

Digital Trust – An Opportunity

Digital Trust Workshop, Huawei, Brussels, 21st June 2024

A Briefing Paper

Produced by

Dr Rob Wortham, Global Digital Foundation

Contents

Introduction	3
Topics for Discussion	4
Trust begins with the Individual	5
Social Trust and Performance Trust	6
Trust and Risk Perception	7
Trust as a Corporate Tool	7
Practical Approaches for Trust Building	8

Introduction

This briefing paper has been prepared in advance of the Digital Trust Workshop, an invitation only event taking place on Friday 21st June 2024. The Workshop forms part of the second Cyber Security Week hosted at Huawei's Brussels Cyber Security Transparency Center. The workshop builds on a previous event held in on 11th December 2023. The [outcome report for that event](#) is available from the Global Digital Foundation web site.

Digital trust, at its core, refers to the confidence and assurance that users place in the reliability, security, and integrity of digital systems, services, and transactions. It encompasses the belief that the digital entities involved will perform as expected, without compromising privacy, confidentiality, or data integrity. Various definitions exist, reflecting the multidimensional nature of digital trust. One commonly accepted definition is the reliance on information systems and technologies that consistently operate as intended, securely handling sensitive data and maintaining user privacy.

Trust, in a broader context, is a fundamental element of human interaction, influencing relationships, decision-making, and societal structures. While digital trust focuses on the online dimension, the foundations of trust are deeply rooted in human psychology and social dynamics. Trust involves the willingness to be vulnerable based on the expectation that others will act in a reliable and responsible manner.

In the global landscape, the significance of trust has been acknowledged in international standards, where trust is often defined as a verifiable expectation. This emphasises the importance of establishing not only subjective confidence but also the capability to verify and validate the factors contributing to that confidence. In the digital domain, this translates to the ability to assess the reliability and security of systems through tangible evidence and transparent practices.

The following sections identify the key topics for consideration, and then explore current research relevant to Digital Trust.

Topics for Discussion

During the Digital Trust Workshop, participants will be invited to discuss the following topics. This paper aims to provide relevant background information.

Topic	Comments
<i>Strategic Importance of Digital Trust</i>	For a commercial organisation, trust is strategically important. Understanding the drivers of trust are fundamental for growth and success.
<i>Identification of Market Barriers</i>	Particularly non-technological barriers, such as cultural differences, local regulations and geopolitical tensions.
<i>Digital Trust vs. Digital Confidence</i>	Alternatively this may be characterised as Social Trust vs. Performance Trust, see section below.
<i>Dynamics of Trust Relationships</i>	How do we build, break and work to restore trust relationships?
<i>Learning from Practice</i>	Examples of Digital Trust best practice. Relevant insights from other domains.

As we explore digital trust, examining the factors influencing trust in the digital realm, we must recognise the geopolitical realities of establishing trust in an increasingly polarised world. At the same time, we must also recognise that trust begins with individuals. Research into the psychological mechanisms of trust provides a useful starting place for our understanding of this crucial topic, and is covered in the following sections.

“Trust should not be seen as a word with a stable reference but as an organising tool for human relations, used in a reasoning context where we wish to justify or challenge behaviour .”

Hugo Grotius¹, 1583–1645

Trust begins with the Individual

Whilst we like to think about reasons that explain behaviour, it is often (perhaps generally) the case that reasons follow post-facto to justify behaviours. Trust, or its inverse - distrust, is one of those words that is often used in such post-facto explanations. We similarly like to partition our behaviours into those that follow from analytic thinking ('left brain') and from emotional responses ('right brain'). Again, this separation of left and right brain is an oversimplification of the biology², but at least points towards the truth of the matter. Human behaviour is the result of complex interplay between emotional states and analytic reasoned decision making. Following on from his ubiquitous 'system 1/system 2' characterisation of decision making³, Daniel Kahneman has subsequently been investigating what he terms 'noise' in human decision making.

The results of Kahneman's studies make for alarming reading⁴. For example, insurance underwriters, expected by their employers to demonstrate uniformity of decision making within a 10% boundary, in fact varied by around 50% in their decision making. Most concerning is the fact that the organisation in question had no awareness of this individual variability, and thus were doing nothing to improve it. Given that these underwriting decisions are informed by detailed organisational

¹ *Hugo Grotius (1583–1645)* - a towering figure in philosophy, political theory, law and associated fields during the seventeenth century and for hundreds of years afterwards. Quote: [The Cambridge Companion to Hugo Grotius](#), Lesaffer, R. and Nijman, J., Cambridge University Press, 2021

² [Left Brain, Right Brain: Facts and Fantasies](#), Corballis, M., PLoS Biology, 2014

³ [Thinking, fast and slow](#), Kahneman, D., Penguin Books, 2012

⁴ [Try to design an approach to making a judgment; don't just go into it trusting your intuition](#), Kahneman, D. and Frueh, S., Issues in Science and Technology, Volume XXXVIII Issue 3, Arizona State University, 2022

policy, combined with specific case data, one can only conclude that the variability must be related to some combination of variation in analytical ability, emotional state, and pre-existing biases. When it comes to commercial decisions involving ‘trust’, how much more must emotional state and bias play a role?

Social Trust and Performance Trust

Proposed by Earle, Siegrist and Gutscher in 2007, the **Trust, Confidence and Cooperation (TCC) Model** unifies a wide variety of trust research by showing how the key forms of trust and confidence interact. The TCC model theorises that (perceived) moral value similarity drives social trust, whilst evidence such as past performance drives confidence (trust in competence). It is then the combination of social trust and confidence that results in cooperative (i.e trusting) behaviour. Critically, it is the distinction between information that has moral implications versus information that has only performance implications, which is central to understanding trust. The subsequent paper by Harvey and Twyman⁵ provides a useful diagrammatic model, shown in Figure 1 below.

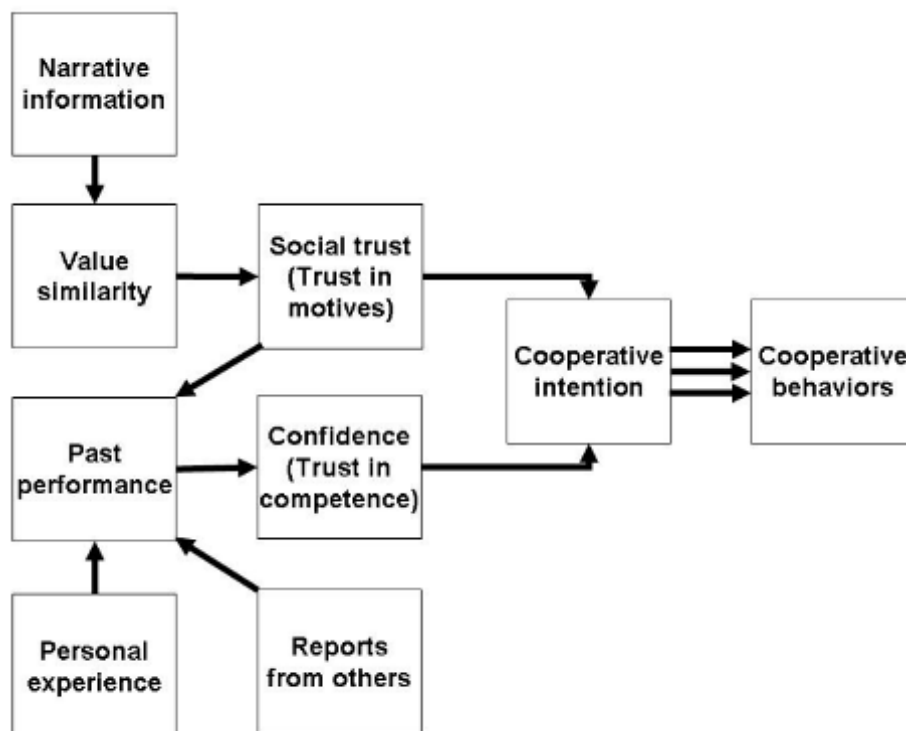


Figure 1 – A representation of the TCC model. Reproduced from Harvey and Twyman, 2007

⁵ [Two-route models of trust in sources of risk communication](#), Harvey, N. and Twyman, M., UCL, 2007

Importantly, this model also provides evidence for an **asymmetric influence relationship** between social trust and perception of past performance. A lack of social trust causes discounting of factual information, whilst the presence of factual information cannot reciprocally encourage trust. If you don't trust the messenger, you don't trust the message. For example, even if a system is certified as meeting some international standard, that certification will be heavily discounted in value if the system provider is not socially trusted; due to perceived misalignment of moral values.

Trust and Risk Perception

Paul Slovic, widely recognised as the founder of risk perception research, was the one of the first researchers to examine the nature of trust and the significance of the relation between trust and the perception of risk. Slovic pointed out that **high public concern about a risk issue** (for example, nuclear power) is **associated with distrust of the managers** responsible for that issue; low public concern (as in the case, for example, of medical uses of radiation) is associated with trust in risk managers⁶. Set in a contemporary context, we see how once the public is concerned about the increasing capabilities of AI, there arises a demand to obtain risk assurances from foundational model providers⁷. Within a commercial supplier/user relationship, when the user expresses confidence in a supplier by relying on them, they expose themselves to the dangers that they expect the supplier to control. We expect our cybersecurity supplier to protect us from cyber-attack, we expect our AI supplier to protect us from bias and erroneous decision making.

Confidence is backward looking: since it is based on familiarity (trust in competence), and we can only be familiar with what has passed, confidence is a force for stasis, for the perpetuation of things as they are. In contrast, **social trust** in its general form can be **forward looking and creative**. Social trust is based on similarity. Trust can be a force for change, a powerful problem-solving tool.

Trust as a Corporate Tool

Trust acts as a 'social glue', holding business relationships together. Business partners that trust each other spend less time and energy defending themselves from being exploited, and both sides achieve greater financial results in negotiations.

⁶ [Perceived Risk, Trust, and Democracy](#), Slovic P., Risk Analysis 13 no. 6, 1993

⁷ [Company Policies](#), UK Government AI Safety Summit, London, Autumn 2023

When your employees know they are trusted and that they are free to express themselves clearly, trust becomes vital in business. They will almost certainly be more driven to be productive and work to their best potential⁸.

Practical Approaches for Trust Building

Previous discussions of digital trust identify several practical approaches⁹. As a first step towards increasing digital trust, we can help people **reduce perceived risks**. We might work towards this goal by working with trusted third parties – especially scientists, academics and think tanks. Indeed, though trust may be about choice and allegiance, **trustworthiness** (verifiable expectation) is verifiable at three levels: Policy, Conformity to regulations, and Standards Compliance. For example the processes of Standards Authentication require many interactions which can build reputation. **Partnership**, particularly with mutually trusted third parties such as standards bodies, university institutes and think tanks can, over time, change the public narrative about who can be trusted.

It is important to recognise that **consumer uptake** is important, even for unrelated business to business commercial transactions. The perception that the ‘layman’ trusts a technology supplier is important. After all, we are all consumers. Public opinion is also influenced by the **alignment or disagreement between businesses and governments on specific issues**. Trust tends to decline when conflicts arise, but it increases significantly when the two entities share the same perspective. It is therefore worthwhile to seek to build consensus with government around the appropriate extent and application of trustworthy digital technologies.

All business interactions involve some element of risk. The benefits of any digital technology deployment must always be weighed against the potential risks. In many cases solid **commercial benefits outweigh perceived theoretical risks**, presenting an opportunity for business benefit whilst managing theoretical risk perception.

⁸ [*Exploring the Relationship Between Corporate Social Responsibility, Trust, Corporate Reputation, and Brand Equity*](#), Zhao, Y., Abbas, M., Samma, M., Ozkut, T. et al, Frontiers in Psychology, 2021

⁹ [*Digital Trust – Strategies for Europe: Outcome Report of the Brussels Digital Trust Workshop*](#), Wortham, R.H., December 2023