

ORIGINAL RESEARCH

Open access

# The Digital Business Resilience Framework: Integrating Strategic Agility, Platform Dependence, Cyber Risk, and Organizational Learning

Michelle Tan<sup>1\*</sup>, Adrian Goh<sup>1</sup>

## Abstract

Digital businesses operate in an environment where competitive advantage increasingly depends on the ability to respond to technological disruption, shifting customer expectations, ecosystem instability, cyber threats, and operational shocks. Resilience in this context cannot be reduced to recovery after disruption, because digital firms must also anticipate risk, adapt strategically, and preserve continuity across interdependent technological and organizational systems. Existing resilience frameworks remain fragmented. Some emphasize agility and dynamic capability development, while others focus on cybersecurity, platform strategy, business continuity, or organizational learning as separate domains. This fragmentation limits understanding of how digital businesses actually withstand disruption when market responsiveness, platform dependence, cyber exposure, and learning capacity interact simultaneously. This article develops the Digital Business Resilience Framework as an original conceptual framework for explaining resilience in digital business. The framework integrates four co-equal pillars: strategic agility, platform dependence awareness, cyber risk management, and organizational learning. It argues that resilience emerges when these pillars mutually reinforce one another rather than when they are managed as isolated capabilities. The framework contributes to digital business and resilience scholarship by shifting attention from isolated adaptive responses to systemic resilience architecture. It also offers managers a diagnostic lens for identifying weak points in digital business resilience and for designing integrated practices that connect agility, platform governance, cyber preparedness, and learning routines.

**Keywords** Organizational learning, Strategic agility, Conceptual framework, Platform dependence, Digital business resilience, Cyber risk

\*Correspondence:

Michelle Tan

michelle.tan@ntu.edu.sg

<sup>1</sup> Department of Digital Business Analytics, Faculty of Business, Nanyang Technological University, Singapore, Singapore

## Introduction

Digital business resilience has become a central strategic concern because firms increasingly compete through digitally mediated products, platforms, infrastructures, analytics, and ecosystem relationships. Digital transformation changes not only how firms create value but also how they become exposed to disruption, since technological renewal can intensify dependency on external infrastructures and accelerate the speed at which failure

spreads across organizations [1]. As digital transformation reshapes innovation and entrepreneurship, firms must manage uncertainty that is simultaneously technological, strategic, organizational, and institutional [2]. Traditional business continuity planning is therefore insufficient when disruption is embedded in the same digital systems that enable growth.

The core problem is that resilience is often discussed through a narrow lens of adaptation or recovery, even

though digital businesses face disruptions that are systemic rather than isolated. Strategic renewal capabilities allow firms to sense and seize digital opportunities, yet the same transformation processes can increase reliance on external platforms, cloud services, data infrastructures, and algorithmic intermediaries [3]. Digital transformation research has shown that firms must coordinate strategy, technology, organizational change, and customer value creation, but resilience requires an additional focus on how these elements remain functional under stress [4]. A digital firm may be agile in market response while remaining fragile in platform dependence, cyber exposure, or organizational learning.

The resilience challenge is also intensified by the platformization of business activity. Platform ecosystems can expand market access, innovation capacity, and coordination across distributed actors, but they also create power asymmetries and dependency conditions that firms may not fully control [5]. In digital platform-based ecosystems, firms benefit from complementarities and network effects, but they may also become vulnerable to governance changes, technical outages, data restrictions, or ecosystem instability [6]. Resilience must therefore include awareness of where strategic flexibility is constrained by dependence on external digital architectures.

This article addresses this problem by proposing the Digital Business Resilience Framework, an original conceptual framework integrating strategic agility, platform dependence awareness, cyber risk management, and organizational learning. Prior resilience scholarship has emphasized resilience as a capability that involves anticipation, coping, and adaptation, yet these processes require reinterpretation for digitally dependent business models [7]. Management research on resilience has also called for more integrated frameworks that connect resilience to organizational capabilities, strategic renewal, and environmental turbulence [8]. The aim of this article is to construct a framework that explains how digital businesses become resilient when agility, dependency awareness, cyber risk management, and learning are treated as mutually reinforcing pillars.

## Conceptual Gap

The first conceptual gap concerns the overextension of strategic agility as a resilience explanation. Digital strategy

research often presents agility, dynamic capabilities, and business model innovation as means through which firms respond to turbulent environments and renew competitive advantage [9]. However, agility does not automatically produce resilience if rapid strategic movement increases exposure to unstable platforms, poorly governed data flows, or under-secured digital infrastructures. A firm that quickly seizes digital opportunities may simultaneously deepen hidden dependencies that become visible only during disruption.

The second gap concerns the separation of platform dependence from organizational resilience. Platform research has clarified how digital platforms reorganize firm boundaries, ecosystem participation, and strategic control, yet resilience models often understate the vulnerability created when firms depend on platforms they do not own [10]. Platform ecosystems may invert traditional firm control by shifting critical innovation and access functions toward external complementors and platform owners [11]. This creates a resilience problem because firms can be strategically agile within a platform ecosystem while structurally constrained by policy changes, access rules, data portability limits, or interface redesigns.

The third gap concerns the weak integration of cyber risk and organizational learning into digital resilience theory. Cybersecurity research increasingly recognizes cyber risk as a managerial and organizational issue, not merely a technical problem, but resilience frameworks still often treat cyber risk as a protective layer rather than as a source of organizational learning [12]. Cyber risk management becomes strategically important when cyber incidents disrupt operations, reputation, trust, and continuity, rather than only information systems [13]. A synthesis is therefore overdue because digital resilience requires a framework that treats agility, platform dependence, cyber risk, and learning as interdependent rather than sequential or peripheral concerns.

## Strategic Agility in Digital Business

Strategic agility refers to the ability of a firm to sense environmental change, seize emerging opportunities, and reconfigure resources in response to shifting strategic conditions. In digital business, this agility is closely tied to dynamic capabilities because digital technologies alter the speed, scope, and modularity of strategic action [3]. Firms

undergoing digital transformation must continually renew routines, structures, and resource commitments while maintaining coherence in value creation [1]. Strategic agility is therefore a foundational pillar of digital resilience because it enables rapid interpretation and response when disruption occurs.

Strategic agility also depends on the capacity to coordinate business model innovation with organizational transformation. Business model innovation research shows that firms must redesign value creation, delivery, and capture mechanisms when environmental conditions change [14]. Digital transformation expands this challenge by requiring organizations to align technology investments, customer interfaces, data practices, and organizational structures [4]. Resilience emerges when agility allows firms not only to move quickly but also to redirect resources without undermining continuity.

However, agility can become a source of fragility when it is pursued without structural awareness. Digital innovation in incumbent firms often involves competing concerns, including experimentation, control, legacy constraints, and strategic coordination [15]. Firms may respond quickly to digital opportunities by adopting external platforms, accelerating digital channels, or scaling data-intensive processes, yet these choices can increase dependency and cyber exposure if governance mechanisms lag behind strategic action. In this sense, agility must be disciplined by resilience logic rather than treated as an unconditional good.

Strategic agility is best understood as a resilience capability when sensing, seizing, and transforming are connected to risk awareness and organizational learning. Dynamic and integrative capabilities are especially important in digital ecosystems because firms must profit from innovation while managing interdependencies across partners, platforms, and technological interfaces [6]. **Table 1** summarises the key dimensions and enablers of strategic agility for digital resilience. The table clarifies that agility contributes to resilience only when each capability is linked to continuity, dependency awareness, and adaptive learning.

**Table 1.** Strategic Agility Dimensions for Digital Resilience: Sensing, Seizing, and Transforming Capabilities

| Strategic agility | Core meaning in digital | Key organizational | Contribution to digital resilience |
|-------------------|-------------------------|--------------------|------------------------------------|
|-------------------|-------------------------|--------------------|------------------------------------|

| dimension                             | business                                                                                                                                              | enablers                                                                                                                                         | resilience                                                                                  |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Sensing digital disruption            | Detecting changes in technologies, markets, customer behaviour, regulation, cyber threats, and platform conditions before they become critical shocks | Environmental scanning, analytics capability, customer feedback systems, platform monitoring, cyber threat intelligence, boundary-spanning teams | Improving early warning capacity allows firms to prepare before disruption escalates        |
| Seizing digital opportunities         | Mobilizing resources to respond to emerging digital opportunities or threats through new products, processes, partnerships, or business models        | Flexible investment routines, rapid decision processes, cross-functional digital teams, modular resource allocation, executive sponsorship       | Enabling timely strategic response while preserving competitive relevance during turbulence |
| Transforming organizational resources | Reconfiguring structures, routines, technologies, and capabilities to sustain adaptation over time                                                    | Dynamic capability development, process redesign, digital talent development, governance routines, learning repositories                         | Converting short-term response into durable resilience capabilities                         |
| Coordinating agility with continuity  | Aligning rapid adaptation with business continuity, cyber preparedness,                                                                               | Resilience governance boards, continuity planning, cyber-risk integration,                                                                       | Preventing agility from undermining operational stability through strategic continuity      |

|                                 |                                                                                               |                                                                                                                              |                                                                                          |
|---------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
|                                 | and platform risk awareness                                                                   | platform dependency reviews, scenario planning                                                                               |                                                                                          |
| Embedding feedback into agility | Using disruptions, near-misses, and implementation outcomes to refine future strategic action | Post-incident reviews, organizational learning routines, knowledge codification, performance dashboards, adaptive governance | Strengthening future sensing, seizing, transforming by turn experience into capabilities |

## Platform Dependence and Vulnerability

Platform dependence is a structural condition in which a digital business relies on external digital infrastructures, marketplaces, cloud systems, app stores, social media channels, data interfaces, or ecosystem rules to reach customers and operate effectively. Platform and infrastructure research shows that digital business activity increasingly occurs through layered architectures that connect firms to external technical and institutional arrangements [16]. This creates strategic opportunity because platforms expand scale, access, and innovation capacity, but it also creates vulnerability because firms may depend on systems whose governance, continuity, and technical evolution they cannot control. Resilience therefore requires more than agility; it requires explicit awareness of where the firm's digital value creation is externally mediated.

Platform dependence becomes particularly important when firms build business models around ecosystem participation. Digital platforms shape boundaries between firms, complementors, users, and infrastructure providers, making strategic control more distributed and less internally owned [17]. Firms may depend on platform interfaces, ranking algorithms, access policies, data visibility, payment systems, or third-party cloud services, and each dependency can become a point of disruption. A platform owner's policy change, pricing revision, outage, or

algorithmic adjustment can weaken a firm's market access even when the firm itself remains operationally capable.

The resilience implications of platform dependence are especially visible in power asymmetries between platform owners and dependent firms. Platform-dependent entrepreneurs face risks linked to unequal bargaining power, changing rules, limited appeal mechanisms, and dependence on platform-mediated customer access [18]. These vulnerabilities show that digital resilience cannot be reduced to internal resource flexibility, because many digital firms are constrained by external governance structures. Platform dependence awareness therefore becomes a distinct pillar of the Digital Business Resilience Framework rather than a subcomponent of agility.

Platform dependence awareness requires firms to map their digital dependencies, assess exposure to platform failure, and develop alternatives where possible. Research on platform competition shows that digital markets are shaped by platform positioning, ecosystem governance, and control over interfaces, which means resilience depends on understanding both technical and strategic dependence [19]. Table 2 identifies the types of platform dependence and their associated resilience vulnerabilities. The table shows that platform dependence can affect market access, operational continuity, data control, strategic autonomy, and learning capacity.

**Table 2.** Platform Dependence and Vulnerability in Digital Business: Types, Risks, and Resilience Implications

| Type of platform dependence | Main source of dependence                                                                           | Resilience vulnerability                                                                              | Business impact during disruption                                                               |
|-----------------------------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Market access dependence    | Reliance on marketplaces, app stores, search platforms, or social media channels to reach customers | Loss of visibility, ranking changes, account suspension, access restrictions, sudden policy revisions | Revenue loss, customer acquisition disruption, weakened brand reach, reduced strategic autonomy |

|                           |                                                                                                                  |                                                                                                       |                                                                                             |
|---------------------------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Infrastructure dependence | Reliance on cloud providers, payment processors, hosting services, or external software infrastructures          | Outages, service degradation, vendor lock-in, limited switching capacity, cascading technical failure | Operational downtime, service interruption, delayed transaction, customer dissatisfaction   |
| Data dependence           | Reliance on platform-controlled customer data, analytics dashboards, APIs, or data-sharing permissions           | Data access restriction, portability limits, analytics opacity, API changes, loss of customer insight | Weakened decision-making, reduced personalization, impaired learning from users and markets |
| Governance dependence     | Exposure to platform rules, moderation systems, pricing policies, algorithmic governance, and dispute procedures | Power asymmetry, unpredictable enforcement, opaque rule changes, limited recourse                     | Strategic uncertainty, compliance burden, sudden business model disruption                  |
| Innovation dependence     | Dependence on platform tools, developer ecosystems, standards, or technical roadmaps                             | Innovation bottlenecks, interface redesign, compatibility problems, dependency on platform priorities | Delayed product development, increased adaptation costs, loss of differentiation            |

## Cyber Risk and Organizational Learning

Cyber risk is a central source of digital business disruption because it threatens operational continuity, data integrity, customer trust, financial stability, and strategic reputation. Cybersecurity challenges are increasingly tied to digital transformation because expanded connectivity, cloud adoption, platform participation, and data-intensive processes enlarge the organizational attack surface [20]. Cyber risk therefore cannot be treated as a technical issue managed separately from business strategy. In a digitally dependent firm, cyber incidents can interrupt value creation directly by disabling systems and indirectly by damaging confidence in the firm's digital capabilities.

The business impact of cyber risk is intensified by the tension between security and agility. Digital firms often accelerate innovation, platform integration, and customer-facing experimentation, yet rapid change can outpace governance, risk assessment, and security controls. Cyber resilience research highlights that organizations must manage cyber risk as part of broader resilience capability, not only as a defensive compliance function [12]. This means cyber risk management should be integrated into strategic agility so that speed does not create unmanaged exposure.

Organizational learning is the mechanism through which cyber incidents, near-misses, and disruptions become sources of strengthened resilience. Resilience research emphasizes that firms adapt through experience, but adaptation is not automatic; it requires routines for interpretation, knowledge codification, and behavioural change [21]. Organizational learning initiatives can help firms convert disruption into improved routines, resource use, innovation capacity, and environmental responsiveness [22]. In the Digital Business Resilience Framework, learning is not a final step after recovery but a continuous process that improves agility, platform awareness, and cyber preparedness.

Learning from cyber risk requires disciplined feedback loops that connect incident response to future capability development. Post-incident reviews, knowledge repositories, scenario exercises, and cross-functional

debriefings can transform localized experience into organization-wide resilience knowledge [23]. Table 3 links cyber risk exposure to organizational learning mechanisms that build resilience. The table emphasizes that cyber resilience depends not only on prevention and response but also on whether organizations institutionalize what they learn from disruption.

**Table 3.** Cyber Risk Management and Organizational Learning: Incident Response, Learning Loops, and Capability Enhancement

| Cyber risk exposure                                     | Immediate management concern                                                      | Organizational learning mechanism                                                                                     | Capability enhancement through learning                          |
|---------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Phishing, social engineering, and credential compromise | Preventing unauthorized access and limiting human-error vulnerabilities           | Behavioural debriefings, targeted training updates, analysis of user decision patterns, reporting culture improvement | Security awareness, employee vigilance, early detection routines |
| Ransomware and system disruption                        | Maintaining continuity, restoring systems, and preventing operational paralysis   | Post-incident recovery analysis, backup testing reviews, continuity simulation, documentation of response bottlenecks | Recovery planning, redundant design, operational coordination    |
| Data breach or privacy failure                          | Protecting sensitive information, meeting legal obligations, and preserving trust | Root-cause analysis, data-flow mapping, policy revision, knowledge sharing across legal, IT, and business units       | Data governance, accountability, compliance learning             |
| Platform or third-party                                 | Managing risk                                                                     | Third-party incident review,                                                                                          | Platform dependence                                              |

|                                       |                                                                      |                                                                                                     |                                                                      |
|---------------------------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| security failure                      | transferred through vendors, cloud providers, and ecosystem partners | dependency mapping, vendor risk learning, contractual risk reassessment                             | awareness, supplier governance, contingency planning                 |
| Repeated near-misses and weak signals | Identifying vulnerabilities before they become major incidents       | Near-miss reporting, pattern analysis, threat intelligence integration, resilience dashboard review | Anticipatory learning, early warning capability, adaptive governance |

## Proposed Digital Business Resilience Framework

The Digital Business Resilience Framework proposes that resilience emerges from the interaction of four co-equal pillars: strategic agility, platform dependence awareness, cyber risk management, and organizational learning. This framework extends prior resilience thinking by connecting capability-based resilience with the distinctive vulnerabilities of digital business environments [7]. It also responds to calls for more dynamic perspectives on firm resilience by showing how resilience is produced through ongoing interaction rather than through a fixed stock of resources [21]. The framework’s central claim is that no single pillar is sufficient when digital disruption is systemic, interconnected, and rapidly evolving.

Strategic agility enables firms to detect and respond to change, but platform dependence awareness disciplines agility by revealing where rapid digital expansion creates structural exposure. Institutional perspectives on digital transformation show that digital change is shaped by rules, norms, and external arrangements, not only by internal technological choice [24]. Platform dependence awareness therefore helps firms identify whether a proposed digital move increases exposure to external control, lock-in, or ecosystem instability. When agility and platform awareness are combined, firms become better able to grow digitally without becoming unknowingly fragile.

Cyber risk management prevents, contains, and recovers from threats that could disrupt digital operations, while organizational learning ensures that response experience strengthens future resilience. Business continuity and resilience management research emphasizes the need to link preparedness, response, recovery, and adaptation into a coherent management logic [25]. Organizational learning deepens this logic by translating disruption into knowledge that improves routines, governance, and strategic interpretation. Cyber risk management without learning remains reactive, while learning without cyber integration may overlook one of the most consequential sources of digital business disruption.

The framework also explains resilience as an emergent property rather than a checklist. Organizational resilience may improve service quality and continuity when resilience capabilities are embedded across systems rather than isolated within emergency planning [26]. Table 4 presents the complete Digital Business Resilience Framework. The table specifies each pillar, its role, its interconnections, and the resilience outcomes produced when the four pillars operate together.

Table 4. Digital Business Resilience Framework: Pillars, Interconnections, and Resilience Outcomes

| Framework pillar              | Core function                                                                                                        | Key managerial question                                                        | Interconnections with other pillars                                                                                 |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Strategic agility             | Enables the firm to sense disruption, seize opportunities, and transform resources under changing digital conditions | Can the firm respond quickly without losing strategic coherence or continuity? | Requires platform awareness to avoid digital risks; cyber management to secure changing learning; improves adaptive |
| Platform dependence awareness | Identifies where value creation depends on external platforms,                                                       | Which digital dependencies could disrupt the business if external              | Shapes decision informs risk assessment and pro learning                                                            |

|                                    |                                                                                                              |                                                                                                 |                                                                                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
|                                    | infrastructures, interfaces, data access, and ecosystem rules                                                | conditions change?                                                                              | after platform disruption                                                                |
| Cyber risk management              | Prevents, detects, contains, and recovers from cyber threats that can interrupt digital operations and trust | Are cyber risks integrated into business strategy rather than treated only as technical issues? | Constrains agility, platform-mediated operations; generates learning incidents near-term |
| Organizational learning            | Converts disruptions, failures, and near-misses into improved routines, knowledge, and future capabilities   | Does the firm systematically learn from disruption and change behaviour accordingly?            | Enhances refinement; deepens awareness; improves preparedness through feedback           |
| Integrated resilience architecture | Aligns the four pillars into a coherent system of diagnosis, response, recovery, and renewal                 | Are resilience responsibilities, metrics, and routines coordinated across the organization?     | Constrains strategic technology platform learning process; one may system                |

Figure 1 presents the Digital Business Resilience Framework, showing how strategic agility, platform dependence awareness, cyber risk management, and organizational learning interact to produce resilient digital business outcomes.

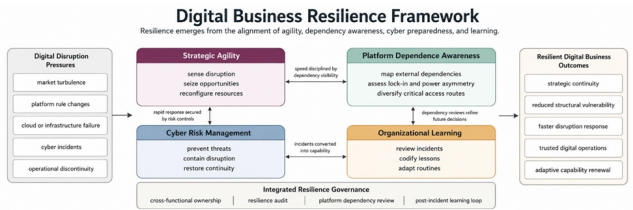


Figure 1. Digital Business Resilience Framework: Integrating Strategic Agility, Platform Dependence

Awareness, Cyber Risk Management, and Organizational Learning

## Implementation Pathway for Managers

Managers can implement the Digital Business Resilience Framework by beginning with a four-pillar resilience audit. This audit should assess whether the firm can sense and respond to disruption, where it depends on external platforms, how cyber risks are connected to business impact, and whether learning routines convert incidents into improved capabilities. Global platform and ecosystem research suggests that firms must understand how platform participation reshapes strategic options across markets and institutional contexts [27]. A practical audit should therefore examine both internal capabilities and external dependencies.

The second step is to establish cross-functional resilience governance. Digital resilience cannot be owned only by strategy teams, IT departments, cybersecurity specialists, or operational managers, because the four pillars cut across organizational boundaries. A resilience team should include strategy, technology, cybersecurity, legal, operations, data governance, and business unit representatives who can evaluate trade-offs between speed, dependence, security, and learning. Research on cyber risk and organizational turbulence indicates that resilience depends on aligning risk management with dynamic environmental conditions rather than treating risk as static compliance [28].

The third step is to institutionalize learning loops and dependency reassessment as recurring managerial routines. Firms should conduct post-incident reviews, platform dependency reviews, continuity simulations, and cyber-learning exercises at regular intervals rather than only after major failures. Digital innovation research shows that incumbents must manage competing concerns over time, which means resilience implementation should be iterative rather than one-time [15]. The pathway moves from diagnosis, to cross-functional coordination, to embedded learning, so that resilience becomes part of strategic management rather than a separate crisis function.

## Limitations and Future Research

The first limitation is that the Digital Business Resilience Framework is conceptual and has not yet been empirically tested. Although it integrates research on digital transformation, platforms, cyber risk, resilience, and learning, its proposed relationships require validation through empirical studies across different digital business contexts. Future research could examine whether firms with stronger alignment among the four pillars recover faster from cyber incidents, platform disruptions, or market shocks. Such work would extend digital transformation research by testing resilience as an outcome of integrated capability architecture rather than as a general adaptive orientation [4].

The second limitation is that the framework simplifies complex interactions among agility, dependence, risk, and learning. In practice, these pillars may conflict, because rapid strategic agility can increase platform dependence, stronger cybersecurity can slow experimentation, and learning routines can become bureaucratic if poorly designed. Future research should examine these trade-offs and identify conditions under which one pillar strengthens or weakens another. Research on digital platforms and ecosystem organizing suggests that such relationships may vary depending on platform governance, technical architecture, and the firm's position in the ecosystem [29].

The third limitation concerns contextual variation. The framework may operate differently across industries, firm sizes, regulatory regimes, and levels of digital maturity, because a financial services firm, a digital marketplace seller, a healthcare platform participant, and a manufacturing firm using cloud infrastructure face different resilience pressures. Future research should develop measurement instruments for the four pillars and test them through comparative case studies, surveys, and longitudinal research designs. This would also help clarify whether organizational learning moderates the relationship between disruption exposure and resilience outcomes, as suggested by research connecting learning, innovation, and resilience under environmental dynamism [22].

## Conclusion

This article proposed the Digital Business Resilience Framework as an original conceptual framework that

integrates strategic agility, platform dependence awareness, cyber risk management, and organizational learning. Its core contribution is to show that resilience in digital business cannot be explained by adaptability alone. Resilience emerges when firms combine speed, dependency awareness, protection, and learning into a coherent system.

The framework shifts digital resilience thinking away from isolated tools, defensive checklists, or generic agility narratives. It argues that digital businesses become resilient when they understand how strategic choices, platform architectures, cyber vulnerabilities, and learning routines interact. In this view, disruption is not only a threat to be survived but also a source of information that can improve future capability.

For researchers, the framework offers a basis for empirical testing, refinement, and measurement development. For managers, it provides a diagnostic and implementation lens for strengthening resilience across strategic, technological, and organizational domains. Digital business resilience should therefore be treated as a systemic, learning-centred

capability that must be designed before disruption, activated during disruption, and improved after disruption.

## Acknowledgements

None

## Conflict of interest

None

## Financial support

None

## Ethics statement

None

Received: 25 Nov 2024   Revised: 10 Jan 2025   Accepted: 20 Feb 2025  
Published online: 18 March 2025

## 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

- Vial G. Understanding digital transformation: A review and a research agenda. *Managing digital transformation*. London: Routledge; 2021. p. 13–66.
- Nambisan S, Wright M, Feldman M. The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Res policy*. 2019;48(8):103773.
- Warner KS, Wäger M. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Plann*. 2019;52(3):326–49.
- Verhoef PC, Broekhuizen T, Bart Y, Bhattacharya A, Dong JQ, Fabian N, et al. Digital transformation: A multidisciplinary reflection and research agenda. *J Bus Res*. 2021;122:889–901.
- Jacobides MG, Cennamo C, Gawer A. Towards a theory of ecosystems. *Strateg Manag 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.
- Duchek S. Organizational resilience: A capability-based conceptualization. *Bus Res*. 2020;13(1):215–46.

Linnenluecke MK. Resilience in business and management research: A review of influential publications and a research agenda. *Int J Manag Rev.* 2017;19(1):4-30.

Clauss T, Abebe M, Tangpong C, Hock M. Strategic agility, business model innovation, and firm performance: An empirical investigation. *IEEE Trans Eng Manag.* 2019;68(3):767-84.

McIntyre DP, Srinivasan A. Networks, platforms, and strategy: Emerging views and next steps. *Strateg Manag J.* 2017;38(1):141-60.

Parker G, Van Alstyne M, Jiang X. Platform ecosystems: How developers invert the firm1. *MIS Q.* 2017;41(1):255-66.

Bagheri S, Ridley G, Williams B. Organisational cyber resilience: Management perspectives. *Australas J Inf Syst.* 2023;27.  
<https://doi.org/10.3127/ajis.v27i0.4183>.

Strupczewski G. Defining cyber risk. *Saf Sci.* 2021;135:105143.

Foss NJ, Saebi T. Fifteen years of research on business model innovation: how far have we come, and where should we go?. *J Manag.* 2017;43(1):200-27.

Svahn F, Mathiassen L, Lindgren R. Embracing digital innovation in incumbent firms: How volvo cars managed competing concerns1. *MIS Q.* 2017;41(1):239-53.

Constantinides P, Henfridsson O, Parker GG. Introduction—platforms and infrastructures in the digital age. *Inf syst res.* 2018;29(2):381-400.

Gawer A. Digital platforms' boundaries: The interplay of firm scope, platform sides, and digital interfaces. *Long Range Plann.* 2021;54(5):102045.

Cutolo D, Kenney M. Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. *Acad Manag Perspect.* 2021;35(4):584-605.

Cennamo C. Competing in digital markets: A platform-based perspective. *Acad Manag Perspect.* 2021;35(2):265-91.

Saeed S, Altamimi SA, Alkayyal NA, Alshehri E, Alabbad DA. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors.* 2023;23(15):6666.

Conz E, Magnani G. A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. *Eur Manag J.* 2020;38(3):400-12.

Do H, Budhwar P, Shipton H, Nguyen HD, Nguyen B. Building organizational resilience, innovation through resource-based management initiatives, organizational learning and environmental dynamism. *J Bus Res.* 2022;141:808-21.

Nava L. Rise from ashes: A dynamic framework of organizational learning and resilience in disaster response. *Bus Soc Rev.* 2022;127:299-318.

Hinings B, Gegenhuber T, Greenwood R. Digital innovation and transformation: An institutional perspective. *Inf Organ.* 2018;28(1):52-61.

Steen R, Haug OJ, Patriarca R. Business continuity and resilience management: A conceptual framework. *J Conting Crisis Manag.* 2024;32(1):e12501.

Annarelli A, Battistella C, Nonino F. A framework to evaluate the effects of organizational resilience on service quality. *Sustainability.* 2020 ;12(3):958.

Nambisan S, Zahra SA, Luo Y. Global platforms and ecosystems. *J Int Bus Stud.* 2019;50(9):1464-86.

Durst S, Hinteregger C, Zieba M. The effect of environmental turbulence on cyber security risk management and organizational resilience. *Comput Secur.* 2024;137:103591.

Sandberg J, Holmström J, Lyytinen K. Digitization and phase transitions in platform organizing logics: Evidence from the process automation industry. *MIS Q.* 2020;44(1):129-54.