In collaboration with Accenture, KPMG and PwC

WORLD ECONOMIC FORUM

Earning Digital Trust: Decision-Making for Trustworthy Technologies

INSIGHT REPORT

NOVEMBER 2022

Images: Getty Images

Contents

Foreword

Building a global consensus for trustworthy technology decision-making.

Paolo Dal Cin
Global Security Lead, Accenture

Sean Joyce
Global Cybersecurity and Privacy Leader, US Cyber, Risk and Regulatory Leader, PwC

Jeremy Jurgens
Managing Director and Head, Centre for Cybersecurity, World Economic Forum

Akhilesh Tuteja
Global Cyber Security Practice Leader, KPMG

Trust is necessary if we are to work together towards common goals in an increasingly fragmented world. This is especially true regarding new technologies, given the rapid pace of innovation and its uneven spread. Following the World Economic Forum's call to rebuild trust in 2021, the Digital Trust initiative was launched to establish a global consensus among key stakeholders regarding what digital trust means and what measurable steps can be taken to improve the trustworthiness of digital technologies.

Developing trustworthy technologies is a decision – and responsibility – for that decision rests with leaders across sectors and industries. To make decisions regarding advanced technologies, leaders must coalesce on clear goals. In other areas of global importance, such as global peace and prosperity and environmental, social and governance (ESG) practices, leaders have benefited from the clarity of global principles and guidance, such as the United Nations' (UN) sustainable development goals, the *Guiding Principles on Business and Human Rights*, and the Forum's Stakeholder Capitalism Metrics. Rapid innovation and implementation of digital technologies requires the same clarity for leaders.

Therefore, the Digital Trust initiative convened a multistakeholder digital trust community, comprised of leaders and experts from across industries (including leading technology innovators), governments, regulators and academic institutions as well as citizen and consumer advocates. This community encourages all stakeholders involved in the development of trustworthy technology to prioritize cybersecurity (including cyber resilience and security-by-design) and responsibility in technology use (including privacy protection, ethical and values-driven innovation, transparency and accountability). To begin this vital effort, the members of the digital trust community have developed a digital trust framework that builds on the Forum's early advocacy for cybersecurity, responsible technology governance and digital trust. The Forum hopes that this framework guides leaders in making decisions that cultivate more trustworthy and responsible technology.

Executive summary

Ensuring digital trust is a leadership responsibility that crosses domains and functions.

Digital trust is a necessity in a world where digital technologies support and mediate virtually all economic transactions, social connections and institutions. At the same, this trust is significantly eroding on a global scale. In order to reverse this trend, leaders and organizations creating and implementing new technologies and digital services must make decisions that are worthy of trust.

The World Economic Forum launched the Digital Trust initiative to help solve the digital trust challenge. The key question the initiative asked was: How can leaders make better, more trustworthy decisions regarding technology?

This insight report represents the first response to that question. It defines digital trust globally and introduces a "digital trust framework", developed by the initiative, as a tool to guide decision-making for leaders.

- Digital trust is individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values

- Only by deciding and acting for digital trust can leaders and organizations meet their obligations to society and individuals.

- The digital trust framework defines shared goals or values that inform the concept of digital trust, including:

  - Security and reliability
  - Accountability and oversight
  - Inclusive, ethical and responsible use.

- The framework also defines dimensions against which the trustworthiness of digital technologies can be operationalized and evaluated:

  - Cybersecurity
  - Safety
  - Transparency
  - Interoperability
  - Auditability
  - Redressability
  - Fairness
  - Privacy

Drawing on expertise in privacy, cybersecurity, technology ethics, law and a variety of other fields, from over 60 experts and leaders in the digital trust community this report presents an interdisciplinary view of what digital trust requires and how to make trustworthy decisions regarding the development or deployment of new technologies and digital services.

In addition to the framework, this report also begins the work of effective implementation of the digital trust principles. It focuses on the important role leaders have in preparing their organizations to make the choice for digital trust through every step of the technology life cycle and the important role that cooperation has to play in rebuilding digital trust globally.

- The digital trust roadmap guides decision-making holistically, beyond recommendations for any dimension of digital trust, to operationalize the framework according to a series of common steps (e.g. commit and lead, plan and design, build and integrate, and monitor and sustain).

- Earning digital trust is a responsibility shared by companies, governments, civil society and all individuals. This digital trust framework begins the work of meeting that responsibility.

Given the breadth of the digital trust topic, this report confines itself to the stakeholders most likely to impact the immediate development of new technologies. Further work in this field will explore the roles and responsibilities of other stakeholders in digital trust.

Introduction

Leaders and organizations earn trust when they commit to strategies, services and technology development that meet individuals' expectations and support their values.

In an era where new digital technologies are fundamental to every aspect of business and social interaction and growth, the most important decision a leader can take is to make those technologies trustworthy.

There is a widening trust gap between individual citizens and consumers, their governments and the businesses that create and deploy digital technologies.[1] From artificial intelligence to connected devices, from the security of personal information to algorithmic predictions, technology developers' and digital service providers' failures have eroded confidence at an unprecedented scale and rate. Significant evidence now shows that increased digitalization leads to widespread improvements in well-being and quality of life.[2] At the same time, all trust surveys have registered an alarming decrease in trust in science and technology as well as a host of other social institutions and links.[3] Without concrete and significant action to earn digital trust, the future is one of fragmentation and stagnation. The only way to reverse this trend is for technology developers and owners – those whose innovations mediate so many social interactions and underpin so many shared institutions – to commit to earning the trust of consumers and citizens.

That decision – to earn trust – is at the heart of digital trust. Digital trust is individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values. It is the key to unlocking greater cooperation, widespread adoption and equal benefits from new technologies. Individuals and governments are increasingly demanding that the companies who develop and deploy new technologies and digital services respect the values and expectations of the society in which they operate – and withhold their trust and support for those who do not.[4]

Digital trust is individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.

BOX 1 **Stakeholders in focus: technology purveyors and developers**

Digital trust has the capacity to unify all stakeholders in high tech landscapes. From the designers, developers and purveyors of technology to citizens and end users (and their civil society advocates) to the government actors who regulate new technologies, all stakeholders have a role to play in cultivating trustworthy technologies. As such, all stakeholders ought to make decisions that favour responsible use of technology. This report focuses on one sub-group of the wide-ranging stakeholder community: the designers, developers and purveyors of digital technologies. These entities – mainly private, profit-making corporations – have an important societal and economic responsibility to build digital technologies that adhere to the expectations and values of the societies in which they will be used. The leaders of these organizations will find the following framework useful in guiding their decision-making in building such trustworthy digital technologies.

Further work by the Forum on digital trust will expand the focus and inform decision-making for other stakeholders, including government actors, civil society and individuals.

Trust is not about the specific technologies developed or deployed, it's about the decisions that leaders make.

Trust is not about the specific technologies developed or deployed, it's about the decisions that leaders make. Across all technologies, when leaders determine which technologies are created or how they are used, they can choose to do so in ways that meet individuals' expectations and sustain their values – and thereby build trust. Where organizations engage stakeholders through technology and data, they must respect the digital dignity of individuals. When making decisions about technology, leaders must recognize that their organizations act as stewards of the social licence stakeholders have bestowed upon them. This social licence is at risk when some actors sow distrust by developing or deploying technologies irresponsibly, without due consideration of the harms that might befall individuals and other stakeholders. This is especially true where data processing and analysis – along with any related security failures, ethical lapses, lack of transparency, in-coded biases or associated issues – can undermine adoption by people who would otherwise benefit the most from technology. This means that leaders must consider trust throughout their organization and the technology and data life cycle – from ideation through design, development, testing, deployment and product feedback about anticipated and actual use.

The digital trust gap cannot be solved by one domain alone. Many factors support trustworthiness in technology: good cybersecurity, effective privacy protection, transparency in deployment, auditability, interoperability between technologies, safety, redressability in the case of harm and fairness in application. When determining how or whether to use new technologies, Chief Executive Officers (CEOs) and other senior leaders must rely on all these domains throughout their organization to ensure their ultimate decisions will pass the test of trustworthiness.[5] All these factors, or dimensions of digital trust, and how they come together to achieve trustworthy technology goals, are explored in depth below. The organizational shifts to move to a more trustworthy operating model are further described in this report. Only by **deciding** and **acting for** digital trust can leaders and organizations meet their obligations to society and individuals.

By adopting the digital trust framework introduced in this report, leaders can declare their commitment to trustworthy technology and begin earning the trust required to sustain innovation in new technologies and capabilities.

1 Digital trust framework: Goals and dimensions

Making digital trust a reality by defining trustworthy ends and the means to achieve them.

> In order to make trustworthy decisions about technology, leaders must keep both the ends in mind as well as the means to get there.

The digital trust framework defines shared goals or values that inform the concept of digital trust, as well as dimensions against which the trustworthiness of digital technologies can be operationalized and evaluated. The framework should be used as a decision-making guide for leaders at the highest levels when considering the development, use or application of digital technologies and services. As trust is a relational concept – a two-way street – this framework specifically addresses what organizations can do to earn the trust of the people who ultimately use or are affected by digital technologies.

Goals and dimensions

Drawing from best practices across technologies from IT infrastructure to smartphone applications, connected devices to artificial intelligence and disciplines such as cybersecurity, privacy, law, policy and applied ethics, the framework examines the goals and demands motivating digital trust as well as the capabilities needed to operationalize them. Starting as close as possible to a universal understanding of the goals implicated in the use of new technologies – **security and reliability**, **accountability and oversight**, and **inclusive, ethical and responsible use** – while also recognizing the need to meet the norms of the society in which the technology operates, the framework provides a foundation from which to explore how technology can be developed and implemented in ways that support the overall goal of earning trust.

In order to make trustworthy decisions about technology, leaders must keep both the ends in mind as well as the means to get there. Both the goals of the technology being developed or implemented and the dimensions of its use must be trustworthy. By organizing and making decisions according to the framework, leaders can demonstrably uphold the broader goals of the society in which technologies are used. Understanding and upholding these goals by defining organizational strategy in terms of the framework can lead to a virtuous circle of better decisions leading to more trustworthy technologies and data uses.

For the leaders of organizations or companies developing and deploying digital technologies and services, the digital trust framework serves as a method to structure and examine the potential effects of their decisions. The dimensions of digital trust, including **cybersecurity**, **safety**, **transparency**, **interoperability**, **auditability**, **redressability**, **fairness** and **privacy** represent the means of achieving the goals of the digital trust framework. The goals and dimensions described in the framework are highly interconnected. Decision-makers themselves must still exercise judgement of how the interplay between the goals and their relative prioritization fits both the values of their organization and the expectations of the society in which they operate.

BOX 2

Definitions

Digital trust: Individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.

Goals: Considerations that motivate or can be achieved by actions or decisions (i.e. dimensions).

Dimension: The aspect of digital trust over which organizational decision-makers, such as CEOs and senior executives, have control and, if applied to a given technology with a human-centric approach, will promote digital trustworthiness.

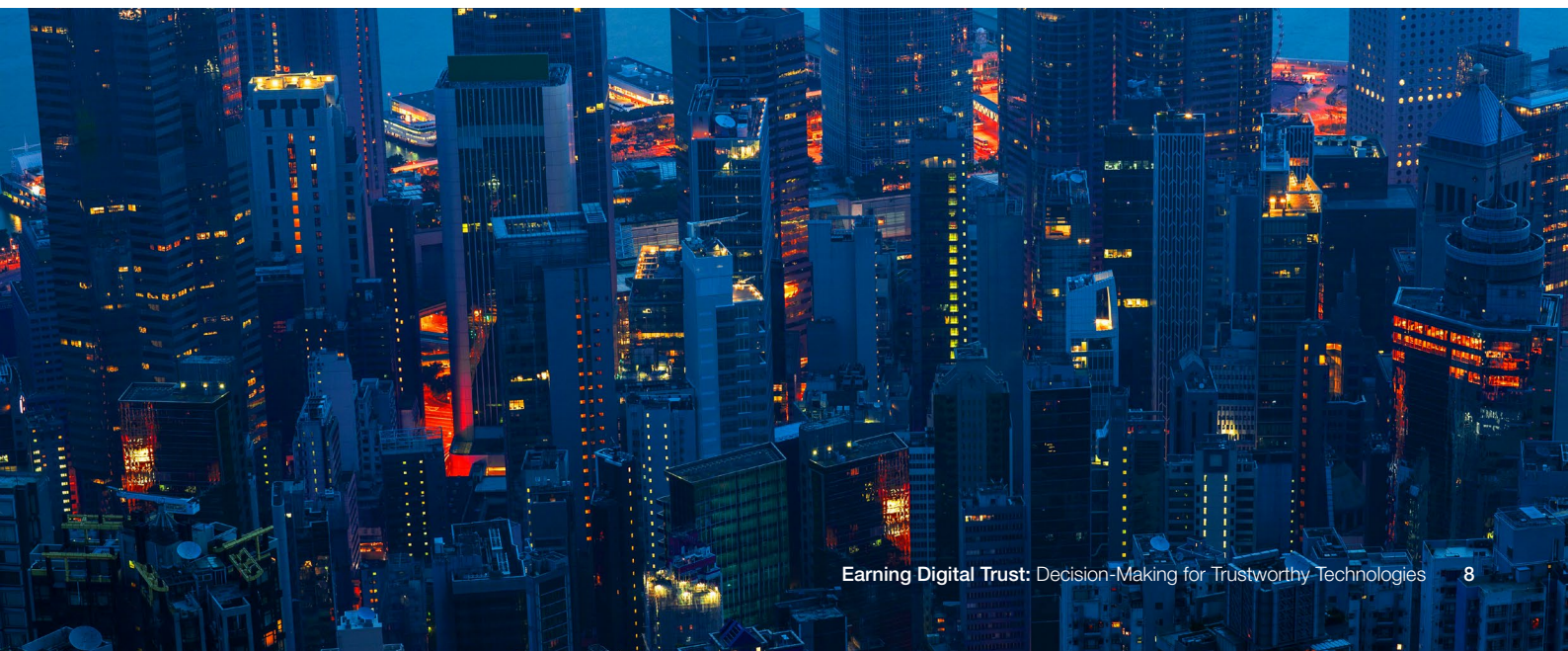
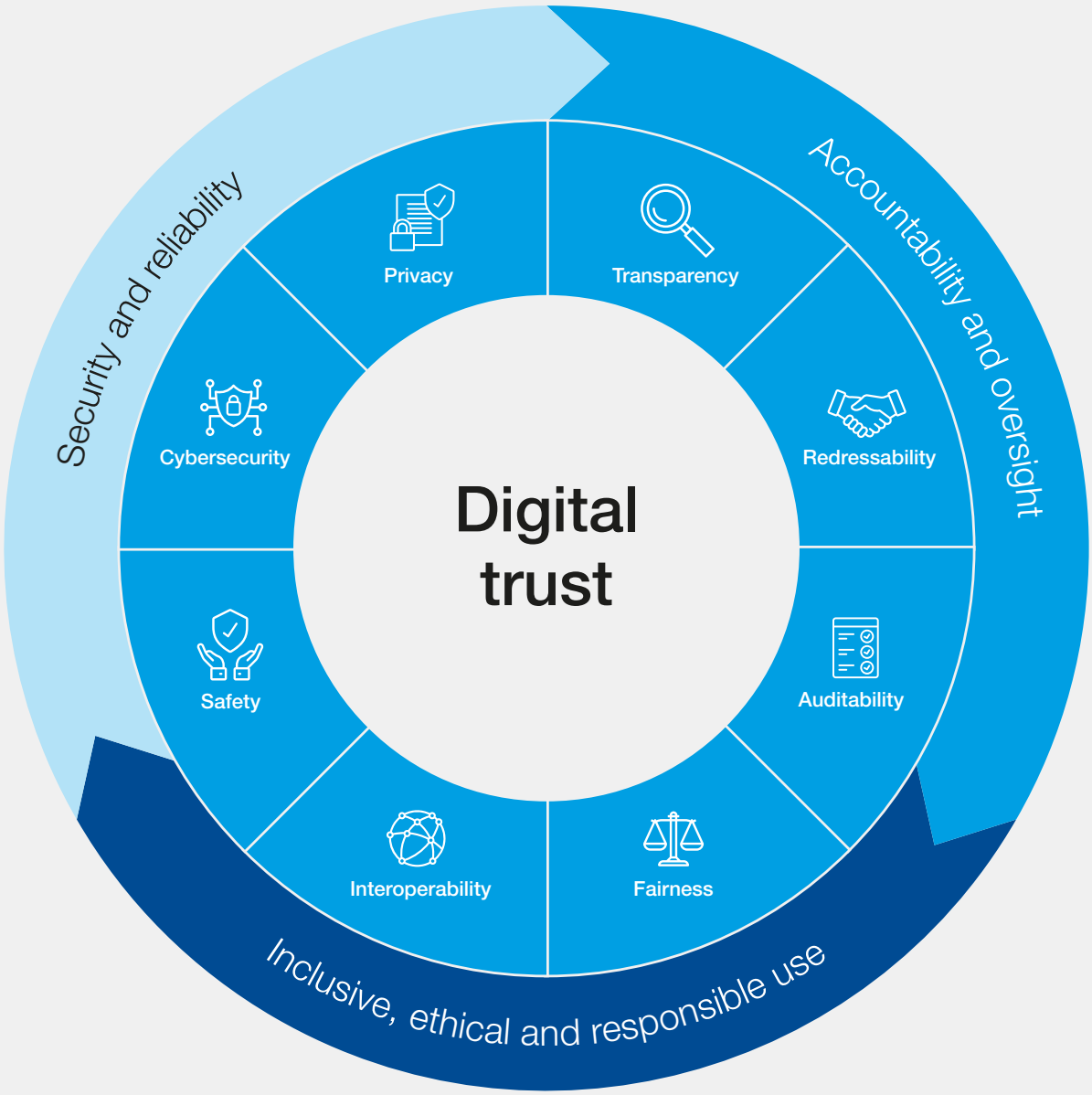


FIGURE 1 | **Digital trust framework**



1.1 Goals related to digital trust

Digital trust demands that technologies adhere to a set of goals that represent expectations across geographies and uses. Pursuit of these goals often also acknowledges the norms of the society in which the technologies are used.[6] By understanding, acknowledging and addressing the shared goals at play in technology applications and services within a given jurisdiction, technology developers, innovators and owners can focus on satisfying society's digital trust expectations. These stakeholders, through values-driven decision-making, work towards satisfying these shared goals by creating more trustworthy technologies, systems and services.

Below, the framework defines each of these three goals and explores how they relate to the concept of digital trust by supporting decision-making that earns trust from organizations' stakeholders. This section also examines the benefits, both to organizations and society as a whole, that accrue when digital trust goals are achieved. Finally, each section provides notable resources that will help leaders understand in more depth the issues involved in digital trust.

Security and reliability

Fulfilling the goal of security and reliability means that an organization's technology and data are well-protected against internal and external attacks, manipulations and interruptions while operating as designed according to a clearly defined set of parameters.[7]

Relevance to digital trust

As the world has become more digital, reliable functionality, connectivity[8] and protection against harm (e.g. protection of personal or proprietary information) have become fundamentally important to the continued functioning of businesses, entire economies and many social interactions. Technology users expect digital services and products to meet their expectations and to protect the data they entrust to the service or product (and thus the provider of the service or product). If a service or product does not function in a predictable, reliable and secure manner, users will withhold support and data or stop using it. The reliability of digital services and products is thus deeply intertwined with the trust that individuals put in them and the provider of the services and products. This goal is closely related to cybersecurity concepts of confidentiality, integrity and availability in digital systems.[9]

Equally important, digital security enables reliability by decreasing the risk of interruptions and manipulations of the services and products.[10] Unfortunately, both reliability and security are goals that are typically not recognized until they are lacking. This means that ultimate users, or those subject to the use of these technologies, often have limited means of assessing whether this goal is being met short of absolute failure. However, as users and citizens become more sophisticated regarding digital technologies they may demand assurance or information about just how reliable and secure a service or product is, and these more sophisticated stakeholders may serve as opinion leaders for the wider society – thus creating either virtuous circles of increasing trust for secure and reliable systems or vicious cycles of decreasing trust for unsecure or unreliable technologies. Therefore, decision-makers do not only need to think about how reliability and security can be achieved, but they also must be deliberate and transparent regarding the baselines of security and reliability users should expect and how they plan to achieve this goal.[11]

Decision-makers do not only need to think about how reliability and security can be achieved, but they also must be deliberate and transparent regarding how they plan to achieve this goal.

Benefit

Business

- Protecting reputations: Reliable and secure products and services are strongly in the economic and reputational interest of organizations for whom customer loyalty (as well as wider reputational factors) are important. In today's connected age, a major cybersecurity incident or even downtime of a few minutes for a major digital service provider can lead to significant reputational and financial damages, particularly where security is also at issue.
- Competitive advantage: Putting reliability and security at the forefront of an organization's decision-making about its services and products means committing to high-quality control standards, thereby avoiding retroactive investments to fix shortcomings in technology and services later on.[12] This can also provide a competitive advantage, especially in sectors that are heavily controlled or regulated.

Societal

- Protecting interconnectivity: Reliability and security have implications for the entire supply chain in which an organization operates. Critical infrastructure providers (and increasingly cloud service providers in the cyber context), for example, underpin the functioning of modern society and, as such, their reliability and security have massive implications for all the organizations that they serve and who rely upon them to deliver their own products and services.
- Protecting health and lives: A technology provider's reliability and security can have a significant impact on individuals' safety, including on their physical or mental health (for example, in the case of the manufacturer of self-driving cars "beta testing" features on unsuspecting pedestrians). Society is rapidly coming to rely on security and reliability in a world of connected devices and online interactions, including critical infrastructure such as utility providers.

BOX 3

Security and reliability resources

Across organizations, to ensure decision-making is aligned to a common set of security and reliability norms, various efforts have defined best practice frameworks. The following are some notable resources on the topic:

Reliability:

- Google Cloud Architecture Framework
- Microsoft Azure Well-Architected Framework

(Cyber)security:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Information Security Forum (ISF) Standard of Good Practice for Information Security
- International Organization for Standardization (ISO) 27001/2
- Control Objectives for Information and Related Technologies (COBIT)

Accountability and oversight

Fulfilling the goal of accountability and oversight means that responsibilities for trustworthiness are well-defined and clearly assigned to specific stakeholders, teams or functions along with provisions for addressing where those responsibilities fail to be satisfied. Further, means are in place to ensure that rules, standards, processes and practices are followed and performed as required.[13]

Relevance to digital trust

An organization's approach to digital trust is shaped by its board, leadership and management through their application of organizational values, vision and goals.

Attention to the good governance of organizations has dramatically increased. Whether through the increasing prominence of environmental, social and governance (ESG) reporting,[14] or through increased regulatory scrutiny on a variety of digital risk domains,[15] organizations are increasingly required to demonstrate better oversight in how they maintain and contribute to both financial and social stability. Likewise, regarding technology and data use, accountability and oversight help ensure that digital trust's dimensions are properly incorporated and implemented into all requisite organizational operations while decreasing information asymmetries between technology developers and individual users or citizens.

An organization's approach to digital trust is shaped by its board, leadership and management through their application of organizational values, vision and goals. Given the presence of data and technology in nearly all business products and operations (e.g. communications, finances, record-keeping, engineering, design and analytics), strong accountability and oversight over how technologies are implemented and how data is used must permeate throughout all levels and areas of an organization to ensure that its digital trust objectives and commitments are fulfilled. To do otherwise would be to demand trust from users, partners and other stakeholders without making a reciprocal commitment to act in a trustworthy way – an unfair and unsustainable operating model.

Good accountability and oversight also ensure that harms experienced by end users, citizens and consumers can be effectively remediated. Technology developers and the companies who implement new technologies are the most likely to be able to remediate problems at the least cost, especially as compared to less sophisticated individuals who may be subject to technology uses beyond their control. As the "least cost avoider"[16] in economic terms, technology developers are best placed to implement the kinds of accountability and oversight mechanisms that can prevent and remediate digital harms. The existence of these mechanisms significantly improves the trustworthiness of new technologies.

Benefit

Business

- Inspiring confidence: Defining and adhering to standards of accountability and oversight encourages stakeholders to use the products and services businesses offer. Consumers' and citizens' peace of mind can help a company ensure financial sustainability and grow its customer base.
- Workforce and culture: Digital technologies impact employees as well as customers. With proper accountability, organizations can take advantage of the efficiency and other gains promised by new technologies while simultaneously forging strong bonds with the personnel companies rely upon to function (for example, human-centric rules regarding algorithms applied to workers can provide clarity and efficiency).

Societal

- Cooperative regulation: Governments often implement societies' digital trust expectations through legal and regulatory requirements and conduct oversight of those requirements through various mechanisms. Digital trust programmes that recognize the impact of social expectations surrounding data and technology, and account for them in oversight mechanisms, can either obviate the need for the most stringent regulations or operate in conjunction with government oversight to fulfil the expectations of society.
- Harm minimization: The impact on all of society from poorly governed technologies stems from both the actual harms experienced by individuals and the opportunity costs

where decreased trust prevents the use or implementation of beneficial technologies. Good accountability and oversight mechanisms can both remediate any harms that result from technology use (making individuals whole) and build up the trust necessary for more widespread adoption of useful technologies.

BOX 4 Accountability and oversight resources

Across organizations, to ensure decision-making is aligned to a common set of accountability and oversight norms, various efforts have defined best practice frameworks. The following are some notable resources on the topic:

Written accountability requirements and standards

- The US Securities and Exchange Commission's (SEC) proposed rule on cybersecurity risk management, strategy, governance and incident disclosure by public companies. (See SEC Regulation S-K, item numbers 106(b)-(d) and 407(j), accessible via the Code of Federal Regulations at 17 C.F.R. 229).
- SOC 2 framework issued by the American Institute of Certified Public Accountants (AICPA).
- Payment Card Industry Data Security Standard (PCI DSS) issued by the Payment Card Industry Security Standards Council.

Independent oversight

- Financial Industry Regulatory Authority (FINRA): A financial industry self-regulatory organization that acts under the authorization of the US Congress and oversight of the SEC to monitor and regulate securities trading, exchange platforms and licensing requirements, as well as to arbitrate claims arising in connection therewith.
- Privacy and Civil Liberties Oversight Board (PCLOB): An independent US government agency responsible for reviewing the government's national security-related policies, procedures and practices to oversee and ascertain their conformance with other privacy and civil liberty statutes and regulations.

Inclusive, ethical and responsible use

Fulfilling the goal of inclusive, ethical and responsible use means that an organization designs, builds and operates its technology and data as a steward for all people, society at large, the natural environment and other stakeholders, with the overall intent to ensure broad access and use resulting in ethically responsible outcomes. This goal also means the organization works to prevent and mitigate exclusionary practices or other harms.[17]

Relevance to digital trust

Standardization is critical when building digital trust through technology products – without it, ethical decisions can appear subjective and ad-hoc.

The more digital technologies and data uses impact individuals' lives and well-being, the more consumers expect technologies to be developed, implemented and applied in ways that respect the dignity of ordinary users and citizens.[18] Organizational decision-makers, therefore, cultivate digital trust by committing to the inclusive, ethical and responsible use of technology and data. Decision-makers should also help individuals understand how the organization is committed to human rights and other universal principles (e.g. respect for human dignity, justice, non-discrimination, privacy, beneficence and agency). When interacting with technology, individuals look for signals that demonstrate how organizations will use data and technology to serve their interests. By committing to inclusive, ethical and responsible technology uses, organizations build trust by meeting citizens' and consumers' expectations while abstaining from harmful uses.

Standardization is critical when building digital trust through technology products – without it, ethical decisions can appear subjective and ad-hoc. Leaders who seek to implement value-driven technology design and product decision-making at scale recognize that organizations need standards to guide decision-making. Standardization builds trustworthiness by limiting arbitrary or capricious uses and ensuring responsible use. When promoting inclusion, consistent and objective outcomes result from a common approach, which is key to building and maintaining digital trust. In short, predictability breeds trust. For example, procurement policies can be a critical lever in increasing accessibility and inclusivity. Effective policies set the expectations, standards and criteria for how goods and services will be purchased. Through this, the organization can ensure the acquisition of universal designed products and services to safeguard equitable development and participation.[19] It is important, therefore, to provide a framework through which any organizational stakeholder, when faced with an ethical quandary, can make decisions or produce outcomes that are objectively consistent in process and result.

Organizations that are inclusive, ethical and responsible in designing and deploying their technology and data not only build trust with the public but demonstrate a way forward to increase trust in technology as a whole. This allows technology solutions to serve both individuals and companies, easing friction and increasing efficiency. Thoughtful design communicates respect for individuals and signals an organization's societal commitments in its decision-making.[20] For example, when making digital decisions, organizations seeking to cultivate digital trust may evaluate potential solutions with ethical frameworks and human-centric expectations, in addition to legal analysis – moving the discussion from "can" to "should".

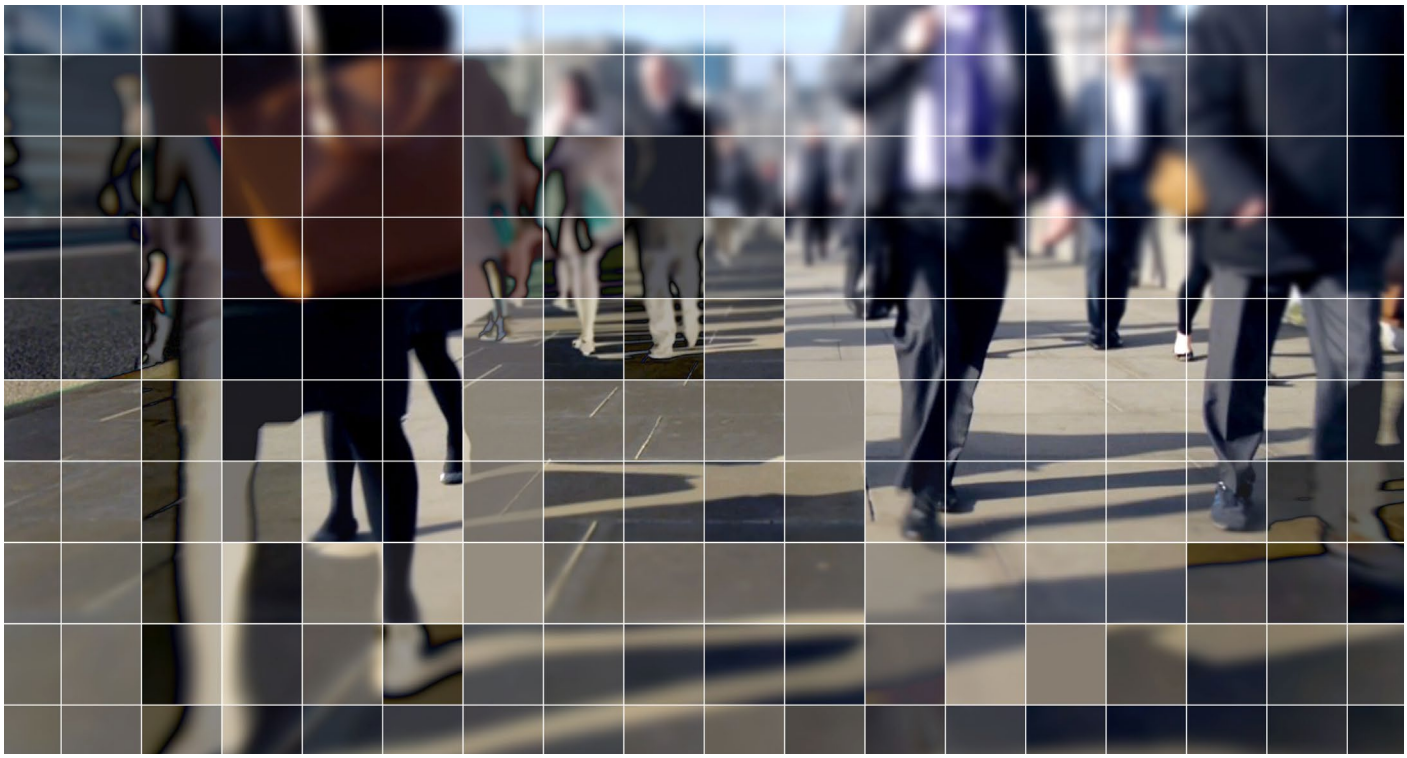
Benefit

Business

- Virtuous circles: Inclusive, ethical and responsible use commitments and decisions ultimately signal an organization's digital trustworthiness, allowing for deeper engagement by the user, better products from the organization, and an increase in the sharing of useful data between end users and technology developers and owners. Organizations seeking to implement this dynamic can be aided with tools for responsible innovation, such as games, workshops, team activities and technical tools.[21]
- Expanding workforce: By adopting a position of inclusive use of technology, organizations will see an increase in the proportion of the population able to contribute to the organization's mission effectively.

Societal

- Increasing opportunity: Increased global connectivity stemming from digital technologies and access to digital services has the potential to significantly advance economic development and improve the lives of a vast proportion of the global population. A commitment to inclusivity will ensure the greatest good reaches the greatest number of people, while dedication to ethical and responsible use ensures that the benefits vastly outweigh potential harms.
- Justice and stability: Equalizing the benefits of technologies and data uses while ensuring a human-centric approach that minimizes the potential for harm helps to nurture stable societies and strong institutions. Rather than further destabilizing social institutions by increasing inequality and raising the spectre of unanticipated harms, inclusive, ethical and responsible use of technology satisfies demands for justice that help improve social structures' overall cohesiveness.



BOX 5 **Inclusive, ethical and responsible use resources**

Across organizations, to ensure decision-making is aligned to a common set of inclusive, ethical and responsible use norms, various efforts have defined best practice frameworks. The following are some notable resources on the topic:

- Center for Democracy and Technology and the American Association of People with Disabilities, *Centering Disability in Technology Policy*
- European Committee for Standardization, European Committee for Electrotechnical Standardization and European Telecommunications Standards Institute, EN 301 549 V3.2: *Accessibility requirements for ICT products and services*
- G20 Global Smart Cities Alliance, *Global Policy Roadmap*
- Microsoft, *Responsible Artificial Intelligence (AI) Standard V 2* and *Inclusive Design Toolkit*
- NIST, *AI Risk Management Framework*
- Office of the United Nations High Commissioner for Human Rights, 49/60: *Statistics and data collection under article 31 of the Convention on the Rights of Persons with Disabilities*
- Office of the United Nations High Commissioner for Human Rights, A/HRC/49/52: *Artificial intelligence and the rights of persons with disabilities*
- Organisation for Economic Co-operation and Development (OECD), AI Principles
- United Nations Educational, Scientific and Cultural Organization, Recommendation on the ethics of artificial intelligence
- World Economic Forum, *A Blueprint for Equity and Inclusion in Artificial Intelligence*
- World Economic Forum, Presidio Principles: Foundational Values for a Decentralized Future

1.2 Dimensions of digital trust

Trust is not a monolith. Even when aligned with the three goals previously described, many factors figure into whether a decision and its results should be trusted. For trustworthy decision-making regarding technology and data uses, the framework identifies eight crucial dimensions of decision-making: cybersecurity, safety, transparency, interoperability, auditability, redressability, fairness and privacy. These dimensions play an important role in ensuring that social values are upheld and enhance digital trust. These aspects of digital trust are so central to the functioning of the trust relationship between an individual and an organization that if they are maximized – consistent with the goal of a given technology or capability – they will lead to the fulfilment of the goals of security and reliability, accountability and oversight, and inclusive, ethical and responsible use.

BOX 6 Mechanical and relational trust[22]

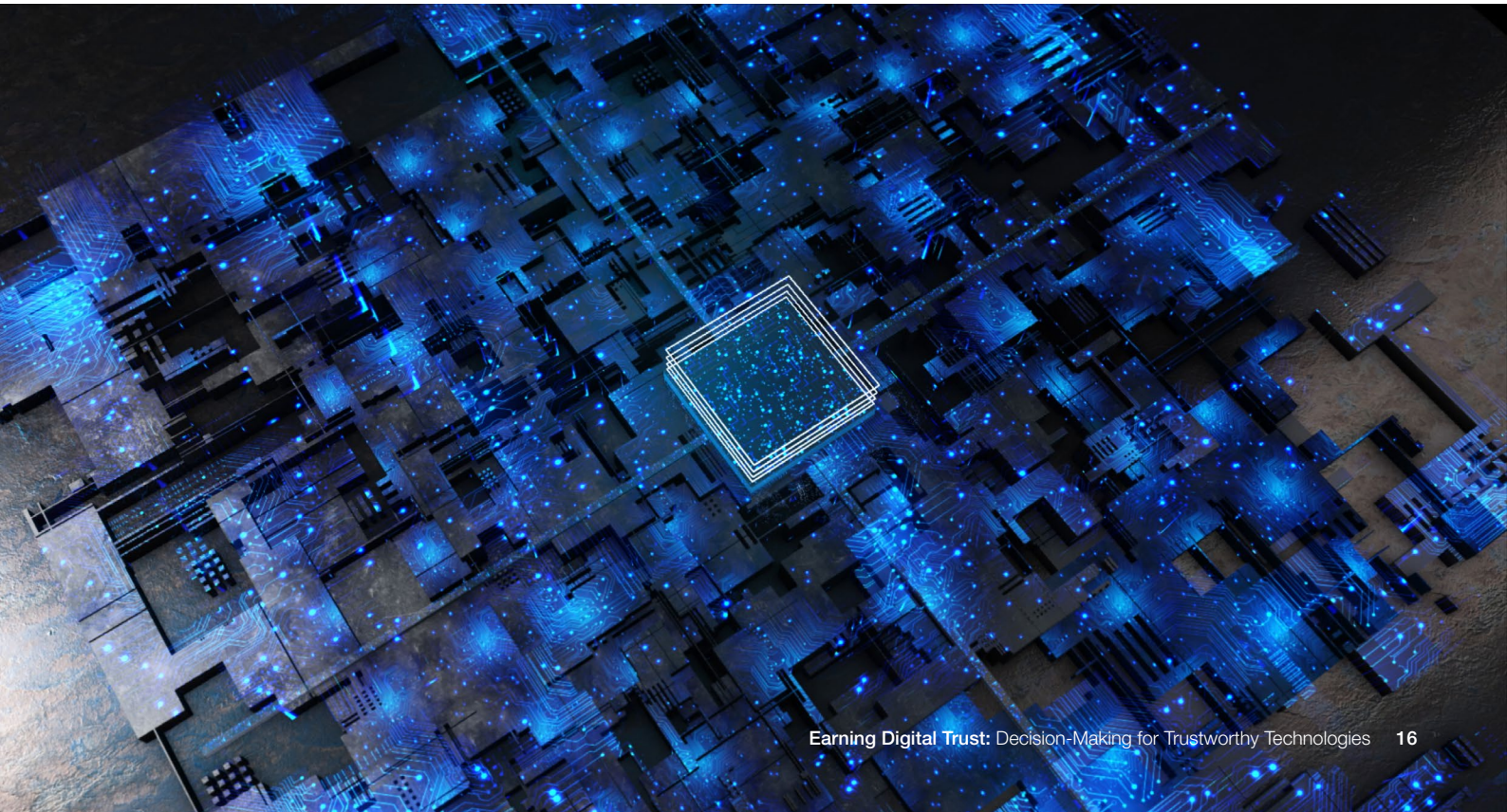
Across any set of dimensions of digital trust, decision-makers must consider what processes, mechanisms and tools are at their disposal to ensure that responsibilities related to each dimension are discharged in practice. It may be worthwhile for leaders to consider the variety of options available to do so, falling into two categories of trust assurance: mechanical and relational.

Mechanical trust is the means and mechanisms that deliver predefined outputs reliably and predictably. Applications of technology, like blockchain or non-discretionary disclosure practices, can be considered "mechanical". Mechanical trust means that, if a system performs predictably in and of itself, individuals will be more willing to use it. That is, they will be more willing to trust it.

Beyond mechanical applications, another equally important form of trust is required: relational trust. Even if all the mechanical systems work, if individual trust givers don't believe that organizations and individuals are all playing by the same rules or believe that organizational decision-makers don't fully consider and seek to align with their users' interests, core trust often breaks down. That is why relational trust – the social norms and agreements that address life's complex realities – is also vital. In the context of digital trust, relational trust often represents a shared agreement on when, where, why and how technologies are used.

As decision-makers review the following dimensions of digital trust, they should keep these two means of achieving results across the dimensions in mind.

For each of the dimensions of digital trust, the framework describes the dimension itself and offers context on how each dimension relates to achieving digital trust goals (security and reliability, accountability and oversight, and inclusive, ethical and responsible use). It also offers some considerations on the implementation of each dimension and likely challenges leaders will face. Taken together, it constitutes the **means** by which digital trust can be achieved.



Cybersecurity

Cybersecurity is focused on the security of digital systems – including underlying data, technologies and processes.[23] Effective cybersecurity mitigates the risk of unauthorized access and damage to digital processes and systems, ensuring resiliency. It also ensures the confidentiality, integrity and availability of data and systems.[24]

Relation to digital trust goals

> Decision-makers thus need to think not only of how cybersecurity can be actually achieved in their offering but also about signalling that it is implemented at acceptable levels.

Inclusive, ethical and responsible use

Good cybersecurity mitigates the risk of unintended uses (i.e. abusive) of technology. Especially with regard to historically marginalized populations, good cybersecurity in digital technologies and systems limits the harm to which customers and citizens are exposed. Naturally, however, the cybersecurity measures in place only cultivate inclusive, ethical and responsible use of the cybersecurity programme of an organization is driven by those goals itself.[25]

Accountability and oversight

Cybersecurity enables accountability by, for example, ensuring access to secured information is only given to the "right" individuals. Oversight is strengthened equally when organizations establish cybersecurity programmes that allow for monitoring and tracking behaviour and processing of data in the digital space.

Security and reliability

Cybersecurity is at the core of digital security and reliability. Given the significant threats digital processes are exposed to, having strong and effective cybersecurity programmes and, as a result, being seen as strongly protective of the data and information that users share, as well as being resilient to potential attacks, is paramount for secure and reliable digital technologies and systems.

Key considerations for decision-makers

Implementation

– **Treat cybersecurity as an organizational imperative**.[26] Stakeholders will demand that the technology they use (including systems and devices) is secure from intrusion, that any data they share is secure from unauthorized access, and, increasingly, that organizations can provide assurance that they take cybersecurity seriously (e.g. in the form of security labels, trust marks or effective cyber risk management practices).[27]

Decision-makers thus need to think not only of how cybersecurity can be **actually achieved** in their offering but also about **signalling that it is implemented** at acceptable levels on par with international cybersecurity best practices or standards and innovating over time to mitigate new risks.[28] Focusing on both these aspects of cybersecurity – the mechanical implementation, as well as the communication of the importance and value that an organization puts on cybersecurity, will be key to building trust.[29]

Challenge

- **Determining the appropriate cyber resources necessary to protect trust.** Cyber risk has enormous ramifications for any entity that gathers, stores or uses data. If a technological process touches data, digital trust demands that the controller of that process makes decisions aimed at securing that data. While cyber risk is always present, strong cybersecurity helps to ensure the confidentiality, integrity and availability of data, including preventing unauthorized changes or tampering with the data that could sow distrust in an organization's processes and the results they provide. Doing this effectively can often come with significant financial and other costs for a given organization.

- **Delineating responsibilities between cybersecurity and other trust dimensions may challenge existing foundational assumptions regarding cybersecurity's role and operating model**. Recognizing the critical and broad role that cybersecurity plays in the areas of business continuity, brand reputation, regulatory exposure and shareholder value, a concerted effort has begun to integrate cybersecurity as a strategic business enabler and to coordinate with other areas such as enterprise risk, product development and data management. Yet, when cybersecurity controls all aspects of an organization's security-related strategy, issues can arise when dimensional- and goal-related ownership is split between two or more teams. For instance, under the dominant confidentiality, integrity and availability (CIA) triad, it is assumed that cybersecurity is primary for keeping data reliable and accessible. Yet, digital trust requires a holistic approach, where cybersecurity is one dimension of trust among many. Digital trust requires questions of security to be considered alongside questions of, for example, whether data is accurate and fit-for-purpose or whether it is responsibly used. These and other similar considerations will require a tailored approach in order to successfully integrate cybersecurity into an organization's broader digital trust programme and its goals.[30] Ultimately, a risk-based approach that considers the context of use while balancing cybersecurity, privacy, digital safety and responsibility, usability, commercial viability and sustainability may prove to be essential.

Safety

Safety encompasses efforts to prevent harm (e.g. emotional, physical, psychological) to people or society from technology uses and data processing.[31]

Relation to digital trust goals

Inclusive, ethical and responsible use

Safety is a core aspect of the social norms and goals that digital trust is designed to uphold and protect.[32] An organization's decisions regarding safety can be addressed in an inclusive, ethical and responsible manner by including in due diligence an examination of the impact of safety mechanisms. For example:

- Is the safeguard in the best interest of the user and their human rights?
- Can all users access the precaution?
- Does the safety mechanism indicate that the organization is a steward for users?

Being able to answer these questions in the affirmative can indicate that an organization is conscientious of the consequences and is offsetting safety concerns in an inclusive, ethical and responsible manner, all of which promote an organization's digital trustworthiness as they act in the interest of the users.

Accountability and oversight

Accountability and oversight for safety requires decision-makers to think broadly about the ramifications of a given technology application or data use. As they develop and are applied to new areas, many technologies represent differing safety risks over their life cycle. For example, protocols and standards supporting data transfer created novel safety vulnerabilities when they were ported over to the physical world in the form of the internet of things. In order to avoid future safety issues, the governance mechanisms established for digital technologies and data uses must be flexible enough to foresee future safety concerns, or the governance mechanisms risk losing the trust of individuals over the long term.

Security and reliability

Safety promotes security and reliability by ensuring that technologies do not cause harm and operate as intended. Considering safety at the development or initial implementation phase ensures that the variety of uses to which new technologies are put continue to meet standards and expectations regarding their security and reliability. Decision-makers must consider how new environments (e.g. moving from purely data-focused to cyber physical systems) will increase the demand for safety assurances relating to increased security and reliability guarantees.

Key considerations for decision-makers

Implementation

- **Take a nuanced approach to harm mitigation and safety.** Safety for technologies and data uses is not one-size-fits-all. On the contrary, organizational approaches to addressing safety in operations, products and services are often contextual, as harm can manifest differently according to factors such as the type of technology, characteristics of the user and the context of technology used. Safety programmes are inherently responsive to the hazards that are endemic to an organization's product or service; therefore, a nuanced approach is recommended. As outlined below, these factors introduce considerations that organizational decision-makers should consider while addressing safety concerns.[33]

Challenges

- **Foreseeing and offsetting a range of possibilities for harm.** Appropriately implementing the proper safety precautions is difficult. The complexity includes factors for the type of technology, characteristics of the user and the context of technology used. Think of the differences across social media settings (e.g. harm to well-being, content moderation), extended reality (XR) experiences (e.g. invasion of personal space, personal space perimeter) and self-driving cars (e.g. reckless driving, safety driver). Within these scenarios, designing with an inclusive mindset and considering not only the archetypal user but also those with a range of abilities and resources is key. Plus, context-dependent norms in various settings (e.g. consumer, employment, educational, medical) can transform the possibilities for harm and safeguards. To address this challenge, organizations can coordinate their safety efforts, whether by industry or according to the user.[34]

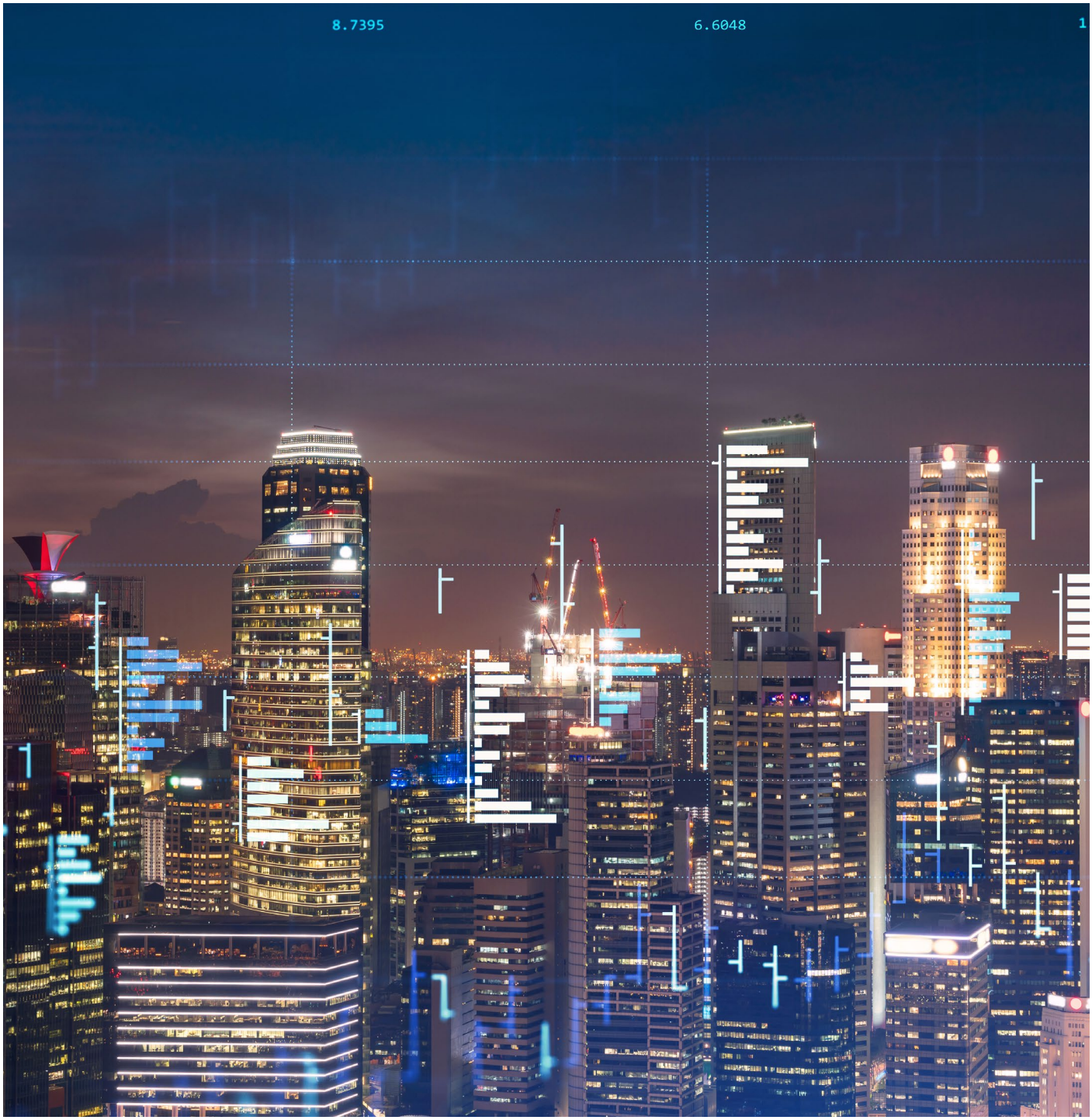
> Safety is a core aspect of the social norms and goals that digital trust is designed to uphold and protect.

BOX 7 | **Singapore: Public-private collaboration in making online safety a priority**

Safety has traditionally been a key expectation of governments, and the same can be true in digital spaces. In Singapore, as the nation progresses through its "Smart Nation" journey, the safety aspect of digital trust has been an important concern. National leaders recognize that citizens and businesses must feel safe when using digital communications and technologies. A lack of safety due to threats such as cybercrime, phishing scams and various online harms will erode public trust in digital technologies and undermine the ability to fully harness the opportunities offered by them.

To cultivate digital trust, the Singapore Ministry of Communications (MCI) works with its agencies, such as the Cyber Security Agency of Singapore (CSA) as well as the Smart Nation and Digital Government Office (SNDGO), to create a safer and trusted digital environment.

MCI collaborates with stakeholders across the private and public sectors to implement regulations, codes of practices and programmes that will enhance the safety of the digital environment. Among these programmes is the Sunlight Alliance for Action, which was launched in 2021 to close the digital safety gap through workstreams such as research, victim support and public education.



Transparency

Transparency requires honesty and clarity around digital operations and uses. Enabling visibility into an organization's digital processes reduces the information asymmetry between an organization and its stakeholders while signalling to individuals that the organization intends not only to act in the individual's interest but also to make those actions known and understandable to those inside and outside of the organization.[35]

Relation to digital trust goals

Inclusive, ethical and responsible use

Transparency showcases how decisions are being made, and thus enables interventions in the interest of inclusive, ethical and responsible use.[36] Where organizations recognize the ethical responsibility to share information about how technologies are used and to what ends, ensuring transparency is a key activity in building trustworthiness.

Accountability and oversight

Transparency provides information about how technologies are developed and implemented, how data is used and how it sets the standard for governance. The mechanisms of accountability and oversight are also rendered more trustworthy if they are transparent. Giving stakeholders insight into how technology decisions are assessed and how issues regarding the development or application of new technologies are handled likewise increases trustworthiness for customers, citizens and other affected parties.

Security and reliability

For the goal of security and reliability to impact the trustworthiness of an organization or technology, the particulars of these goals, and progress in reaching them, must be transparent. Even relatively straightforward mechanisms to publicly track security incidents or reliability failures and their remediation can significantly improve trustworthiness.[37] These mechanisms help to set stakeholder expectations of security and reliability as well as the expectation that these goals are taken seriously by the organizations with which they are entrusting data or their physical or digital safety.

Key considerations for decision-makers

Implementation

- **Design with user-friendly transparency in mind.** Leaders should encourage their teams to work backwards. First, identify the details that may need to be disclosed in the future. Then, when building out an organization's technology stack, (both for internal development as well as in the products the organization provides externally) document design decisions can include capabilities to track the use of data and flow of information in a manner that can be communicated, as needed, to a range of stakeholders in a timely and useful way.[38]

Challenges

- **Meeting agency expectations.** Beyond being able to access relevant information about how their data is being used, trust givers need to be able to **understand, appreciate and act upon** the information provided in order to make an informed decision as to whether they want to give their trust or not. Transparency enables agency of the trust giver; understanding and acting upon the information being provided is central to meeting agency expectations.

- **Determining appropriate disclosure.** Being radically transparent and providing broad access to information about how users' data is collected and used, particularly with a significant amount of detail, may often conflict with an organizations' other interests. As such, the scope of the audience and level of data provided need to be evaluated. Audiences can – as a first step – be divided into internal (e.g. employees, legal and compliance functions) and external (e.g. customers, regulators and watchdogs). From there, considerations, including purpose and level of expertise, can further inform the content of the disclosure. While this balance will undoubtedly be difficult to achieve, and an organization will rarely receive plaudits from all audiences, it is a critical path to follow to build and maintain digital trust.

“Transparency provides information about how technologies are developed and implemented, how data is used and how it sets the standard for governance.

Interoperability

Interoperability is the ability of information systems to connect and exchange information for mutual use without undue burden or restriction.[39]

Relation to digital trust goals

Inclusive, ethical and responsible use

When considering interoperability, organizations must ensure that all connected technologies also satisfy their ethical and responsible use goals. This may require a balance between wide-scale interoperability and adherence to the organization's commitments to ethical and responsible use. Thus, the extent to which technologies are made interoperable must be subject to senior leaders' judgement and should not be considered merely a technical question. Likewise, interoperability may promote inclusivity by allowing a larger set of stakeholders access to beneficial technologies (for example, the portability of health data.[40] Still, the benefits and risks of these interconnections must be assessed concerning the organization's goals and the expectations of its stakeholders.[41]

Accountability and oversight

Interoperability enables many individuals and organizations to collaborate on and improve technology. This large number of collaborators offers the opportunity for additional oversight but also requires further accountability mechanisms within individual organizations. Where collaboration promotes and facilitates group problem-solving, this will include inputs that should be considered within individual collaborating organizations' accountability functions. It is likewise the responsibility of each organization developing interoperating technologies to ensure that its accountability and oversight mechanisms meet the standards of the whole system and the expectations of all stakeholders affected by the technologies.[42]

Security and reliability

Interoperability requirements and controls make significant contributions to technology security and reliability. For technology to co-exist and connect with other technologies and data, a degree of openness – including open-source code and common data standards – is necessary, even if not in itself sufficient, to enable sharing and integration.[43] Further, when source code is public and accessible, users can help to verify that the technology operates as intended and identify the dependencies of their safeguards on other technologies and organizations. Even if source code cannot be made public, adequate assurances of security and reliability promote interoperability between systems, which is both a result of digital trust and helps build greater trust among stakeholders.[44]

Key considerations for decision-makers

Implementation

- **Laying the groundwork for interoperability.** Interoperability requires that different systems can interpret and present data as it is received, while also preserving its original context. This requires consideration of the governance and operating rules for the technology designed to establish how participants in the interoperability arrangement will make decisions, jointly manage operations and consider risk. Business agreements must also balance the economic interests of parties and incentivize the exchange of source code and data. Finally, designers must plan for technical infrastructure that connects parties, systems and their data.

- **Uniform technology expectations and standards are key.** Industry-specific technology standards can lead to broad economic growth and social good. History is replete with such examples. In the late 19th century, a collective decision by the southern United States to convert, in just 36 hours, 13,000 miles of track to standard-gauge width led to substantial stock price increases for southern railroads and the eventual demise of the steamship freight industry.[45] The 1970s introduction of UPCs (bar codes) caused a worldwide revolution in supply chain efficiency that experts calculate saved the grocery industry 5.65% (or $17 billion) of total annual sales in 1999.[46] More recently, Kenya's issuance of mobile phone remittance transfer requirements sparked a "mobile money" revolution that delivered financial inclusion to impoverished rural communities, thereby reducing poverty and increasing occupational change (particularly for women), agricultural modernization and private sector development.[47] In each of these instances, competing organizations' adoption of common standards enabled wider dissemination of critical goods, money and information due to users' and companies' independence from specific systems and networks.

"The extent to which technologies are made interoperable must be subject to senior leaders' judgement and should not be considered merely a technical question.

Challenges

– **Protecting security and privacy.** While interoperability is key to an open and pro-competitive internet, unrestrained system integration poses significant privacy and security issues. For example, privacy principles stipulate that users should be able to control and limit third-party access to their personal information. Therefore, system integration can infringe upon privacy rights if users do not have adequate notice and the ability to consent to sharing their personal information before the system integration is consummated. Similarly, the system connectors that enable interoperability also provide an additional attack surface for malicious actors who seek to access data without authorization. With this in mind, trustworthy interoperability should be promoted, with a clear recognition and plan for any privacy and security risks.

Auditability

Auditability is the ability for both an organization and third parties to review and confirm the activities and results of technology, data processing and governance processes. Auditability serves as a check on an organization's commitments and signals the intent of an organization to follow through on those commitments.[48]

Relation to digital trust goals

Inclusive, ethical and responsible use

Comprehensive audits can allow organizations to measure their own progress against their ethical goals. In addition, making the results available can help prove to individuals and other stakeholders that an organization is meeting its commitments to achieve this goal. When considering how to audit its technology decision-making, organizations should pay attention to the ramifications of these decisions. Audits of digital trust must consider whether technologies developed, implemented or used are adequately inclusive of a wide array of potential users and stakeholders (and meeting their expectations) as well as whether the technology meets the organization's ethical and responsibility goals and commitments.

Accountability and oversight

Audits drive effective governance, accountability and oversight.[49] It is impossible for an organization to adequately meet this goal without a robust audit mechanism in place. For the accountability and oversight of digital technologies (especially emerging technologies like AI) to be effective, auditability must be addressed at the development stage. Ever more complex technologies, if developed without

auditability in mind, represent significant challenges to audits after the fact. Trustworthy organizations avoid developing or implementing technologies where operations exist in a "black box", defying the ability to examine how they function and deliver results.

Security and reliability

Auditability can help correct for the otherwise limited means of assessing security and reliability, an opportunity that typically only presents itself when there is an actual, significant security or reliability problem. External publication of such security audits and running related bug bounty programmes can signal to trust givers the importance an organization places on security and reliability. External reporting of factors such as security breaches or uptime[50] as well as measures taken to improve those factors, aids in building trust with an organization's stakeholders.

Key considerations for decision-makers

Implementation

- **Defining the scope of an organization's audit landscape.** Organizations are likely well-versed in auditing their quantitative procedures, decisions and associated data. However, documenting and applying auditability standards and processes to qualitative procedures and decisions are all the more important when seeking to earn digital trust due to the potential for variability and claims that an organization is not meeting its commitments. Organizations must, therefore, make efforts to compensate for the potential documentation challenges that can arise in the context of such procedures and decisions.

Challenges

- **Understanding the implications of data retention:** The ability to store the information captured will determine the available time frame for a potential audit. As storage decisions are often a function of hardware, financial and legal constraints, each of which may have implications for the relevant retention period, it is important that these be accounted for in any auditability plan and process.
- **Examining the role of internal or external auditors:** The audience of the audit's findings will change depending on which trust givers an organization seeks to cultivate trust with. For example, internal audits will satisfy internal stakeholders, however, may not bolster trust with external parties. As such, it is likely that an organization will need both internal and external audits. Beyond legally required audits, however, it may not be sustainable to have regular external audits given the cost and the impact on internal resources that need to be focused on revenue-generating activities, so an organization will need to think carefully about how to structure such audits and how often they are needed. In this context, it may be worth considering how the building and maintenance of digital trust impacts an organization's bottom line because for organizations for whom digital trust is key (e.g. holders or processors of large amounts of or highly sensitive trust giver data), regular audits may well be worth conducting, even given the significant expense and impact on other operations.

Redressability

Redressability represents the possibility of obtaining recourse where individuals, groups or entities have been negatively affected by technological processes, systems or data uses. With the understanding that unintentional errors or unexpected factors can cause unanticipated harms, trustworthy organizations have robust methods for redress when recourse is sought and mechanisms in place to make individuals whole when they have been harmed.[51]

Relation to digital trust goals

Inclusive, ethical and responsible use

Designing avenues for recourse and having processes and culture to provide redress builds trust by maximizing agency. This also demonstrates an organization's respect for the individual and their interests, needs and expectations. External opportunities to identify problems and redress harms are vital to earning trust when developing or implementing new technologies. While responsibility can be achieved by internal measures of accountability, ethical and responsible organizations create avenues for redress when the technology they develop or control causes harm to external stakeholders. These external avenues also serve as checks where an organization falls short of meeting the goal of inclusive, ethical and responsible use.

A trustworthy organization uses its oversight function to ensure that it is accountable to itself and all stakeholders for technology-related decisions and the consequences of those decisions.

Accountability and oversight

Redress mechanisms are critical components of any accountability and oversight programme. Rather than focusing its oversight solely on how to improve internal delivery or maximize efficiency or profit, a trustworthy organization uses its oversight function to ensure that it is accountable to itself and all stakeholders for technology-related decisions and the consequences of those decisions. Organizations should hold themselves accountable for making human-centric decisions that consider the impact of activities on individual citizens or consumers and actively seek opportunities to remedy harms those decisions have caused.

Security and reliability

Security and reliability failures impact the organization and its network of partners, users and other stakeholders. Significant downtime, or a data breach, has a negative impact on trustworthiness. When these events are coupled with a lack of redress or an unwillingness to make affected partners, customers or individuals whole in response to their losses, this loss of trust is compounded. For these stakeholders, having a clear, easy-to-use avenue for redress when security or reliability cannot be adequately achieved enables an appropriate response to assess and correct the harm that may have occurred.

Key considerations for decision-makers

Implementation

- **Enable effective redressability**: Commitments to redressability may build upon existing procedures. Organizations are likely to have an existing support function for users, customers or clients. Such functionality may be tiered, starting with automated self-service for frequently asked questions (FAQs), which can lead to support over email, phone call or chat message with a bot and then, if necessary, an agent. Redressability may take advantage of these functions and tiered processes to ensure it can be achieved effectively and at a limited cost to the organization. It is also important for organizations to take actions that engender trust through transparency and other self-service resolutions, such as using FAQs as a feedback mechanism and designing products/services.[52]

Challenges

- **Minimizing customer burdens:** Efforts in recent years to automate and outsource support functionality have been a cost-saving method for many organizations. However, many of these functions merely push the burden of dedicated time to seeking redress onto the harmed individual. Reinvestment support for customers – the opportunity to engage with a knowledgeable, capable employee, easily and directly, who is empowered to provide redress for harmed individuals – will help to bolster an organization's trustworthiness.

- **Defining the scope of the redress process:** Defining the scope of a complaint process promotes individual autonomy and respect. As with any system, however, it is possible for users, customers, clients or third parties to abuse such a process. As a result of offering guaranteed compensation for victims of severe airline delays, the EU also incentivized companies to arbitrage claims filing and processing for 30-40% of the guarantee. Organizations will need to set the boundaries of what types of decisions are subject to redress and which are not and be transparent regarding such decisions. Ultimately, an organization must balance what is appropriate for an individual with what is feasible at scale and in the case of redress, recognizing that redress may be required across not just one individual but a relatively large segment of users, customers or clients.

Fairness

Fairness requires that an organization's technology and data processing be aware of the potential for disparate impact and aim to achieve just and equitable outcomes for all stakeholders, given the relevant circumstances and expectations.[53]

Relation to digital trust goals

> Standardization enhances fairness by ensuring that decisions are objectively consistent in processes and outcomes – and aligned to a common set of ethical, inclusive and responsible use norms.

Inclusive, ethical and responsible use

Fairness is deeply connected to meeting the goal of inclusive, ethical and responsible use. Defining what is fair in a given scenario is ultimately a subjective decision. It requires balancing questions of equity, equality, consistency and many others. For example, in some scenarios, equality may not be just, and therefore equity considerations may motivate additional steps for certain individuals or groups to better level the playing field. Decisions like the determination of equality versus equity are prime example of the need for standardization referenced in the inclusive, ethical and responsible use section above. This standardization enhances fairness by ensuring that such decisions are objectively consistent in processes and outcomes – a key hallmark of fairness[54] – and aligned to a common set of ethical, inclusive and responsible use norms defined in best practices frameworks.[55]

Accountability and oversight

Being fair in both process and outcome is a key goal of accountability and oversight activities, sending a signal of trustworthiness to customers and individuals. Organizations should include fairness as an issue for which they hold themselves accountable, consistent with their values and those of the society in which they operate. This might mean different standards for fairness in different geographies for the same organization. Integrating fairness into oversight processes in pursuit of this goal means that organizations should not consider questions of "what is fair" or "what is just" to be exogenous to their decision-making processes. Creating opportunities for internal and external validation of whether a decision is fair (as consistently defined within the organization) can help organizations act in a trustworthy manner.

Security and reliability

Fairness commitments support security and reliability goals, as one core conception of fairness is achieving similar outcomes for different people across similar situations. Where fairness is considered "treating similarly situated individuals similarly", the mechanisms for protecting data and ensuring its availability for use for beneficial purposes must be equally applied. Good security itself is an exercise in promoting fairness. As organizations are the controllers of individuals' data and receive benefits from using such data, fairness demands that they reciprocate that value by making efforts to protect the data they have received.

Key considerations for decision-makers

Implementation

- **Documenting fairness judgement calls:** Beyond any jurisdiction-specific discrimination protections (e.g. fair lending or fair housing), decisions regarding fairness generally result in reasonably consistent treatment of all individuals. Such decisions may be addressed in an organization's diversity, inclusion or accessibility initiatives – or responsible AI efforts when using artificial intelligence. When defining and operationalizing fairness within an organization's technology and data processing, documenting the justification of associated decisions ensures that both the process and outcome are fair. For example, the trade-off between standardization and personalization can have fairness connotations, as there is often a fine line between appropriate personalization and biased (i.e. discriminatory; exclusionary) experience. As such, in making design decisions, it will often be helpful to document the assessment of fairness and equity in those processes, as what's fair can mean different things in different contexts to different people. As part of this documented process, fairness may require impact assessment that includes the identification of affected stakeholders, potential harms and benefits, and steps necessary to mitigate those harms.

Challenges

- **Assessing the fairness of the system/product/process:** Assessing existing infrastructure and new products for fairness considerations will aid in signalling trustworthiness to external trust givers. These could include evaluating the proper scope of monitoring data use and assessing time frames and need for data retention. Fairness can be relative to particular individuals or groups, so organizations are encouraged to consider multiple personas when they assess fairness decisions.

Privacy

Privacy, for individuals, is the expectation of control over or confidentiality of their personal or personally identifiable information.[56] For organizations, privacy is the meeting of this expectation through the design and manifestation of data processing that facilitates individual autonomy through notice and control over the collection, use and sharing of personal information.[57]

Relation to digital trust issues

Inclusive, ethical and responsible use

Privacy serves as a requirement to respect individuals' rights regarding their personal information and a check on organizational momentum towards processing personal data autonomously and without restriction. A focus on this goal ensures that organizations can unlock the benefits and value of data while protecting individuals – especially historically marginalized or at-risk populations – from the harms of privacy loss. It effectuates inclusive, ethical and responsible data use – or digital dignity[58] – by ensuring that personal data is collected and processed for legitimate purpose(s) (e.g. consent, contractual necessity, public interest, etc.).

Accountability and oversight

Privacy cannot be achieved without accountability and oversight. Given organizations' exclusive access and control over their systems' data processing, privacy requires internal corporate accountability and oversight to ensure that data processing is limited to permitted uses. Achieving this goal also requires mechanisms for external validation or review to assure individuals of adequate privacy protection. As an example in practice, the appointment of, and substantial authority given to Chief Privacy Officers and Data Protection Officers ensures an organization-wide, fundamental commitment to a cohesive approach to an organization's data functions.[59]

Security and reliability

Privacy is intertwined with, and reliant upon, the goals of security and reliability. Security ensures that privacy expectations are vindicated by preventing unauthorized access to individuals' data. Reliability ensures that data uses are predictable and expectations regarding consent and deletion can be satisfied. For example, a significant number of privacy regulations[60] enumerate specific categories of sensitive data that require greater data protection, such as de-identification, obfuscation and encryption. Privacy similarly implicates technological reliability through individual rights and consent management by requiring that organizations stop processing data when user consent is revoked and delete, share or modify data in response to an individual data rights request.

Key considerations for decision-makers

> A comprehensive and coordinated data governance programme is necessary for organizations to effectively operationalize privacy requirements.

Implementation

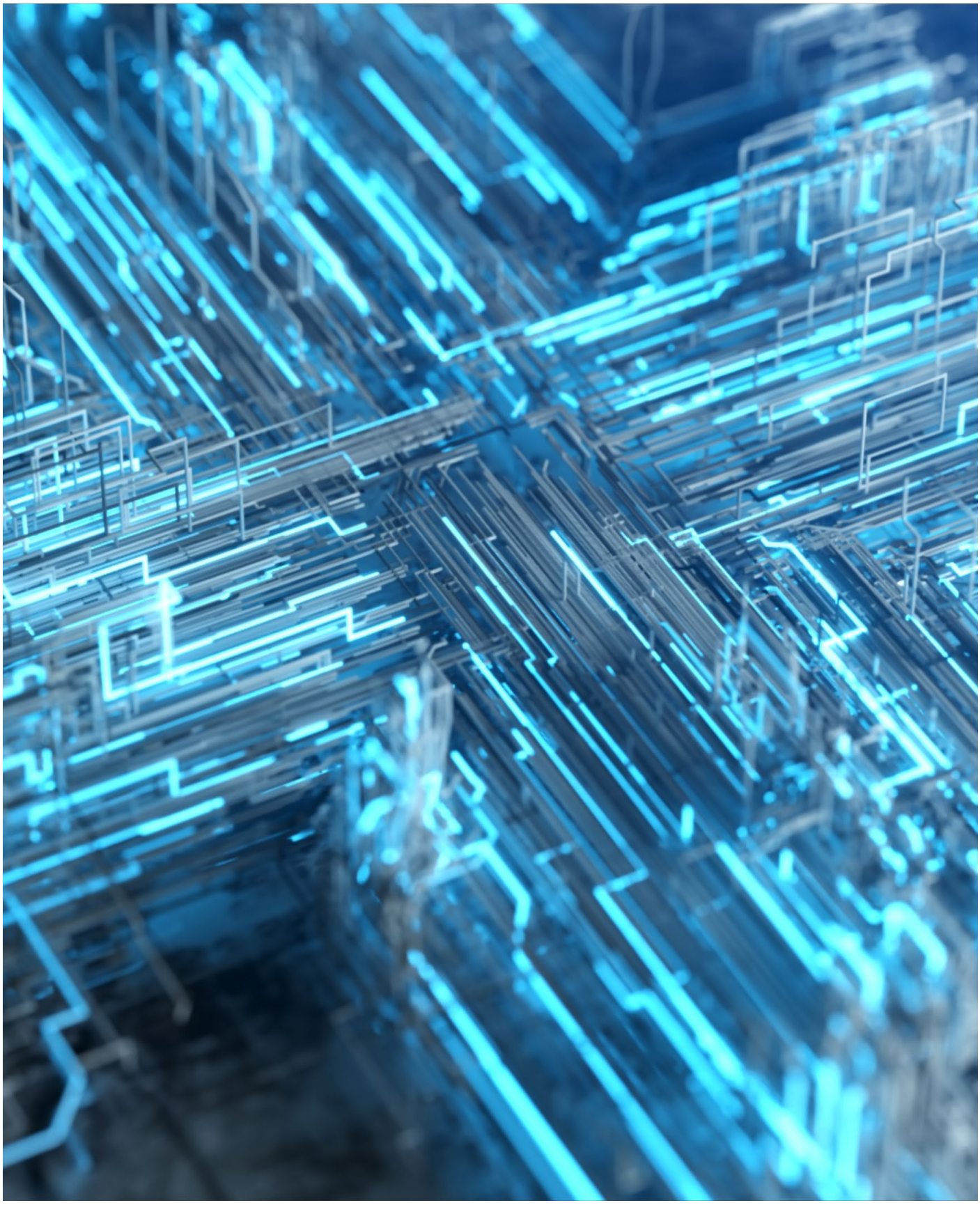
- **Privacy programmes require broad, cross-functional implementation to adequately manage and effectuate individual's rights and freedoms over their personal information:** Technical and process implementation of privacy requirements have a substantial impact on many core business functions, such as data security, product development, marketing, communications, human resources, legal and third-party risk. Indeed, privacy programmes comprised of the following domains have been observed to provide effective combination compliance and business enablement:
  - **Strategy and governance:** Designated resource(s) coordinate and maintain responsibility for the privacy programme and provide relevant capabilities to the organization.
  - **Policy management:** Privacy policies, procedures and guidelines are formally documented, aligned and consistent with applicable laws and regulations.
  - **Cross-border data strategy:** Consent is obtained (where applicable), and appropriate safeguards are implemented when transferring data across jurisdictional borders.
  - **Data life cycle management:** A personal data inventory exists and catalogues data sources, locations and flow. Data is tagged and classified according to its sensitivity and risk levels.
  - **Consent management:** Consent for personal data processing is obtained (where applicable), tracked and effectuated.
  - **Individual rights processing:** Data subject inquiries are executed across appropriate systems and third parties; responses are timely and in accordance with applicable laws and regulations.
  - **Privacy by design:** Appropriate privacy considerations are embedded in the design, acquisition or implementation of new products or services.
  - **Information security:** Personal information is safeguarded and protected to ensure ongoing confidentiality, integrity and data availability.
  - **Privacy incident management:** Policies and procedures are established to manage and remediate suspected personal data breaches.
  - **Data processor accountability:** Privacy requirements are agreed to and documented before granting third-party access to personal data. Third-party access to and processing of personal data is regularly monitored, reviewed and audited.
  - **Training and awareness:** Privacy awareness and training requirements are documented, provided to employees and monitored for compliance.[61]

Challenges

- **Information governance is essential to achieving meaningful privacy compliance:** Information governance is the organizational management of data storage, quality and integrity. It ensures that data can be relied on to be accurate and complete for all functions in an organization. A comprehensive and coordinated data governance programme, therefore, is necessary for organizations to effectively operationalize privacy data management requirements.
- **Threshold measurements of adequate privacy programme maturity are underdeveloped and vague:** Statutes, customer expectations and corporate policies often describe data privacy principles, guidelines and requirements but do not identify the specific operational components of a successful privacy programme. As a result, privacy programme maturity standards remain somewhat undefined, and compliance practices are often inconsistent from one organization to the next.
- **Ever-shifting compliance requirements and deadlines inhibit the organized design and development of deliberate, structured privacy programmes**: Privacy operations have been in intensive, costly cycles of development and implementation to comply with a group of regulations that came in quick succession – the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and more than 2,500 other global laws – and show no signs of abating. Consumers are also increasing their privacy IQ, cementing their personal data management expectations, and are increasingly likely to exercise their data rights. As a result, compliance programmes emerged in a piecemeal fashion to comply with new, separate regulations and market expectations. Yet a continued piecemeal approach is untenable. Forward-thinking privacy leadership and programme design – founded upon data management and compliance agility – is, therefore, necessary to sustainably grow and manage organizational privacy programmes.

2 Digital trust roadmap

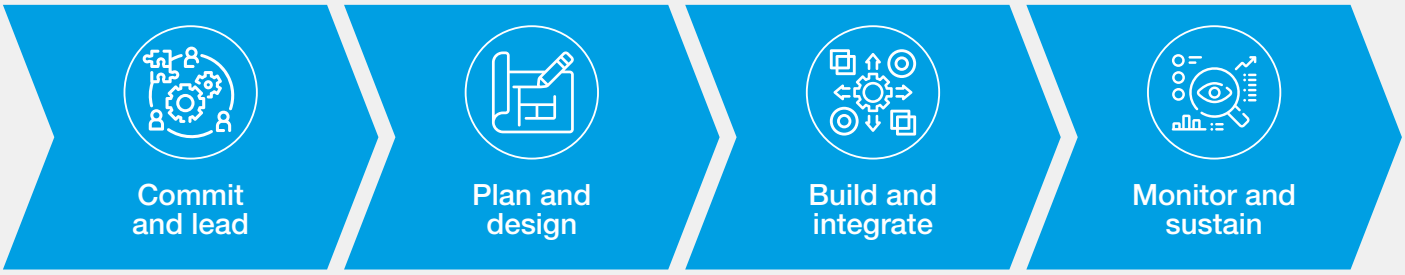
Effective digital trust programmes are aligned with values and organizational structures.



The digital trust framework seeks to spur organizations beyond compliance and take a comprehensive approach to digital trust, its associated goals and underlying dimensions. The following roadmap will support decision-makers as they seek to align with individual and societal expectations and act to earn digital trust. It details the steps necessary to build a collaborative – rather than isolated – approach to technology decisions by designing, developing, building and maintaining the dimensions of digital trust. Therefore, this roadmap guides decision-making holistically, beyond recommendations for any dimension of digital trust, to operationalize the framework.

By following the recommended roadmap, organizations will be able to adopt, commit to and maintain a viable digital trust programme. The roadmap guides leaders in following these steps in implementing the digital trust framework:

FIGURE 2 **The digital trust roadmap**



Commit and lead

> Making digital trust an essential organizational value and goal will require affirmative steps that broadly integrate digital trust dimensions and goals into business operations.

Digital trust will require commitment from the highest levels of leadership to succeed. Most organizations will therefore need CEO and board endorsement to deliver long-term, sustained commitment to developing its digital trust programme. Indeed, in recognition of digital trust's multidisciplinary and cross-functional requirements, CEOs, especially, have a crucial leadership role to play in bringing disparate stakeholders and teams together to plan and design accordingly.

Of course, considerable preparation and groundwork are required before presenting and proposing a digital trust programme to a CEO. To gain leadership support and funding, any such proposal must have a clear strategy and vision supported by a compelling, integrated and thorough **business case**. The business case should, in turn, identify both the qualitative and quantitative benefits of digital trust adoption and transformation efforts, such as:

- Articulating the role and value that digital trust would provide to the broader organizational strategy and reputation, including in relation to the organization's core values.[62]
- Identifying how digital trust will align with other organizational initiatives and business areas.
- Emphasizing digital trust's strategic input into other key business areas, such as product development, marketing, risk management, privacy and cybersecurity.
- Include a cost/benefit analysis of the decision to build and maintain a robust digital trust programme.

Making digital trust an essential organizational value and goal will require affirmative steps that broadly integrate digital trust dimensions and goals into business operations by, for example, pledging to exclusively develop, procure or affiliate with trustworthy technologies that responsibly manage and process data or establishing and aligning a new digital trust programme with existing commitments and plans for growth.

Plan and design

Organizations must subsequently identify and articulate their case (or need) for a digital trust programme. Organizations will often begin this task by performing a "digital trust gap assessment" that identifies current-state functional capabilities and deficits (or "gaps") against the framework's requirements. Assessment reports should include the following:

- Current-state observations: A summary of the "grouped" gap analysis findings mapped to the framework.
- Recommendations: A high-level list of future state recommendations.
- Governance, risk management and compliance (GRC) findings: A list of gaps that are specific to regulatory and/or other compliance requirements.
- Benefits derived: An overview of the main benefits that digital trust improvements will provide.
- Risk(s) mitigated: An identification of risk areas that digital trust improvements will mitigate.
- Timetable and dependencies: The estimated duration of the initiative and high-level descriptions of potential interruptive dependencies.
- Initiative governance and staffing: The specific teams and resource staffing needed to support and implement the initiative (i.e. Cyber, Privacy, Audit, ESG, Product, Marketing, Operations, Contractors, etc.).
- Organizational impact: A description of the initiative's impact from an operational and end-user standpoint.

In sum, the digital trust gap assessment will specify the tasks, resources and subject matter expertise required to construct and improve current-state capabilities necessary to operationalize the framework and reach the organization's desired state of digital trust maturity.

Build and integrate

The development and implementation of an organization's digital trust capability requires action in the areas of people, process and technology.

With regard to people, focus is required in three key areas:

- Adopt **leadership and behavioural changes** necessary to the success of digital change management, assign ownership of the organization's digital trust programme, and ensure that project progress is visible to executive sponsors.
- Identify and **develop workforce skills** necessary to meet digital trust capability requirements, allocate or obtain new resources necessary to attain the desired target state, and organize digital trust teams and stakeholders to encourage development, collaboration and innovation with the right balance of centralization and proximity across the business.
- Deploy a structured approach to **change management and communications** to ensure the success of the digital trust programme or transformation, including a communications and training strategy.

“ Identify, build and connect tools that will enable the adoption, management and success of the organization’s digital trust programme.

As for processes, new policies, practices and procedures combined with robust information management are necessary:

- Employ established **change management practices** required to support the journey to digital trust operationalization. Develop project timelines, budgets and implementation priority areas.
- Define and operationalize the organization’s **digital trust decision-making structure and processes**, modifying the roles and responsibilities of existing digital trust-related functions (e.g. cybersecurity, audit, privacy, etc.) and stakeholders accordingly. Align existing teams and practices following the organization’s digital trust framework, strategy and operating model. Integrate digital trust requirements and controls into areas such as product design and development, data governance and risk management. Identify and consider additional strategic, tactical and operational process improvements where appropriate and required.
- **Identify and understand existing data assets**, enabling the organization to derive the full benefit of digital trust implementation. Consider the use of master data management and data quality-related business requirements. Integrate or migrate existing data repositories into a singular location that serves as the source of truth and reduces the costs of data redundancy.

Lastly, in connection with technology requirements, identify, build and connect tools that will enable the adoption, management and success of the organization’s digital trust programme. While individual technologies cannot, in themselves, create digital trust, the application of technologies consistent with an organization’s values and goals can effectively support the development of a digital trust programme. Consider the use of the following:

- AI-based data monitoring helps to validate data accuracy, authenticity and reliability by uncovering missing data, anomalies or unexpected data, including fake or manipulated documents, images and videos that are not otherwise identifiable via manual examination.
- Cloud-enabled data trusts govern, control and secure data processing and access rights for authorized systems and stakeholders.
- Blockchain, a type of distributed ledger technology, preserves immutable records of transactions. Such documentation illustrates provenance and protects against record-keeping tampering.[63]

Monitor and sustain

Upon the successful implementation of a digital trust programme, concerted efforts will still be required to ensure its continued effectiveness and longevity as digital trust transitions into a business-as-usual organizational component. To do so:

- Establish performance and risk measurement tied to incentive structures to ensure comprehensive and robust adoption.
- Conduct board as well as public reporting regularly, which could include maturity metrics to further support broad adoption.
- Ensure continuous improvement in light of evolving expectations and business requirements for digital trust.

This roadmap, used in conjunction with guidance in the digital trust framework, offers the opportunity for leaders to give effect to their decisions in favour of trustworthy technologies. By coupling better decision-making with clear and motivated action, leaders and their organizations can begin earning digital trust.

Conclusion: Public-private cooperation for digital trust

The goal of building and implementing more trustworthy technologies is within reach. By focusing on earning digital trust, leaders of organizations that develop and deploy new technologies can both make decisions and take action on one of the most crucial technology issues of this decade. The digital trust framework and roadmap offer a way forward that ensures technology serves the goals of individuals and society.

By cultivating digital trust, leaders will ensure that the benefits of digital technologies are more widespread and available to a wider segment of the globe than ever before. At the same time, decision-making that focuses on the trustworthiness of these technologies will help to ensure that any harms arising from new technologies are no longer treated as externalities to be borne by unconnected individuals.

There are, of course, many stakeholders in digital trust. While this publication focuses on those who ultimately decide which technologies are developed, governments, civil society, and individuals themselves all have a role to play. Between states (and private enterprises), questions of digital sovereignty, data trade and other issues will significantly impact digital trust in the coming years. Governments also influence the development of technology through their own acquisitions and investments – an area where questions of digital trust arise ever more frequently. Likewise, the role of civil society, both as an advocate for digital dignity and protection of individuals and as a user of digital technologies is a vital aspect of the digital trust landscape. Individual citizens and consumers, themselves, should be empowered to advocate for and enforce their rights and expectations with regard to new technologies. Future work under the Digital Trust initiative will develop guidance for these stakeholders as well. The Forum welcomes all stakeholders to engage in and support these efforts as part of the global digital trust community.

While this report represents an important step on the journey towards rebuilding digital trust, it must be followed by further action. Here, it is recognized that leaders must take the downsides of technology use seriously, make technology decisions that focus on individuals and plan to do better. The next steps will be to encourage others to adopt these same goals and work with this community to plan to become more trustworthy actors in digital environments.

In the end, earning digital trust is a responsibility shared by companies, governments, civil society and all individuals. This digital trust framework begins the work of meeting that responsibility.

Contributors

Lead author

Daniel Dobrygowski
Head, Governance and Trust, Centre for Cybersecurity, World Economic Forum

Digital Trust initiative Project Fellows

Assaf Ben-Atar
Manager, Cyber Risk and Regulatory: Data Risk and Privacy, PwC

Augustinus Mohn
Manager, Cyber Strategy and Risk, KPMG

Amanda Stanhaus
Manager, Metaverse Continuum Business Group, Accenture

World Economic Forum

Sean Doyle
Lead, Centre for Cybersecurity

Akshay Joshi
Head, Industry and Partnerships, Centre for Cybersecurity

Jeremy Jurgens
Managing Director and Head, Centre for Cybersecurity

Project advisers

Sean Joyce
Global Cybersecurity and Privacy Leader, US Cyber, Risk and Regulatory Leader, PwC

Toby Spry
Platform Fellow, Centre for Cybersecurity, World Economic Forum; Principal, Data Risk and Privacy, PwC

Steven Tiell
Platform Fellow, Centre for Cybersecurity, World Economic Forum; Senior Principal, Technology Innovation Strategy, Accenture

David Treat
Senior Managing Director, Lead Metaverse Continuum Business Group, Accenture

Akhilesh Tuteja
Global Cyber Security Practice Leader, KPMG

Annemarie Zielstra
Platform Fellow, Centre for Cybersecurity, World Economic Forum; Partner, Cybersecurity, KPMG

Digital trust community

Digital Trust initiative steering committee

Ajay Bhalla
President, Cyber and Intelligence Solutions, Mastercard

Nozha Boujemaa
Global Vice-President, Digital Ethics and Responsible AI, Ingka Group (IKEA)

Julie Brill
Chief Privacy Officer, Corporate Vice-President, Microsoft

Keith Enright
Vice-President and Chief Privacy Officer, Google

Nancy Flores
Executive Vice-President, Chief Information Officer and Chief Technology Officer, McKesson

Aaron Karczmer
Executive Vice-President and Head, Risk, Legal and Customer Operations, PayPal

Thibaut Kleiner
Director, Policy, Strategy and Outreach, DG Connect, European Commission

David Koh
Chief Executive and Chief, Cyber Security Agency of Singapore, Digital Security & Technology, Ministry of Communications and Information of Singapore

Helena Leurent
Director-General, Consumers International

Nuala O'Connor
Senior Vice-President, Chief Counsel, Digital Citizenship, Walmart

Vikram Rao
Chief Trust Officer, Salesforce

John Scimone
Senior Vice-President and Chief Security Officer, Dell Technologies

Digital Trust initiative working group

Justiin Ang
Director, Security and Resilience Division, Ministry of Communications and Information of Singapore

David Bartram-Shaw
Senior Vice-President, Global Head of Data Science, Edelman

Jenny Brinkley
Director, AWS Security, Amazon

Ravi Shankar Chaturvedi
Director and Founding Member, Digital Planet, The Fletcher School of Law and Diplomacy, Tufts University

Natasha Crampton
Chief Responsible AI Officer, Microsoft

Lecio DePaula
Vice-President, Data Protection, KnowBe4

Stuart Dobbie
Senior Vice-President, Innovation, Callsign

Shannon Donahue
Senior Vice-President, Content & Publishing, ISACA

Heather Evans
Senior Advisor, Office of Policy and Strategic Planning, US Department of Commerce

Nicolas Fischbach
Senior Director, Security & Privacy SRE, Google

Francisco Fraga
Senior Vice-President, Chief Information Officer, US Pharmaceuticals, McKesson

Vera Heitmann
Leader, Digital and Growth, Public Affairs, Ingka Group (IKEA)

Randy Herold
Chief Information Security Officer, ManpowerGroup

Joshua Jaffe
Vice-President, Cyber Security, Dell Technologies

Jamil Jaffer
Founder and Executive Director, National Security Institute, George Mason University

Jutta Juliane Meier
Founder and Chief Executive Officer, Identity Valley

Niniane Paeffgen
Managing Director, Swiss Digital Initiative

Jorge Pardo
International Trade Specialist, Office of Digital Services Industries

Jules Polonetsky
Chief Executive Officer, Future of Privacy Forum

Dan Rice
Vice-President, Digital Governance, Walmart

Trevor Rudolph
Vice-President, Global Digital Public Policy, Schneider Electric

Karen Silverman
Founder and Chief Executive Officer, The Cantellus Group

Mark Silverman
Adviser, International Committee of the Red Cross

Jacob Springer
Chief Privacy Officer, Abbott

Alissa Starzak
Head, Public Policy, Cloudflare

Courtney Stout
Chief Privacy Officer, Coca-Cola

Michael Thornberry
Senior Director, Apple

Jennifer Trotsko
Chief Data Privacy Officer, Business Risk and Compliance, International Finance Corporation

Paul Trueman
Senior Vice-President, Cyber and Intelligence Solutions, Mastercard

Charles Walton
Senior Vice-President, General Manager, Identity, Avast Software

Shahar Ziv
Vice-President, Global Resolutions, Identity, and Trust, PayPal

The Digital Trust initiative project team and wider digital trust community would also like to thank the following individuals for their contributions of time and insights to this effort: Mansur Abilkasimov (Schneider Electric), Deanna Draper (Dell Technologies), Paolo Dal Cin (Accenture), David Ferbrache (KPMG), Kai Hermsen, William Hoffman, Lydia Kostopoulos (KnowBe4), Chris McClean (Avanade), Jake Meek (PwC), Sridhar Sriram (Microsoft), Nicholas Zahn (Swiss Digital Initiative) and Denise Zheng (Accenture).

Endnotes

1. Hayat, Zia, "Digital trust: How to unleash the trillion-dollar opportunity for our global economy", *World Economic Forum*, 17 August 2022, https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.
2. Parviainen, Päivi, Maarit Tihinen, Jukka Kääriäinen and Susanna Teppola, "Tackling the digitalization challenge: How to benefit from digitalization in practice", *International Journal of Information Systems and Project Management*, vol. 5, no. 1, 2017, pp. 63-77, https://revistas.uminho.pt/index.php/ijispm/article/view/3856.
3. Richard Edelman, "2021 Trust Barometer: Trust in Technology", *Edelman*, 30 March 2021, https://www.edelman.com/trust/2021-trust-barometer/trust-technology; Public Affairs Council, *2021 Public Affairs, Pulse Survey Report*, 2021, https://pac.org/wp-content/uploads/Pulse_2021_Report.pdf; KPMG, *KPMG Cyber trust insights 2022: Building trust through cybersecurity and privacy*, 2022, https://home.kpmg/xx/en/home/insights/2022/09/cyber-trust-insights-2022.html.
4. "Why Digital Trust Truly Matters", *McKinsey*, 12 September 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters.
5. ISACA, *State of Digital Trust 2022*, 2022.
6. "Our 2030 Goals", Dell, n.d., https://www.dell.com/en-us/dt/corporate/social-impact/reporting/2030-goals.htm.
7. Burtescu, Emil, "Reliability and Security – Convergence or Divergence", *Informatica Economica*, vol. 14, no. 4, 2010, pp. 68; Jouini, Mouna, "Classification of Security Threats in Information Systems", *Procedia Computer Science,* vol. 32, 2014, 489-496, https://www.sciencedirect.com/science/article/pii/S1877050914006528.
8. "Edison Alliance", *Edison Alliance*, https://www.edisonalliance.org/home; "The first alliance to accelerate digital inclusion", *World Economic Forum*, 17 January 2022, https://www.weforum.org/impact/digital-inclusion/.
9. "Computer Security Resource Center", *National Institute of Standards and Technology (NIST)*, n.d., https://csrc.nist.gov/glossary/term/confidentiality_integrity_availability.
10. McKinsey & Company, *Cybersecurity in a Digital Era*, 2020, pp. 66, 109 and 132-138.
11. Regulatory expectations are well advanced around both security and reliability of services in many sectors, and thus require organizations to adopt relevant measures.
12. An example of this is the concept of security-by-design, which aims to include security considerations early on in the software development life cycle to minimize post-development costs for implementing security measures later on, at a time when the core components of the software have already been developed and additional changes mean higher costs.
13. Farson, Stuart and Reg Whitaker, "Accounting for the Future or the Past?: Developing Accountability and Oversight Systems to Meet Future Intelligence Needs", in *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, pp. 673-689, Oxford Handbooks, 2010, https://doi.org/10.1093/oxfordhb/9780195375886.003.0041.
14. World Economic Forum, *Measuring Stakeholder Capitalism*, 2020, https://www3.weforum.org/docs/WEF_IBC_Measuring_Stakeholder_Capitalism_Report_2020.pdf.
15. US Securities and Exchange Commission (SEC), *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, US Security and Exchange Commission Proposed Rulemaking*, 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
16. Rosenzweig, Paul, "Cybersecurity and the Least Cost Avoider", *Lawfare*, 5 November 2013, https://www.lawfareblog.com/cybersecurity-and-least-cost-avoider.
17. Chang, Felix, "To Build More-Inclusive Technology, Change Your Design Process", *Harvard Business Review,* 19 October 2020, https://hbr.org/2020/10/to-build-more-inclusive-technology-change-your-design-process; Veritas Consortium, *Veritas Document 3B: FEAT Ethics and Accountability Principles Assessment Methodology*, 2022, https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Veritas-Document-3B---FEAT-Ethics-and-Accountability-Principles-Assessment-Methodology.pdf; Hao, Karen, "Stop talking about AI ethics. It's time to talk about power", *MIT Technology Review*, 23 April 2021, https://www.technologyreview.com/2021/04/23/1023549/kate-crawford-atlas-of-ai-review/.
18. Chakravorti, Bhaskar, Ravi Shankar Chaturvedi, Christina Filipovic and Griffin Brewer, *Digital in the Time of COVID: Trust in the Digital Economy and Its Evolution Across 90 Economies as the Planet Paused for a Pandemic*, Digital Planet, 2020; Wiles, Jackie, "What's New in Artificial Intelligence from the 2022 Gartner Hype Cycle", *Gartner*, 15 September 2022, https://www.gartner.com/en/articles/what-s-new-in-artificial-intelligence-from-the-2022-gartner-hype-cycle.
19. G20 Global Smart Cities Alliance, *ICT Accessibility*, n.d., https://globalsmartcitiesalliance.org/?p=244.
20. Rigot, Afsaneh, *Design From the Margins*, Harvard Kennedy School Belfer Center for Science and International Affairs, 2022.
21. World Economic Forum, *Responsible Use of Technology: The Microsoft Case Study*, 2021.
22. Dobrygowski, Daniel and William Hoffman, "We Need to Build Up 'Digital Trust' in Tech", *Wired,* 28 May 2019, https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/.
23. The World Economic Forum's Centre for Cybersecurity leads the global response to address systemic cybersecurity challenges and improve digital trust through a leadership emphasis on cyber resilience, promoting global cooperation and assessing cyber risks from new technologies. For more information, see: "Centre for Cybersecurity", *World Economic Forum*, n.d., https://www.weforum.org/platforms/the-centre-for-cybersecurity.

24. "Cybersecurity", *Computer Security Resource Center, NIST*, n.d., https://csrc.nist.gov/glossary/term/cybersecurity.

25. Organizations have recognized this important link and have taken action to solidify their commitment to the relation of cybersecurity and digital trust; see for example: "Charter of Trust", *Charter of Trust*, n.d., https://www.charteroftrust.com/.

26. World Economic Forum, National Association of Corporate Directors, and Internet Security Alliance, *Principles for Board Governance of Cyber Risk*, 2021, https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk.

27. Thompson, Frauke Mattison, Sven Tuzovic and Corina Braun, "Trustmarks: Strategies for exploiting their full potential in e-commerce", *Business Horizons*, vol. 62, issue 2, 2019, pp. 237-247, https://doi.org/10.1016/j.bushor.2018.09.004. See also SSL/TLS Certificates (certificate provided by a certificate authority (e.g. Cloudflare) used to verify the transfer of encrypted data from an authentic website) and EU trust mark (assuring that the online transactions provided by a servicer are safe and secure insofar as they meet the requirements set forth by the EU in: The Eurpopean Parliament and the Council fo the European Union, *Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, 2014).

28. Regulatory requirements also need to be considered in this process, for example obligations to timely report breaches; in the US, e.g. "Health Breach Notification Rule", *Federal Trade Commission*, n.d., https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

29. The Forum's Partnership against Cybercrime initiative provides a platform for organizations to exchange views on and collectively tackle pressing cybersecurity issues such as the increase of cybercrime: "Partnership against Cybercrime", *World Economic Forum*, n.d., https://www.weforum.org/projects/partnership-against-cybercime.

30. Relevant cybersecurity standards include non-IT/cyber functions of organizations in their control frameworks, such as: NIST, Clean Skies for Tomorrow (CSF), Information Security Forum (ISF) Standard of Good Practice, International Organization for Standardization (ISO), Control Objectives for Information and Related Technologies (COBIT), etc.

31. World Economic Forum, *Advancing Digital Safety: A Framework to Align Global Action*, 2021, https://www3.weforum.org/docs/WEF_Advancing_Digital_Safety_A_Framework_to_Align_Global_Action_2021.pdf.

32. The World Economic Forum's Coalition on Digital Safety represents an important global effort to improve digital safety (and build trust) through public-private cooperation to tackle harmful content online and drive forward collaboration on programmes to enhance digital media literacy. For more information, see: "A Global Coalition for Digital Safety", *World Economic Forum*, n.d., https://initiatives.weforum.org/global-coalition-for-digital-safety/home. Where the digital world meets the physical, the Forum's Future of the Connected World platform works to strengthen global governance of internet of things and related technologies to maximize positive benefits and minimize harm. For more information, see" "Future of the Connected World, *World Economic Forum*, n.d., https://www.weforum.org/connectedworld/about.

33. "SG Cyber Safe Seniors Programme", *Cyber Security Agency of Singapore*, n.d., https://www.csa.gov.sg/Programmes/sg-cyber-safe-seniors/about.

34. Consumers International, *Consumers International Guidelines for Online Product Safety*, 2021; World Economic Forum, *State of the Connected World: 2020 Edition*, 2020; West, Tony, "Sharing to Build a Safer Industry", *Uber Newsroom*, 11 March 2021, https://www.uber.com/newsroom/industry-sharing-safety/; Information Commissioner's Office, *Age appropriate design: a code of practice for online services*, 2020.

35. Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, U.S. Department of Health, Education & Welfare, 1973; Zittrain, Jonathan, "The Hidden Costs of Automated Thinking," *The New Yorker*, 23 July 2019, https://www.newyorker.com/tech/annals-of-technology/the-hidden-costs-of-automated-thinking; Basl, John, Ronald Sandler and Steven Tiell, *Getting from Commitment to Content in AI and Data Ethics: Justice and Explainability*, Atlantic Council, 2021.

36. Pasquale, Frank, *The Black Box Society,* Harvard University Press, 2016; "Recommendations for the U.S. National Action Plan on Responsible Business Conduct in the Technology Sector", *Berkman Klein Center*, 24 August 2022, https://cyber.harvard.edu/story/2022-08/recommendations-us-national-action-plan-responsible-business-conduct-technology.

37. "Success is built on trust. Trust starts with transparency", *Salesforce*, https://trust.salesforce.com/en/.

38. "The Digital Trust Label", *The Swiss Digital Initiative*, n.d., https://www.swiss-digital-initiative.org/digital-trust-label/; "Cybersecurity Labelling Scheme", *Cyber Security Agency of Singapore*, https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls.

39. Soares, Delfina and Luis Amaral, "Reflections on the Concept of Interoperability in Information Systems", in *Proceedings of the 16th International Conference on Enterprise Information Systems (ICEIS-2014)*, vol. 3, SCITEPRESS, 2014, pp. 331-339; "ISO/IEC 17788: Information technology — Cloud computing — Overview and vocabulary", *International Organization for Standardization*, 2014, https://www.iso.org/standard/60544.html.

40. Federal Register, *Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers*, 2020, https://www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and.

41. NIST, *Privacy Framework*, 2020, https://www.nist.gov/privacy-framework/privacy-framework; CSA, *Cloud Controls Matrix and CAIQ v4*, 2021, https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/; World Economic Forum, *Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation*, 2020, https://www.weforum.org/reports/measuring-stakeholder-capitalism-towards-common-metrics-and-consistent-reporting-of-sustainable-value-creation; European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25: Data Protection by Design and by Default*, 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

42. CSA, *Cloud Controls Matrix and CAIQ v4*, 2021, https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/; World Economic Forum, *Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation*, 2020, https://www.weforum.org/reports/measuring-stakeholder-capitalism-towards-common-metrics-and-consistent-reporting-of-sustainable-value-creation; European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25: Data Protection by Design and by Default*, 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

43. Almeida, Fernando, José Oliveira and José Cruz, "Open Standards and Open Source: Enabling Interoperability", *International Journal of Software Engineering & Applications (IJSEA)*, vol. 2, no. 1, January 2011.

44. NIST, *Security and Privacy Controls for Information Systems and Organizations*, 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final; CSA, *Cloud Controls Matrix and CAIQ v4*, 2021, https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/; "Secure Controls Framework", *Secure Controls Framework (SCF)*, 2021, https://www.securecontrolsframework.com/secure-controls-framework.

45. Gross, Daniel P., "Collusive Investments in Technological Compatibility: Lessons from U.S. Railroads in the Late 19th Century", *Harvard Business School Working Paper*, no. 17-044, December 2016; Puffert, Douglas J., "The Standardization of Track Gauge on North American Railways, 1830-1890", *The Journal of Economic History*, vol. 60, no. 4, December 2000, pp. 933-960, https://www.jstor.org/stable/2698082.

46. Nelson, John E., "Scanning Silver's Celebration," in *Twenty-Five Years Behind Bars*, edited by Alan L. Haberman, 29, Cambridge: Harvard University Press, 2001.

47. Batista, Catia and Pedro C. Vicente, "Improving Access to Savings through Mobile Money: Experimental Evidence from African Smallholder Farmers", *World Development*, vol. 129, 2020; Suri, Tavneet and William Jack, "The long-run poverty and gender impacts of mobile money", *Science*, vol. 354, issue 6,317, 2016, pp. 1,288-1,292.

48. Johnson, Khari, "The Movement to Hold AI Accountable Gains Steam", *Wired*, 2 December 2021, https://www.wired.com/story/movement-hold-ai-accountable-gains-steam/.

49. "Sandvig v. Barr - First Amendment Challenge to Federal Computer Fraud and Abuse Act", *ACLU*, n.d., https://www.acludc.org/en/cases/sandvig-v-barr-first-amendment-challenge-federal-computer-fraud-and-abuse-act.

50. "Success is built on trust. Trust starts with transparency", *Salesforce*, n.d., https://trust.salesforce.com/en/.

51. Shell, Michelle A. and Ryan W. Buell, "Why Anxious Customers Prefer Human Customer Service", *Harvard Business Review*, 15 April 2019, https://hbr.org/2019/04/why-anxious-customers-prefer-human-customer-service; "How Salesforce is Helping Companies Break Through in Connected Customer Service", *Wired*, n.d., https://www.wired.com/sponsored/story/how-salesforce-is-helping-companies-break-through-in-connected-customer-service/.

52. The Forum provides relevant guidance for decision-makers: World Economic Forum , *Pathways to Digital Justice*, 2021, https://www3.weforum.org/docs/WEF_Pathways_to_Digital_Justice_2021.pdf.

53. World Economic Forum, *Pathways to Digital Justice*, 2021; Veritas Consortium, *Veritas Document 3A: FEAT Fairness Principles Assessment Methodology*, 2022; Basl, John, Ronald Sandler and Steven Tiell, *Getting from Commitment to Content in AI and Data Ethics: Justice and Explainability*, Atlantic Council, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/specifying-normative-content/.

54. Veritas Consortium, *Veritas Document 3A: FEAT Fairness Principles Assessment Methodology*, 2022.

55. Microsoft, *Responsible AI Standard, v2*, 2022.

56. The World Economic Forum's Platform on Data Policy supports privacy and other data-related aspects of digital trust through forward-looking, interoperable and trustworthy data policies. For more information, see: "Shaping the Future of Technology Governance: Data Policy", *World Economic Forum*, n.d., https://www.weforum.org/platforms/shaping-the-future-of-data-policy.

57. European Union, *General Data Protection Regulation (GDPR)*, 2016.

58. Solove, Daniel J., "A taxonomy of privacy", *University of Pennsylvania Law Review*, vol. 154, issue 3, 2006, pp. 447-560; Khanna, Ro and Amartya Sen, *Dignity in a Digital Age: Making Tech Work for All of Us*, Simon & Schuster, 2022; "Digital Citizenship: Ethical Use of Data & Responsible Use of Technology", *Walmart*, 28 February, 2022, https://corporate.walmart.com/esgreport/governance/digital-citizenship-ethical-use-of-data-responsible-use-of-technology.

59. Shaw, Thomas, *DPO Handbook: Data Protection Officers Under the GDPR, 2nd Edition*, International Association of Privacy Professionals, 2018.

60. European Union, *General Data Protection Regulation (GDPR)*, 2016.

61. PwC, "Is Yor Privacy Governance Ready for AI", *Harvard Business Review*, 18 March 2021, https://hbr.org/sponsored/2021/03/is-your-privacy-governance-ready-for-ai.

62. Hayward, Simon, "How modern leaders create winning cultures", *Accenture*, 24 August 2022, https://www.accenture.com/us-en/blogs/business-functions-blog/how-modern-leaders-create-winning-cultures.

63. The World Economic Forum's Platform on Blockchain and Digital Assets promotes digital trust in blockchain and distributed ledger technologies through equity, interoperability and transparency. For more information, see: "Shaping the Future of Technology Governance: Blockchain and Digital Assets, n.d., https://www.weforum.org/platforms/shaping-the-future-of-blockchain-and-digital-assets.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org