AB Journals

British Journal of Computer, Networking and Information Technology

ISSN 2689-5315 • Volume 9, Issue 3, 2026 • pp. 40–59

RESEARCH ARTICLE Received: 1 Sep 2026, Accepted: 26 Oct 2026, Published: 12 Nov 2026

Corporate Crisis and Disaster Management in the Digital Era: Building Organisational Resilience through Digital Transformation

Aderombi Adeyemi

Business Lecturer, Icon College of Technology and Management, Unit 21, 1-13 Adler Street, London, E1 1EG, United Kingdom.

Email: adeyemi.aderombi@outlook.com

Abstract

Corporate crises are increasingly shaped by interconnected digital infrastructures, global supply chains, cloud services, artificial intelligence and data-intensive business models. This conceptual article examines how digital transformation is changing the character and management of corporate crises. It develops an integrated Digital Crisis Resilience Framework (DCRF). Drawing on crisis management, organisational resilience, dynamic capabilities, stakeholder and socio-technical systems theories, the article conceptualises resilience as a continuous strategic capability rather than a reactive emergency function. The DCRF integrates eight capabilities across the crisis lifecycle. Comparative analysis of the NotPetya/Maersk, SolarWinds, COVID-19, Colonial Pipeline and CrowdStrike cases illuminates the Digital Resilience Paradox: digitalisation can simultaneously strengthen adaptive capacity and increase systemic vulnerability. A five-level Digital Crisis Resilience Maturity Model, research propositions and an implementation roadmap are proposed. The article contributes by integrating fragmented research streams and extending crisis resilience from the firm level to the wider digital ecosystem.

Keywords: Corporate Crisis Management, Organisational Resilience, Digital Transformation, Cybersecurity, Digital Ecosystem Resilience

How to Cite: Adeyemi, A. (2026). Corporate Crisis and Disaster Management in the Digital Era: Building Organisational Resilience through Digital Transformation. British Journal of Computer, Networking and Information Technology, 9(3), 40–59. https://doi.org/10.52589/BJCNIT-CIDUVK

© 2026 by the authors. Published by AB Journals. This is an open access article distributed under the terms of the Creative Commons Attribution (CC BY 4.0) license.

INTRODUCTION

The increasing levels of digitalisation have altered the speed, scale and interconnectedness of corporate crises (Williams et al., 2017; Aderombi, 2020). Organisations increasingly depend on cloud infrastructure, artificial intelligence (AI), platform ecosystems, third-party technology providers, globally distributed supply chains and social media. These technologies create major opportunities for efficiency and innovation, but they also expose firms to cyberattacks, ransomware, software failures, misinformation, data breaches, supply-chain interruptions, pandemics, geopolitical shocks and climate-related disruption that can propagate rapidly across organisational and national boundaries (Ivanov & Dolgui, 2020; Khurana et al., 2022).

Traditional crisis management scholarship conceptualises crises as low-probability, high-impact events requiring preparation, containment, response, recovery and learning (Pearson & Mitroff, 1993; Pearson & Clair, 1998; Boin et al., 2017). Crisis communication research further shows that stakeholder attribution and organisational response influence reputational outcomes (Coombs, 2007, 2015; Coombs & Holladay, 2012; Jin et al., 2014). In digitally dependent organisations, however, crisis management must be embedded within strategy, governance, technology, culture, stakeholder relationships and continuous learning (Williams et al., 2017; Conz & Magnani, 2020).

Organisational resilience research has correspondingly moved beyond a narrow focus on recovery towards anticipation, coping, adaptation and renewal (Lengnick-Hall et al., 2011; Linnenluecke, 2017; Duchek, 2020; Conz & Magnani, 2020). Digital transformation can strengthen these capabilities through automation, virtual collaboration, real-time monitoring, data-driven decision-making, cloud-enabled continuity and predictive analytics (Vial, 2019; Verhoef et al., 2021; Browder et al., 2024; Awad & Martín-Rojas, 2024; Li et al., 2025). Recent empirical evidence further confirms that digital transformation enhances organisational resilience and supports the persistence of superior performance during periods of adversity and crisis (Li, Du, Liu & Su, 2025; Wang & Jia, 2025). Yet crisis management, digital transformation, resilience, AI governance, cybersecurity, stakeholder engagement and business continuity remain comparatively fragmented research streams (Williams et al., 2017; Tarigan et al., 2025).

This article addresses that fragmentation by developing the Digital Crisis Resilience Framework (DCRF), a theory-building model explaining how digitally enabled capabilities can strengthen resilience across the crisis lifecycle while also creating new systemic dependencies. It further proposes a Digital Crisis Resilience Maturity Model (DCRMM), research propositions and an agenda for future empirical validation.

The remainder of the article is organised as follows. Section 2 reviews and synthesises the relevant literature and identifies research gaps. Section 3 presents the theoretical foundations. Section 4 examines contemporary digital risks and enabling technologies. Section 5 develops the Digital Crisis Resilience Framework and associated research propositions. Section 6 presents a comparative analysis of five major crises. Section 7 outlines methodological positioning and future empirical validation. Section 8 discusses practical application and the maturity model. Section 9 elaborates theoretical contribution and the Digital Resilience Paradox. Section 10 sets out limitations and future research directions. Section 11 presents managerial and policy implications. Section 12 concludes.

LITERATURE REVIEW

Evolution of Corporate Crisis Management

Corporate crisis management has evolved from a predominantly reactive operational discipline into a strategic organisational capability. Earlier scholarship emphasised prevention, preparedness, response, containment and recovery (Pearson & Mitroff, 1993; Pearson & Clair, 1998; Mitroff, 2005). These contributions remain foundational, but contemporary crises frequently develop through interconnected digital and organisational systems and therefore resist simple linear treatment.

Situational Crisis Communication Theory emphasises the relationship between crisis responsibility, stakeholder attribution and appropriate response strategies (Coombs & Holladay, 2002; Coombs, 2007). The increasing prevalence of social media has transformed crisis communication by increasing the speed, visibility and participatory character of stakeholder reactions (Austin et al., 2012; Jin et al., 2014). Crisis management in the digital era therefore requires continuous monitoring and engagement rather than communication confined to the acute crisis period.

Organisational Resilience

Organisational resilience explains why some organisations maintain functioning, adapt and renew themselves under adversity while others experience prolonged decline. Resilience has been conceptualised as a multidimensional capability involving anticipation, coping, adaptation, learning and transformation (Bhamra et al., 2011; Linnenluecke, 2017; Duchek, 2020). Weick and Sutcliffe (2015) highlight organisational mindfulness and sensitivity to weak signals, while Lengnick-Hall et al. (2011) emphasise cognitive, behavioural and contextual capacities.

Recent research has increasingly confirmed the connection between resilience and digital capability. Digital tools support virtual access, data-driven decisions, collaboration and adaptation during disruption (Browder et al., 2024). Digital transformation also strengthens resilience and supports innovation and organisational learning (Awad & Martín-Rojas, 2024; Li et al., 2025; Wang & Jia, 2025).

Digital Transformation as a Strategic Resilience Capability

Digital transformation goes beyond the adoption of new information technology. It involves changes to organisational structures, capabilities, value creation, processes and business models (Vial, 2019; Verhoef et al., 2021). An effective digital business strategy integrates information technology with corporate strategy, making digital capability essential to organisational competitiveness (Bharadwaj et al., 2013).

Organisational resilience and flexibility are enhanced during disruption through the deployment of cloud computing, digital collaboration, automation, analytics and digitally enabled operating models. The COVID-19 crisis demonstrated how digital transformation could accelerate under pressure and enable remote work, digital customer interfaces and organisational reconfiguration (Fletcher & Griffiths, 2020; Papadopoulos et al., 2020).

Artificial Intelligence, Cybersecurity and Digital Governance

AI capabilities enhance crisis management through predictive analytics, anomaly detection,

decision support, resource allocation and scenario modelling. However, increasing AI deployment creates governance challenges involving bias, privacy, accountability, misinformation, explainability and cyber risk. Responsible deployment of AI therefore requires governance mechanisms that combine technical controls with organisational accountability (Gasser & Almeida, 2017; Jobin et al., 2019; NIST, 2023).

Cybersecurity is inseparable from business resilience. The NIST Cybersecurity Framework 2.0 underscores the importance of governance alongside identification, protection, detection, response and recovery (NIST, 2024). Cyber risk should therefore be governed at the enterprise level rather than restricted solely to an information technology function.

Dynamic Capabilities and Organisational Adaptation

Dynamic capabilities theory offers an important strategic mechanism for understanding resilience. Firms require capabilities to sense environmental change, seize opportunities and transform resources and organisational arrangements (Teece, 2007; Teece et al., 2016). Digital risk intelligence can strengthen sensing; cloud infrastructure, automation and collaboration technologies can improve seizing; and continuous organisational learning can support transformation. Dynamic capabilities therefore provide a theoretical bridge between digital transformation and organisational resilience.

Stakeholder Trust and Business Continuity

Operational recovery alone does not constitute successful crisis recovery. Customers, employees, regulators, investors, suppliers and communities evaluate organisational competence, transparency, responsibility and responsiveness. Stakeholder theory therefore complements crisis communication theory by recognising trust and legitimacy as strategic organisational resources (Freeman, 1984).

Business continuity management provides the formal mechanisms for maintaining and restoring critical activities. Contemporary supply-chain research demonstrates the importance of visibility, redundancy, survivability and digital twins for disruption management (ISO, 2019; Ivanov & Dolgui, 2020, 2021). Digital resilience therefore extends beyond internal systems to encompass suppliers, platforms, cloud providers and the wider ecosystem.

Research Gap

Four gaps emerge from the literature. First, crisis management, organisational resilience, digital transformation, AI governance, cybersecurity and stakeholder management have remained fragmented research streams. Second, digital transformation is generally examined as a source of efficiency, innovation and competitiveness rather than explicitly as a resilience capability. Third, established crisis frameworks have not fully incorporated recent developments in generative and agentic AI, cloud dependency, digital ecosystems and systemic technology breakdowns. Fourth, relatively few conceptual models have integrated digital capabilities, governance, business continuity, stakeholder trust, learning and strategic transformation across the entire crisis lifecycle. The DCRF is developed to address these gaps.

THEORETICAL FOUNDATIONS

The primary theoretical approaches adopted in this study are organisational resilience theory and dynamic capabilities theory. These are complemented by stakeholder theory and socio-technical systems theory. The DCRF integrates these perspectives because digitally enabled crises are simultaneously technological, organisational, strategic and social. No single theory can sufficiently explain how organisations detect emerging risks, mobilise digital resources, sustain operations, preserve stakeholder trust, learn from disruption and subsequently transform.

Table 1 summarises the principal theoretical perspectives informing the DCRF and their specific contributions to the framework.

Table 1: Theoretical foundations of the Digital Crisis Resilience Framework (DCRF)

Theoretical perspective	Principal contribution to the DCRF
Crisis Management Theory	Preparedness, response, recovery and crisis lifecycle orientation.
Organisational Resilience Theory	Anticipation, coping, adaptation, learning and strategic renewal.
Dynamic Capabilities Theory	Sensing, seizing and transforming under conditions of uncertainty.
Stakeholder Theory	Trust, legitimacy, accountability and multi-stakeholder relationships.
Socio-Technical Systems Theory	Interdependence of people, technology, processes, culture and governance.

Note: The table integrates complementary theoretical lenses that underwrite the eight DCRF capabilities. Source: Author, synthesised from the literature (2026).

Digital Risks and Technologies in Contemporary Organisations

The defining feature of contemporary digital risk is interdependence. Disruption may originate within the focal organisation or in a supplier, platform, cloud provider, critical-infrastructure operator or wider social system. Relevant exposures include cyberattack and ransomware, cloud and third-party failures, AI errors and governance failures, misinformation, software-supply-chain compromise, operational-technology vulnerabilities, geopolitical disruption, climate-related shocks and pandemics. Resilience therefore increasingly requires ecosystem-level awareness rather than a purely firm-centric risk perspective.

Table 2 outlines key digital technologies and their potential contributions to crisis management and organisational resilience.

Table 2: Digital technologies supporting crisis management and organisational resilience

Technology	Resilience contribution
Artificial intelligence and machine learning	Prediction, anomaly detection, decision support and resource optimisation.
Big data analytics	Situational awareness, trend identification and risk intelligence.
Cloud computing	Remote operations, redundancy, scalable

	infrastructure and recovery.
Internet of Things (IoT)	Real-time monitoring of assets, environments and operational conditions.
Digital twins	Simulation, scenario testing, predictive maintenance and supply-chain modelling.
Automation and RPA	Rapid execution of repetitive response and recovery processes.
Knowledge management systems	Institutional learning and dissemination of lessons learned.
Digital communication platforms	Cross-functional coordination and continuous stakeholder engagement.

Note: Technologies are illustrative rather than exhaustive; their resilience value depends on governance, integration and organisational capability. Source: Author (2026).

Digital Crisis Resilience Framework (DCRF)

The DCRF is built on six pivotal assumptions: crises cannot be eliminated completely; digital transformation creates both resilience opportunities and systemic vulnerabilities; resilience is dynamic; crisis management is a strategic governance responsibility; stakeholder trust is integral to recovery; and organisational learning converts disruption into future capability and strategic renewal (Duchek, 2020; Teece et al., 2016; Williams et al., 2017).

The framework comprises eight interdependent capabilities: (1) Environmental scanning; (2) Digital risk intelligence; (3) Preparedness and capability development; (4) Rapid digital response; (5) Business continuity and recovery; (6) Stakeholder engagement; (7) Organisational learning; and (8) Strategic transformation.

Figure 1 presents the Digital Crisis Resilience Framework. Table 3 contrasts the traditional crisis-management paradigm with the DCRF orientation.

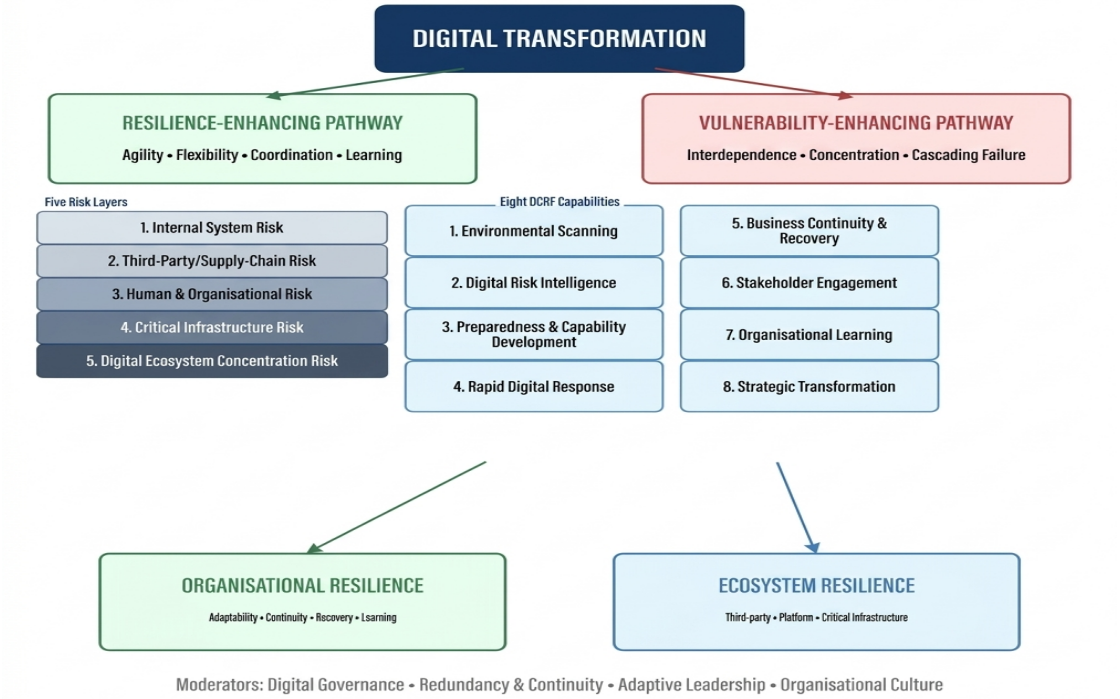


Figure 1: Digital Crisis Resilience Framework (DCRF): the Digital Resilience Paradox, five risk layers, eight resilience capabilities and pathways to organisational and ecosystem resilience

Note: The framework shows how digital transformation simultaneously creates resilience opportunities and systemic vulnerabilities (the Digital Resilience Paradox). The eight capabilities operate as a continuous cycle, moderated by governance, redundancy, leadership and culture. Source: Author-generated (2026).

Table 3: Comparison of traditional crisis management and the Digital Crisis Resilience Framework

Traditional crisis management	Digital Crisis Resilience Framework (DCRF)
Reactive emphasis	Predictive and adaptive emphasis
Sequential stages	Continuous iterative cycle
Operational recovery focus	Strategic transformation focus
Technology as support function	Digital capability as strategic resilience
Crisis-period communication	Continuous stakeholder engagement
Business continuity as recovery	Business continuity as integrated capability
Post-crisis evaluation	Continuous organisational learning
Firm-centred risk perspective	Digital ecosystem and third-party risk

Note: The comparison highlights the shift from episodic, firm-centred response to continuous, ecosystem-aware resilience. Source: Author (2026).

Research Propositions

The following propositions are advanced for future empirical testing:

P1: Digital risk intelligence positively influences organisational preparedness by improving environmental scanning, early warning and strategic decision-making.

P2: Digital transformation has a conditional relationship with organisational resilience, strengthening adaptive capacity while also increasing vulnerability through technological interdependence and concentration risk.

P2a: Effective digital governance positively moderates the relationship between digital transformation and organisational resilience.

P2b: Digital ecosystem dependency negatively moderates the relationship between digital transformation and organisational resilience where redundancy and continuity mechanisms are inadequate.

P3: AI-supported decision systems positively influence the speed and quality of crisis response, resource allocation and operational coordination.

P4: Effective digital governance strengthens organisational resilience and supports stakeholder trust and legitimacy.

P5: Business continuity capability mediates the relationship between digital transformation and organisational resilience.

P6: Continuous digital stakeholder engagement positively influences post-crisis organisational recovery.

P7: Organisational learning positively influences long-term strategic resilience through continuous capability development.

P8: Adaptive digital leadership positively moderates the relationship between digital transformation and organisational resilience.

P9: Organisational culture positively moderates the relationship between digital capability and organisational resilience.

P10: Strategic transformation positively influences sustainable competitive advantage through continuous organisational resilience.

P11: Organisational resilience increasingly depends on the resilience of the wider digital ecosystem in which the organisation operates.

P12: Greater digital ecosystem concentration increases the probability that localised technology failures will generate cascading organisational and cross-sector disruption.

COMPARATIVE ANALYSIS OF MAJOR CRISES

Five illustrative cases are analysed to ground the framework empirically and to illuminate the Digital Resilience Paradox.

COVID-19 Pandemic

The COVID-19 pandemic was a multidimensional systemic crisis that affected public health, workforces, supply chains, consumer demand, logistics, regulation and essential services. Organisations with established digital capabilities were generally better positioned to adopt remote work, virtual collaboration, digital customer interfaces, analytics and flexible operating models (Fletcher & Griffiths, 2020; Papadopoulos et al., 2020). The case demonstrates that resilience is socio-technical: digital capability matters, but so do workforce resilience, leadership, institutional coordination, business continuity and organisational learning. For the DCRF, COVID-19 illustrates the need to anticipate and adapt to disruption originating from outside the organisation.

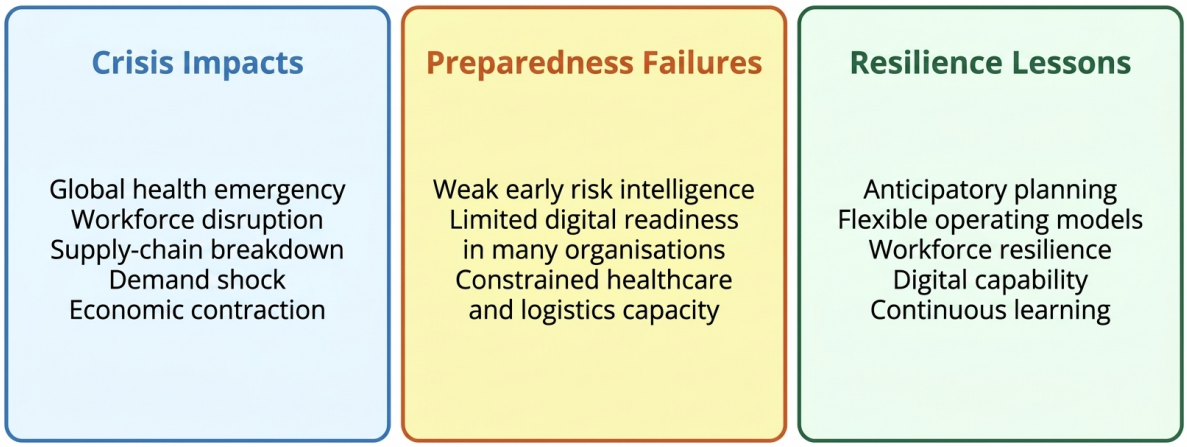


Figure 2: COVID-19 pandemic: crisis impacts, preparedness failures and organisational resilience lessons

Note: The COVID-19 case highlights that digital capability alone is insufficient; resilience also depends on workforce adaptability, leadership and institutional coordination. Source: Author-generated (2026).

Colonial Pipeline Ransomware Attack

The 7 May 2021 Colonial Pipeline ransomware attack demonstrated how cyber disruption in a private critical-infrastructure operator can produce wider economic and social consequences. The shutdown contributed to fuel shortages, queues, panic buying and public concern across the eastern United States. The case shows that cybersecurity cannot remain confined to the CIO or CISO function. For the DCRF, it is an enterprise governance and continuity issue requiring security by design, board oversight, IT/OT resilience, coordinated stakeholder communication and government–industry collaboration.

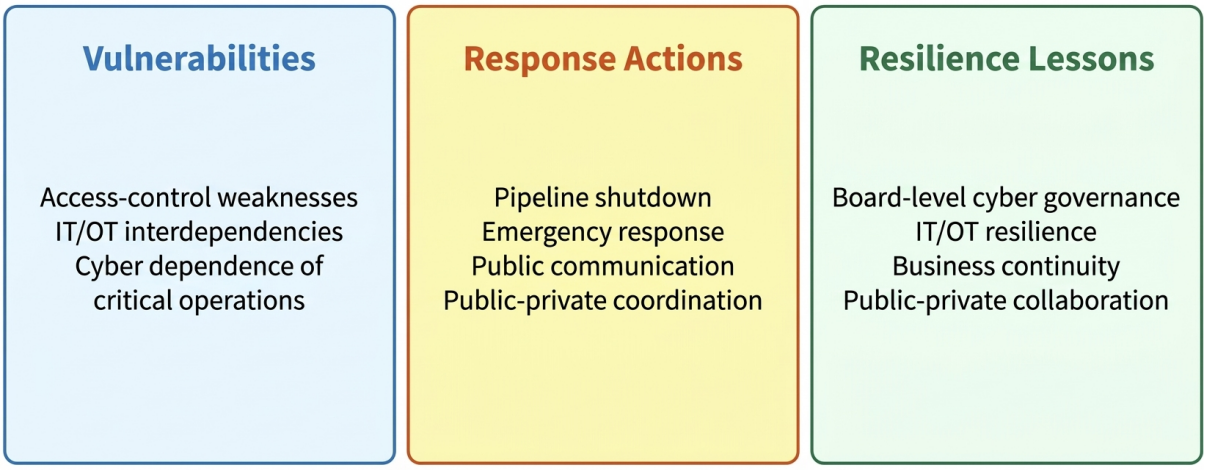


Figure 3: Colonial Pipeline attack: vulnerabilities, response actions and critical-infrastructure resilience lessons

Note. The Colonial Pipeline incident demonstrates that cyber risk in critical infrastructure is an enterprise governance and continuity issue, not merely a technical IT problem. Source: Author-generated (2026).

SolarWinds Supply-Chain Compromise

The December 2020 SolarWinds supply-chain compromise demonstrated the systemic risk embedded in trusted software supply chains. Attackers inserted the SUNBURST backdoor into legitimate Orion software updates, exposing approximately 18,000 public- and private-sector organisations. Strong internal controls do not eliminate exposure to third-party compromise. The DCRF therefore extends digital risk intelligence and governance beyond the legal boundary of the firm to software vendors, contractors, cloud providers and technology partners.

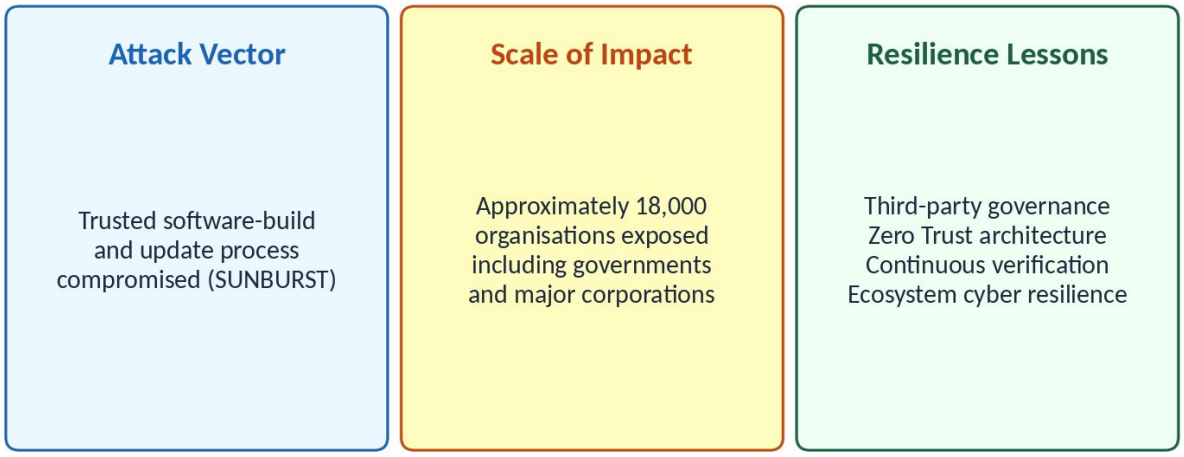


Figure 4: SolarWinds cyberattack: software-supply-chain compromise and third-party resilience lessons

Note: SolarWinds shows that strong internal controls cannot eliminate third-party risk; continuous verification and Zero Trust principles become essential. Source: Author-generated (2026).

Maersk/NotPetya

The June 2017 NotPetya attack spread internationally through compromised Ukrainian accounting software and caused extensive disruption to globally connected organisations. At Maersk, the incident disrupted shipping and logistics operations on a massive scale that required extensive rebuilding of IT infrastructure. The resilience lesson extends beyond cybersecurity technology to include network segmentation, credential protection, offline recovery, manual workarounds, employee adaptability and business continuity. NotPetya provides a clear example of the Digital Resilience Paradox.

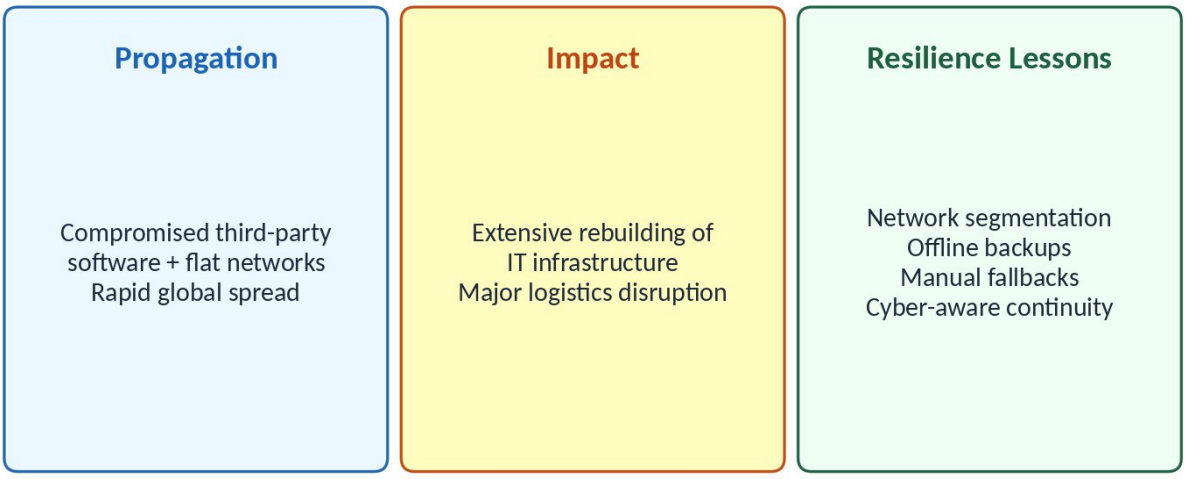


Figure 5: Maersk/NotPetya attack: propagation, recovery and internal-network resilience lessons

Note: NotPetya illustrates how flat networks and third-party software dependencies can turn a localised cyber incident into a global operational crisis. Source: Author-generated (2026).

CrowdStrike Global IT Outage

On 19 July 2024, a defective CrowdStrike Falcon configuration update caused millions of Microsoft Windows systems to crash, disrupting critical services and business operations globally. The incident was not a cyberattack; it resulted from a trusted security platform whose deep system integration and widespread adoption amplified the effects of a faulty update. CrowdStrike highlights systemic technology concentration risk. Advanced technology can improve resilience while simultaneously creating common-mode failure points.

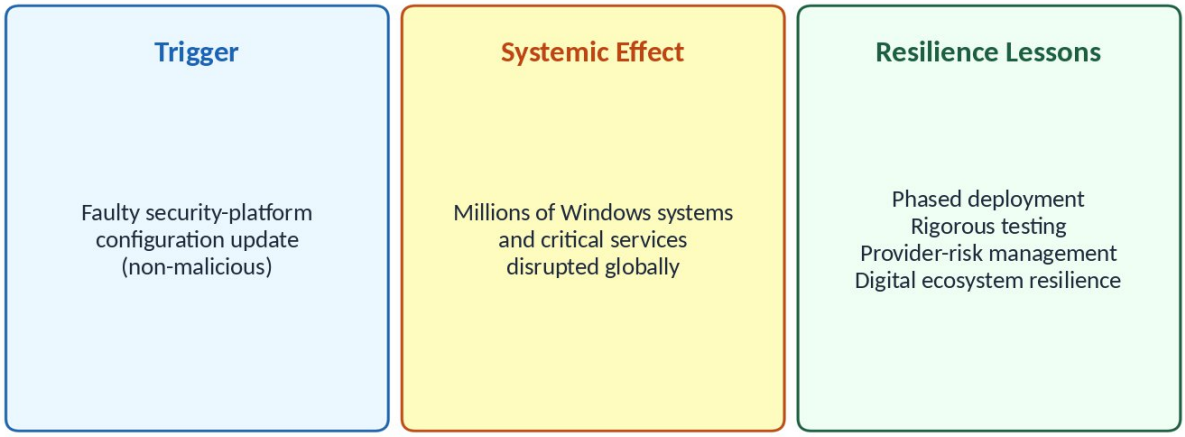


Figure 6: CrowdStrike outage: software failure, systemic propagation and digital-ecosystem resilience lessons

Note: The CrowdStrike outage reveals concentration risk: a single trusted platform can create common-mode failure across otherwise unrelated organisations. Source: Author-generated (2026).

Cross-Case Synthesis and the Digital Resilience Paradox

Across the five cases, the boundary of resilience expands from internal networks to suppliers, critical infrastructure and the wider digital ecosystem. Table 4 provides a structured cross-case synthesis. The cases support a central paradox: the same digital technologies that increase efficiency, connectivity, information processing and adaptive capacity can also increase dependency, concentration risk and the speed at which disruption cascades.

Table 4: Cross-case synthesis of five major digital-era crises

Crisis	Primary type & trigger	Scale of impact	Main resilience lesson
Maersk/NotPetya (2017)	Destructive cyberattack via compromised third-party software and flat networks	Global shipping & logistics; extensive IT rebuild	Segmentation, offline backups, manual fallbacks and cyber-aware continuity
COVID-19 (2020)	Global pandemic; weak early risk intelligence and supply-chain constraints	Global health, economic, workforce and societal disruption	Anticipatory planning, flexible models, workforce resilience and continuous learning

SolarWinds (2020)	Supply-chain cyber-espionage via trusted software update process	Thousands of organisations, including governments and major firms	Third-party governance, Zero Trust and continuous verification
Colonial Pipeline (2021)	Ransomware; access-control weaknesses in critical infrastructure	Fuel-distribution disruption and broader societal consequences	Board-level cyber governance, IT/OT resilience and public–private collaboration
CrowdStrike (2024)	Non-malicious software failure; concentration on a common security platform	Millions of Windows systems and critical services disrupted globally	Phased deployment, provider-risk management, redundancy and ecosystem resilience

Note: Cases selected for illustrative richness of digital interdependence and systemic risk. Source: Author, based on public case evidence (2026).

Table 5 further elaborates the dual pathways of the Digital Resilience Paradox by linking digital capability or dependency in each case to the vulnerability created and the resulting resilience implication.

Table 5: Digital capability, vulnerability and resilience implications across the five cases

Case	Digital capability / dependency	Vulnerability exposed	Resilience implication
Maersk/NotPetya	Highly interconnected global IT	Rapid malware propagation across flat networks	Segmentation, offline recovery, operational redundancy
SolarWinds	Reliance on trusted enterprise software	Compromise via legitimate software updates	Third-party governance and Zero Trust architecture
COVID-19	Digital platforms for remote operations	Limited digital capability constrained adaptation; broader dependencies remained	Digital flexibility combined with human and operational resilience
Colonial Pipeline	Digitally dependent critical infrastructure	Cyber disruption translated into physical economic impact	IT/OT resilience, executive governance, public–private coordination
CrowdStrike	Large-scale reliance on a common security platform	Faulty legitimate update propagated globally	Technology diversification, staged deployment, ecosystem resilience

Note: The table operationalises the Digital Resilience Paradox: the same digital dependencies that enable efficiency can become channels for cascading failure. Source: Author (2026).

The Digital Resilience Paradox can be expressed as two simultaneous pathways. The resilience-enhancing pathway links digital transformation to agility, flexibility, coordination, learning and resilience. The vulnerability-enhancing pathway links digital transformation to interconnectedness, dependency, concentration, cascading failure and systemic vulnerability. Governance, cybersecurity, redundancy, business continuity, adaptive leadership, organisational culture, stakeholder collaboration and learning determine which pathway dominates.

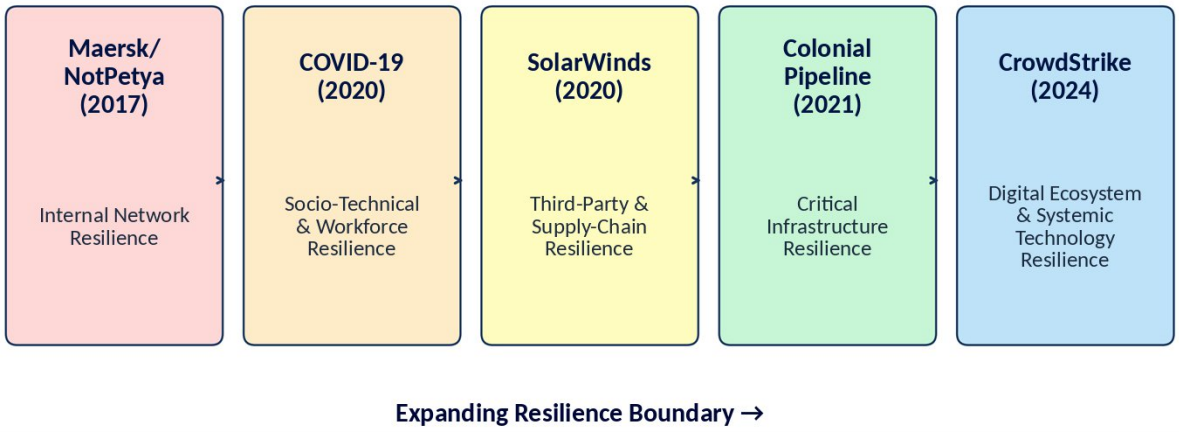


Figure 7: Evolution of organisational resilience across the five cases: from internal network resilience to digital ecosystem and systemic technology resilience

Note: Across the five cases, the boundary of resilience expands from internal networks to the wider digital ecosystem, reinforcing the need for ecosystem-level resilience thinking. Source: Author-generated (2026).

Methodological Positioning and Future Empirical Validation

This article adopts a theory-building conceptual research design supported by a critical integrative literature review. Conceptual articles are vital in advancing knowledge by integrating fragmented literature, clarifying constructs, developing explanatory frameworks, and generating propositions for future empirical testing (Jaakkola, 2020). Integrative reviews are particularly appropriate when a research problem spans multiple disciplines and requires theoretical synthesis (Torraco, 2016; Snyder, 2019).

The literature synthesis draws on crisis management, organisational resilience, strategic management, information systems, digital transformation, cybersecurity, artificial intelligence, stakeholder management, business continuity, and supply-chain resilience. The theoretical development process proceeds from the identification of fragmented research streams, through comparison and integration of complementary theories, to the development of the DCRF, propositions, and a future empirical research agenda.

Table 6 presents illustrative constructs and indicators that can guide future operationalisation and measurement of the DCRF.

Table 6: Illustrative constructs and indicators for empirical validation of the DCRF

Construct	Illustrative indicators
Digital Risk Intelligence	Predictive analytics use, environmental scanning frequency, cyber-threat monitoring, real-time dashboards
Digital Transformation	Cloud adoption, automation intensity, AI implementation, digital maturity score
Digital Governance	Board oversight of cyber/AI risk, formal AI governance, compliance maturity
Business Continuity	Recovery-time objectives, disaster-recovery capability, critical-process availability
Stakeholder Engagement	Transparency of communication, communication quality, measured trust and satisfaction
Organisational Learning	After-action reviews, knowledge-management systems, policy revision frequency
Organisational Resilience	Adaptability, continuity performance, strategic flexibility, recovery speed

Note: Indicators are illustrative and require psychometric validation. Longitudinal designs are particularly appropriate because resilience is demonstrated over time. Source: Author (2026).

Practical Application and the Digital Crisis Resilience Maturity Model

The DCRF can be adapted across sectors because the configuration of digital dependence, stakeholder exposure and criticality vary by industry. Table 7 illustrates how the framework translates into sector-specific priorities and expected outcomes.

Table 7: Sector-specific application of the Digital Crisis Resilience Framework

Industry	Primary digital risks	DCRF priorities	Expected outcomes
Financial services	Cybercrime, fraud, AI misuse, platform outages	AI governance, cyber resilience, regulatory compliance	Financial stability and customer trust
Healthcare	Ransomware, clinical-system failure, connected-device risk	Patient safety, secure continuity, resilient health data	Clinical continuity and patient safety
Manufacturing	Industrial IoT failure, supply-chain disruption	Digital twins, predictive maintenance, cyber resilience	Production continuity
Energy & utilities	Critical-infrastructure attack, climate events	Infrastructure monitoring, redundancy, digital governance	Energy security
Aviation	Software failure, ecosystem dependency	Provider resilience, crisis communication	Operational reliability
Government	National cyber threats,	Critical-infrastructure	Institutional and

	public-service disruption	protection, public–private coordination	national resilience
Retail & e-commerce	Cloud outages, payment and logistics disruption	Cloud resilience, demand intelligence, supply-chain visibility	Service continuity and customer confidence

Note: Priorities are indicative and should be tailored to organisational context, regulatory environment and risk appetite. Source: Author (2026).

The Digital Crisis Resilience Maturity Model (DCRMM) operationalises the framework as a five-level progression from ad hoc crisis response to resilience as an embedded strategic capability (Table 8 and Figure 8). It is intended as a diagnostic and developmental model rather than a claim that maturity is linear or irreversible.

Table 8: Digital Crisis Resilience Maturity Model (DCRMM)

Level	Description	Key characteristics
1 – Reactive	Ad hoc crisis management	Limited planning, fragmented technology, weak governance
2 – Prepared	Basic crisis and continuity arrangements	Formal procedures, periodic training, limited digital integration
3 – Integrated	Resilience embedded in enterprise risk management	Cross-functional coordination, digital governance, integrated cybersecurity
4 – Adaptive	Data and learning drive proactive resilience	AI/analytics, continuous monitoring, rapid adaptation
5 –Transformational	Resilience as a strategic capability	Continuous digital transformation, ecosystem collaboration, strategic renewal

Note: Progression is neither strictly linear nor irreversible; organisations may move between levels depending on investment, leadership and context. Source: Author (2026).

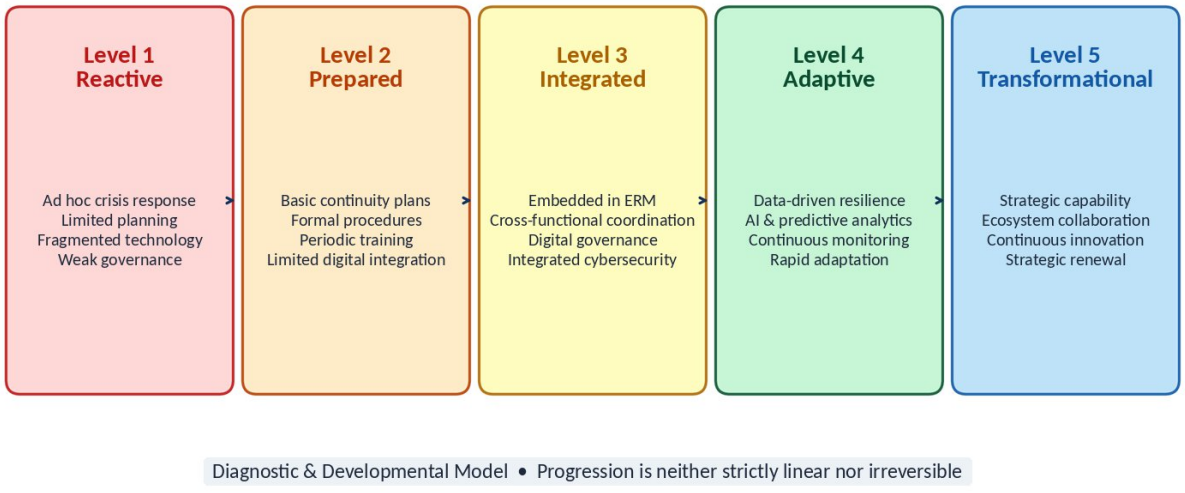


Figure 8: Digital Crisis Resilience Maturity Model (DCRMM): progression from reactive to transformational resilience

Note: The DCRMM is a diagnostic and developmental model. Source: Author-generated (2026).

An indicative implementation roadmap is presented in Table 9.

Table 9: Implementation roadmap for digital crisis resilience

Phase	Time horizon	Priority activities
Foundation	0–6 months	Governance structures, resilience assessment, critical-asset mapping and dependency analysis
Integration	6–18 months	Cyber resilience, crisis simulation, cloud continuity, digital skills and stakeholder protocols
Optimisation	18–36 months	Predictive analytics, AI-supported risk intelligence, digital twins and maturity assessment
Transformation	Beyond 36 months	Continuous innovation, ecosystem resilience, strategic renewal and advanced digital governance

Note: Time horizons are indicative and should be adjusted to organisational size, sector and starting maturity. Source: Author (2026).

DISCUSSION AND THEORETICAL CONTRIBUTION

The DCRF advances crisis management theory by shifting the unit of analysis from episodic response and organisational recovery towards continuous, digitally enabled and ecosystem-aware resilience. It integrates dynamic capabilities, organisational resilience, stakeholder and socio-technical perspectives within a single mid-range framework. Dynamic capabilities explain sensing, seizing and transforming; resilience theory explains anticipation, coping, adaptation and learning; stakeholder theory foregrounds trust and legitimacy; and socio-technical systems thinking captures the interdependence of people, technology, processes, culture and governance.

A central theoretical contribution is the Digital Resilience Paradox. Digital transformation is neither inherently destabilising nor inherently resilience-enhancing. It creates both capability and interdependence simultaneously. While digitalisation can improve situational awareness, coordination, flexibility and learning, it also creates common dependencies, concentrates risk and opens channels for cascading failure. The resilience value of digital transformation is therefore conditional on adequate governance, redundancy, preparedness, continuity, adaptive leadership and organisational learning.

Managerial and Policy Implications

Corporate boards and leaders should elevate resilience to a strategic priority and integrate cybersecurity, AI governance, data governance and business continuity into enterprise risk oversight. Executive teams should develop digital literacy and adaptive leadership, conduct regular simulations, institutionalise lessons learned and treat stakeholder trust as a strategic asset before, during and after crises.

Governments should recognise the increasing interdependence between corporate resilience and national resilience. Policy priorities include cybersecurity standards, AI governance, critical infrastructure protection, digital skills, threat-information sharing and public–private

crisis exercises. Regulatory approaches should balance innovation with accountability and systemic risk reduction.

CONCLUSION

Cyber resilience is in a new phase where the biggest risk is no longer the attack itself, but its impact on services, data and trust. The expanding digital era has therefore fundamentally transformed corporate crisis and disaster management and this will continue at a faster pace as technology and innovation increases. Organisations now operate in a global business environment where increasing levels of cyber threats, software dependencies, AI, geopolitical uncertainty, climate risk, stakeholder expectations and digital interdependence continually reshape exposure to disruption. Reactive crisis plans and isolated technical controls are therefore insufficient to manage and contain the emerging threats.

This article argues that sustainable resilience emerges from the strategic integration of digital capability, adaptive leadership, governance, business continuity, stakeholder engagement, organisational learning and continuous transformation. The DCRF links environmental scanning and digital risk intelligence with preparedness, rapid response, recovery, stakeholder trust, learning and strategic renewal, while the DCRMM provides a practical maturity pathway from a reactive to a transformational capability.

The five cases examined demonstrate that digital transformation produces both resilience potential and systemic vulnerability. The central proposition is that corporate crisis management in the digital era must go beyond firm-centered preparedness towards an ecosystem-based resilience system.

As a conceptual theory-building study, this article does not present primary empirical data. The research propositions and the maturity model therefore remain to be tested. The five cases were selected for their illustrative value rather than statistical representativeness, and the framework is most directly applicable to digitally intensive organisations. Its transferability to organisations with lower levels of digitalisation will require further investigation. In addition, the rapid development of generative and agentic AI may call for periodic updating of the digital risk and capability categories proposed in this study.

Future empirical research should test the DCRF across different sectors, organisational sizes and national contexts, refine measurement scales for its constructs, and examine how governance quality and ecosystem dependency determine the relationship between digital transformation and organisational resilience. Longitudinal and multi-case designs would be particularly useful in capturing how resilience capabilities develop and perform over time.

Acknowledgments

The author thanks the editors and anonymous reviewers of BJCNIT for constructive comments that substantially improved the manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Conflict of Interest

The author declares no conflict of interest.

AI Disclosure

All conceptual development, theoretical synthesis, case analysis, propositions and conclusions are the author's own intellectual work. The author takes full responsibility for the content of the manuscript.

REFERENCES

Aderombi, A. O. (2020). The impact of a crisis or disaster on corporate organisations in the digital era: A better management of crises and disasters. University of East London Repository. https://uel-repository.worktribe.com/output/481123

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

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. International Journal of Production Research, 49(18), 5375–5393. https://doi.org/10.1080/00207543.2011.563826

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471–482.

Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2017). The politics of crisis management: Public leadership under pressure (2nd ed.). Cambridge University Press.

Browder, R. E., Aldrich, H. E., & Bradley, S. W. (2024). Upgrading adaptation: How digital transformation promotes organisational resilience. Strategic Entrepreneurship Journal. https://doi.org/10.1002/sej.1483

Conz, E., & Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. European Management Journal, 38(3), 400–412. https://doi.org/10.1016/j.emj.2019.12.004

Coombs, W. T. (2007). Ongoing crisis communication: Planning, managing, and responding (2nd ed.). Sage.

Coombs, W. T. (2015). Ongoing crisis communication: Planning, managing, and responding (4th ed.). Sage.

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial tests of the Situational Crisis Communication Theory. Management Communication Quarterly, 16(2), 165–186.

Coombs, W. T., & Holladay, S. J. (2012). The paracrisis: The challenges created by publicly managing crisis prevention. Public Relations Review, 38(3), 408–415. https://doi.org/10.1016/j.pubrev.2012.04.004

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

Fletcher, G., & Griffiths, M. (2020). Digital transformation during a lockdown. International Journal of Information Management, 55, Article 102185. https://doi.org/10.1016/j.ijinfomgt.2020.102185

Freeman, R. E. (1984). Strategic management: A stakeholder approach. Pitman.

Gasser, U., & Almeida, V. A. F. (2017). A layered model for AI governance. IEEE Internet Computing, 21(6), 58–62.

Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. International Journal of Production Research, 58(10), 2904–2915. https://doi.org/10.1080/00207543.2020.1750727

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control, 32(9), 775–788.

Jin, Y., Liu, B. F., & Austin, L. L. (2014). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses. Communication Research, 41(1), 74–94. https://doi.org/10.1177/0093650211423918

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1, 389–399.

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

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review, 21(3), 243–255. https://doi.org/10.1016/j.hrmr.2010.10.004

Li, G., Du, K., Liu, L., & Su, F. (2025). Digital transformation and organizational resilience: Unveiling the path to sustainable performance in adversity and crisis. International Journal of Information Management, 84, Article 102934. https://doi.org/10.1016/j.ijinfomgt.2025.102934

Li, W., Yun, K., & Li, F. (2025). The dynamic driving path of organizational resilience to digital transformation—An empirical study based on TJ-QCA. Journal of the Knowledge Economy, 16, 13753–13775. https://doi.org/10.1007/s13132-024-02361-6

Linnenluecke, M. K. (2017). Resilience in business and management research: A review of influential publications and a research agenda. International Journal of Management Reviews, 19(1), 4–30. https://doi.org/10.1111/ijmr.12076

Mitroff, I. I. (2005). Why some companies emerge stronger and better from a crisis: Seven essential lessons for surviving disaster. AMACOM.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST.

National Institute of Standards and Technology. (2024). Cybersecurity Framework 2.0. NIST.

Papadopoulos, T., Baltas, K. N., & Balta, M. E. (2020). The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. International Journal of Information Management, 55, Article 102192. https://doi.org/10.1016/j.ijinfomgt.2020.102192

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. Academy of Management Review, 23(1), 59–76. https://doi.org/10.5465/amr.1998.192960

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. Academy of Management Executive, 7(1), 48–59. https://doi.org/10.5465/ame.1993.9409142058

Tarigan, M. K., Simatupang, T. M., & Bangun, Y. R. (2025). Building resilience through digital transformation: A systematic literature review and comprehensive framework for large enterprises. International Journal of Business Innovation and Research, 36(5), 1–28. https://doi.org/10.1504/IJBIR.2025.145665

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. Strategic Management Journal, 28(13), 1319–1350.

Teece, D. J., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. California Management Review, 58(4), 13–35. https://doi.org/10.1525/cmr.2016.58.4.13

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Wang, Z., & Jia, J. (2025). Digital transformation and organizational resilience. Finance Research Letters, 78, Article 107165. https://doi.org/10.1016/j.frl.2025.107165

Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). Wiley.

Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational response to adversity: Fusing crisis management and resilience research streams. Academy of Management Annals, 11(2), 733–769. https://doi.org/10.5465/annals.2015.0134