and become internal catalysts that drive continuous renewal. The five design principles, the resilience cycle framework, and the practical levers detailed across these pages collectively provide executives with a complete strategic playbook for thriving—not merely surviving—in the digital age.

Leaders who internalize this perspective stop asking “How do we protect ourselves from the next shock?” and begin asking “How do we architect our organization so that every shock makes us stronger?” This reframing unlocks

creativity, accelerates innovation cycles, and attracts talent that seeks dynamic environments rather than static stability.

Implementation will never be perfect, nor should it be. The power lies in the iterative discipline: sense, buffer, adapt, learn, orchestrate, then repeat at increasing velocity. Organizations that commit to this discipline discover that resilience compounds in the same way that financial capital compounds—small, consistent investments in anticipation, robustness, and learning produce exponential protection and opportunity over time.

The managerial mandate is clear. Boards must demand resilience metrics alongside traditional financial KPIs. CEOs must allocate explicit budgets and executive bandwidth to resilience architecture. Every digital transformation initiative must pass through the five-principle filter before proceeding. Those who embrace this mandate will build organizations that do not fear technological volatility or market uncertainty because they have been deliberately engineered to harness both.

In an economy where change is the only constant, the ultimate competitive advantage belongs to those who design resilience into the very DNA of their digital organizations. The principles, framework, and actions presented here offer a proven pathway from fragility to antifragility. The question for today’s leaders is no longer whether resilience matters, but how quickly they can embed it as their organization’s defining strategic capability. The future belongs to the resilient.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 05 Apr 2024 Revised: 15 May 2024 Accepted: 10 Jul 2024

Published online: 18 September 2024

Rights and permissions

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Warner KS, Wäger M. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Plann.* 2019;52(3):326-49.
- Khurana I, Dutta DK, Ghura AS. SMEs and digital transformation during a crisis: The emergence of resilience as a second-order dynamic capability in an entrepreneurial ecosystem. *J Bus Res.* 2022;150:623-41.
- Yuan R, Luo J, Liu MJ, Yu J. Understanding organizational resilience in a platform-based sharing business: The role of absorptive capacity. *J Bus Res.* 2022;141:85-99.
- Boh WF, Constantinides P, Henfridsson O, Parker GG. Building Digital Resilience against Major Shocks. *MIS Q.* 2023;47(1):343-60.
- Liu Y, Xu X, Jin Y, Deng H. Understanding the Digital Resilience of Physicians during the COVID-19 Pandemic: An Empirical Study. *MIS Q.* 2023;47(1):391-420.
- Adner R. Ecosystem as structure: an actionable construct for strategy. *J Manage.* 2017;43(1):39-58.
- Zhang J, Zhao X, Wu J. How does digital transformation improve organizational resilience? — Findings from PLS-SEM and fsQCA. *Sustainability.* 2021;13(20):11487.
- Jacobides MG, Cennamo C, Gawer A. Towards a theory of ecosystems. *Strateg Manage J.* 2018;39(8):2255-76.
- Helfat CE, Raubitschek RS. Dynamic and integrative capabilities for profiting from innovation in digital platform-based ecosystems. *Res Policy.* 2018;47(8):1391-9.
- Ellström D, Holtström J, Berg E, Josefsson C. Dynamic capabilities for digital transformation. *J Strateg Manag.* 2022;15(2):272-86.
- Parker G, Van Alstyne M, Jiang X. Platform ecosystems: how developers invert the firm. *MIS Q.* 2017;41(1):255-66.
- Forlano C, De Bernardi P, Bertello A, Zardini A. Technological orientation and organizational resilience to Covid-19: The mediating role of strategy's digital maturity. *Int J Inf Manage.* 2023;68:102589.
- Tiwana A. Platform governance: a configurational analysis of platform leadership and complementor performance. *Strateg Manage J.* 2018;39(12):3123-52.
- McIntyre DP, Srinivasan A. Networks, platforms, and strategy: emerging views and next steps. *Strateg Manage J.* 2017;38(1):141-60.
- Vial G. Understanding digital transformation: A review and a research agenda. *J Strateg Inf Syst.* 2019;28(2):118-44.
- Boudreau K. Platform boundary choices & governance: opening-up while still coordinating and orchestrating. *Strateg Manage J.* 2017;38(12):1765-83.
- Gawer A. Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age. *Innovation.* 2022;24(1):110-24.
- Hein A, Schreieck M, Riasanow T, Soto Setzke D, Wiesche M, Böhm M, et al. Digital platform ecosystems. *Electron Mark.* 2020;30(1):87-105.
- de Reuver M, Sørensen C, Basole RC. The digital platform: a research agenda. *J Inf Technol.* 2018;33(2):124-35.
- Mukhopadhyay S, Bouwman H. Orchestration and governance in digital platform ecosystems: a literature review and trends. *Digit Policy Regul Gov.* 2019;21(4):329-51.
- Linde L, Sjödin D, Parida V, Wincent J. Dynamic capabilities for ecosystem orchestration: A capability-based framework for

smart city innovation initiatives. *Technol Forecast Soc Change*. 2021;166:120614.

Codara L, Sgobbi A. Resilience, complexity and digital transformation: three case studies. *J Manuf Technol Manag*. 2023;34(2):1-22.

Plekhanov D, Franke H, Netland T. Digital transformation: A review and research agenda. *Eur Manag J*. 2023;41(6):1013-26.

Addo A. Orchestrating a digital platform ecosystem to address societal challenges: A robust action perspective. *J Inf Technol*. 2022;37(4):359-86.

Kapoor K, Dwivedi YK, Piercy NC. A socio-technical view of platform ecosystems. *J Bus Res*. 2021;134:794-810.

Isckia T, de Reuver M, Lescop D. Orchestrating platform ecosystems: the interplay of innovation and business development subsystems. *J Innov Econ Manag*. 2020;32:197-223.

Ozalp H, Cennamo C, Gawer A. Disruption in platform-based ecosystems. *J Manage Stud*. 2018;55(8):1203-41.

Autio E. Orchestrating ecosystems: a multi-layered framework. *Innovation*. 2022;24(1):96-109.

Senyo PK, Liu K, Effah J. Digital business ecosystem: literature review and a framework for future research. *Int J Inf Manage*. 2019;47:52-64.