

ORIGINAL RESEARCH

Open access

Managing Digital Trust across Customers, Employees, Platforms, and Regulators in Data-Driven Business Ecosystems

Amira Khalil^{1*}, Sara Fathy¹, Mahmoud Adel², Hany Nabil¹, Rania Mostafa²

Abstract

Trust has become a central strategic condition of participation in the digital economy. Data-driven firms depend on customers who share personal information, employees who accept digital systems at work, platforms that coordinate ecosystem participation, and regulators who evaluate organizational credibility. When trust weakens in any of these domains, the consequences can extend beyond the original stakeholder group. Existing research has produced valuable insights into customer privacy, algorithmic fairness, employee surveillance, platform dependence, and governance. However, these domains are often treated separately, which limits the ability of managers to understand how digital trust crises unfold across stakeholder boundaries. A data breach, opaque algorithmic decision, or platform governance failure can simultaneously damage market confidence, employee morale, ecosystem relationships, and regulatory legitimacy. This article develops a unified Digital Trust Management Framework for data-driven business ecosystems. The framework treats digital trust as a systemic managerial capability rather than as a set of isolated stakeholder concerns. It integrates trust-building, trust-maintenance, and trust-repair mechanisms across customers, employees, platforms, and regulators. The article is based on a conceptual synthesis of peer-reviewed articles published. These studies are integrated across strategic management, organizational trust, digital business, information systems, platform ecosystems, data privacy, artificial intelligence governance, and stakeholder management. The synthesis supports a framework that links stakeholder-specific trust drivers with shared managerial mechanisms such as transparency, accountability, participation, security, fairness, and governance credibility. The framework shows that digital trust must be managed as an interconnected ecosystem property. It identifies how trust erosion cascades across stakeholder groups and how integrated trust governance can help firms prevent, contain, and repair digital trust failures. The article contributes a practical roadmap for managers seeking to sustain legitimacy and performance in data-driven business ecosystems.

Keywords Customer trust, Digital trust, Employee trust, Platform trust, Regulatory trust, Framework

*Correspondence:

Amira Khalil

amira.khalil@alexu.edu.eg

¹ Department of Digital Enterprise Management, Faculty of Commerce, Alexandria University, Alexandria, Egypt

² Department of Business Intelligence Systems, Faculty of Economics and Political Science, Cairo University, Cairo, Egypt

Introduction

Trust has long supported exchange, coordination, and legitimacy, but its role has become more complex in data-driven business ecosystems. Customers now evaluate firms not only through products and services but also through how personal data are collected, protected, interpreted, and monetised, making privacy a direct determinant of customer and firm performance [1]. At the same time, employees must decide whether to trust algorithmic systems that monitor work, evaluate performance, and reshape job design [2]. Platforms and regulators further intensify this trust environment

because firms increasingly depend on platform infrastructures and governance expectations that extend beyond traditional bilateral business relationships [3].

The central problem is that digital trust is frequently managed in silos. Marketing teams may focus on customer privacy, human resource units may address employee acceptance of automated tools, compliance teams may manage regulatory expectations, and partnership teams may negotiate platform participation. Yet research on trustworthy artificial intelligence suggests that trust depends on interconnected technical, ethical, organizational, and governance conditions rather than on isolated design features [4]. Fragmented trust management therefore leaves firms vulnerable to failures that migrate from one stakeholder relationship to another.

Digital trust failures are especially likely to cascade because digital systems make organizational actions visible, traceable, and contestable. A privacy violation can reduce customer confidence, invite regulatory scrutiny, create employee concern about internal data practices, and weaken platform-partner perceptions of governance maturity [5]. Similarly, opaque algorithmic decisions can undermine accountability because transparency alone is insufficient unless stakeholders can understand who is responsible, how decisions are made, and how harms can be corrected [6]. The result is a managerial challenge in which trust erosion is not contained within the domain where it begins.

This article proposes a Digital Trust Management Framework for customers, employees, platforms, and regulators. The framework synthesises research on artificial intelligence trust, data privacy, platform ecosystems, algorithmic accountability, and governance to show how trust can be built, maintained, and repaired across stakeholder groups [7]. The article proceeds by conceptualising digital trust as a management challenge, analysing customer trust in data-driven business, examining employee trust in digital systems, discussing platform and regulatory trust, and presenting an integrated framework for managerial application. Its core argument is that digital trust must be governed as a systemic property of the business ecosystem rather than as a communication problem after a failure has occurred.

Digital Trust as a Management Challenge

Digital trust differs from traditional organizational trust because digital interactions are mediated by data systems, algorithmic infrastructures, and platform rules that many stakeholders cannot directly observe. Trust in artificial intelligence depends not only on whether the system performs accurately but also on whether stakeholders perceive it as fair, reliable, understandable, and aligned with legitimate purposes [7]. This makes digital trust partly technical, partly relational, and partly institutional. Managers must therefore govern both the design of digital systems and the meanings stakeholders attach to those systems.

A major challenge is that digital trust is shaped by opacity. Algorithmic decision-making can conceal how inputs are selected, how models classify people, and how outputs affect opportunities, prices, services, or employment outcomes [8]. Transparency is often proposed as a remedy, but transparency must be contextual because different stakeholders need different forms of explanation to judge whether a system is trustworthy [9]. Digital trust management therefore requires firms to translate complex data practices into stakeholder-relevant assurances rather than assuming that disclosure alone produces confidence.

Digital trust is also affected by platform dependence. Firms increasingly operate within platform ecosystems where access, visibility, data flows, and complementor opportunities are shaped by platform governance [10]. Platform ecosystems can create value by coordinating participants, but they can also generate vulnerability when rules, data access, or competitive conditions change asymmetrically [11]. As a result, trust in data-driven business extends beyond the firm's own conduct to include the fairness and predictability of the digital infrastructures on which the firm relies.

The four stakeholder groups examined in this article are interdependent because customers, employees, platforms, and regulators observe overlapping signals of organizational integrity. Customers judge whether firms use data responsibly, employees judge whether internal systems respect fairness and autonomy, platforms judge whether ecosystem

participants can be relied on, and regulators judge whether firms demonstrate credible compliance and good faith. Work on layered artificial intelligence governance suggests that digital accountability must operate across technical, organizational, and institutional layers rather than through a single control point [12]. Digital trust management therefore becomes a strategic capability for aligning stakeholder expectations across the entire data-driven ecosystem.

Customer Trust in Data-Driven Business

Customer trust in data-driven business is grounded in expectations that firms will collect, use, share, and protect personal data responsibly. Research on data privacy shows that privacy practices affect both customer outcomes and firm performance, which means trust is not merely an ethical preference but also a market asset [1]. Customers are more willing to engage with digital services when they perceive that data practices are transparent, proportionate, secure, and aligned with the value they receive. For this reason, customer trust must be designed into data strategy rather than added as a reputational message after concerns emerge.

Privacy concerns intensify when customers believe that firms benefit from personalisation while customers carry the risks of exposure, manipulation, or loss of control. The personalisation–privacy tension shows that service customisation can increase perceived value, but only when transparency features help customers understand and evaluate the trade-off [13]. Broader marketing research also indicates that data privacy is central to customer relationships because customers interpret privacy practices as signals of respect, fairness, and organizational intent [14]. Data-driven firms therefore need mechanisms that make personalisation explainable, adjustable, and revocable.

Customer trust erodes when firms appear careless, exploitative, or opaque in their handling of data. Privacy violations impose a trust penalty because customers reinterpret the firm’s prior assurances through the lens of harm, negligence, or betrayal [5]. Algorithmic opacity can deepen this erosion when customers cannot understand why they received a price, recommendation, decision, or service outcome [6]. In digital business, trust repair therefore requires more than apology; it requires visible accountability, evidence of corrective action, and meaningful restoration of user control.

Customer trust can be rebuilt through transparent data practices, strong protection mechanisms, fair algorithmic treatment, and credible repair processes. Research on digital technologies and privacy tensions suggests that firms must manage privacy, data use, and customer value as simultaneous design concerns rather than as competing afterthoughts [15]. **Table 1** summarises the antecedents, erosion factors, and rebuilding mechanisms of customer trust. These mechanisms support the broader framework by showing how customer trust becomes a foundation for wider ecosystem legitimacy.

Table 1. Customer Trust in Data-Driven Business: Antecedents, Erosion Triggers, and Repair Strategies

Customer trust dimension	Core antecedents	Main erosion triggers	Repair and rebuilding strategies	Managerial implication
Data transparency	Clear explanation of what data are collected, why they are collected, how long they are retained, and who can access them	Hidden data collection, vague consent language, unexpected secondary use, and unclear data-sharing arrangements	Plain-language privacy notices, layered consent, customer dashboards, data-use explanations, and periodic transparency updates	Treat transparency as an ongoing relationship mechanism, not a one-time disclosure
Privacy protection	Secure storage, minimisation of unnecessary data,	Data breaches, excessive collection, weak access controls, and perceived	Breach notification, independent security review, data	Link privacy protection to customer value and

	restricted access, and privacy-by-design routines	misuse of sensitive information	minimisation reforms, compensation where appropriate, and visible corrective action	organizational credibility
Algorithmic fairness	Fair treatment across customer groups, explainable outputs, and proportional use of automated decisions	Biased recommendations, discriminatory pricing, unexplained denial of access, or opaque automated decisions	Bias audits, explainable decision notices, appeal channels, and human review for consequential decisions	Make fairness auditable before customer harm becomes reputational harm
User control	Meaningful ability to opt in, opt out, correct data, delete data, and adjust personalisation settings	Forced consent, confusing controls, dark patterns, and limited ability to contest data use	Preference centres, revocable consent, correction mechanisms, deletion options, and easy escalation routes	Convert control from a compliance feature into a trust-building experience
Trust repair after failure	Prior credibility, timely acknowledgement, responsibility-taking, and evidence of remediation	Delayed communication, denial, blaming third parties, and unclear responsibility	Public accountability, customer-specific remediation, procedural changes, monitoring reports, and leadership communication	Repair must demonstrate changed behaviour, not merely express regret

Employee Trust in Digital Systems

Employee trust in digital systems is shaped by whether workers perceive automation, monitoring, and algorithmic decision-making as legitimate extensions of organizational coordination or as instruments of hidden control. Algorithmic management changes the terrain of workplace authority because it can assign tasks, evaluate performance, discipline workers, and structure opportunities through rules that employees may not fully understand [2]. This makes employee trust especially fragile when digital systems are introduced without explanation, participation, or procedural safeguards. Trust therefore depends not only on system accuracy but also on whether employees believe the system respects their dignity, autonomy, and right to fair treatment.

Digital monitoring can undermine trust when employees experience surveillance as excessive, asymmetric, or disconnected from meaningful work improvement. Research on algorithms as work designers shows that digital systems can alter job autonomy, task discretion, feedback, and workload intensity, thereby reshaping how employees experience the employment relationship [16]. If workers believe that monitoring data are used mainly for punishment, ranking, or replacement, digital tools become symbols of managerial suspicion rather than support. Employee trust is strengthened when monitoring is proportionate, purpose-specific, transparent, and linked to safety, learning, coordination, or service quality.

Algorithmic fairness is central to employee trust because automated decisions can affect hiring, scheduling, promotion, pay, and performance evaluation. Studies of algorithmic management show that workers respond emotionally and morally to automated decisions, especially when they perceive them as unfair, impersonal, or difficult to contest [17]. Concerns about unfair bias are particularly important because trust in artificial intelligence depends on whether employees see automated systems as procedurally just and open to challenge [18]. **Table 2** identifies the dimensions of employee trust in digital monitoring and algorithmic management.

Table 2. Employee Trust in Digital Systems: Transparency, Fairness, Autonomy, and Voice

Employee trust dimension	Trust-building condition	Trust erosion risk	Practical design mechanism	Managerial responsibility
Transparency	Employees understand what data are collected, how systems work, and how outputs are used	Hidden monitoring, unclear scoring rules, unexplained rankings, and ambiguous data retention	System notices, plain-language model explanations, data-use maps, and role-specific training	Explain digital systems before implementation and update explanations when systems change
Fairness	Automated processes are perceived as consistent, unbiased, and procedurally just	Biased evaluation, unequal error rates, opaque promotion or scheduling decisions, and algorithmic reductionism	Bias testing, procedural justice reviews, human appeal routes, and fairness dashboards	Treat fairness as an ongoing governance process rather than a one-time technical validation
Autonomy	Digital systems support work quality without removing necessary discretion	Over-standardisation, micromanagement, work intensification, and reduced professional judgement	Adjustable decision support, human override, context-sensitive rules, and autonomy safeguards	Preserve meaningful human discretion where work requires judgement and contextual knowledge
Voice	Employees can question, contest, and improve digital systems	No appeal process, fear of retaliation, exclusion from design, and ignored worker feedback	Consultation forums, appeal channels, participatory design workshops, and feedback loops	Include employees as stakeholders in system design, evaluation, and revision
Trust repair	Management acknowledges harm and corrects unfair or intrusive system use	Defensive communication, denial of bias, continued use of contested tools, and lack of accountability	Independent review, suspension of harmful practices, corrective redesign, and communication of remedies	Repair trust through changed governance, not only through reassurance

Employee trust also depends on whether digital systems are framed as augmentation or substitution. The automation–augmentation paradox shows that artificial intelligence can enhance managerial and operational capabilities, but it can also create anxiety when employees perceive automation as a threat to judgement, status, or job security [19]. Motivation research further suggests that algorithmic management can weaken worker motivation when it frustrates autonomy, competence, or relatedness [20]. For this reason, firms should position digital systems as tools that improve decision quality while preserving voice, learning, and accountable human oversight.

Platform and Regulatory Trust

Platform trust concerns whether firms believe that digital platforms will govern access, data, visibility, and ecosystem participation fairly. Platform ecosystems can invert the traditional firm by enabling external complementors to create value around platform infrastructures, but this also gives platform owners considerable influence over rules, interfaces, and market opportunities [3]. Businesses therefore assess whether platforms provide predictable governance, reasonable data reciprocity, and fair treatment of ecosystem participants. Trust weakens when platform owners appear to exploit dependence, change rules without warning, or compete against participants using privileged data.

Digital platforms also create trust challenges because they operate as meta-organizations that coordinate many actors without fully absorbing them into a single hierarchy. Research on platform ecosystems as meta-organizations shows that platform strategies shape participation, complementor incentives, and the distribution of value across the ecosystem [11]. This means that trust is not only interpersonal or contractual but also architectural, because governance rules are embedded in technical interfaces, ranking systems, access protocols, and data infrastructures. Firms must therefore evaluate platform trust as a strategic risk rather than as a simple channel-management issue.

Platform dependence becomes particularly problematic when digital markets concentrate power around a small number of infrastructures. Studies of platform competition show that firms operating in digital markets face strategic constraints because platform owners can shape visibility, standards, interoperability, and competitive positioning [21]. The maturation of the platform economy further highlights concerns about platform power, pervasiveness, and asymmetrical control over data and market access [22]. Trust in platforms therefore requires credible commitments to fair governance, transparent rule changes, non-discriminatory access, and accountable dispute resolution.

Regulatory trust concerns whether regulators believe that firms act in good faith when collecting data, deploying algorithms, managing privacy, and responding to harm. AI governance research suggests that accountability must be layered across technical design, organizational processes, and institutional oversight, which means firms cannot rely only on internal assurances [12]. Regulatory confidence is strengthened when firms maintain documentation, cooperate with oversight, disclose material risks, and demonstrate a history of corrective action. Once regulatory trust is lost, compliance becomes more costly because regulators may interpret later behaviour through suspicion rather than credibility.

Proposed Digital Trust Management Framework

The proposed Digital Trust Management Framework treats trust as a systemic property of data-driven business ecosystems. Its premise is that customers, employees, platforms, and regulators each evaluate different signals, but these signals are connected through shared expectations of transparency, fairness, accountability, security, and responsible governance. Research on internet privacy concern shows that stakeholder judgments are multidimensional and shaped by perceived risks, institutional conditions, and organizational practices [23]. A firm therefore cannot credibly claim to be trustworthy to customers while ignoring employee surveillance harms, platform dependence risks, or regulatory accountability.

Figure 1 presents the Digital Trust Management Framework as an integrated system linking customers, employees, platforms, and regulators through shared trust mechanisms.

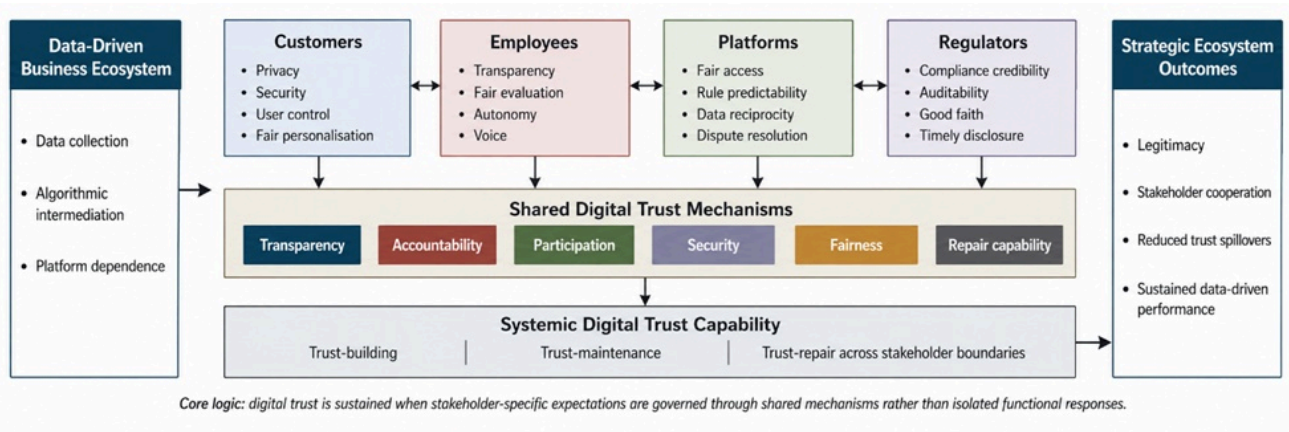


Figure 1. Digital Trust Management Framework for Customers, Employees, Platforms, and Regulators in Data-Driven Business Ecosystems

The framework has two layers. The first layer identifies stakeholder-specific trust drivers: privacy and control for customers, fairness and autonomy for employees, reciprocity and predictability for platforms, and integrity and compliance credibility for regulators. The second layer identifies cross-stakeholder mechanisms that apply across all groups, including transparency, accountability, participation, security, explainability, and repair capability. This layered design extends trustworthy artificial intelligence research by translating technical and ethical trust principles into a managerial framework for ecosystem-level trust governance [4].

The framework also highlights trust spillovers. A customer data breach can weaken employee trust if workers conclude that internal data systems are similarly unsafe, and it can reduce regulatory trust if the breach reveals poor documentation or delayed disclosure. A biased algorithmic HR system can also damage customer trust if the firm’s public identity depends on fairness, responsibility, or ethical technology use, while platform partners may question whether the firm can meet ecosystem standards. Research on AI fairness shows that fairness problems are not merely technical defects but socially interpreted failures of responsibility and legitimacy [24].

Table 3 presents the proposed Digital Trust Management Framework across all stakeholder groups. The framework is designed as a practical integration device rather than a diagnostic checklist because the main managerial task is to coordinate trust responsibilities across functions that normally operate separately. It helps managers ask whether customer-facing data practices, employee-facing digital systems, platform relationships, and regulatory commitments are mutually reinforcing or mutually undermining. In this sense, digital trust management becomes a strategic governance capability that connects data strategy, organizational design, ecosystem participation, and institutional legitimacy.

Table 3. Digital Trust Management Framework: Stakeholder-Specific Trust Mechanisms and Cross-Stakeholder Integration

Stakeholder group	Primary trust concern	Main trust drivers	Erosion triggers	Building mechanisms	Repair mechanisms	Cross-stakeholder integration logic
Customers	Whether the firm collects, uses, protects, and explains personal data responsibly	Privacy, security, transparency, control, fairness, and value alignment	Data breaches, hidden data use, manipulative personalisation, biased automated decisions, and weak consent	Privacy-by-design, clear consent, explainable personalisation, security assurance, user control, and customer education	Breach response, apology with accountability, compensation where appropriate, data-use reform, and public progress reporting	Customer trust signals market legitimacy and influences regulator confidence, platform reputation, and employee pride
Employees	Whether digital systems treat workers fairly and support rather than control them	Transparency, procedural justice, autonomy, voice, explainability, and human oversight	Intrusive surveillance, opaque scoring, biased HR automation, reduced discretion, and displacement fears	Participatory design, fairness audits, appeal rights, human-in-the-loop governance, and role-specific training	Independent review, redesign of contested systems, reinstatement of voice channels, and transparent correction of unfair outcomes	Employee trust affects implementation quality, ethical culture, customer service, and credibility

						during external scrutiny
Platforms	Whether ecosystem governance is fair, predictable, and mutually beneficial	Reciprocity, rule stability, data access clarity, dispute resolution, and non-discriminatory treatment	Sudden rule changes, data asymmetry, self-preferencing, opaque rankings, and unfair access restrictions	Contract clarity, ecosystem communication, shared standards, transparent governance rules, and dispute mechanisms	Renegotiation, mediation, data-sharing correction, restoration of access, and governance commitments	Platform trust shapes ecosystem resilience, business continuity, and the firm's ability to deliver customer value
Regulators	Whether the firm demonstrates good faith, compliance credibility, and responsible governance	Documentation, cooperation, auditability, risk controls, ethical intent, and timely disclosure	Non-compliance, delayed reporting, weak accountability, repeated incidents, and misleading assurances	Compliance-by-design, audit trails, risk registers, governance boards, and proactive regulatory engagement	Corrective action plans, independent audits, transparent reporting, leadership accountability, and sustained monitoring	Regulatory trust influences public legitimacy, customer confidence, platform eligibility, and employee perceptions of organizational integrity
Integrated ecosystem	Whether trust mechanisms are coordinated across all stakeholder relationships	Shared governance, cross-functional accountability, consistent communication, and systemic risk awareness	Siloed responses, inconsistent messages, unresolved spillovers, and narrow compliance thinking	Trust councils, integrated dashboards, stakeholder mapping, scenario planning, and aligned metrics	Cross-stakeholder repair protocols, coordinated communication, root-cause analysis, and long-term assurance reporting	Digital trust is sustained when each stakeholder relationship reinforces the others rather than transferring risk between them

Managerial Application

Managers can apply the framework by beginning with a digital trust audit that maps where stakeholder expectations are strongest and where current practices are weakest. Such an audit should examine customer privacy practices, employee-facing algorithms, platform dependencies, and regulatory documentation as parts of one trust system. Work on data privacy and marketing shows that privacy choices affect customer relationships and firm performance, which means trust audits should connect ethical exposure with strategic outcomes [14]. The audit should identify not only direct risks but also spillover pathways through which one stakeholder failure could affect others.

A second application is the creation of cross-functional trust governance. Digital trust cannot be assigned only to legal, compliance, information security, marketing, or human resources because each function sees only part of the trust system. Transparency research shows that stakeholders need explanations that fit their context, which requires

coordination among technical experts, managers, legal teams, and communication functions [9]. A cross-functional trust council can align data policies, employee system design, platform commitments, and regulatory reporting so that the firm speaks and acts consistently across stakeholder groups.

A third application is integrated communication before, during, and after digital trust events. In normal conditions, firms should communicate how data are used, how algorithms are governed, how employees can contest automated decisions, how platforms are engaged, and how compliance responsibilities are monitored. In crisis conditions, communication must move quickly from acknowledgement to accountability and remedy because privacy violations damage online trust when firms appear evasive or irresponsible [5]. Trust repair therefore requires coordinated messaging that addresses customers, employees, platforms, and regulators without creating contradictions among them.

Figure 2 illustrates how trust erosion in one stakeholder domain can cascade across the wider digital business ecosystem and how coordinated repair mechanisms can contain the damage.

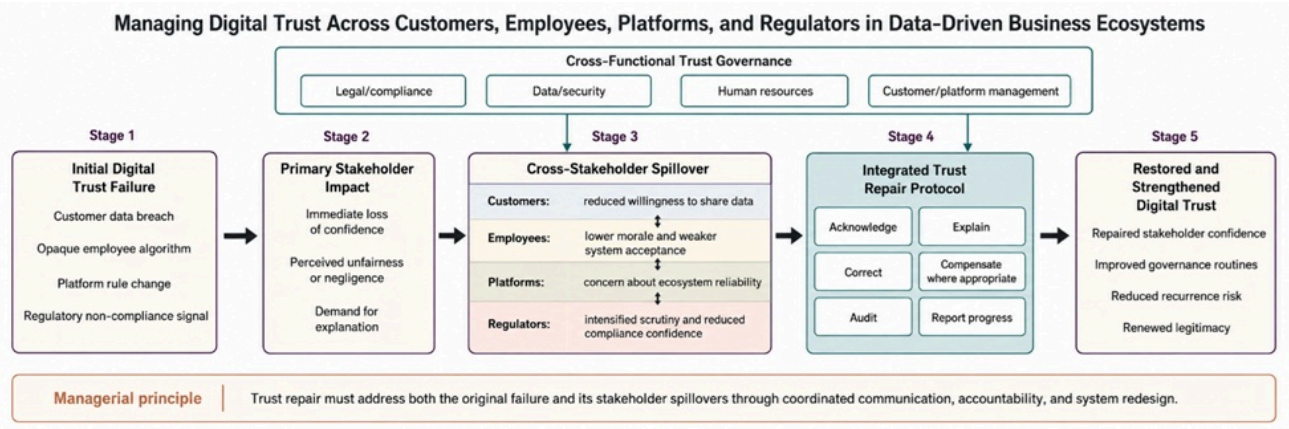


Figure 2. Cross-Stakeholder Trust Spillover and Repair Pathway in Data-Driven Business Ecosystems

A fourth application is the development of trust repair protocols. These protocols should define escalation triggers, responsible decision makers, stakeholder-specific remedies, communication standards, independent review procedures, and post-incident monitoring. Procedural justice research in algorithmic human resource decisions shows that eliminating one form of bias may still be perceived as unfair if affected individuals do not experience the process as legitimate [25]. Managers should therefore repair both substantive harm and procedural harm by correcting outcomes, explaining processes, enabling appeals, and showing how governance has changed.

Conclusion

This article has argued that digital trust is a systemic asset in data-driven business ecosystems. Customers, employees, platforms, and regulators do not evaluate organizational trustworthiness in isolation because the same data practices, algorithmic systems, and governance failures can affect multiple stakeholder relationships. Trust erosion in one domain can therefore cascade across the ecosystem and damage legitimacy, cooperation, and performance.

The proposed Digital Trust Management Framework contributes an integrated way to understand and manage these interdependencies. It identifies stakeholder-specific trust drivers while also showing that transparency, accountability, participation, security, fairness, and repair capability operate across all stakeholder groups. The framework shifts managerial attention from isolated trust problems to the governance of trust as an interconnected organizational capability.

Firms that compete through data, platforms, and digital systems need trust strategies that are proactive, coordinated, and repair-ready. Future research can empirically test the framework, examine which trust mechanisms are most effective under different conditions, and explore how trust spillovers unfold over time. For managers, the central implication is clear: digital trust must be designed, monitored, and repaired as a whole ecosystem rather than as a series of disconnected stakeholder concerns.

Acknowledgements

None

Conflict of Interest

None

Financial Support

None

Ethics Statement

None

Received: 05 Jun 2025

Revised: 20 Jul 2025

Accepted: 05 Sep 2025

Published online: 18 September 2025

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

- Martin KD, Borah A, Palmatier RW. Data privacy: Effects on customer and firm performance. *J Mark.* 2017;81(1):36-58.
- Kellogg KC, Valentine MA, Christin A. Algorithms at work: The new contested terrain of control. *Acad Manag Annal.* 2020;14(1):366-410.
- Parker G, Van Alstyne M, Jiang X. Platform ecosystems: How developers invert the firm1. *MIS Q.* 2017;41(1):255-66.
- Thiebes S, Lins S, Sunyaev A. Trustworthy artificial intelligence. *Electron Mark.* 2021;31(2):447-64.
- Martin K. The penalty for privacy violations: How privacy violations impact trust online. *J Bus Res.* 2018;82:103-16.

- De Laat PB. Algorithmic decision-making based on machine learning from big data: can transparency restore accountability?. *Philos Technol.* 2018;31(4):525-41.
- Glikson E, Woolley AW. Human trust in artificial intelligence: Review of empirical research. *Acad Manag Annal.* 2020;14(2):627-60.
- Martin K. Ethical Implications and Accountability of Algorithms. *J Bus Ethics.* 2019;160(4):835-50.
- Felzmann H, Villaronga EF, Lutz C, Tamò-Larrieux A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data Soc.* 2019;6(1):2053951719860542.
- Constantinides P, Henfridsson O, Parker GG. Introduction—platforms and infrastructures in the digital age. *Inf Syst Res.* 2018;29(2):381-400.
- Kretschmer T, Leiponen A, Schilling M, Vasudeva G. Platform ecosystems as meta-organizations: Implications for platform strategies. *Strateg Manag J.* 2022;43(3):405-24.
- Gasser U, Almeida VA. A layered model for AI governance. *IEEE Internet Comput.* 2017;21(6):58-62.
- Karwatzki S, Dytnynko O, Trenz M, Veit D. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *J Manag Inf Syst.* 2017;34(2):369-400.
- Martin KD, Murphy PE. The role of data privacy in marketing. *J Acad Mark Sci.* 2017;45(2):135-55.
- Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digital technologies: Tensions in privacy and data. *J Acad Mark Sci.* 2022;50(6):1299-323.
- Parent-Rochelleau X, Parker SK. Algorithms as work designers: How algorithmic management influences the design of jobs. *Hum Res Manag Rev.* 2022;32(3):100838.
- Lee MK. Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management. *Big Data Soci.* 2018;5(1):2053951718756684.
- Langer M, König CJ, Back C, Hemsing V. Trust in artificial intelligence: Comparing trust processes between human and automated trustees in light of unfair bias. *J Bus Psychol.* 2023;38(3):493-508.
- Raisch S, Krakowski S. Artificial intelligence and management: The automation–augmentation paradox. *Acad Manag Rev.* 2021;46(1):192-210.
- Gagné M, Parent-Rochelleau X, Bujold A, Gaudet MC, Lirio P. How algorithmic management influences worker motivation: A self-determination theory perspective. *Can Psychol.* 2022;63(2):247.
- Cennamo C. Competing in digital markets: A platform-based perspective. *Acad Manag Perspect.* 2021;35(2):265-91.
- Kenney M, Bearson D, Zysman J. The platform economy matures: Measuring pervasiveness and exploring power. *Soc Econ Rev.* 2021;19(4):1451-83.
- Hong W, Chan FK, Thong JY. Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *J Bus Ethics.* 2021;168(3):539-64.
- John-Mathews JM, Cardon D, Balagué C. From reality to world. A critical perspective on AI fairness. *J Bus Ethics.* 2022;178(4):945-59.
- Newman DT, Fast NJ, Harmon DJ. When eliminating bias isn't fair: Algorithmic reductionism and procedural justice in human resource decisions. *Organ Behav Hum Decis Process.* 2020;160:149-67.