IDC

SPOTLIGHT

Sponsored by: Google Cloud

Digital business, and the accompanying increase in the importance and complexity of trust, have given rise to the need for trusted ecosystems of partners.

Trust and Trusted (Digital) Ecosystems: What They Are and Why Trust Matters

March 2024

Written by: Grace Trinidad, Research Director, Future of Trust

Introduction

The importance of trust to a functioning society is not new or novel. Trust is our long-used heuristic to evaluate the cooperativeness or non-cooperativeness of a member of a community or a society and to determine our willingness to accept risk in dealing with that person or entity. In solving problems of trust, actors employ strategies to reduce uncertainty or decrease vulnerability. Such strategies change depending on the social context in which a set of actors are operating.

In modern societies, efforts to reduce vulnerability and engender trust in business take the form of enforceable contracts, insurance, laws and regulations, and similar mechanisms that govern behavior. The processes put in place to limit losses from distrust are based on resolving the lack of information regarding the intentions (transparency, fidelity, and integrity) and the competence of a business partner. Transparency and resolution of information asymmetries generate the conditions under which trust can emerge.

AT A GLANCE

KEY STATS

- Companies that have secured high trust will more quickly bounce back from an adverse event when compared with their low-trust peers.
- 73% of respondents agree the statement "the trust and trustworthiness of my organization protects us against the adverse effects of negative events such as data breaches or data loss" (source: IDC's *Worldwide Future of Trust Survey,* August 2023).

Trust is especially important now because the number and scope of digital risks as we transact and interact digitally have increased exponentially as our reliance on digital infrastructures has grown and matured. As our digital worlds increase in complexity, strategies that increase trust and trustworthiness have also increased in complexity. Customers and customer organizations must work with an increasingly fragmented and expanding set of digital services providers, all while having to trust that the providers they transact with:

- Have robust security measures to protect the reliability of digital services and avoid data breaches
- Have measures that ensure compliance with the existing privacy laws and regulations as well as an approach that is consistent with the data privacy that customers expect
- Are compliant with existing laws and regulations put forth by governments and governmental organizations globally
- Indicate through their environmental, social, and governance (ESG) commitments that partner organizations are ethically managed and are thus sustainable or "future proof"

Within each of these areas are unknowns inherent in transacting with any company, but the sheer number of companies that we must now interact with to enable our daily work and lives has made trust even more necessary. Trust is what we have to resolve the information asymmetries that complicate every transaction of our digital experience.

Definition

The term *trusted ecosystems* refers to multicompany systems that are characterized by high trust. Ecosystems in this context are groups of companies that do not belong to any one organization but are instead connected through their contribution to a network of complementary data or services. As part of a trusted ecosystem, each company within this system exhibits each of the four components of trust: competence, transparency, fidelity, and integrity in ways appropriate to that ecosystem's needs.

The Impact of Trusted Ecosystems

Digital business and the accompanying increase in the importance and complexity of trust have given rise to the need for trusted ecosystems of partners. The digital ecosystems within which we operate are groups of interconnected information technology (IT) partners and resources that must function as a unit to deliver the services that support our processes and infrastructures. While ecosystem risks and vulnerabilities were previously managed at the organizational level, adoption of cloud infrastructures and platforms has required an evolution of trusted ecosystem concepts. The responsibility to manage the risks and vulnerabilities that accompany integration of multiple platforms no longer sits with the implementing organization alone but also with the platforms and their respective service offerings.

As ecosystems and the businesses they include undergo this evolution, organizational or brand partnerships and relationships have long-term implications for both partners and their extended networks. If one organization falls victim to a breach of security, its associated network of partner organizations may also suffer compromised data or resources. If an organization is revealed to be or is even accused of abusing customer data at the point of collection, storage, or use, the resulting loss of customer trust can ripple across that organization's entire network. These partnership vulnerabilities take on greater urgency as an increasing number of services providers are consolidating services or partnering with organizations with expertise in complementary services to increase the robustness of service offerings, improve customer experience, and secure a more competitive position in the marketplace.

Given the shared nature of risks in these partner relationships, organizations and digital services providers must signal trustworthiness to each other in multiple ways:

- **Radical transparency:** In establishing any partnership, necessary first steps have always included a mutually beneficial contractual agreement that aligns goals, consideration of known strengths and weaknesses of the organizations in question, an outline of respective roles and expectations, and a plan that forecasts the future of the partnership as both organizations grow and mature. In today's trusted ecosystem, however, partnerships must go beyond these usual requirements and establish radical, ongoing transparency. The increase in vulnerabilities and an ever-evolving regulatory landscape require transparent sharing of known and emerging risks to the organization and planned steps to mitigate these risks. More traditional organizations might find this shift difficult at the outset. Laying out and being transparent about strategic plans and forecasts may represent a dramatic departure from a long-held competitive mindset.

- **Integrated messaging:** The consequences of trust violations, such as unauthorized data use or other privacy violations, misleading ESG communications, or failure to show compliance with laws, can spread across a network. Participants in a trusted ecosystem of partners must agree on how to message their trustworthiness to customers and, in so doing, must agree on their customer commitments. It would not make sense if one ecosystem partner promised its customers total control of their individual-level data while its partner organizations — that might hold data for that same customer — did not.
- **Sustainability:** Sustainability commitments show that organizations are planning for the future of their business, working to manage and mitigate environmental and social risks to their business and, through those efforts, acting to safeguard future business and future generations. When participants in a trusted ecosystem are aligned in their sustainability goals, their impact on future economies and resources is stronger and promises greater resilience for the ecosystem in the long term.
- **Speed and agile innovation:** Research shows that trust facilitates more efficient operations. When trust is present, any friction that might exist in an interaction or transaction is reduced or eliminated. Teams characterized by high-trust levels evidence greater innovation and agility. Employees have greater confidence that their ideas and organizational concerns will be met with serious consideration and respect — and so move more quickly and confidently to innovate. Trust at the ecosystem level delivers a myriad of benefits to customers. Shared best practices lead to better governance and processes, and radical transparency between ecosystem partners leads to better service offerings and resolution of service gaps.
- **Maintenance of relationships in the long term:** Trust is built through multiple positive interactions over time and is maintained through a commitment to the core tenets. Partners that operate in a trusted ecosystem build a network defined by radical transparency, integrated messaging, and shared sustainability and have established a track record of speed and agile innovation to the benefit of all trusted partners. This shared history creates the backdrop for long-standing, mutually beneficial partnerships over the long term. A trusted ecosystem also serves as an enforcer of trustworthy behavior, incentivizing continued trustworthiness to maintain inclusion in the ecosystem and thus access to the benefits the ecosystem confers.

Features of Trusted Partners

As trust and trustworthiness are contextual, personal, and time sensitive, there is no single, defined approach that can ensure an organization is trustworthy. IDC conducts customer research annually examining the changing nature of trust and which security, privacy, compliance, and ESG offerings most lend themselves to trustworthiness at that time. The following are the offerings in security, privacy, compliance, and ESG that most contribute to brand trust and trustworthiness, according to IDC's August 2023 *Worldwide Future of Trust Survey*:

- **Security:** The greatest proportion of respondents (35%) indicated that threat detection and response, or the identification and neutralization of any malicious activity that could compromise a network, contributes most to an organization's trustworthiness. The second area that most contributes to brand trust and trustworthiness is availability of skilled cloud cybersecurity staff and leadership (31%).
- **Privacy:** 28% of respondents said that data obfuscation and data integrity — including masking, randomization, and encryption — contribute most to organization or brand trust and trustworthiness, followed by data loss prevention and information rights management (25%).

- **Compliance:** 44% of respondents indicated that the presence of a trust center, or information and guidance on security, privacy, and compliance adherence, contributes most to organizational or brand trust and trustworthiness. According to IDC's 2023 *Worldwide Future of Trust Survey,* the availability of skilled staff and leadership in global regulatory compliance contributes most to trust and trustworthiness (37% of respondents worldwide). This skill set is growing more valuable as organizations navigate an increasingly complex patchwork of regulations and laws. The presence of an easy-to-access trust center increasingly contributes to purchasing.
- **ESG:** Regarding efforts in ESG, 46% of IDC's 2023 *Worldwide Future of Trust Survey* respondents stated that good governance, best practices, accountability, and responsibilities contribute most to brand trust and trustworthiness, followed by 40% that selected ESG metrics.

Benefits

Trusted Ecosystems: Benefits to Participating Organizations

Although 72% of business leaders agree that "high trust in our organization improves our bottom line" and 77% agree that "trust is critical for our organization to flourish," 27% stated that "the lack of a clear link between trust initiatives and desired improvements on priority business outcomes was a top challenge to improving their organization's perceived trust and trustworthiness" (source: IDC's *Worldwide Future of Trust Survey*, August 2023).

A closer look at the data suggests otherwise. Survey respondents report, on average, 13–17% annual improvements in revenue growth, cost savings, profit, improved customer experience, increased operational efficiency, faster innovation, improved business agility, business resilience, and increased sustainability because of their organization's investment in the trust-related functions of IT security, data privacy, compliance, and ESG initiatives. These findings confirm previous IDC research that identified statistically significant associations between prioritization of and investment in trust programs with business resilience, operational efficiency, and sustainability (source: IDC's *Worldwide Future of Trust Survey*, January 2022).

When fully realized through radical transparency, integrated messaging, customer commitment, sustainability posture, agile innovation, and commitment to the network of partners, participation in a trusted ecosystem confers not only the aforementioned business outcome benefits but can also be a solution to brand distrust or loss of trust.

IDC's research found that three events were most likely to be "trust breaking." Personally identifiable information (customer or employee) that was compromised in a data breach was the top trust-breaking event cited by 38% of respondents to IDC's August 2023 *Worldwide Future of Trust Survey*. Next was withholding information from the public regarding a data breach or other adverse event (31%), followed by a top executive's involvement in a scandal of national importance (26%). As no organization is immune to data breaches, participation in a trusted ecosystem helps to manage these risks by virtue of the radical transparency required from all partners to participate. Vulnerabilities and risks must be transparently communicated and managed, resulting in stronger security and privacy postures for all participating organizations.

Trusted Ecosystems: Benefits to Customers

Fully realized trusted ecosystems capitalize on the strengths of their partner organizations, providing access to improved services and skills for security, privacy, compliance, and ESG across the entire ecosystem to their customers. Customers gain improved, comprehensive, and reliable services, in addition to greater transparency, competence, and quality from

their selected vendors. Customers are also more likely to stay on the leading edge of innovative advances. As business environments continue to evolve and change, trusted ecosystems of complementary service partners set the stage for more rapid acquisition and deployment of novel, trustworthy technologies for themselves and for their customers. Trust reduces friction and increases speed.

Trends

Although trust has steadily declined for all industries to varying degrees, it remains "the currency of business." Organizations that demonstrate high trust from their customers also command greater market share, as well as greater resilience in the wake of an adverse event such as a data breach. Research shows that companies that have secured high trust will more quickly bounce back from that adverse event when compared with their low-trust peers. In IDC research, 73% of respondents agree with the statement "the trust and trustworthiness of my organization protects us against the adverse effects of negative events such as data breaches or data loss" (source: IDC's *Worldwide Future of Trust Survey,* August 2023).

Considering Google Cloud

Google Cloud has created a trusted ecosystem of security technology independent software vendors (ISVs) that work in concert to address increasingly sophisticated threats to the security and privacy of customer data. This trusted ecosystem of security partners helps deliver best-in-class security infrastructure to Google Cloud customers that seek total control over their own data and require a flexible platform that scales with their evolving business needs.

Google Cloud exemplifies the trusted ecosystem through its "shared fate" approach to cloud platforms. In its shared fate model, Google Cloud is equally invested in the security outcomes of its customers and partners utilizing the Google Cloud platform. In a trusted ecosystem, the success and trustworthiness of one participant can impact the ecosystem to the benefit of all ecosystem participants. Thus radical transparency is a key requirement for all participants in a trusted ecosystem — Google Cloud included.

Google's shared fate model emerged first in 2016 with the announcement of Google Customer Reliability Engineering (CRE) and articulation of the responsibility of both cloud platforms and customers to provide a reliable and secure infrastructure. It is a sometimes overlooked reality that for trust to exist, both partners must have confidence in the other's intentions. In trusted ecosystems, this willingness to be vulnerable to the intentions of another is scaled to an entire network of connected entities that evidence bidirectional trust. Together, trusted ecosystems and Google Cloud's shared fate model establish a foundation that is greater than the sum of its parts. In the case of Google Cloud, customers are provided with layers of support consisting of mutual trust, ongoing and secure innovation, and an ecosystem of top security partners that are committed to maintaining customer and partner trust in their products and in their brand.

Google Cloud's foundational infrastructure was built on cloud-native security and configured for integration of the security solutions offered by the ISVs that join the Google Cloud trusted partner ecosystem. Google Cloud ecosystem partners are full partners in co-innovation, analytics, and development of new capabilities, strengthened by multiple layers of protections provided by Google. This shared investment of resources in developing solutions to meet current and emerging customer needs means that Google Cloud's trusted ecosystem becomes more robust and stable over time, resulting in greater customer service quality. This service stability also supports the shared ethos of trusted ecosystems, positioning transparency, and shared responsibility as the default norm for all Google Cloud partners.

When the ethos of trusted ecosystems extends the partner relationship, it also extends customer service offerings. When done in earnest, trust and trusted ecosystems establish virtuous cycles of transparency, commitment, and reliability that extend into all areas of business. Why? Because when trustworthiness is the benchmark against which a partnership is tested, all partners expected to commit to the core tenets of trusted ecosystems will be quick to point out inconsistencies when identified. If failures are not addressed, then the trusted ecosystem will cease to exist. Thus Google Cloud and its partners provide customers with complete ownership and control of their data, reliable data access, streamlined network configurations, maintenance of compliance and regulatory requirements, and commitment to environmental goals.

Challenges

Google Cloud, as the founder of the shared fate approach and initiator of its trusted ecosystem, may face some challenges as its competitive ascent is mapped out. Though the Google Cloud trusted ecosystem is built on bidirectional trust and partnership with other ISVs, solidifying these trust commitments into contractual language can be challenging — although required — to clarify each partner's responsibilities and a plan of action once activities inconsistent with the trusted ecosystem model are identified. When issues are identified, there is the additional issue of governance. How will governance decisions be made in the ecosystem? Ideally, enforcement responsibilities are spread equally between partners. Participation in a trusted ecosystem is also additional work for all involved — it is critical to devote adequate resources to the maintenance of trusted partner relationships while developing and advancing product offerings.

Trust is also fragile. Failure to adhere to the core tenets of a trusted ecosystem can signal the total demise of any ecosystem defined by trust between members. It is imperative that all partners commit to the requirements of a trusted ecosystem and share the responsibility of maintaining its integrity. The radical nature of this commitment cannot be overstated. Organizations may want to be part of a trusted ecosystem, but Google Cloud participation requirements may run contrary to how their business is currently understood. Full transparency, co-creation, shared responsibility, and shared weaknesses and strengths may be challenging, especially at the outset.

Conclusion

The importance of trust has increased in visibility as the complexity of the digital landscape has grown. This complexity renders any individual or organization unable to fully estimate the risks and asymmetries that may accompany a partnership. Therefore, we turn to signals and indications of trustworthiness so we can continue to compete. Trusted ecosystems establish trustworthiness through adherence to core tenets of radical transparency, integrated messaging, sustainability, speed and agile innovation, and maintenance of relationships with both ecosystem partners and their customers in the long term. Such an ecosystem is maintained through the rigor demanded from participation. Google Cloud presents one example of a trusted ecosystem as exemplified by the shared fate model. As digital infrastructures continue to transform to accommodate AI, generative AI, and automation, already established trusted ecosystems will be best able to meet the needs of customers.

The importance of trust has increased in visibility as the complexity of the digital landscape has grown.

About the Analyst

Grace Trinidad, *Research Director, Future of Trust*

Grace Trinidad is research director in IDC's Security and Trust research practice responsible for the Future of Trust research program. In this role, she provides strategic guidance and research support on approaches to trust that include risk, security, compliance, privacy, ethics, and social responsibility.

MESSAGE FROM THE SPONSOR

Google Cloud is built from the ground up with the knowledge and experience that come from protecting the data of billions of users. Google Cloud's unique shared fate model means it takes an active stake in its customers' security posture. Google Cloud provides its trusted partners with tools so they can augment many capabilities including Data Cloud, Open Infrastructure Cloud, Trusted Cloud, and Collaboration Cloud with Google Workspace. Google Cloud's partners leverage the foundation of trust and the technologies we provide to build security capabilities and integrations. Together, we provide our shared customers with solutions that meet you on your cloud security journey and address your unique needs.

Find out more about the Google Cloud trusted security partner ecosystem.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com