REVIEW **Open access**

Digital Business Resilience: A Critical Review of Organizational Agility, Data Governance, Cyber Risk, and Strategic Continuity

Burak Demir[1*], Elif Arslan[2], Mehmet Kaya[1], Selin Kurt[2]

Abstract

Digital disruption has become a persistent condition of contemporary business rather than an exceptional crisis event. Firms now confront cyber incidents, platform failures, data integrity problems, supply chain shocks, algorithmic dependencies, and rapid shifts in digital markets. These disruptions challenge not only operational continuity but also the strategic capacity of organizations to maintain direction, value creation, and stakeholder confidence. The literature on resilience has expanded significantly, yet digital business resilience remains conceptually fragmented. Studies of organizational agility, data governance, cybersecurity, digital transformation, and business continuity often develop in parallel rather than as an integrated body of work. This fragmentation limits the ability of scholars and managers to understand how digital resilience is actually produced across interconnected systems. This critical review examines digital business resilience through four interdependent pillars: organizational agility, data governance, cyber risk management, and strategic continuity. It argues that resilience should not be reduced to rapid response, technical recovery, or compliance-based continuity planning. Instead, digital business resilience is better understood as a systemic capability that enables firms to anticipate, absorb, respond to, recover from, and adapt to digitally mediated disruptions. The review concludes that digital business resilience emerges from alignment rather than from isolated investment in tools, controls, or agile routines. Organizations need governance architectures that connect adaptive responsiveness with reliable data, cyber preparedness, and strategic discipline. A critical and integrative perspective is therefore essential for future research and managerial practice.

Keywords Organizational agility, Data governance, Critical review, Digital business resilience, Cyber risk, Strategic continuity

*Correspondence:
Burak Demir
burak.demir@metu.edu.tr
[1] Department of Digital Business Management, Faculty of Economics, Middle East Technical University, Ankara, Turkey
[2] Department of E-Business and Analytics, Faculty of Business, Istanbul Technical University, Istanbul, Turkey

Introduction

Digital disruptions have intensified the managerial challenge of resilience because firms now depend on interconnected information systems, data infrastructures, algorithmic processes, digital platforms, and cyber-physical supply networks. Traditional resilience research has examined adversity, crisis response, and recovery as organizational capabilities, but digital disruption adds speed, opacity, interdependence, and systemic vulnerability to these established concerns [1]. Reviews of business and organizational resilience show that the concept has become influential, yet they also reveal persistent ambiguity over whether resilience is a capacity, process, outcome, or strategic orientation [2, 3]. This ambiguity becomes more problematic when disruption is digitally mediated and cannot be managed through conventional continuity planning alone.

Digital transformation research has clarified how firms use digital technologies to alter strategy, operations, structures, and value creation, but it often emphasises transformation

more than continuity under disruption [4]. Digital transformation is not simply the adoption of new tools; it changes organizational routines, decision rights, data dependencies, and competitive logics [5]. When these changes are treated as innovation or efficiency projects without resilience thinking, they may increase exposure to disruption even while improving responsiveness. This creates a central problem for digital business resilience: the same digital systems that enable flexibility, speed, and scale may also create fragility.

The literature remains fragmented across several partially connected streams. Organizational agility research examines rapid strategic response and IT-enabled flexibility [6], data governance research focuses on accountability, quality, access, and stewardship [7], and cybersecurity research analyses threats, intelligence, compliance, and incident response [8, 9]. Yet these streams rarely converge around the question of how firms maintain strategic continuity during digital shocks. As a result, resilience is often reduced either to agility, to cybersecurity preparedness, or to business continuity, rather than being treated as an integrated organizational logic.

This critical review addresses that gap by synthesising the literature on digital business resilience across four pillars: organizational agility, data governance, cyber risk management, and strategic continuity. The objective is not to present new empirical data but to interrogate how existing research explains, neglects, or misaligns these pillars. Critical reviews of resilience and digital transformation indicate that integrative theorisation is needed when organizational adaptation, technological change, and continuity pressures interact [10, 11]. The review therefore develops a conceptual foundation for understanding digital business resilience as an emergent property of connected managerial, informational, and security capabilities.

Digital Business Resilience Logic

Digital business resilience extends traditional resilience by locating disruption within digitally enabled systems of coordination, decision-making, value creation, and risk exposure. Earlier resilience research emphasises the capacity to respond to adversity and recover from shocks, but digital contexts require attention to how technological infrastructures shape both vulnerability and adaptation [1, 2]. A capability-based view defines resilience through anticipation, coping, and adaptation, which is especially relevant when firms must respond before digital failures become visible to customers, regulators, or ecosystem partners [10]. Digital resilience therefore cannot be separated from the systems through which organizations sense disruption, interpret signals, and reconfigure operations.

The logic of digital business resilience also differs from traditional business continuity planning. Continuity planning commonly focuses on maintaining critical operations after a disruption, whereas digital resilience requires continuous monitoring, rapid reconfiguration, trustworthy data, cyber preparedness, and strategic learning [12, 13]. Industry 4.0 and digital supply chain research shows that connected technologies can reduce blind spots but may also transmit risk across organizational boundaries more rapidly [14, 15]. This means resilience is not only about restoring a prior state; it is about sustaining strategic function while adapting to a changed digital environment.

Four pillars form the foundation of digital business resilience: organizational agility, data governance, cyber risk management, and strategic continuity. Agility enables sensing, seizing, and rapid response, but without governance it may become reactive or fragmented [6, 16]. Data governance provides the informational infrastructure needed for reliable decisions, while cyber risk management protects the systems and assets on which continuity depends [7, 8]. Strategic continuity integrates these pillars by ensuring that adaptive action remains aligned with core value propositions and long-term direction rather than degenerating into improvisational survival.

A critical issue is that the four pillars are mutually dependent rather than additive. Agile response requires trustworthy data, cyber preparedness requires coordinated decision-making, and strategic continuity requires both adaptive movement and operational discipline [17, 18]. Resilience is therefore weakened when firms invest in agility without governance, data without accountability, or cybersecurity without continuity integration. **Table 1** defines the core components and logic of digital business resilience.

Table 1. Digital Business Resilience Logic: Definitions, Core Components, and Foundational Principles

Core component	Definition in digital business resilience	Foundational principle	Crit impli
Anticipation	The ability to detect emerging digital threats, vulnerabilities, and strategic discontinuities before they escalate	Resilience begins before disruption becomes visible	Firms sen systen integ opera cyber, d market
Response	The ability to mobilise decisions, resources, and routines rapidly during digital disruption	Speed must be coordinated rather than improvised	Agility governa gene confus dupli act
Recovery	The ability to restore critical digital operations, information access, and stakeholder confidence	Recovery depends on prepared infrastructures	Data ir cyber i respon conti plannir be con
Adaptation	The ability to learn from disruption and reconfigure routines, systems, and strategies	Resilience is developmental, not merely restorative	Firms instituti learnin than s return cri opera
Organizational agility	Strategic and operational responsiveness enabled by dynamic capabilities and digital systems	Flexibility must be disciplined	Ag contrib resilien when a with st prio
Data governance	Structures and responsibilities ensuring data quality, availability, lineage, and stewardship	Data is resilience infrastructure	Po gover under situa awaren deci relia
Cyber risk management	Identification, prevention, response, and recovery from digital security threats	Security is a continuity condition	Cybers mus integra busi continu strat deci mal
Strategic continuity	Preservation of strategic direction, value propositions, and critical capabilities during disruption	Continuity is more than operational survival	Resil should fut competi as w imme functi

Figure 1 presents the integrated logic of digital business resilience as the alignment of agility, data governance, cyber risk management, and strategic continuity.

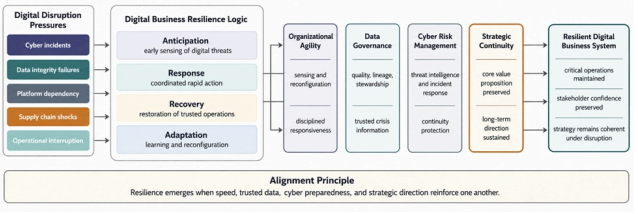

Figure 1. Integrated Digital Business Resilience Framework Linking Organizational Agility, Data Governance, Cyber Risk Management, and Strategic Continuity

Organizational Agility and Strategic Response

Organizational agility is central to digital business resilience because digital disruptions often demand rapid sensing, interpretation, and coordinated response. IT-enabled agility research shows that information systems can support responsiveness by improving visibility, decision speed, and resource reconfiguration [6]. Dynamic capability research similarly frames digital transformation as an ongoing process of strategic renewal rather than a discrete technology implementation [16]. In resilience terms, agility

matters because it allows firms to avoid rigid dependence on pre-disruption routines.

Strategic agility contributes to resilience through sensing market or operational shifts, seizing opportunities for response, and transforming structures when existing arrangements no longer fit the environment. Research on digital strategizing highlights that firms must overcome cognitive barriers, reconfigure routines, and develop new organizational forms to operate effectively in digital environments [19]. Studies of business model innovation also show that agility can strengthen performance when firms adapt their value creation and delivery mechanisms under uncertainty [20]. However, agility is not automatically resilient if rapid action produces incoherent priorities or undermines organizational stability.

The critical limitation of agility is that it can become a managerial ideology of speed. Digital transformation literature often celebrates responsiveness, experimentation, and fluid structures, but excessive emphasis on adaptation may weaken accountability, continuity, and learning [4, 18]. Crisis-driven digital transformation among smaller firms shows that resilience may emerge as a second-order dynamic capability, yet this also depends on ecosystem support, managerial interpretation, and accumulated organizational experience [21]. Agility therefore contributes to resilience only when it is embedded in a broader system of data reliability, cyber preparedness, and strategic discipline.

A resilient organization must balance adaptive movement with stabilising mechanisms. Digital transformation is most consequential when it changes coordination, governance, routines, and strategic assumptions, not merely when it introduces new technological tools [17, 22]. Agility should therefore be treated as one pillar of resilience rather than as a substitute for resilience itself. **Table 2** synthesises the role of organizational agility in enabling strategic response to digital disruptions.

Table 2. Organizational Agility and Strategic Response: Types, Enablers, and Contributions to Digital Resilience

Type of agility	Main enablers	Contribution to digital resilience	Critica limitati
Strategic agility	Dynamic capabilities, strategic sensing, leadership attention, flexible business models	Enables firms to redirect priorities during digital disruption while preserving long-term orientation	May bec opportuni disconne from conti and governa
Operational agility	Modular processes, cross-functional coordination, rapid resource redeployment, digital workflow visibility	Supports fast response and restoration of critical activities	May proc local optimisa withou enterprise coherer
IT-enabled agility	Integrated platforms, analytics, interoperable systems, real-time information access	Improves speed and quality of response through digital visibility	Can incre dependen fragile poorly govern systen
Ecosystem agility	Partner coordination, supply chain visibility, platform relationships, shared standards	Extends resilience beyond firm boundaries	May exp firms t external c data, a continuity
Learning agility	Post-disruption review, experimentation, knowledge retention, adaptive routines	Converts disruption experience into future resilience capability	Learning remai episodic i institutiona
Governance-enabled agility	Decision rights, escalation protocols, accountable roles, resilience leadership	Balances speed with discipline and accountability	Excess control r slow resp and redu adapti capaci

Data Governance as Resilience Infrastructure

Data governance should be understood as resilience infrastructure rather than merely as a compliance, reporting, or administrative function. In digitally dependent organizations, resilience requires that decision-makers can access reliable, timely, interpretable, and accountable data during disruption. A conceptual review of data governance shows that governance arrangements define roles, responsibilities, standards, and decision rights for data assets, making them foundational to organizational coordination [7]. When disruption occurs, weak data governance can turn uncertainty into paralysis because managers cannot distinguish reliable signals from incomplete, duplicated, or corrupted information.

Data quality, accessibility, lineage, and stewardship are especially important during digital shocks because resilience depends on situational awareness. Data governance activities connect technical data management with organizational accountability, ensuring that data is not only stored but also usable for coordinated action [23]. Collective-action perspectives further show that data governance fails when responsibilities are dispersed but no actor has sufficient authority or incentive to maintain shared data quality [24]. In resilience terms, such failures create hidden fragility because firms may appear digitally mature while lacking the informational discipline needed for crisis response.

The rise of analytics and artificial intelligence strengthens the resilience value of governance but also increases the cost of governance failure. Data governance for trustworthy artificial intelligence requires attention to data provenance, accountability, transparency, and institutional arrangements that support responsible use [25]. Big data analytics capability research shows that firms derive value when data resources are combined with managerial, technical, and organizational capabilities [26]. However, resilience requires more than analytic sophistication; it requires assurance that the data informing decisions remains accurate, available, and secure during disruption.

Data governance also connects directly to strategic continuity because digital firms increasingly rely on data to coordinate operations, serve customers, comply with obligations, and adapt strategy. Big data analytics can improve firm performance when embedded in dynamic capabilities, but performance benefits do not automatically imply resilience [27]. Strategic value from analytics depends on business alignment, governance, and the ability to convert data into decision-relevant insight [28]. Thus, data governance functions as a stabilising layer that allows agility and cyber response to operate on trustworthy informational foundations.

Cyber Risk and Business Continuity

Cyber risk is a central challenge for digital business resilience because cyber incidents can simultaneously disrupt operations, compromise data, damage trust, and interrupt strategic execution. Research on technical threat intelligence shows that cyber attacks have become more sophisticated, requiring organizations to move beyond perimeter defence toward continuous intelligence, monitoring, and adaptive response [8]. Cyber threat intelligence sharing can improve preparedness, but it also requires governance arrangements that determine what information is shared, how it is interpreted, and how it informs action [9]. This makes cyber resilience an organizational and strategic issue, not only a technical security problem.

The integration of cybersecurity with business continuity remains underdeveloped in much of the literature. Cyber-threat intelligence can support security decision-making, but its practical value depends on whether intelligence is translated into prioritised organizational action [29]. Studies of financial institutions show that cyber-resilience requires the ability to maintain critical functions and confidence even when digital systems are compromised [30]. If incident response teams and continuity planners operate separately, firms may contain technical threats without sustaining business processes, or restore operations without addressing underlying vulnerabilities.

Cyber risk also exposes a tension between preventive security and operational flexibility. Security controls can reduce exposure, but excessive control may slow response, constrain experimentation, and weaken the agility required during disruption. Research on information security policy compliance shows that individual behaviour, organizational context, and policy design all shape security outcomes [31]. This implies that resilience depends not only on security technologies but also on human adherence, managerial incentives, and routines that connect security discipline with operational continuity.

Cyber risk should therefore be analysed through both threat type and continuity implication. The practical question is not only whether a firm can prevent cyber incidents, but whether it can preserve critical operations, data integrity, stakeholder trust, and strategic direction when incidents occur. The tensions of cyber-resilience research show that organizations often struggle to move from abstract sensemaking to embedded practice [32]. **Table 3** maps cyber risk dimensions and their implications for business continuity and resilience.

Table 3. Cyber Risk Landscape and Business Continuity: Threat Types, Vulnerabilities, and Resilience Implications

Cyber risk dimension	Typical vulnerability	Business continuity implication	Resilienc implicati
Ransomware	Inadequate backups, weak access controls, delayed detection	Critical systems may become unavailable, halting operations and customer service	Resilienc requires recovery protocols backup integrity, a decisior escalatio
Data breach	Poor data classification, weak governance, excessive access privileges	Sensitive data exposure can trigger regulatory, reputational, and operational consequences	Resilienc depends data stewardsh incident communica and trust re
Supply chain attack	Dependence on third-party platforms, software, vendors, or digital partners	Disruption may originate outside the firm but cascade into internal operations	Resilienc must exte beyond fi boundarie through ecosystem governan
Insider threat	Weak monitoring, poor role definition, low security culture	Continuity may be undermined by trusted actors or compromised credentials	Resilienc requires behaviou controls access governanc
Denial-of-service attack	Limited redundancy, weak traffic filtering, poor infrastructure scalability	Customer-facing services and digital channels may become unavailable	Resilienc depends infrastructu redundan and rapi service restoratic
Data corruption	Inadequate validation, poor lineage, compromised systems	Decision-making may continue using inaccurate or manipulated data	Resilienc requires d integrity che and truste recovery pc
Policy non-compliance	Misaligned incentives, complex rules, low employee engagement	Security routines may fail during normal operations or crises	Resilienc requires us policies training, a organizatic reinforcem
Incident-response fragmentation	Separation between technical response and continuity planning	Technical containment may not protect critical business functions	Resilienc requires integrate cyber-contir governan

Strategic Continuity Under Digital Disruption

Strategic continuity refers to the ability to maintain strategic direction, core value propositions, stakeholder confidence, and critical capabilities during disruption. It differs from operational continuity because it concerns what the organization continues to be and pursue, not merely which processes continue to function. Resilience research emphasises adaptation and recovery, but digital contexts require a stronger focus on sustaining strategic coherence when technologies, markets, data systems, and security conditions shift simultaneously [10, 12]. Without this perspective, firms may survive a disruption operationally while losing strategic focus.

The three preceding pillars collectively enable strategic continuity. Organizational agility allows rapid response and

reconfiguration, data governance provides reliable information for decision-making, and cyber risk management protects the digital assets and systems on which the business depends [6, 7, 30]. Digital transformation research shows that firms must continually renew structures and routines to remain viable in changing environments [16]. Strategic continuity depends on ensuring that this renewal does not dissolve the strategic commitments, customer value propositions, and organizational capabilities that define competitive identity.

When one pillar is absent or misaligned, resilience becomes partial. A firm with strong agility but weak data governance may respond quickly using unreliable information, while a firm with strong cybersecurity but low agility may preserve systems without adapting to market shifts [23, 31]. Similarly, extensive analytics capability can improve performance, yet without continuity logic it may optimise short-term decisions rather than protect long-term strategic direction [27, 28]. Strategic continuity therefore requires alignment across speed, information, security, and purpose.

Digital business resilience also has an ecosystem dimension because many firms depend on suppliers, platforms, cloud providers, software vendors, and data-sharing partners. Research on ripple effects and Industry 4.0 shows that digital technologies can both improve visibility and amplify interdependence across supply networks [14]. Supply chain resilience studies under digital and pandemic conditions further show that technological capabilities must be connected to organizational and interorganizational resilience practices [15]. Strategic continuity under digital disruption therefore cannot be secured inside the firm alone; it requires attention to the broader digital ecosystem through which value is created and disrupted.

Critical Research Gaps

The first major gap is the absence of integrative models that connect agility, data governance, cyber risk, and strategic continuity. Existing resilience reviews identify conceptual diversity and fragmentation, but they rarely specify how digital infrastructures alter the relationships among response, recovery, adaptation, and strategic preservation [2, 3]. Digital transformation reviews similarly offer broad research agendas, yet resilience often appears as an implied benefit rather than as a central organizing construct [4, 11]. This leaves scholars without a coherent framework for explaining why some digitally advanced firms remain fragile while others sustain continuity under disruption.

A second gap concerns the overemphasis on capabilities without sufficient attention to trade-offs. Agility research highlights responsiveness and dynamic reconfiguration, but less attention is given to the possibility that speed can undermine governance, coordination, and accountability [6, 19]. Cybersecurity research emphasises controls, compliance, and intelligence, but it has not fully resolved how firms should balance security discipline with operational flexibility [29, 31]. Data governance research likewise recognises accountability and stewardship, but it often remains separated from crisis response, cyber recovery, and strategic continuity [7, 24].

A third gap involves context, scale, and human dynamics. Crisis-driven digital transformation research indicates that small and medium-sized enterprises may develop resilience differently from large firms because they face distinct resource constraints, ecosystem dependencies, and managerial pressures [21]. However, much digital resilience thinking still assumes that firms possess sufficient resources to invest simultaneously in agility, analytics, governance, and cybersecurity. Human and cultural dimensions are also underdeveloped, even though security compliance, data stewardship, and agile response all depend on behaviour, interpretation, trust, and organizational routines [25, 32].

A fourth gap is methodological and temporal. Many studies examine digital transformation, analytics, or resilience as capability states, but fewer trace how resilience develops, erodes, or becomes institutionalised over time [16, 18]. The literature needs longitudinal and configurational research that examines how combinations of agility, governance, security, and continuity produce different resilience outcomes across industries. **Table 4** consolidates critical research gaps and proposes an integrated research agenda.

Table 4. Critical Gaps in Digital Business Resilience Research: Fragmentation, Neglected Themes, and Integrated Research Directions

Critical gap	How the gap appears in current research	Why it matters for digital business resilience	Inte res dir
Fragmented treatment of resilience pillars	Agility, data governance, cybersecurity, and continuity are often studied separately	Fragmentation obscures how resilience emerges from interdependence	De inte mode ad infor secu str co cap
Overemphasis on agility as speed	Agility is often treated as inherently beneficial	Excessive speed can weaken coordination, governance, and strategic discipline	Stu cor und a stren und res
Underdeveloped data-governance resilience logic	Data governance is often framed as compliance or data management	Resilience requires trustworthy information during disruption	Exan q lir stew avail c res cap
Weak integration of cyber risk and continuity	Cybersecurity and business continuity are frequently treated as separate domains	Technical containment does not guarantee operational or strategic continuity	Ar c co gov mod inci re de pa
Limited SME and resource-constrained contexts	Research often assumes access to advanced systems and capabilities	Smaller firms face distinctive resilience constraints and ecosystem dependencies	Co com studi firr sec digita
Neglect of human and cultural dimensions	Security, data, and agility are sometimes treated as technical or structural problems	Resilience depends on behaviour, trust, compliance, interpretation, and routines	Int cu lea em beh and into res m
Lack of longitudinal evidence	Resilience is often studied at a single point in time	Resilience evolves through disruption experience, learning, and institutionalisation	long des t res ca deve and
Insufficient attention to trade-offs	Literature often treats resilience capabilities as mutually reinforcing	Agility, control, security, and continuity may conflict in practice	I confi and or the c bu res

Figure 2 translates the critical gaps in digital business resilience research into an integrated future research and managerial agenda.

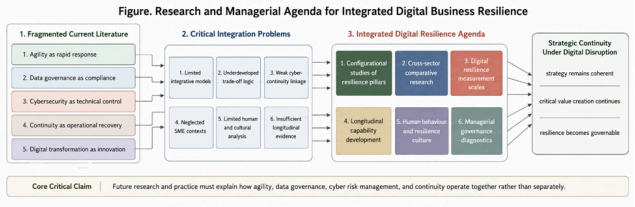

Figure 2. From Fragmented Resilience Research to an Integrated Digital Business Resilience Agenda

Future Research and Managerial Implications

Future research should move from pillar-specific analysis toward configurational explanations of digital business resilience. Scholars should examine how different combinations of agility, data governance, cyber risk management, and continuity planning produce resilience under varying conditions [3, 6]. Configurational studies

would help explain why some firms benefit from high agility while others require stronger stabilising governance before agility becomes useful [19, 20]. This agenda would also connect resilience research with digital transformation scholarship by treating resilience as an outcome of systemic alignment rather than as a background assumption [5, 18].

The development of measurement tools is another priority. Existing work on resilience, analytics capability, and data governance offers useful conceptual foundations, but digital business resilience requires measures that capture cross-pillar alignment [7, 10, 26]. Such measures should assess not only response speed or recovery time but also data reliability, cyber preparedness, decision accountability, ecosystem exposure, and strategic continuity. Cross-sector comparative studies would be especially useful because digital disruption differs across finance, manufacturing, retail, public services, and platform-dependent businesses [14, 30].

For managers, the central implication is that resilience cannot be delegated to a single function. A practical diagnostic model should assess whether the organization has adaptive capacity, trustworthy data, cyber-continuity integration, and a clear strategic continuity logic [13, 28, 32]. Senior leaders should create governance forums where digital transformation, data stewardship, cybersecurity, risk, operations, and strategy are examined together rather than in separate reporting channels. The managerial goal is not to maximise agility, control, or security independently, but to design a resilience system in which these elements reinforce rather than undermine one another.

Conclusion

Digital business resilience is not a single capability, a technology investment, or a continuity checklist. It is an emergent property of an integrated system in which organizational agility, data governance, and cyber risk management collectively support strategic continuity. This perspective shifts resilience thinking from recovery after disruption toward the sustained capacity to preserve strategic direction while adapting under digital uncertainty.

The review has argued that fragmented treatment of resilience pillars limits both scholarship and practice. Agility without governance can become disorderly, data without stewardship can become unreliable, cybersecurity without continuity integration can become narrow, and continuity without adaptation can become rigidity. A critical review of digital business resilience must therefore focus on alignment, interdependence, and trade-offs.

Future research and managerial practice should treat digital business resilience as a strategic design problem. Firms need structures, routines, and governance mechanisms that connect speed with discipline, data with accountability, security with continuity, and adaptation with strategic purpose. Such an integrated paradigm is essential for organizations seeking not only to survive digital disruption but to sustain value creation through it.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 20 Nov 2024 Revised: 05 Jan 2025 Accepted: 15 Feb 2025
Published online: 18 March 2025

References

Williams TA, Gruber DA, Sutcliffe KM, Shepherd DA, Zhao EY. Organizational response to adversity: Fusing crisis management and resilience research streams. Acad Manag Annal. 2017;11(2):733-69.

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.

Hillmann J, Guenther E. Organizational resilience: a valuable construct for management research?. Int J Manag Rev. 2021;23(1):7-44.

Vial G. Understanding digital transformation: A review and a research agenda. Managing digital transformation.London: Routledge; 2021. p. 13–66.

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.

Tallon PP, Queiroz M, Coltman T, Sharma R. Information technology and the search for organizational agility: A systematic review with future research possibilities. J Strateg Inf Syst. 2019;28(2):218-37.

Abraham R, Schneider J, Vom Brocke J. Data governance: A conceptual framework, structured review, and research agenda. Int J Inf Manag. 2019;49:424-38.

Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur. 2018;72:212-33.

Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Comput Secur. 2019;87:101589.

Duchek S. Organizational resilience: A capability-based conceptualization. Bus Res. 2020;13(1):215-46.

Plekhanov D, Franke H, Netland TH. Digital transformation: A review and research agenda. Eur Manag J. 2023;41(6):821-44.

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.

Sahebjamnia N, Torabi SA, Mansouri SA. Building organizational resilience in the face of multiple disruptions. Int J Prod Econ. 2018;197:63-83.

Ivanov D, Dolgui A, Sokolov B. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Int J Prod Res. 2019;57(3):829-46.

Spieske A, Birkel H. Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic. Comput Ind Eng. 2021;158:107452.

Warner KS, Wäger M. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. Long Range Plann. 2019;52(3):326-49.

Wessel LK, Baiyere A, Ologeanu-Taddei R, Cha J, Jensen TB. Unpacking the difference between digital transformation and IT-enabled organizational transformation. J Assoc Inf Syst. 2021;22(1):102-29.

Hanelt A, Bohnsack R, Marz D, Antunes Marante C. A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. J Manag Stud. 2021;58(5):1159-97.

Volberda HW, Khanagha S, Baden-Fuller C, Mihalache OR, Birkinshaw J. Strategizing in a digital world: Overcoming cognitive barriers, reconfiguring routines and introducing new organizational forms. Long Range Plann. 2021;54(5):102110.

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.

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.

Gong C, Ribiere V. Developing a unified definition of digital transformation. Technovation. 2021;102:102217.

Alhassan I, Sammon D, Daly M. Data governance activities: A comparison between scientific and practice-oriented literature. J Enterp Inf Manag. 2018;31(2):300-16.

Benfeldt O, Persson JS, Madsen S. Data governance as a collective action problem. Inf Syst Front. 2020;22(2):299-313.

Janssen M, Brous P, Estevez E, Barbosa LS, Janowski T. Data governance: Organizing data for trustworthy artificial intelligence. Gov Inf Q. 2020;37(3):101493.

Mikalef P, Pappas IO, Krogstie J, Giannakos M. Big data analytics capabilities: a systematic literature review and research agenda. Inf Syst E-Bus Manag. 2018;16(3):547-78.

Wamba SF, Gunasekaran A, Akter S, Ren SJ, Dubey R, Childe SJ. Big data analytics and firm performance: Effects of dynamic capabilities. J Bus Res. 2017;70:356-65.

Grover V, Chiang RH, Liang TP, Zhang D. Creating strategic business value from big data analytics: A research framework. J Manag Inf Syst. 2018;35(2):388-423.

Ainslie S, Thompson D, Maynard S, Ahmad A. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Comput Secur. 2023;132:103352.

Dupont B. The cyber-resilience of financial institutions: Significance and applicability. J Cybersecur. 2019;5(1):tyz013.

Cram WA, D'arcy J, Proudfoot JG. Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance1. MIS Q. 2019;43(2):525-53.

Dupont B, Shearing C, Bernier M, Leukfeldt R. The tensions of cyber-resilience: From sensemaking to practice. Comput Secur. 2023;132:103372.