

ORIGINAL RESEARCH

Open access

The Digital Service Recovery Model: Explaining How Firms Restore Customer Confidence After Platform Failures, Data Errors, and Online Service Breakdowns

Priya Nambiar^{1*}, Suresh Menon¹, Kavita Pillai²

Abstract

Digital service failures have become routine features of contemporary markets, yet their consequences are rarely routine for customers. Platform outages, data breaches, personalisation errors, failed transactions, and online service breakdowns can quickly damage customer confidence because they interrupt access, create uncertainty, and expose the fragility of digital relationships. Traditional service recovery models provide important foundations, but they do not fully address the speed, visibility, scale, and technical opacity of digital failure. The central problem addressed in this article is that digital service failures differ from face-to-face or phone-based failures in both mechanism and meaning. A late employee apology or a replacement offer may work in a human-delivered service encounter, but digital failures often involve thousands or millions of affected users, automated systems, sensitive data, and unclear accountability. These characteristics require a dedicated conceptual model that connects failure type to recovery response. The objective of this article is to propose the Digital Service Recovery Model. The model explains how firms can restore customer confidence after three core categories of digital service failure: platform failures, data errors, and online service breakdowns. It argues that recovery effectiveness depends on matching the recovery strategy to the failure mechanism rather than applying a generic service recovery script. The resulting model identifies failure triggers, recovery strategy selection, confidence restoration pathways, and feedback loops for systemic improvement. It shows that rapid response, transparent communication, tangible redress, personalised reassurance, and demonstrable technical fixes are not separate tactics but interdependent recovery capabilities. The article contributes a practical and forward-looking framework for firms operating in the digital trust economy.

Keywords Conceptual model, Digital service recovery, Customer confidence, Platform failures, Data errors, Service breakdowns

*Correspondence:

Priya Nambiar

priya.nambiar@iisc.ac.in

¹ Department of Digital Business Systems, Faculty of Management, Indian Institute of Science, Bengaluru, India

² Department of Business Analytics and Strategy, Faculty of Commerce, Anna University, Chennai, India

Introduction

Digital services fail routinely, and each failure can create a moment in which customers reconsider whether the firm deserves continued confidence. Online service failure research shows that customers interpret breakdowns through perceived responsibility, fairness, emotion, and the quality of recovery actions, which means that a failure is not merely a technical event but a relationship event [1]. In digital markets, this relationship event unfolds rapidly because customers experience disruption while simultaneously observing how other affected users, platforms, and firms respond [2].

Existing service recovery theory offers valuable constructs, particularly perceived justice, customer participation, compensation, and post-recovery satisfaction, but much of this work was developed for service encounters where employees and customers interact directly. Meta-analytic evidence on service recovery shows that recovery outcomes depend on attribution and justice perceptions, yet digital failures add platform dependence, algorithmic invisibility, and scale effects that traditional encounter-based models only partially capture [1]. The service recovery journey literature therefore provides a foundation, but the digital context requires a more explicit account of technical failure triggers and confidence restoration pathways [3].

The problem is especially acute because digital failures are often ambiguous to customers. A failed payment, inaccessible account, inaccurate recommendation, or chatbot misdiagnosis may appear as a single inconvenience, but it can signal deeper concerns about competence, security, fairness, or organisational integrity. Studies of online service failure and recovery show that customers evaluate not only the outcome of recovery but also the firm's responsiveness, transparency, and willingness to learn from the failure [4, 5].

This article therefore proposes the Digital Service Recovery Model as an original conceptual framework for explaining how firms restore customer confidence after platform failures, data errors, and online service breakdowns. The model builds on service recovery research, digital service evidence, and trust restoration work to argue that recovery must be failure-type specific rather than generic. It positions confidence restoration as a dynamic process that moves from disruption recognition to recovery strategy selection, customer reassurance, and systemic improvement [6, 7].

Digital Service Failure as a Management Problem

Digital service failure is a distinct management problem because it combines operational disruption with reputational exposure. In online settings, a service breakdown may be experienced privately by one user but become publicly visible through reviews, social media posts, screenshots, and peer-to-peer complaint networks. Research on online service failure during crisis conditions shows that recovery is shaped by networks of actors rather than by the firm-customer dyad alone, making digital recovery a distributed management challenge [2].

Digital failures also differ from traditional failures because customers often cannot diagnose what has gone wrong. Technical ambiguity creates uncertainty about whether the problem is temporary, personal, systemic, malicious, or negligent. This ambiguity matters because attribution theory suggests that customers react more negatively when they believe the firm had control over the failure and failed to prevent it [1].

Management teams therefore face pressure to respond before they have complete technical certainty. Digital recovery requires firms to communicate early without overclaiming, compensate fairly without encouraging opportunism, and fix systems without making the recovery process feel impersonal. Research on service recovery transparency shows that openness can help retain customers after online failures, but only when communication signals accountability rather than defensive impression management [8].

The insufficiency of current recovery playbooks lies in their assumption that a failure can be contained within a discrete encounter. Digital service systems are continuous, data-intensive, and often automated, so breakdowns may persist across channels, devices, accounts, and future recommendations. Service research priorities have therefore emphasised the need to manage technology-enabled turbulence, while corporate digital responsibility research highlights that firms must treat digital competence, data use, and customer protection as strategic responsibilities rather than back-office concerns [7, 9].

Platform Failures and Customer Disruption

Platform failures occur when the digital infrastructure through which customers access value becomes unavailable, unreliable, slow, or functionally degraded. E-commerce sites, mobile applications, SaaS tools, food delivery platforms, and account portals are not merely channels; they are the service environment itself. When that environment fails, the customer experiences disruption as loss of access, loss of control, and often loss of trust in the firm's capability [6].

The immediate impact of platform failure depends on severity, timing, task criticality, and the customer's available alternatives. A slow-loading shopping page may be irritating, but a failed payment, locked account, crashed booking flow, or inaccessible financial service can become urgent and confidence-damaging. Research on online retail recovery and operational service recovery shows that customers evaluate the firm through both the practical consequence of the disruption and the perceived fairness of the response [10, 11].

Platform failures are aggravated when customers receive vague explanations, repeated automated messages, or no visible acknowledgement that the firm recognises the problem. In contrast, disruption can be mitigated when firms provide status updates, realistic resolution expectations, alternative access routes, and evidence that the underlying issue is being corrected. Studies of chatbot and artificial intelligence service failure further show that automated recovery can either help or harm depending on whether the response displays competence, warmth, and appropriate escalation [12–14].

For conceptual model development, platform failures should be treated as confidence shocks that begin with access disruption and intensify when customers infer systemic unreliability. **Table 1** categorises platform failure types and their immediate impacts on customer experience. This categorisation clarifies why a recovery model must distinguish between simple inconvenience, transaction interruption, service exclusion, and high-severity platform collapse rather than treating all digital failures as equivalent [15, 16].

Table 1. Platform Failure Types and Customer Disruption: Categorisation, Immediate Consequences, and Severity Levels

Platform failure type	Typical digital context	Immediate customer consequence	Confidence risk mechanism	Indicative severity level
Full platform outage	E-commerce site, banking app, SaaS dashboard, booking portal	Customers cannot access the service or complete intended tasks	Signals systemic unreliability and weak operational resilience	High
Severe slowdown or latency	Mobile app, streaming platform, online checkout, support portal	Customers experience delay, uncertainty, and task abandonment	Creates frustration and doubts about platform competence	Medium to high
Transaction failure	Payment page, subscription renewal, order confirmation, digital wallet	Customers cannot complete, verify, or trust the transaction	Undermines confidence in accuracy, reliability, and financial safety	High
Feature-level malfunction	Search, recommendations, login, account settings, chatbot support	Customers can access the platform but cannot use a critical function	Produces perceived inconsistency and reduced usability	Medium
Accessibility or compatibility failure	Device-specific app failure, browser issue, assistive technology breakdown	Some customers are excluded from normal service access	Creates perceived neglect, unfairness, and service exclusion	Medium to high
Intermittent degradation	Repeated app crashes, unstable sessions, broken	Customers face recurring uncertainty and repeated	Encourages defection because the service feels	Medium

	links, partial loading	task disruption	unpredictable	
Recovery-channel failure	Status page unavailable, support bot loops, help centre crash	Customers cannot obtain help during the failure	Intensifies anger by making the recovery system part of the breakdown	High

Data Errors and Service Breakdown

Data errors represent a second major category of digital service failure because they damage confidence not by blocking access but by corrupting the informational basis of the relationship. Incorrect customer profiles, inaccurate personalisation, billing mistakes, duplicate charges, failed identity verification, and recommendation errors suggest that the firm does not understand, protect, or competently use customer data. In digital services, where customers often exchange data for convenience, relevance, and continuity, such errors can feel more personal than a temporary platform outage [9].

The confidence damage caused by data errors is especially severe when the error involves sensitive information or financial consequences. Data breach research shows that customer behaviour can change after breach announcements, while emotional responses such as fear and anger shape how customers interpret the firm's responsibility and future trustworthiness [17, 18]. Even when a data problem is not malicious, customers may infer that the firm lacks adequate controls, accountability, or respect for the data relationship.

Data errors also create service breakdowns because digital systems reuse prior data across multiple touchpoints. A wrong address may affect delivery, billing, customer support, and fraud detection; a flawed recommendation profile may repeatedly misclassify customer needs; and a billing error may trigger both financial anxiety and support escalation. Research on consumer responses after data breaches shows that awareness does not always lead to immediate action, but it changes how customers evaluate future digital risk and self-protection [19].

The Digital Service Recovery Model therefore treats data errors as trust-erosion mechanisms rather than isolated accuracy problems. Table 2 outlines data error types and associated service breakdowns that undermine customer confidence. This view is consistent with research showing that the timing and openness of breach announcements matter because firms that are forthcoming can support trust restoration more effectively than firms that delay, obscure, or minimise the problem [20, 21].

Table 2. Data Errors and Online Service Breakdowns: Error Types, System Vulnerabilities, and Trust Erosion Mechanisms

Data error type	System vulnerability	Service breakdown created	Trust erosion mechanism	Recovery priority
Incorrect customer profile	Poor data integration, outdated records, weak identity matching	Wrong account details, irrelevant offers, failed recognition	Customers doubt whether the firm knows them accurately	Correct records and confirm the fix
Billing or transaction data error	Payment processing fault, reconciliation failure, duplicate data entry	Overcharge, duplicate charge, missing refund, unclear account balance	Customers fear financial harm and procedural unfairness	Immediate correction, refund, and explanation

Personalisation failure	Algorithmic misclassification, biased training data, weak preference capture	Inappropriate recommendations, irrelevant content, mistargeted messages	Customers perceive incompetence or intrusive data use	Explain and recalibrate preference logic
Data breach or leak	Security weakness, access-control failure, third-party exposure	Exposure of personal, financial, or behavioural information	Customers question integrity, safety, and future vulnerability	Notify, protect, compensate, and show safeguards
Recommendation breakdown	Faulty model update, poor contextual inference, corrupted behavioural data	Repeatedly poor product, content, or service suggestions	Customers lose confidence in digital intelligence and relevance	Reset model assumptions and offer user control
Identity or authentication error	Failed verification logic, account-linking failure, fraud-screening error	Legitimate customers are locked out or wrongly challenged	Customers perceive exclusion and lack of procedural justice	Escalate quickly and restore access securely
Consent or preference error	Misapplied privacy settings, weak consent governance, channel mismatch	Messages or uses of data violate stated preferences	Customers infer disrespect and loss of control	Apologise, correct consent state, and audit governance

Customer Confidence Restoration

Customer confidence restoration begins when the firm recognises that digital recovery is not only a correction of the failed service but a repair of customer expectations about future reliability. Service recovery studies show that perceived justice remains central, because customers assess whether the outcome is fair, whether the process is timely and accessible, and whether the communication is respectful [22]. In digital settings, these justice dimensions must be translated into visible speed, transparent system explanation, proportionate redress, and evidence of technical learning.

Speed is essential because digital failures unfold in real time and customers often have immediate alternatives. However, speed alone is insufficient if the firm communicates in a way that appears scripted, evasive, or emotionally indifferent. Research on social media recovery indicates that transparency helps retain customers, while studies of recovery messages show that warmth-oriented and competence-oriented communication can shape observers’ reactions on online platforms [8, 23].

Compensation remains important, but digital recovery requires a broader understanding of redress than simple monetary payment. Customers may value refunds, credits, fee waivers, restored access, data protection services, priority support, or non-monetary assurances depending on the failure type and harm experienced. Research on service recovery compensation, customer participation, and co-creation indicates that effective redress depends on perceived fairness, customer involvement, and the firm’s ability to convert failure into a credible recovery process [24–26].

The model therefore proposes that confidence restoration is strongest when firms combine transparent acknowledgement, rapid stabilisation, tangible redress, personalised communication, and demonstrable systemic improvement. **Table 3** summarises digital-specific recovery strategies for rebuilding customer confidence. This synthesis aligns with evidence that customer emotions shape recovery outcomes and that apology, appreciation, and message framing must be selected carefully because different responses can restore or weaken perceived relational value [27, 28].

Table 3. Digital Service Recovery Strategies: Transparency, Speed, Compensation, and Personalised Communication for Confidence Restoration

Recovery strategy	Primary purpose	Best suited failure type	Customer confidence effect	Managerial implementation requirement
Proactive notification	Acknowledge the failure before customers must search for answers	Platform outage, data breach, major service breakdown	Reduces uncertainty and signals accountability	Monitoring systems, status alerts, and coordinated communication
Rapid stabilisation	Restore access, continuity, or basic service functionality	Platform crash, transaction failure, account lockout	Signals operational competence and urgency	Incident response teams and escalation protocols
Transparent explanation	Clarify what happened, what is known, and what remains under investigation	Data error, breach, algorithmic failure, repeated breakdown	Builds credibility by reducing perceived concealment	Clear language, legal alignment, and technical accuracy
Tangible redress	Compensate for inconvenience, loss, risk, or disruption	Billing error, outage, failed transaction, breach exposure	Supports distributive justice and perceived fairness	Refund rules, credits, fee waivers, and risk-based compensation
Personalised reassurance	Address the customer's specific account, data, or transaction situation	Data error, personalisation failure, identity problem	Rebuilds perceived recognition and care	Customer-level diagnostics and tailored messaging
Human escalation	Move from automation to accountable human support when stakes are high	Sensitive data issue, repeated chatbot failure, severe complaint	Restores interactional justice and emotional confidence	Escalation triggers and trained recovery agents
Systemic fix disclosure	Show what has changed to prevent recurrence	Recurring platform failure, breach, data governance problem	Converts recovery from apology into credible improvement	Root-cause analysis and post-incident reporting
Customer control restoration	Give customers tools to correct, reset, verify, or manage data	Personalisation error, consent error, recommendation breakdown	Rebuilds autonomy and reduces perceived vulnerability	Preference centres, correction workflows, and audit trails

Proposed Digital Service Recovery Model

The Digital Service Recovery Model begins with three trigger events: platform failure, data error, and online service breakdown. Platform failure refers to degraded or unavailable digital infrastructure, data error refers to inaccurate or unsafe information processing, and online service breakdown refers to failed digital interaction, support, fulfilment, or automated assistance. This trigger-based structure extends traditional recovery models by locating the source of confidence damage in the digital system rather than only in the customer's immediate complaint [3, 6].

Figure 1 visualises the core architecture of the Digital Service Recovery Model by linking digital failure triggers to recovery strategy selection and customer confidence restoration.

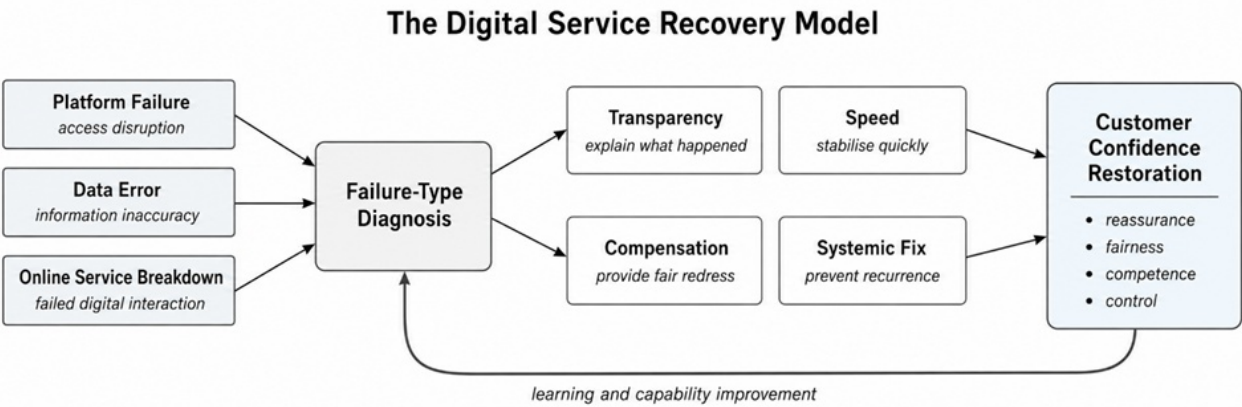


Figure 1. The Digital Service Recovery Model: From Digital Failure Triggers to Recovery Strategy Selection and Customer Confidence Restoration

After the trigger event is identified, the model requires recovery strategy selection across four interdependent dimensions: transparency, speed, compensation, and systemic fix. Transparency answers the question of what happened, speed addresses immediate disruption, compensation addresses fairness, and systemic fix addresses future confidence. Research on online service failure, crisis recovery, and food delivery app recovery suggests that customers evaluate recovery not as one action but as a sequence of signals about competence, fairness, and willingness to repair the relationship [29, 30].

The model also includes moderators that explain why the same recovery action can have different effects across firms and customers. Brand equity may buffer damage when customers believe the firm has a history of reliability, while failure severity can overwhelm otherwise effective recovery actions. Prior trust and customer participation further shape the recovery pathway because customers who feel involved in correction may interpret the firm as more responsive and less indifferent [22, 26, 31].

The model is dynamic because recovery does not end when the immediate problem is solved. Table 4 presents the complete Digital Service Recovery Model with its components and recovery pathways. Its feedback loop requires firms to convert incident learning into platform resilience, data governance improvement, communication redesign, and recovery capability building, reflecting the broader service research priority of managing technology-enabled service turbulence [7, 16].

Table 4. Digital Service Recovery Model: Trigger Events, Recovery Dimensions, Confidence Restoration Path, and Feedback Loops

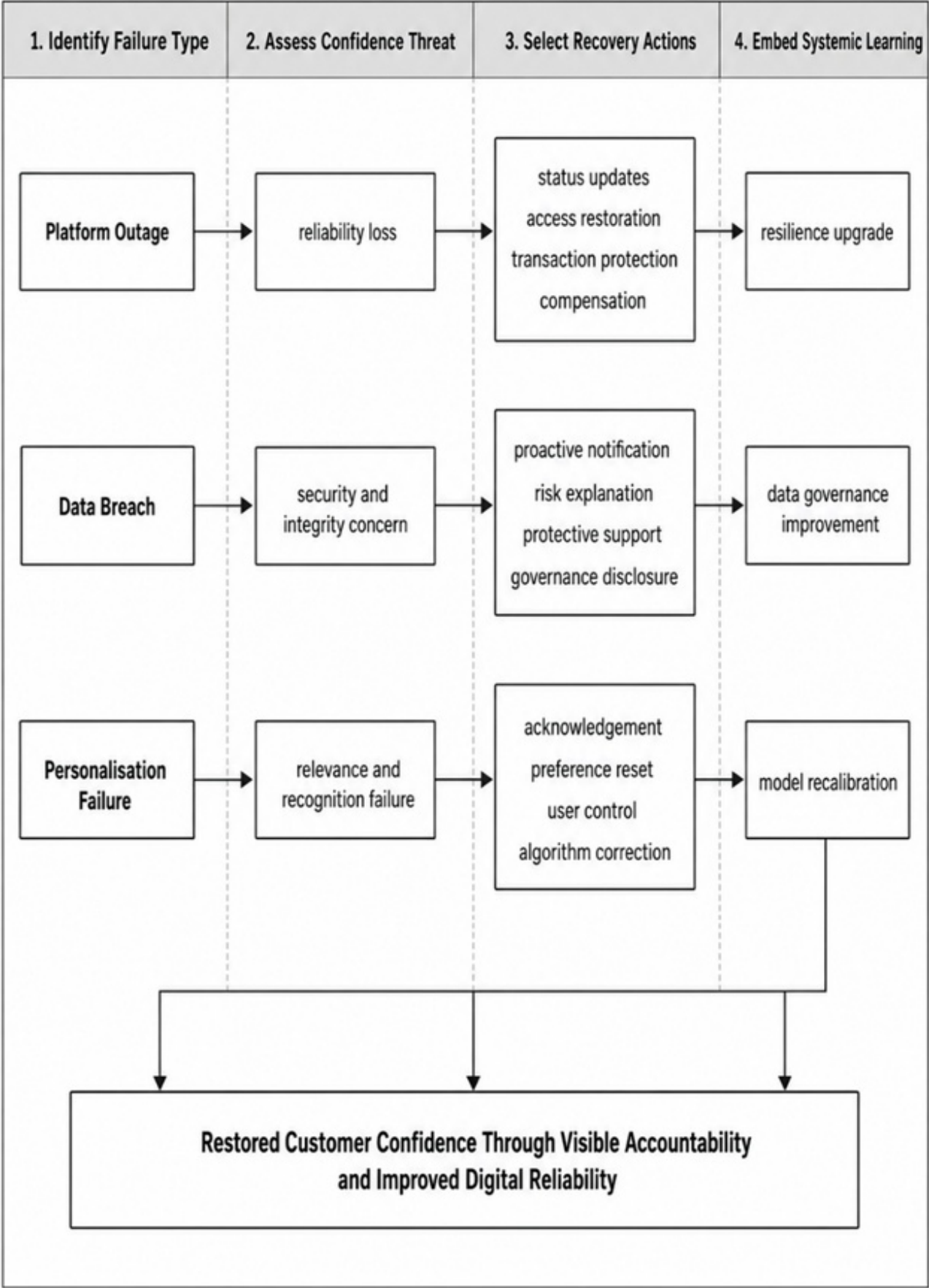
Model stage	Core component	Conceptual role	Key managerial question	Expected confidence outcome
Trigger diagnosis	Platform failure	Identifies access, availability, performance, or transaction disruption	What part of the digital platform prevented customers from receiving value?	Customers see that the firm recognises the operational source of failure
Trigger diagnosis	Data error	Identifies incorrect, unsafe, or misused customer data	What data process produced inaccuracy, exposure, or inappropriate personalisation?	Customers see that the firm treats data accuracy and protection as central

Trigger diagnosis	Online service breakdown	Identifies failed support, fulfilment, automation, or cross-channel service continuity	Where did the digital service journey break down after access was available?	Customers see that the firm understands the full service journey
Strategy selection	Transparency	Provides timely, honest, and comprehensible explanation	What can be disclosed now without misleading customers?	Reduced uncertainty and increased credibility
Strategy selection	Speed	Restores access, corrects records, or stabilises interaction quickly	What action will reduce customer harm fastest?	Recovered sense of competence and urgency
Strategy selection	Compensation	Provides fair redress for inconvenience, loss, risk, or emotional cost	What form of redress matches the harm and customer expectation?	Restored distributive justice and reduced resentment
Strategy selection	Systemic fix	Prevents recurrence through technical, data, or process improvement	What must change so customers believe the failure will not repeat?	Rebuilt future-oriented confidence
Moderating conditions	Severity, prior trust, brand equity, customer dependence	Explains variation in recovery effectiveness	Which customers are most vulnerable to defection or distrust?	More precise recovery prioritisation
Restoration path	Reassurance, fairness, competence, control	Converts recovery actions into confidence restoration	How does each action help customers feel safe, respected, and in control?	Renewed confidence and continued engagement
Feedback loop	Learning and capability building	Embeds recovery lessons into digital operations	What operational changes are documented, tested, and communicated?	Improved resilience and stronger trust over time

Managerial Application and Use Cases

In the first use case, a major e-commerce platform experiences a checkout outage during a high-demand sales period. The model guides managers to diagnose the incident as a platform failure with transaction consequences, communicate the outage proactively, preserve shopping carts, extend promotional windows, and provide credits or fee waivers where customers lost a time-sensitive opportunity. This approach reflects evidence from online shopping recovery that perceived justice, satisfaction, and word-of-mouth depend on how customers interpret the fairness and adequacy of the recovery response [10].

Figure 2 illustrates how managers can operationalise the Digital Service Recovery Model by matching failure type, customer confidence threat, recovery action, and systemic learning.



Breach, and Personalisation Failure Scenarios

In the second use case, a fintech app discovers that customer data may have been exposed through a security weakness. The model identifies the incident as a data error with high sensitivity and requires rapid notification, clear risk explanation, protective services, account monitoring, and visible governance improvements. Data breach studies show that announcements influence customer behaviour, while the scope and emotional framing of a breach affect whether customers respond with fear, anger, avoidance, or continued engagement [17, 18].

In the third use case, a streaming service repeatedly recommends inappropriate or irrelevant content after a model update. The model treats the problem as a personalisation failure that erodes confidence in relevance, competence, and data interpretation, even if the platform remains available. Research on artificial intelligence service recovery and AI response methods suggests that customers judge automated recovery through perceived intelligence, appropriateness, and the ability to correct the failure without creating further frustration [32, 33].

These three use cases demonstrate that the model is intended to help managers match recovery action to failure type rather than defaulting to generic apologies. Table 5 illustrates the application of the model through three use cases. The table shows how outage recovery, breach recovery, and personalisation recovery differ in trigger diagnosis, customer harm, recovery priorities, and systemic learning requirements [14, 34].

Table 5. Managerial Use Cases for the Digital Service Recovery Model: Platform Outage, Data Breach, and Personalisation Failure Scenarios

Use case	Failure trigger	Customer confidence threat	Immediate recovery actions	Tangible redress	Systemic improvement signal
E-commerce checkout outage	Platform failure affecting transaction completion	Customers doubt reliability, lose purchase opportunity, and may defect to competitors	Status update, cart preservation, alternative checkout route, extended sale window	Discount extension, delivery upgrade, credit, or fee waiver	Post-incident explanation of capacity upgrade and transaction monitoring
Fintech data breach	Data error involving exposure or risk of sensitive information	Customers fear financial harm, identity misuse, and organisational negligence	Direct notification, risk assessment, account protection steps, dedicated support	Monitoring support, reimbursement guarantees, fee waivers, or protective services	Security audit, access-control improvement, and transparent governance update
Streaming personalisation failure	Data and algorithmic service breakdown	Customers feel misunderstood, misclassified, or intrusively profiled	Acknowledge recommendation issue, allow profile reset, explain preference controls	Free month, content credit, or enhanced control features where disruption is severe	Model recalibration, user feedback loop, and preference transparency

SaaS dashboard degradation	Platform slowdown and feature malfunction	Business users question operational continuity and vendor dependability	Incident alerts, uptime updates, workaround guidance, priority support	Service credits under service-level terms	Reliability engineering review and customer-facing uptime report
Automated support loop failure	Online service breakdown caused by chatbot escalation failure	Customers feel trapped, ignored, and denied interactional justice	Human escalation, transcript transfer, apology, case ownership	Priority handling or account credit for repeated unresolved contacts	Bot escalation rule redesign and failure monitoring
Billing data mismatch	Data processing error affecting charges or account balance	Customers suspect unfairness, financial risk, or poor record control	Immediate correction, written confirmation, support contact, audit of affected accounts	Refund, fee reversal, interest correction, or goodwill credit	Billing reconciliation controls and customer verification workflow

Limitations and Future Research

The Digital Service Recovery Model is conceptual and therefore requires empirical validation. Although it synthesises service recovery, digital failure, data breach, and trust restoration research, it does not test causal pathways among failure type, recovery action, perceived justice, and restored confidence. Future studies could use experiments to compare whether transparency, compensation, speed, and systemic-fix disclosure have different effects across platform outages, data errors, and online service breakdowns [1, 31].

A second limitation is that the model may not fully capture cultural, regulatory, or industry differences in trust repair. Customers in highly regulated sectors such as banking, health, and insurance may interpret data errors differently from customers in entertainment or retail contexts, while cultural expectations about apology, compensation, and privacy may shape recovery preferences. Future research should examine how customer participation and emotion vary across countries, sectors, and service dependence conditions [24, 28].

A third limitation concerns boundary conditions in markets where customers have limited alternatives. Monopolistic platforms, essential digital infrastructures, and locked-in enterprise systems may reduce immediate defection while still damaging confidence, voice behaviour, and long-term relational commitment. Longitudinal studies could examine whether systemic fix disclosure, corporate digital responsibility, and repeated recovery performance create durable confidence after severe digital failures [9, 20].

Conclusion

This article proposed the Digital Service Recovery Model as a structured framework for restoring customer confidence after platform failures, data errors, and online service breakdowns. Its central contribution is to shift recovery thinking from generic complaint handling to failure-type-specific confidence restoration. The model shows that digital recovery must begin with accurate diagnosis of the failure mechanism before the firm selects the appropriate recovery response.

The article argued that speed and transparency are necessary but not sufficient. Customers also require tangible redress, personalised reassurance, and evidence that the firm has corrected the underlying system rather than merely contained

the immediate complaint. In digital environments, recovery is therefore both a customer-facing communication process and an internal capability for operational learning.

Firms that treat digital recovery as a strategic capability will be better positioned to retain customer confidence when failures occur. As digital services become more automated, data-intensive, and platform-dependent, recovery competence will become a visible marker of managerial quality. The Digital Service Recovery Model offers a roadmap for building that competence in the digital trust economy.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 05 Dec 2025

Revised: 20 Jan 2026

Accepted: 05 Mar 2026

Published online: 18 March 2026

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

Das M, Jebarajarkirthy C, Maseeh HI, Lim WM, Shah JS. Online service failure and recovery: An integrated meta-analytic perspective of attribution and justice theories. *J Bus Res.* 2026;202:115752.

Ozuem W, Ranfagni S, Willis M, Rovai S, Howell K. Exploring customers' responses to online service failure and recovery strategies during Covid-19 pandemic: An actor–network theory perspective. *Psychol Mark.* 2021;38(9):1440-59.

Van Vaerenbergh Y, Varga D, De Keyser A, Orsingher C. The service recovery journey: conceptualization, integration, and directions for future research. *J Serv Res.* 2019;22(2):103-19.

Azemi Y, Ozuem W, Howell KE, Lancaster G. An exploration into the practice of online service failure and recovery strategies in the Balkans. *J Bus Res.* 2019;94:420-31.

Manu C, Sreejesh S. 'Do not be deteriorated by service failures, learn from them and start managing it': Conditions and mechanisms for managing online service failures. *J Retail Consum Serv.* 2024;81:104017.

Reis JCG, Santos V, Amorim M, Melão N. Addressing service failure and recovery in digital service systems: opportunities and challenges. *J Rev Glob Econ.* 2019;8:149.

Ostrom AL, Field JM, Fotheringham D, Subramony M, Gustafsson A, Lemon KN, et al. Service research priorities: Managing and delivering service in turbulent times. *J Serv Res.* 2021;24(3):329-53.

Honora A, Chih WH, Wang KY. Managing social media recovery: The important role of service recovery transparency in retaining customers. *J Retail Consum Serv.* 2022;64:102814.

Lobschat L, Mueller B, Eggers F, Brandimarte L, Diefenbach S, Kroschke M, et al. Corporate digital responsibility. *J Bus Res.* 2021;122:875-88.

Jung NY, Seock YK. Effect of service recovery on customers' perceived justice, satisfaction, and word-of-mouth intentions on online shopping websites. *J Retail Consum Serv.* 2017;37:23-30.

Song Y, Xiu Y, Zhou L, Wang J. Implementing multi-attribute utility theory in service recovery: An operational management perspective on online retailing. *J Retail Consum Serv.* 2024;81:103968.

Haupt M, Rozumowski A, Freidank J, Haas A. Seeking empathy or suggesting a solution? Effects of chatbot messages on service failure recovery. *Electron Mark.* 2023;33(1):56.

Choi S, Mattila AS, Bolton LE. To err is human (-oid): how do consumers react to robot service failure and recovery?. *J Serv Res.* 2021;24(3):354-71.

Xing X, Song M, Duan Y, Mou J. Effects of different service failure types and recovery strategies on the consumer response mechanism of chatbots. *Technol Soc.* 2022;70:102049.

Schaarschmidt M, Walsh G, Dose DB, Christ-Brendemühl S. Customer integration, fairness perceptions, and silent endurance in digital versus human service interactions. *Eur Manag J.* 2023;41(1):34-46.

Wirtz J, Zeithaml V. Cost-effective service excellence. *J Acad Mark Sci.* 2018;46(1):59-80.

Janakiraman R, Lim JH, Rishika R. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *J Mark.* 2018;82(2):85-105.

Chatterjee S, Gao X, Sarkar S, Uzmanoglu C. Reacting to the scope of a data breach: The differential role of fear and anger. *J Bus Res.* 2019;101:183-93.

Mayer P, Zou Y, Lowens BM, Dyer HA, Le K, Schaub F, et al. Awareness, intention,(in) action: Individuals' reactions to data breaches. *ACM Trans Comput Hum Interact.* 2023;30(5):1-53.

Muzatko S, Bansal G. It pays to be forthcoming: Timing of data breach announcement, trust violation, and trust restoration. *Internet Res.* 2024;34(5):1629-63.

Curtis SR, Carre JR, Jones DN. Consumer security behaviors and trust following a data breach. *Manag Audit J.* 2018;33(4):425-35.

Van Vaerenbergh Y, Hazée S, Costers A. Customer participation in service recovery: A meta-analysis. *Mark Lett.* 2018;29(4):465-83.

Huang R, Ha S. The effects of warmth-oriented and competence-oriented service recovery messages on observers on online platforms. *J Bus Res.* 2020;121:616-27.

Bagherzadeh R, Rawal M, Wei S, Torres JL. The journey from customer participation in service failure to co-creation in service recovery. *J Retail Consum Serv.* 2020;54:102058.

Arsenovic J, Edvardsson B, Otterbring T, Tronvoll B. Money for nothing: The impact of compensation on customers' bad-mouthing in service recovery encounters. *Mark Lett.* 2023;34(1):69-82.

Hazée S, Van Vaerenbergh Y, Armirotto V. Co-creating service recovery after service failure: The role of brand equity. *J Bus Res.* 2017;74:101-9.

You Y, Yang X, Wang L, Deng X. When and why saying "thank you" is better than saying "sorry" in redressing service failures: The role of self-esteem. *J Mark.* 2020;84(2):133-50.

Valentini S, Orsingher C, Polyakova A. Customers' emotions in service failure and recovery: A meta-analysis. *Mark Lett.* 2020;31(2):199-216.

Foroudi P, Tabaghdehi SA, Cillo V, Cuomo MT. E-service failure and recovery strategy in times of crisis: Effect on peer attitudes, expectation and future intention. *Rev Manag Sci.* 2025;19(2):537-71.

Kaur P, Talwar S, Islam N, Salo J, Dhir A. The effect of the valence of forgiveness to service recovery strategies and service outcomes in food delivery apps. *J Bus Res.* 2022;147:142-57.

Khamitov M, Rajavi K, Huang DW, Hong Y. Consumer trust: Meta-analysis of 50 years of empirical research. *J Consum Res.* 2024;51(1):7-18.

Xu XA, Liu J. Artificial intelligence humor in service recovery. *Ann Tour Res.* 2022;95:103439.

Yang Z, Zhou J, Yang H. The impact of AI's response method on service recovery satisfaction in the context of service failure. *Sustainability.* 2023;15(4):3294.

Lajante M, Remisch D, Dorofeev N. Can robots recover a service using interactional justice as employees do? A literature review-based assessment. *Serv Bus.* 2023;17(1):315-57.