Deloitte.
Insights

FEATURE

Building digital trust: Technology can lead the way

Business leaders can put technologies at work to build the four pillars of digital trust

Nancy Albinson, Sam Balaji, and Yang Chu

Technologies used for digital transformation can also be leveraged to enhance trust—when they're used to enhance transparency, reinforce ethical practices, boost data privacy, and harden security.

GAINING CUSTOMERS' TRUST—not just in a business's products and services, but in its core purpose and principles—is fundamental to an enterprise's success. But what if efforts to drive your business's success also increase the risk of sparking customers' *dis*trust?

That's the dilemma that many business leaders find themselves in today as they pursue digital transformation efforts to embed technology into every facet of their operations. With the advent of digital technology, businesses have been asking customers to trust them in new and deeper ways, from asking for their personal information to tracking their online behavior through digital breadcrumbs.

At the same time, technology issues like security hacks, inappropriate or illegal surveillance, misuse of personal data, spread of fake news and misinformation, algorithmic bias, and lack of transparency are regularly hitting the headlines. The resulting distrust these incidents breed in stakeholders—employees, investors, and regulators as well as customers—can significantly damage an organization's reputation. Beyond that, it can weaken overall trust in the business community's ability to use technology responsibly.

The good news is that the same tools and technologies that drive digital transformation—and whose careless or unethical use can sabotage trust—can also help *build* trust among stakeholders and create benefits for society. What's more, their potential to help strengthen trust doesn't end with simply avoiding *negative* incidents such as data breaches. When used to enhance transparency, reinforce ethical and responsible practices, boost data privacy, and harden security—activities that we call *the four pillars of trust* (see figure 1)—digital tools and technologies can serve as *positive* enablers of both transformation and trust.

Pillar I: Transparency and accessibility

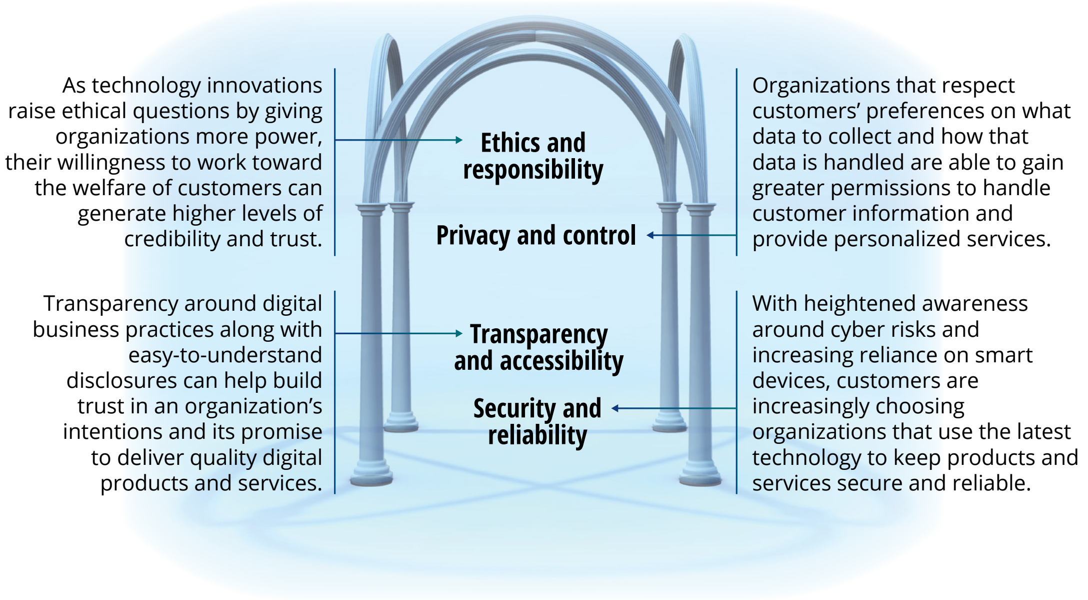
With the proliferation of digital products and services, stakeholders have become used to expecting increased transparency from the organizations they interact with. Even before they engage with digital platforms, consumers can summon up a vast amount of information online, not just about the products and services they're interested in but on the companies offering them as well. In return, they often provide personal and other confidential information to the company in question. They do this with an expectation of transparency about how this information is stored and used, including in the application of artificial intelligence (AI) or other decision-making tools. In fact, according to one survey, nearly nine out of 10 Americans (86 percent) believe that business transparency is more important today than ever before, and seven out of 10 (73 percent) will pay for products that promise total transparency.[1]

The upshot? Transparency and plain talk are imperative for companies looking to compete and gain an edge in the digital world. Here are some ways companies can seek to leverage technologies to foster transparency and accessibility, the first pillar of digital trust:

Enabling customers to easily evaluate the company and its offerings. One of the things digital platforms are experimenting with is providing more transparency around their

FIGURE 1

The four pillars of trust


As technology innovations raise ethical questions by giving organizations more power, their willingness to work toward the welfare of customers can generate higher levels of credibility and trust.
Ethics and responsibility
Organizations that respect customers' preferences on what data to collect and how that data is handled are able to gain greater permissions to handle customer information and provide personalized services.
Privacy and control
Transparency around digital business practices along with easy-to-understand disclosures can help build trust in an organization's intentions and its promise to deliver quality digital products and services.
Transparency and accessibility
With heightened awareness around cyber risks and increasing reliance on smart devices, customers are increasingly choosing organizations that use the latest technology to keep products and services secure and reliable.
Security and reliability

Source: Deloitte analysis.

business models. For example, some companies label sponsored or promotional content as such on their websites or platforms; others identify the sponsors that help fund free offerings provided by the company. Likewise, some brands and retailers are bringing credibility to customer feedback on their platforms by calling out voluntary reviews from verified purchasers while disclosing which ones they solicited.

Making business terms such as additional fees, privacy policies, and terms of service readily accessible and easily understandable. This can take the friction out of an otherwise challenging customer experience. For instance, some insurers and wealth management firms are introducing conversational interfaces that break down complex financial products (including fees) into everyday terms. Customers can interact with such on-demand helpdesks across different channels—audio, visual, desktop, or mobile—weighing their options and making their selections with confidence.

Clarifying how self-learning algorithms operate. The black box nature of machine learning (i.e., the opacity around how the software arrives at a decision) can lead to confusion and skepticism among customers at the receiving end of an automated decision. Organizations are starting to adopt explainable AI (XAI) technologies that make it clear how they arrive at decisions. For instance, to enhance confidence in AI-supported medical diagnoses, health care companies are developing solutions that explain the diagnosis by reporting the probability and contribution of each patient symptom (e.g., vital signs, signals from medical reports, and lifestyle traits) to the conclusion. These solutions also generate a confidence score for each conclusion so clinical professionals can understand why the conclusion was made and use human interpretation to reach a different conclusion if required.

Providing line of sight into supply chains. Amid growing public and regulatory calls for ethical and trustworthy sourcing, manufacturers and logistics companies are implementing technologies such as blockchain across their supply chains. Such technologies can track production sources and handling conditions, mitigating concerns about product safety (e.g., food and medicine), sustainability and social responsibility (e.g., apparel and fisheries), authenticity (e.g., luxury goods), and more.

Pillar II: Ethics and responsibility

For all its marvels, technology has a potential dark side: It's only as ethical as its creators and users design it to be—the logic of machines might not distinguish right from wrong the same way human beings do.[2] This means that companies have to evaluate how they can use technology in a way that is aligned with their fundamental purpose and core principles. They have a chance to establish themselves as worthy of trust by deploying digital tools in the service of customer needs and societal benefit. By doing this, organizations can tap into much-yearned-for goals of fairness, inclusion, and well-being, while curbing disinformation and promoting socially beneficial uses of technology.

Companies can bolster their reputation as ethical and responsible stewards of digital technologies and build the second pillar of trust by:

Ironing out complaints in a sensitive and timely manner. Who among us hasn't followed an automated answering system only to get stranded midway in the call with no resolution in sight? Digital technologies can help triage consumer complaints, ensuring that the most urgent and complicated ones go straight to a human. For example, one e-commerce site uses sentiment analysis on email correspondence to identify the most urgent customer complaints and route them to specially trained agents for manual intervention. Meanwhile, an insurance company employs computer vision technologies to review photos of damaged assets and predict repair quotes and post-accident insurance coverage. Such capabilities reduce the need for tedious form filling and follow-up calls with human customer care representatives.

Stopping misinformation in its tracks. Spoofing, deepfakes, or plain old-fashioned rumors—any organization can find itself caught in the midst of such malpractices. Here again, technologies can be leveraged to stop misinformation in its tracks. Some such digital solutions are one-to-one, as in the case of a communications provider that lets users forward suspicious messages for immediate verification or debunking.

Encouraging inclusion with tools that test fairness and detect biases. Digital systems can perpetuate historical biases and unfair treatment, or they can be designed to root out these issues and enable organizations to operate in line with their principles.[3] For instance, a city government developed an algorithm toolkit in collaboration with policy institutes that identifies ways to minimize unintended harm to constituents by limiting biases in law enforcement, higher education institutions, and the criminal justice system.

Implementing safeguards to promote stakeholder welfare along with digital controls that prevent unethical or inappropriate use of technology. This can involve preventing users from engaging with technology in unhealthy or irresponsible ways. Examples include a gaming company that imposes time and spend limits on games that are habit-forming or a content aggregator that prompts users to be skeptical about the veracity of crowdsourced information. It can also involve warning customers about behaviors that can negatively impact them, such as cloud computing providers that automatically issue alerts when customers are about to go over budget or automobile-makers using sensors to detect distracted driving and issuing alerts to prevent accidents.

Pillar III: Privacy and control

People have long traded data for access, convenience, and a more personalized experience. But this consent has its limits. If consumers have reason to believe their data is being used in ways they don't agree with, the results can include calls for boycotts, public inquiries, and even severe penalties under strict regulations, such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act. On the flip side, a Deloitte survey revealed that 79 percent of respondents agreed that they would be willing to share their data if there was a clear benefit to them.[4]

Here's how companies can deploy digital technologies to encourage safe sharing of data and build the third pillar of trust:

Putting control of personal data in users' hands. Often, the problem with data sharing is not so much the actual loss of privacy as the perception of loss of control, which leaves consumers feeling worried and powerless. One way to respond is by letting consumers take the reins. A technology company is doing this by offering its customers a privacy dashboard where users can keep tabs on what data is being collected, how their data is being used, and how long their personal data is stored by the company. A few digital companies publish transparency reports to share information on third party requests for user data and content moderation on their platforms. Other digital platform companies are going a step further by allowing users to redact or delete their data at will or download and transfer it to a different provider.

Improving the accuracy of consumer data. Data sharing can provide more personalized services to consumers seamlessly—but only if the data is accurate. That's often not the case with third-party data, which may be outdated, incomplete, or incorrectly inferenced from sources such as public records, social media, and location services.[5] Instead of inferring consumer preferences and behavior from these sources, organizations increasingly are turning toward "zero-party data," called so because the data comes directly from the consumer. Consumer products companies, telecommunications firms, and media entities are adopting zero-party data collection platforms that incentivize consumers to volunteer data around their preferences and motivations in exchange for personalized benefits.

Being frugal with personally identifiable information. With sweeping privacy protection requirements making their way out of legislatures, the consequences for organizations that fail to protect personal data can be severe. Many organizations are finding ways to preserve privacy while analyzing customer data or using less customer data in the first place. For instance, recent technology developments enable organizations to perform analytics and calculations on encrypted customer data without decrypting it, thus protecting customer privacy. In another example, a mobile devices company developed a privacy preserving technique that analyzes customer data on users' devices. As a result, the company does not need to transfer or store customers' personal data on its servers.

Pillar IV: Security and reliability

While consumers appreciate the convenience that digital technologies provide, they also believe that businesses should be held accountable for the security of online user and personal data, according to a Deloitte UK survey.[6] And as data breaches continue to hit the headlines,[7] consumers are taking note: In a recent survey, half of the respondents said they take a company's cybersecurity record into account before they agree to use its services.[8] In other words, an organization's reputation hinges on the strength of its data security practices.

In this environment, organizations can differentiate themselves by building the fourth pillar of digital trust—security and reliability—by:

Verifying the identity of people claiming to be customers or providers to reduce impersonation and fraud. At a time when mistaken and stolen identities are a common source of error and fraud, emerging digital biometrics or multifactor authentication solutions can help identify customers based on their online behavior alone, providing a more frictionless experience. A financial services provider, for instance, records cursor movements, keystroke speed, and other gestures to verify customers for online transactions. Meanwhile, the company's call center uses voice recognition technology to verify phone transactions, to clamp down on errors and fraud. Such practices, however, raise further questions about customers' privacy.

To master the trust equation, what is needed is a combination of the right grounding with guardrails along the way—a cohesive effort across leadership and governance, strategy, principles, policies, processes, and culture.

Using automation and AI to reduce errors and fraud. Automation and AI can help reduce human errors and can process more information than humans are able to. For example, a financial services provider has deployed a secure chatbot to provide customer support for requests that involve sensitive financial and personal information, thereby protecting the data from human operators. These capabilities not only provide quick and consistent service to customers, they also help reduce opportunities for fraud. In another example, an insurance provider uses AI-based fraud detection tools to flag suspicious insurance claims to combat medical identity theft. The tool detects subtle anomalous patterns that would be difficult for human analysts to detect.

Proactively alerting users in the event of suspicious account activity. Organizations can use intelligent threat detection tools to caution users against anomalous and suspicious activity in their accounts. For example, many technology providers alert users about suspicious account login attempts, especially if they are new devices or foreign locations, and many financial institutions require users to authenticate unusual or significant transactions. In another example, a technology platform allows users to customize suspicious activity alerts based on their tolerance threshold of the severity of threats and the significance of the personal data that may be affected.

How the four pillars of trust can support digital transformation

Digital transformation is often viewed as a new vehicle for exponential growth and a way to fundamentally disrupt business models. Of course, it can be those things and more, but only if it earns the trust of relevant stakeholders. To build this trust, organizations can work toward building the four pillars of digital trust—*transparency and accessibility; ethics and responsibility; privacy and control;* and *security and reliability*. Like we explained, they can use the very technologies that enable digital transformation for this purpose.

But technology alone can't build long-term trust. To master the trust equation, what is needed is a combination of the right grounding with guardrails along the way—a cohesive effort across leadership and governance, strategy, principles, policies, processes, and culture. Teams such as technology, marketing, sales, operations, and even third parties need to collaborate to weave trustworthiness into the very fabric of an organization. To ensure cross-organization alignment, they must keep in sight the organization's fundamental purpose and core principles.

At any given point in time, different organizations and industries are likely to be at different stages of digital transformation and long-term stakeholder trust relationships. This is why each organization needs to adopt a plan designed to support its individual trust journey.

Organizational leaders can play a big role in facilitating this journey. To do this, they could start with evaluating whether their colleagues across functions understand the potential strategic, operational, reputational, and financial impacts of garnering stakeholder trust. Next, they could ask whether any transformation efforts that are already underway have adequately integrated trust considerations from the beginning. For new transformation initiatives, they could insist that trust considerations be integrated from the outset instead of as an afterthought.

Transformation efforts that thus integrate the four pillars of trust—enabled by digital technologies—can help organizations build long-term digital trust and strengthen their relationships with their stakeholders.

Endnotes

1. Sprout Social, *#BrandsGetReal: Social media & the evolution of transparency*, accessed August 30, 2019.
2. Amy Dockser Marcus, "How new technology is illuminating a classic ethical dilemma," *Wall Street Journal*, June 8, 2016.
3. Deloitte, *AI ethics: A new imperative for businesses, boards, and C-suites*, accessed August 30, 2019.
4. Gina Pingitore et al., *To share or not to share: What consumers really think about sharing their personal information*, Deloitte University Press, September 5, 2017.
5. John Lucker, Susan K. Hogan, and Trevor Bischoff, "Predictably inaccurate: The prevalence and perils of bad big data," *Deloitte Review* 21, July 31, 2017.
6. Deloitte, *The Deloitte Consumer Review*, accessed August 30, 2019.
7. Verizon, *2019 data breach investigations report*, accessed August 30, 2019.
8. Andrew Ross, "Cyber security mishaps make customers think twice about using a brand's services," *Information Age*, May 31, 2019.

Acknowledgments

The authors would like to thank **Anand Ananthapadmanabhan**, **Kashvi Bhachawat**, and **Udisha Sinha** for their contributions and insights in shaping this research article and **Ed Hida**, **Nicole Sandford**, **Ash Raghavan**, **Jeff Lui**, and **David Jarvis**, who shared their valuable time and insights.

About the authors

Nancy Albinson | nalbinson@deloitte.com

Nancy Albinson is the Deloitte Risk & Financial Advisory and Global Risk Advisory Innovation leader as a Deloitte & Touche LLP managing director. She focuses on innovation strategy, sensing emerging trends, experimentation, and efforts to invest in and scale new or adjacent solutions. She leads a program focused on making strategic investments in emerging megatrends and technologies and is engaged in efforts to transform core offerings with digital technologies. She leads talent development for Risk & Financial Advisory to help shape the workforce of the future. Connect with her on LinkedIn at https://www.linkedin.com/in/nancy-albinson-b1105848/ and on Twitter @albinson_nancy.

Sam Balaji | sbalaji@deloitte.com

Sam Balaji is a Deloitte Global Business leader for Consulting as a principal at Deloitte Touche Tohmatsu Limited. He has three decades of experience spanning client, practice, and global leadership roles. In his former role, he served as the Global Business leader for Financial Advisory and Risk Advisory. He has served many of Deloitte's largest clients in the technology, telecommunications, media, and entertainment industries driving large, complex business transformations resulting from mergers, acquisitions, and innovation. He has previously served on the global board of directors and is currently a vice chairman on the US board of directors. Balaji has lived and worked in the US, Europe, and Asia during his career. Connect with him on LinkedIn at https://www.linkedin.com/in/sam-balaji/ and on Twitter @sambalaji.

Yang Chu | yangchu@deloitte.com

Yang Chu is a senior manager at Deloitte & Touche LLP. She is a specialist in strategic, financial, operational, technological, and regulatory risk and focuses on exploring emerging trends for opportunities and threats for clients and for Deloitte. Connect with her on LinkedIn at https://www.linkedin.com/in/yangchu/.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

Nancy Albinson
Global Risk Advisory Innovation leader
Managing director | Deloitte & Touche LLP
+1 973 602 4523 | nalbinson@deloitte.com

Nancy Albinson focuses on innovation strategy, sensing of emerging trends, experimentation, and efforts to invest in and scale new or adjacent solutions. She leads a program focused on making strategic investments in emerging megatrends and technologies and is engaged in efforts to transform core offerings with digital technologies. She is based in Parsippany, New Jersey.

Deloitte Risk & Financial Advisory helps organizations effectively navigate business risks and opportunities—from strategic, reputation, and financial risks to operational, cyber, and regulatory risks—to gain competitive advantage. We apply our experience in ongoing business operations and corporate life cycle. We leverage next-generation solutions in our Investments portfolio and Managed Services and Products business to help clients become stronger and more resilient. Our market-leading teams help clients embrace complexity to accelerate performance, disrupt through innovation, and lead in their industries
Visit Deloitte.com to learn more.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Prakriti Singhania, Preetha Devan, Anya George Tharakan, and Nairita Gangopadhyay
Creative: Kevin Weier, Adamya Manshiva, and Emily Moreano
Promotion: Hannah Rapp
Cover artwork: J. F. Podevin

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.