ORIGINAL RESEARCH **Open access**

Classifying Digital Business Risks: Strategic Lock-In, Data Privacy, Algorithmic Bias, Platform Dependence, Workforce Displacement, and Reputation Loss

Camila Ortega[1*], Diego Molina[1], Andres Perez[2], Valeria Soto[1]

Abstract

Digital transformation has expanded the risk exposure of firms beyond conventional operational, financial, and compliance categories. As organizations adopt artificial intelligence, cloud infrastructure, digital platforms, data-intensive business models, and automation, they face risks that are technically embedded, strategically consequential, and socially visible. These risks often emerge simultaneously across technology architectures, data practices, organizational routines, labor systems, and stakeholder relationships. Despite the growing importance of digital risk, existing business risk frameworks frequently classify these risks in fragmented ways. Some frameworks treat privacy as a legal compliance matter, bias as a technical problem, platform dependence as a sourcing issue, and workforce disruption as a human resource concern. This fragmentation limits managerial understanding of how digital risks interact, accumulate, and escalate across the firm. This article develops an original taxonomy of digital business risks. It classifies the risk landscape into six categories: strategic lock-in, data privacy, algorithmic bias, platform dependence, workforce displacement, and reputation loss. The taxonomy is designed to distinguish categories clearly while also showing how they may interact in practice. The article follows a conceptual taxonomy development approach based on synthesis of peer-reviewed journal articles published. It applies formal classification criteria related to risk source, impact domain, time horizon, controllability, regulatory exposure, and organizational response capability. The resulting taxonomy provides definitions, sub-dimensions, comparative criteria, and managerial use cases. The contribution of the article is a systematic classification framework for digital business risk identification and assessment. It offers a shared language for researchers, managers, boards, and risk professionals seeking to govern digital transformation more effectively. The taxonomy also creates a foundation for future empirical validation and integration into enterprise risk management and digital strategy processes.

Keywords Platform dependence, Algorithmic bias, Taxonomy, Digital business risks, Strategic lock-in, Data privacy

*Correspondence:
Camila Ortega
camila.ortega@gmail.com
[1] Department of Digital Transformation Management, Faculty of Business, University of Lima, Lima, Peru
[2] Department of Analytics and Strategic Systems, Faculty of Economics, Pontifical Catholic University of Peru, Lima, Peru

Introduction

Digital transformation has shifted business risk from discrete technology failures toward interconnected strategic, organizational, legal, and reputational vulnerabilities. Research on digital innovation shows that digital technologies alter how firms create value, coordinate activities, and renew strategy, making risk inseparable from digital business model design [1]. Digital transformation is therefore not only a modernization process but also a restructuring of organizational exposure to new forms of uncertainty, dependency, and control [2].

A central challenge is that digital risks often outpace the categories used in traditional risk management. Studies of digital transformation show that firms increasingly rely on data infrastructures, algorithmic systems, platforms, and digitally enabled routines that cut across functional boundaries [3]. This means that a failure in one domain, such as data governance or platform access, can rapidly affect customer trust, operational continuity, strategic flexibility, and regulatory compliance.

Existing research has identified several important digital risk domains, but these domains are often studied separately. Strategy scholars emphasize digital renewal and ecosystem positioning, while information systems scholars examine platforms, infrastructures, and digital options [4, 5]. At the same time, marketing and ethics research has examined privacy, algorithmic accountability, and consumer trust as distinct concerns rather than as elements of a broader digital business risk architecture [6, 7].

This article addresses that gap by proposing a taxonomy that classifies digital business risks into six categories: strategic lock-in, data privacy, algorithmic bias, platform dependence, workforce displacement, and reputation loss. These categories are selected because they represent recurring risk patterns in digital business research and because each has a distinct source, impact domain, and governance challenge [8-13]. The article first explains why a dedicated taxonomy is needed, then defines classification criteria, develops each risk category, compares the six categories in a matrix, and discusses managerial use cases.

Need for a Digital Business Risk Taxonomy

A dedicated taxonomy is needed because digital risks are not simply conventional risks expressed through new tools. Digital transformation changes the architecture of firms by embedding software, data, platforms, automation, and algorithmic decision-making into core value creation processes [2]. As a result, digital risks may arise from the same technologies that generate efficiency, personalization, scalability, and strategic renewal [8].

The absence of a systematic taxonomy creates conceptual ambiguity. For example, dependence on a cloud provider may be interpreted as a procurement risk, an infrastructure risk, a strategic lock-in risk, or a platform dependence risk depending on the analytical frame used [5, 14]. Similarly, algorithmic bias may be treated as a model quality issue, an ethical concern, a legal exposure, or a reputational threat, even though these interpretations refer to different aspects of the same underlying risk chain [7, 15].

A taxonomy is also necessary because digital risks interact across organizational boundaries. Platform dependence can reduce bargaining power and limit strategic flexibility, while privacy failures can damage consumer trust and trigger reputational consequences [10, 16]. By classifying digital risks according to explicit criteria, managers can move from isolated issue management toward integrated digital risk governance.

Figure 1 presents the proposed six-category taxonomy of digital business risks and shows how the categories organize the fragmented risk landscape created by digital transformation.

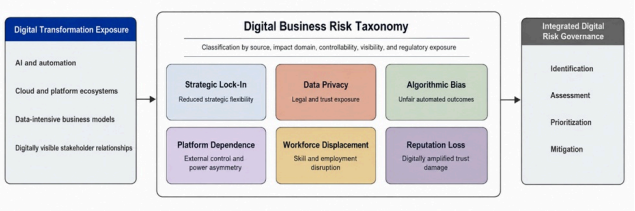

Figure 1. Six-Category Taxonomy of Digital Business Risks in Digitally Transforming Firms

Classification Criteria

The taxonomy is built on the principle that a risk category must be defined by more than its visible outcome. A data breach, for example, may produce reputational damage, regulatory penalties, operational disruption, and customer churn, but its primary classification depends on the underlying source of exposure and the organizational capability required to control it [6, 17]. This approach follows the logic that digital business risks should be classified by causal origin, impact pathway, and governance response rather than by surface-level symptoms alone.

The first classification criterion is risk source. Digital business risks may originate from technology architecture, data collection and processing, algorithmic decision-making, platform intermediation, workforce automation, or public stakeholder reaction [1, 11-13]. Distinguishing the source of risk is necessary because different sources

require different controls, such as technical interoperability for lock-in, privacy governance for data risk, fairness auditing for algorithmic bias, or reskilling strategies for displacement.

The second criterion is impact domain. Some digital risks primarily threaten strategic flexibility, while others create legal exposure, operational fragility, labor disruption, or reputational loss [18-21]. The taxonomy therefore treats impact as multidimensional but assigns each category according to its dominant organizational consequence, so that overlap does not erase conceptual distinction.

The third criterion is controllability, which refers to the degree to which the firm can prevent, mitigate, transfer, or adapt to the risk through internal governance. Strategic lock-in may be partially controllable through modular architecture, while platform dependence may be less controllable when external platform owners control rules, interfaces, or data access [22, 23]. **Table 1** outlines the classification criteria used to differentiate the six digital business risk categories.

Table 1. Classification Criteria for Digital Business Risks: Dimensions of Risk Source, Impact Domain, and Controllability

Classification criterion	Definition	Application to digital business risk classification	Illus disti produ the c
Risk source	The primary origin of the risk within the digital business system.	Separates risks generated by technology architecture, data practices, algorithms, platforms, automation, or stakeholder reactions.	Strate in orig tech and choice algo bias o in mode decisi
Impact domain	The main organizational area affected by the risk.	Identifies whether the dominant consequence is strategic, legal, operational, workforce-related, reputational, or market-facing.	Data risk produc and conse w worl displa ma proc capab empl conse
Controllability	The extent to which the firm can directly prevent, reduce, or govern the risk.	Distinguishes risks that are mainly internally governable from those shaped by external platforms, regulators, public audiences, or labor markets.	Algo bias red thr interna while depe ma constr ext pla gove
Time horizon	The expected speed and duration of risk emergence.	Differentiates slow-building strategic risks from sudden reputational or compliance crises.	Strate in accu over whe reputa can e rapidl visibl fai
Visibility	The extent to which the risk is observable to managers, regulators, customers, employees, or the public.	Helps classify hidden technical exposures separately from highly visible stakeholder-facing failures.	Vendo may invisi switc require pri breac bec publicl imme
Regulatory exposure	The degree to which laws, standards, or formal accountability mechanisms shape the risk.	Identifies categories that require legal compliance, auditability, documentation, or external reporting.	Data a algo bias stro regu impli than for

			strate i
Interdependence potential	The likelihood that one risk category will trigger or intensify another.	Captures cascading effects across digital business systems.	A b algorit trig repu loss pla depe can ir data and s lock-i
Managerial response capability	The organizational capability most needed to assess and mitigate the risk.	Links each category to practical governance mechanisms, such as architecture design, privacy management, fairness review, platform strategy, workforce planning, or crisis communication.	Wor displa req reskill work r w reputa require monito stake resp capa

Figure 2 illustrates how the classification criteria convert broad digital transformation exposure into six mutually distinguishable digital business risk categories.

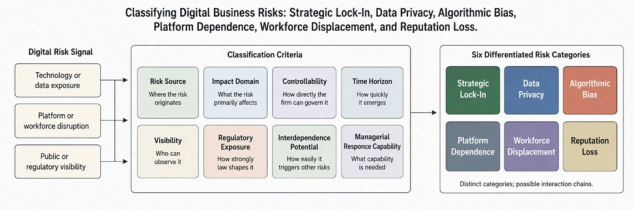

Figure 2. Classification Logic for Differentiating Digital Business Risk Categories

Strategic and Platform-Related Risks

Strategic lock-in refers to the risk that digital transformation choices reduce a firm's future strategic flexibility. This risk emerges when firms commit deeply to particular technologies, vendors, data architectures, software stacks, or integration pathways that become costly to reverse [8]. Digital strategy research suggests that these choices matter because digital technologies can shift firms from incremental tool adoption toward more fundamental changes in business design and competitive positioning [18].

Strategic lock-in is distinct from ordinary procurement dependence because it accumulates through technical interconnection, data migration barriers, organizational learning effects, and complementary investments. Once a firm's processes, employees, analytics models, and customer interfaces are built around a specific vendor or architecture, switching becomes difficult even when superior alternatives appear [14]. Platform and ecosystem research shows that such dependence is intensified when firms operate within interdependent digital environments where standards, interfaces, and governance rules are shaped by powerful external actors [22].

Platform dependence is the related but distinct risk of relying heavily on external digital platforms for market access, infrastructure, customer interaction, or data visibility. Digital platform scholarship emphasizes that firms using platforms may benefit from scale, network effects, and innovation opportunities while also losing control over rules, ranking systems, pricing structures, and access to users [5, 9]. Gawer's analysis of digital platform boundaries further shows that platform dependence is shaped by the interaction between firm scope, platform sides, and digital interfaces [24].

For taxonomy purposes, strategic lock-in is classified as a strategic flexibility risk, whereas platform dependence is classified as an external control and power-asymmetry risk. The two risks often overlap, but they are not identical: a firm may be locked into its own legacy enterprise architecture without being platform-dependent, or it may be platform-dependent even when its internal systems remain technically flexible [16, 23]. **Table 2** defines strategic lock-in and platform dependence risks with sub-categories, triggers, and examples.

Table 2. Strategic and Platform-Related Digital Business Risks: Definitions, Sub-Types, and Illustrative Cases

Risk category	Core definition	Main sub-types	Typical triggers

Strategic lock-in	Loss of future strategic flexibility caused by deep commitment to specific technologies, vendors, architectures, or digital routines.	Vendor lock-in; architecture lock-in; data format lock-in; workflow lock-in; capability lock-in.	Proprietary systems, long term contracts high switching costs, comple integrations, accumulated technical debt
Technology path dependence	Progressive narrowing of strategic options because earlier technology decisions constrain later choices.	Legacy system dependence; sunk-cost escalation; integration dependency; internal skill dependence.	Prior investments, staff specialization incompatible systems, lack of documentation cumulative customization
Platform dependence	Reliance on third-party digital platforms for infrastructure, market access, transactions, data flows, or customer visibility.	Cloud dependence; marketplace dependence; app-store dependence; social-media dependence; payment-platform dependence.	Platform concentration API reliance, rule changes, ranking opacity, dependence on platform analytics.
Platform power asymmetry	Exposure to decisions made by platform owners that the dependent firm cannot easily influence.	Rule-setting dependence; visibility dependence; pricing dependence; data-access dependence.	Platform governance changes, unilateral policy updates algorithmic ranking changes, restricted data access.
Combined strategic-platform risk	Risk generated when internal lock-in and external platform dependence reinforce one another.	Embedded platform architecture; platform-specific data models; dependent ecosystem capability.	Deep integration int one platform, lack of portability, organizationa dependence on platform-specific tools.

Data Privacy and Algorithmic Bias Risks

Data privacy risk refers to the exposure created by collecting, storing, processing, sharing, and monetizing personal or sensitive data. Marketing and consumer research shows that privacy is not merely a compliance issue but a central condition of customer trust and firm performance in data-driven markets [6, 10]. As firms increase personalization, predictive analytics, and cross-channel data integration, privacy risk becomes a recurring feature of digital business models rather than an exceptional legal problem.

The taxonomy classifies privacy risk as a data-driven legal and trust risk. Its sources include excessive data collection, weak consent mechanisms, insecure storage, unauthorized sharing, secondary use of data, and cross-border data transfer complexity [17]. Digital economics research further shows that data-based innovation depends on information flows, but these same flows create risks when consumer expectations, regulatory duties, and business incentives are misaligned [25].

Algorithmic bias risk refers to the possibility that automated or AI-supported decisions produce unfair, discriminatory, or systematically distorted outcomes. This risk emerges from biased training data, proxy variables, model design choices, feedback loops, and organizational overreliance on algorithmic outputs [15, 26]. It is especially important in digital business because algorithmic systems increasingly shape pricing, hiring, credit, service prioritization, recommendation, moderation, and customer segmentation.

The relationship between privacy and algorithmic bias is complex because attempts to reduce one risk may intensify the other. For example, fairness auditing may require demographic or sensitive data, while privacy minimization

may limit the ability to detect discriminatory outcomes [27, 28]. **Table 3** defines data privacy and algorithmic bias risks with their key characteristics and regulatory implications.

Table 3. Data Privacy and Algorithmic Bias Risks: Nature, Drivers, and Organizational Consequences

Risk category	Core definition	Main drivers	Ke charact
Data privacy risk	Exposure arising from improper, excessive, insecure, or non-transparent handling of personal or sensitive data.	Data collection expansion, personalization, third-party sharing, weak consent, poor data security, cross-border processing.	Leg sensi custom depend high vi after b stro docume nee
Consent and transparency risk	Risk that users do not understand or meaningfully control how their data are used.	Complex privacy notices, bundled consent, opaque data reuse, behavioral tracking.	Trust-b commun sensi difficu correc user ba
Data security and breach risk	Risk that personal or sensitive data are exposed through cyberattack, unauthorized access, or poor controls.	Weak access control, vendor exposure, cloud misconfiguration, insider misuse, inadequate encryption.	Sud escala public v strong and fin consequ
Algorithmic bias risk	Exposure arising when algorithmic systems produce unfair, discriminatory, or systematically unequal outcomes.	Biased training data, proxy variables, unrepresentative samples, feedback loops, model opacity.	Often h until aud challe ethic sensi lega consequ
Explainability and accountability risk	Risk that organizations cannot justify or contest algorithmic decisions.	Black-box models, fragmented ownership, weak documentation, lack of human review.	Govern inten linke mana accoun difficu compl syste
Privacy-bias interaction risk	Risk generated when privacy protection and fairness assessment create governance trade-offs.	Data minimization, demographic-data restrictions, fairness auditing needs, anonymization limits.	Cro functi lega comp techn diffic

Workforce and Reputation Risks

Workforce displacement risk refers to the possibility that automation, artificial intelligence, robotics, and algorithmic systems will reduce demand for some jobs, alter skill requirements, or destabilize established work arrangements. Studies of automation exposure show that digital technologies can substitute for routine tasks while also changing the composition of work across sectors and occupations [12, 29]. In a taxonomy of digital business risks, this category is therefore classified as a people-driven capability and organizational disruption risk.

Workforce displacement should not be reduced to job loss alone. Employee perceptions of smart technologies, artificial intelligence, robotics, and algorithms influence acceptance, anxiety, resistance, and adaptation in digital workplaces [30]. Research on the labor impact of artificial intelligence also suggests that the effects of AI depend on task structure, organizational redesign, education, labor-market institutions, and the distribution of complementary skills [31].

The managerial challenge is that digital automation can produce both displacement and augmentation. Work design research argues that automation and algorithms require careful attention to autonomy, task meaning, coordination, and human capability development [20]. Similarly, the automation–augmentation paradox shows that AI can

simultaneously replace managerial or operational tasks and create new demands for judgment, oversight, and complementary human expertise [32].

Reputation loss risk refers to digitally amplified damage to stakeholder trust after visible failures such as data breaches, unfair algorithms, platform controversies, automation backlash, or unethical digital practices. Evidence on data breach announcements shows that privacy and security failures can affect customer behavior, while research on cyberattacks indicates that successful attacks can harm firm reputation and market valuation [13, 21]. **Table 4** defines workforce displacement and reputation loss risks, linking technological triggers to organizational impacts.

Table 4. Workforce Displacement and Reputation Loss Risks: Mechanisms, Amplifiers, and Strategic Implications

Risk category	Core definition	Main mechanisms	Digital amplifier
Workforce displacement risk	Exposure arising when digital technologies automate tasks, reduce job demand, or make existing skills obsolete.	Task substitution, process automation, AI decision support, robotics deployment, workflow redesign.	Rapid scali of automatio algorithmi manageme platform-based labo models, remote digi coordinatic
Skill obsolescence risk	Risk that employee capabilities no longer match digitally transformed work systems.	New analytics tools, AI-enabled workflows, cloud-based operations, data-intensive decision-making.	Fast technolog cycles, vendor-specific too continuou software updates.
Organizational disruption risk	Risk that automation changes coordination, authority, and accountability faster than the organization can absorb.	Algorithmic control, automated monitoring, changed decision rights, reduced human discretion.	Real-time analytics performan dashboard automate workflow allocation
Reputation loss risk	Stakeholder trust damage caused by visible digital failures or perceived irresponsible technology use.	Breaches, biased algorithms, service outages, unethical data practices, automation controversies.	Social mec acceleratio online reviews, news virali activist scrutiny, public dashboard
Cascading reputation risk	Reputational damage triggered by another digital risk category.	Privacy breach, discriminatory AI, platform failure, workforce backlash, vendor incident.	Rapid pub interpretatio screenshot algorithmi amplificatio influence commenta

Comparative Risk Taxonomy Matrix

The six categories can now be compared as a structured taxonomy rather than as isolated issues. Strategic lock-in and platform dependence are primarily strategic and structural, while data privacy and algorithmic bias are strongly tied to legal accountability, trust, and responsible data use [7, 10, 16]. Workforce displacement and reputation loss, by contrast, emphasize organizational adaptation and stakeholder perception, although both can be triggered by the other four risk categories [21, 30].

The taxonomy distinguishes categories by dominant source, dominant impact, time horizon, controllability, regulatory exposure, and mitigation difficulty. Strategic lock-in usually develops gradually as firms accumulate technical debt, platform-specific capabilities, and switching costs [14]. Reputation loss, however, may occur suddenly when a digital failure becomes public, even if its underlying causes have accumulated over many years [13].

Interrelationships are central to the taxonomy because digital risks often form chains. A platform-dependent firm may lack control over data access, which can weaken

privacy governance and reduce its ability to audit algorithmic outcomes [5, 24]. A biased AI system can then trigger legal scrutiny, customer backlash, employee concern, and reputation loss, demonstrating why risk categories must be differentiated but not treated as independent silos [26, 27].

The comparative matrix is designed to support systematic assessment without collapsing all risks into a single severity score. A firm can use the matrix to identify which risks are internal or external, immediate or cumulative, technical or social, and legally regulated or reputation-driven [17, 32]. **Table 5** presents the complete comparative taxonomy matrix across all six risk categories.

Table 5. Comparative Taxonomy Matrix of Digital Business Risks: Comparison across Strategic, Privacy, Bias, Platform, Workforce, and Reputation Dimensions

Risk category	Dominant risk source	Primary impact domain	Typical time horizon
Strategic lock-in	Technology architecture, vendor contracts, proprietary systems, accumulated technical debt.	Strategic flexibility, investment options, innovation capacity.	Medium to long term.
Data privacy	Personal data collection, processing, storage, sharing, and secondary use.	Legal compliance, customer trust, data governance.	Immediate to long term.
Algorithmic bias	Training data, model design, proxy variables, feedback loops, decision automation.	Fairness, legal accountability, decision legitimacy.	Medium term, but may become immediate after audit or public challenge.
Platform dependence	External platform governance, APIs, marketplace rules, cloud infrastructure, ranking systems.	Market access, bargaining power, operational continuity, data access.	Medium to long term, with sudden shocks after platform changes.
Workforce displacement	Automation, AI-enabled work redesign, robotics, algorithmic management.	Human capital, employment relations, organizational capability.	Medium to long term.
Reputation loss	Public stakeholder reaction to digital failures, ethical concerns, breaches, or algorithmic harm.	Trust, brand value, legitimacy, customer and investor confidence.	Immediate once visible, though causes may accumulate slowly.

Managerial Use Cases and Risk Assessment

The taxonomy can be used as a practical risk inventorying tool. Managers can map digital initiatives against the six categories before major investments in AI, cloud migration, platform partnerships, automation programs, or data-intensive customer systems [3]. This shifts digital risk assessment from reactive incident response toward

proactive classification of exposure sources, likely consequences, and governance responsibilities.

The taxonomy also supports prioritization and resource allocation. For example, a firm launching an AI-powered customer scoring system would need to assess data privacy risk from personal data processing, algorithmic bias risk from model outputs, reputation loss risk from public backlash, and strategic lock-in risk if the system depends on a proprietary vendor [15, 33]. By separating the categories, managers can avoid treating the initiative as only an IT, legal, marketing, or compliance matter.

A sample assessment scenario illustrates the taxonomy's practical logic. A retailer expanding through a major online marketplace and implementing automated personalization may identify platform dependence as the dominant external control risk, data privacy as the dominant legal trust risk, algorithmic bias as the dominant fairness risk, and reputation loss as the likely cascade if customers perceive manipulation or discrimination [10, 24, 26]. The taxonomy therefore helps managers assign ownership across strategy, technology, legal, human resources, marketing, and enterprise risk management rather than leaving digital risk fragmented across departments.

Figure 3 shows how managers can use the taxonomy to identify digital risk chains and assign coordinated governance responses across strategy, technology, legal, workforce, and reputation domains.

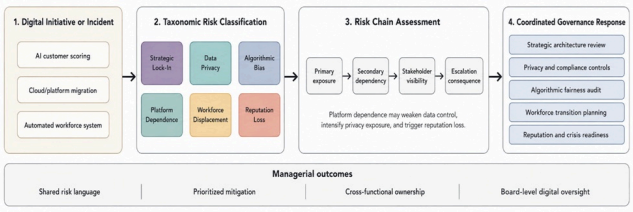

Figure 3. Managerial Use of the Digital Business Risk Taxonomy for Risk Chains, Prioritization, and Governance Response

Conclusion

This article has proposed a taxonomy for classifying digital business risks into six categories: strategic lock-in, data privacy, algorithmic bias, platform dependence, workforce displacement, and reputation loss. The taxonomy responds to the inadequacy of traditional risk frameworks for understanding risks generated by digital transformation, data-intensive business models, algorithmic systems, and platform-based competition. Its contribution lies in creating a structured language for distinguishing digital risks while recognizing their interdependence.

The taxonomy clarifies that digital business risks differ in source, impact domain, controllability, time horizon, visibility, regulatory exposure, and managerial response capability. Strategic lock-in and platform dependence threaten flexibility and control; data privacy and algorithmic bias threaten legality, fairness, and trust; workforce displacement and reputation loss threaten organizational continuity and stakeholder legitimacy. Together, these categories provide a practical basis for systematic identification, assessment, comparison, and mitigation.

Future research should empirically validate the taxonomy across industries, firm sizes, and digital maturity levels. Scholars can test whether the six categories capture distinct risk patterns, while managers can integrate the taxonomy into enterprise risk management, digital strategy formulation, technology governance, and board-level oversight. As digital transformation continues to reshape business systems, rigorous classification will become essential for responsible and strategically informed risk governance.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 10 May 2025 Revised: 20 Jun 2025 Accepted: 01 Aug 2025
Published online: 18 September 2025

References

Nambisan S, Lyytinen K, Majchrzak A, Song M. Digital innovation management: Reinventing innovation management research in a digital world. MIS Q. 2017;41(1):223-38.

Vial G. Understanding digital transformation: A review and a research agenda. Manag Digit Transform. 2021:13-66.

Verhoef PC, Broekhuizen T, Bart Y, Bhattacharya A, Dong JQ, Fabian N, et al. Digital transformation: A multidisciplinary reflection and research agenda. J Bus Res. 2021;122:889-901.

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

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

Martin KD, Murphy PE. The role of data privacy in marketing. J Acad Mark Sci. 2017;45(2):135-55.

Martin K. Ethical Implications and Accountability of Algorithms. J Bus Ethics. 2019;160(4):835-50.

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

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

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.

Frey CB, Osborne MA. The future of employment: How susceptible are jobs to computerisation?. Technol Forecast Soc Change. 2017;114:254-80.

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.

Rolland KH, Mathiassen L, Rai A. Managing digital platforms in user organizations: The interactions between digital options and digital debt. Inf Syst Res. 2018;29(2):419-43.

Rai A. Explainable AI: From black box to glass box. J Acad Mark Sci. 2020;48(1):137-41.

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

Bleier A, Goldfarb A, Tucker C. Consumer privacy and the future of data-based innovation and marketing. Int J Res Mark. 2020;37(3):466-80.

Adner R, Puranam P, Zhu F. What is different about digital strategy? From quantitative to qualitative change. Strateg Sci. 2019;4(4):253-61.

Acquisti A, Brandimarte L, Loewenstein G. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. J Consum Psychol. 2020;30(4):736-58.

Parker SK, Grote G. Automation, algorithms, and beyond: Why work design matters more than ever in a digital world. Appl psychol. 2022;71(4):1171-204.

Kamiya S, Kang JK, Kim J, Milidonis A, Stulz RM. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J Financ Econ. 2021;139(3):719-49.

Jacobides MG, Cennamo C, Gawer A. Towards a theory of ecosystems. Strateg Manag J. 2018;39(8):2255-76.

Karhu K, Gustafsson R, Lyytinen K. Exploiting and defending open digital platforms with boundary resources: Android's five platform forks. Inf Syst Res. 2018;29(2):479-97.

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

Goldfarb A, Tucker C. Digital economics. J Econ Lit. 2019;57(1):3-43.

Akter S, McCarthy G, Sajib S, Michael K, Dwivedi YK, D'Ambra J, et al. Algorithmic bias in data-driven innovation in the age of AI. Int J Inf Manag. 2021;60:102387.

Mittelstadt B. Principles alone cannot guarantee ethical AI. Nat mach intell. 2019;1(11):501-7.

Mehrabi N, Morstatter F, Saxena N, Lerman K, Galstyan A. A survey on bias and fairness in machine learning. ACM Comput Surv (CSUR). 2021;54(6):1-35.

Arntz M, Gregory T, Zierahn U. Revisiting the risk of automation. Econ Lett. 2017;159:157-60.

Brougham D, Haar J. Smart technology, artificial intelligence, robotics, and algorithms (STARA): Employees' perceptions of our future workplace. J Manag Organ. 2018;24(2):239-57.

Frank MR, Autor D, Bessen JE, Brynjolfsson E, Cebrian M, Deming DJ, et al. Toward understanding the impact of artificial intelligence on labor. Proc Natl Acad Sci U S A. 2019;116(14):6531-9.

Raisch S, Krakowski S. Artificial intelligence and management: The automation–augmentation paradox. Acad Manag Rev. 2021;46(1):192-210.

Shrestha YR, Ben-Menahem SM, Von Krogh G. Organizational decision-making structures in the age of artificial intelligence. Calif Manag Rev. 2019;61(4):66-83.