Swiss Re Institute

May 2022

Decoding digital trust

An insurance perspective

Content

Key takeaways

Decoding the determinants of digital trust

1. **The concept of trust – and digital trust – is mutable. Be ready to adapt.**
   There is no magic formula to creating digital trust. Bonds of trust vary between countries and between social groups within countries. Be aware who your product/service is targeting and be ready to adapt to specific and local circumstance.

2. **The role of trust fulfils different functions at an individual level.**
   Trust begins at a level of functionality – does a service or product do what it says it will while making my life easier? It then moves to a level of security – are my purchases, investments or assets safe with this counterparty? And finally, it demands reassurance – am I doing the right thing? This provides a framework to best think about evaluating digital trust.

3. **Digital trust does not happen in one place. It happens along the value chain.**
   Trust comes at many points on the digital journey, no more so than with insurance. It can involve product design; sales and distribution; underwriting, pricing and risk assessment; and claims. The more these functions talk to each other, the greater the levels of trust they can build.

4. **The relationship between guidelines, principles, pledges, legislation and trust is not linear.**
   Consumers may be reassured to some degree by legal and ethical frameworks but do not want to read all the small print. Highly dependent on local conditions, digital trust will not, past a certain point, necessarily increase by adding further levels of rule-based protocol.

5. **The benefits of digital trust may not always be easily visible – but losing digital trust can be devastating.**
   The cost of a loss of digital trust and digital misinformation, in fields from climate change to health and from political stability to brand value, can be huge. Once that trust is lost, it is very difficult to rebuild.

6. **Digital technologies may bolster the trust quotient in insurance.**
   Trust between insurers and customers is not always easily realised – customers are worried about opacity, of claims being denied, or being penalised for submitting claims. Ultimately, insurance is a promise to compensate policyholders for losses arising from specific eventualities. Payment of claims, supported by trust and transparency, are at the heart of this promise. Technologies such as blockchain can improve trust and transparency.

7. **Humans remain a part of the digital trust pyramid.**
   Digital technologies can do many, many tasks with much greater reach and efficiency than humans. However, the role of humans in complementing technology in building trust will remain valuable.

8. **Insurers can be conduits of digital trust.**
   Insurance already helps build trust in societal sectors from road traffic to health and from natural catastrophes to supply chain management. It is making its first steps into digital trust, most notably with cyber security products. There could be other lines where insurers might have an impact.

Foreword

A matter of trust

Christoph Nabholz
Chief Research Officer
Swiss Re Institute

As a re/insurer, we like to think we know a bit about trust. When you buy an insurance policy, you receive nothing but a promise. A promise that we will provide you financial recompense if a clearly defined event should happen in the future. Those clearly defined events frequently occur at times of high stress and emotion – a health condition, a theft, a car accident, severe weather damage or even death. Our customers rely on us – trust us – to keep to our promises.

However, trust is not an easily isolated phenomenon. It is many things to many people. Economists see it as mutual self-interest. Anthropologists and biologists view it as a highly effective evolutionary tactic. Philosophers approach it from many angles: we can maintain trust through fear of what might happen if we break the bonds of that trust; or from love, that my good nature will engender the better side of others and so create a better community.

While whole books have been written on the subject of trust, we have neither the luxury of time nor space to rehearse those theories here. For the purposes of this document, then, we shall rely on three concepts that occur repeatedly in the literature. The first is reliability. This is mechanistic. Will a person or a thing do what we expect them to do rationally? Is it easy to use or comprehend? The second is security and a sense of safety. Will my side of the bargain – my money, my data – be protected and used in acceptable ways? The third is reassurance. It seeks affirmation in the face of uncertainty, both rational and emotional. Have I done the right thing?

And so, to digital. Most likely, all of those reading this paper will have begun their digital journey long ago. They work, shop, play and socialise online. A high level of trust in digital devices already exists. However, most in this audience are also aware that their digital journey is far from over. The way we use digital today will not be the same as the next generation. Tech innovations will change the way we manage our health, our mobility, our property and possessions, our work and much more. There are many digital frontiers still to cross. We still need to build and develop digital trust.

In this document we have created a framework through which to understand digital trust. It builds on the concepts of reliability, security and reassurance, examining how these could break down and be relevant against the backdrop of increasing digital automation, both in insurance and in other industries. Ultimately, we pose the question: Is there a natural barrier to our digital trust?

This paper made me stop more than once to consider how trust makes me think about the digitalisation of the insurance industry. I hope it does the same for you.

Introduction

Constructing the digital trust pyramid

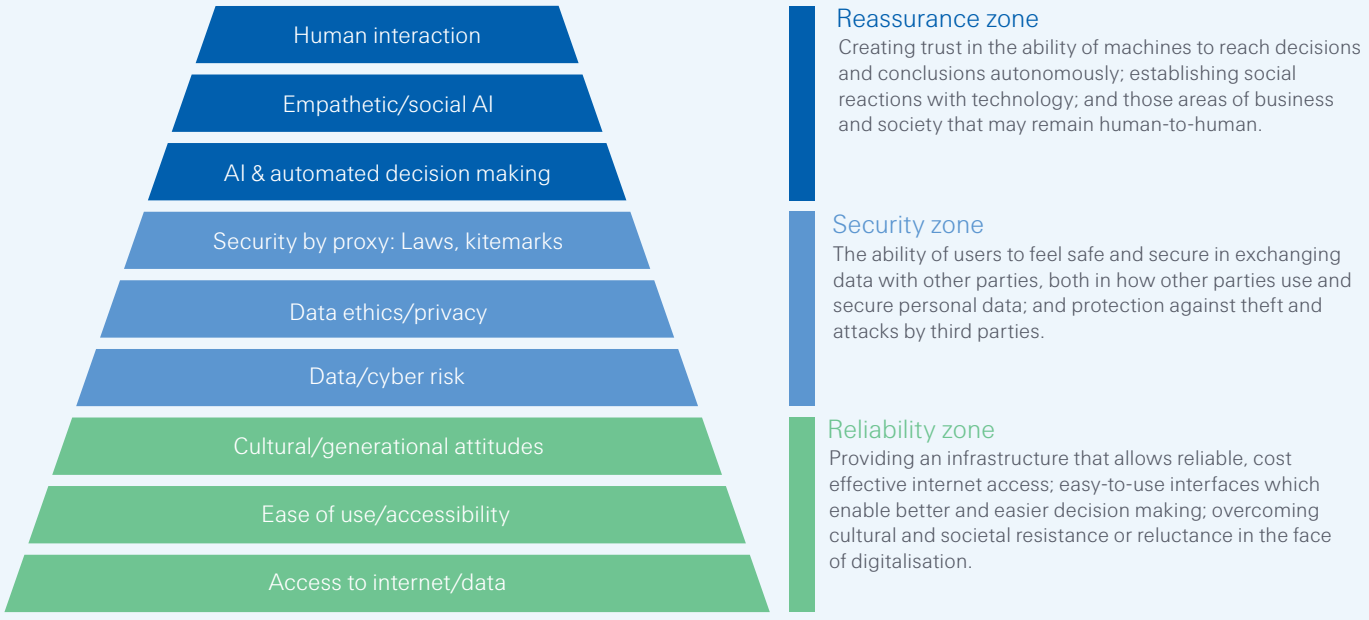
The concept of digital trust is amorphous and subjective. We have developed a nine-step methodology as a means of better understanding the concept and as a lens through which to approach digital trust.

There is no single data point that can define digital trust. It is not a commodity to be bought, not an asset that can be traded, not a risk that can be underwritten. If trust has a value, then it is in the perceived strength of the relationship between the individual, business or institution and the party with which it seeks to interact. The notion of trust is, to a large extent, subjective and mutable, making it difficult to measure.

Just because digital trust defies a simple variable or interaction, it does not mean that it is a quality we should ignore. For an insurer, the march towards digital can be transformative across the business. It provides a point of interaction with clients; it can automate practically all processes across the insurance customer journey; and it can enhance understanding of our portfolios and can optimise how we cover risk. Underpinning these processes of digitalisation is trust: trust from our employees, trust from our regulators, our stakeholders, our shareholders and most importantly, our customers.

We thus need a means of conceptualising and understanding what trust means in a digital context. One method of doing this is the digital trust pyramid.

Figure 1:
Digital trust pyramid



Source: Swiss Re Institute

This pyramid is constructed of nine building blocks within three zones. The first of these zones – **reliability** – is largely mechanistic. It seeks to understand the physical and mental constraints of digital trust. No one can or will establish digital relationships if they do not have consistent and reliable data and internet access. This is not a given across the world. Access to the internet will only be advantageous if it allows the user access to services they could not otherwise receive; or easier, more convenient access to goods and services they could get elsewhere. In essence, the question is one of ease and, specifically, how easy it is to use your digital portal, at least, on the supply side. The demand side also plays a role. We ask if there are cultural, age or other societal factors at play that influence our willingness to trust the digital interface. As people process information differently, intrinsic factors come into play that influence individual levels of trust: Does a digital interface allow individuals to make informed decisions based on the available information?

Our second zone is that of **security**. We assume that access, ability and willingness are already there for a digital relationship to blossom. But how do companies maintain that trust as the relationship develops? Our starting point is security and the forceable intrusion of third parties – cyber risk in its many forms, from identity theft to blackmail, from data hijacking to digital larceny. With security from attack assured, clients and customers will focus on fresh concerns: they do not want their digital trust abused; their data used without consent; or the storage of data outside of contractual obligation. We discuss the role of legislation in forming trust and whether companies should create their own standards for consumers.

Lastly, we reach the **zone of reassurance**. The future is inherently uncertain. We have to make decisions today that will affect us tomorrow. Will we let technology – in the form of artificial intelligence – make these decisions for us? Either immediate decisions – the automation of processes such as driving – or decision points affecting longer-term outcomes. Do we trust technology to do the right thing, both emotionally and rationally, and to avoid the pitfalls of algorithmic bias – or are there areas of our lives where we will continue to seek human reassurance? Put another way, will humans ultimately complement and contribute to our trust in digital?

In each of these sections, insurers are in a position to influence the mechanics of digital trust. As discussed in a previous Swiss Re Institute publication, insurers can use the three 'E's to shape the digital pyramid in a way which supports their value proposition:[1]

- Empowerment: Insurers should empower their customers by enabling them to access relevant information to make informed decisions. This way insurers can establish a relationship based on trust.
- Engagement: Better insights into customers' interests and experiences – with their permission – help companies to design and offer solutions that will be more appreciated and valued.
- Emotional connection: This should result from a combination of companies' ethical and social responsibilities: the way they treat their employees and customers, the causes they champion, and the value they place on the relationship-building experience.

Ticking the box across the zones and their elements lays the foundations of digital trust.

[1] *Why insurers need to transform digital distribution and how to do it in the digital age*, Swiss Re Institute, September 2020.

Reliability
Access to data/access to the internet

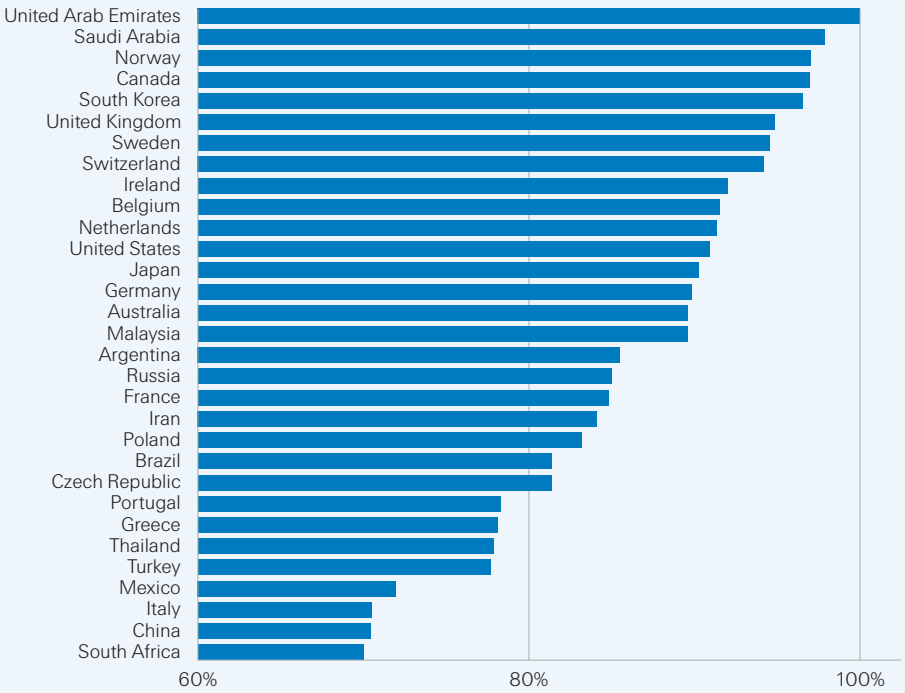
Key takeaway: Do not take available, affordable and uncensored data and internet access as a given. Moreover, freely available internet access may not easily correlate with trust.

Internet penetration

It may be an obvious point, but a point that nonetheless needs to be made: You cannot build a digital relationship with someone who doesn't have digital. The International Telecommunication Union (ITU) estimates that 4.9 billion people had access to the internet in 2021, a huge number, but only 63% of the total global population. Around 2.9 billion do not have access.[2] In terms of geographic breakdown, the range runs from 6.5% of the population in South Sudan (2020) having internet access to 100% in the United Arab Emirates.

One might expect internet penetration to be closely correlated with both wealth and economic development and up to a certain point, this appears to be the case. Developing economies typically have lower internet penetration rates – only one sub-Saharan African state, for example, reaches 70% internet penetration. But at a certain point of income, the relationship becomes weaker. Iran, Morocco and Azerbaijan all achieve around 85% internet penetration with relatively modest GDPs per capita. This is around the same level as France, with GDP per capita just short of USD 40,000 in 2020. Around one in ten people in the US, Japan and Germany do not have access to the internet. In Italy, a G7 economy, internet penetration is only a little over 70%.[3]

Figure 2:
Internet penetration, selected states, % 2020



Source: ITU

[2] All statistics, *International Telecommunication Union (ITU)*.
[3] As was highlighted in the Covid19 pandemic. Investments are now underway to correct such underperformance. See A. Perrone, "Italy's bad internet connection: Italians have one of the lowest levels of digital skills in Europe and are struggling to understand implications of the new pandemic world", Index on Censorship, June 2020.

Internet availability and reliability

Access to the internet is not a given. It is dependent on fixed and mobile infrastructure as well as the costs of accessing data, both factors which will influence the number of users and amount of internet usage. The Inclusive Internet Index of the Economist Intelligence Unit provides an extensive scoring methodology for selected countries, based on both the supply and demand sides.[4] In terms of affordability, Canada sits at the top of the 2020 rankings, followed by the UK, France and Italy, suggesting that cost is not a factor in the relatively low internet penetration of the latter two states. Availability, however, is another matter, with France ranking just 19th, and Italy, 36th. Meanwhile, Germany places 20th, Japan 17th, the UK 16th and the US 12th. Smaller developed economies including Singapore, Hong Kong, South Korea, Switzerland and Denmark dominate the top of the availability rankings.

Internet freedom

Quality of access to the internet can be as important as quantity. Freedom House describes China's right to internet access as "profoundly oppressive".[5] The government controls international internet gateways (the Great Firewall of China), through which all internet providers must operate. The New York Times, the BBC and Reuters are among the international websites banned in China, alongside a plethora of Chinese diaspora sites. All major Western social media sites are banned, as is Wikipedia and Reddit. Other states with low scores on the Freedom House internet freedom ranking include Russia, Saudi Arabia, Turkey, Thailand and Egypt. India is in the category of partially free, citing "frequent internet shutdowns" and controversial new data protection legislation. Iraq, South Korea, Indonesia, Brazil and Mexico are all accorded partially free status by Freedom House. States with free internet access are listed by Freedom House as including Japan, South Africa, the UK, Germany, the US and Argentina.

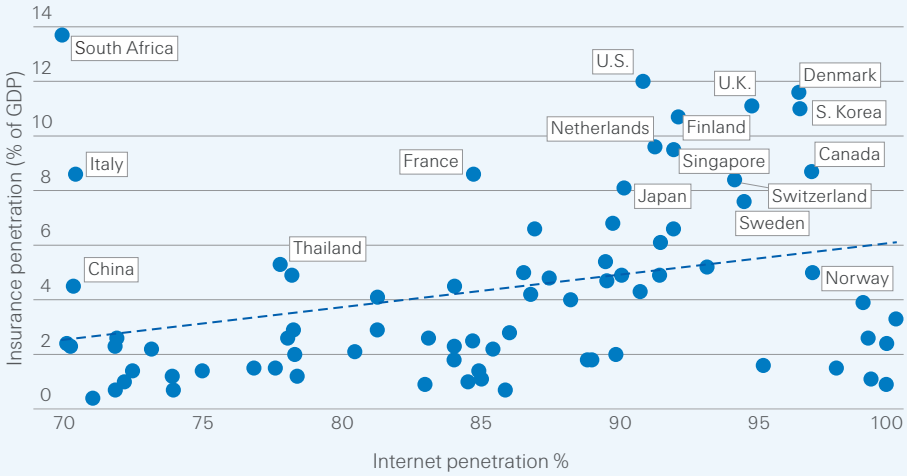
Box 1: Internet shutdowns

Authoritarian regimes can be quick to cut internet access in periods of political stress. China enforced a 10-month internet blackout in Xinjiang in 2009 following unrest. The Egyptian regime turned off the internet for a week at the height of the Arab Spring in 2011. In 2020, Access Now reported 155 internet shutdowns in 29 countries, the most frequent transgressor being India, with Myanmar shutting down internet access in Rakhine and Chin states for nineteen months.

Insurance and internet penetration

Should this trouble industry sectors such as insurance? At one level, probably not that much. The majority of insured populations in developed and emerging economies have access to the internet. There is a positive correlation between internet and insurance penetration, but it is not particularly strong, at least not at the upper levels, with a number of outliers.

Figure 3:
Insurance & Internet penetration, selected countries, 2020



Source: ITU and Swiss Re Institute

[4] *The Inclusive Internet Index*, The Economist, 2021.
[5] *"Karshare Release Karmate App, Using The Floow's FloowDrive Solution, as Part of Pioneering Project to Help Mobilise COVID-19 Workers"*, The Floow, 15 April 2020.

Nonetheless, there are take-outs that insurers should consider:

- Even in some developed economies, there are, at least in absolute numbers, still large populations not using the internet, including 30 million US citizens.
- There are some states – Italy and South Africa most obviously, but France and Japan to a lesser extent – where insurance penetration is relatively high, despite significant numbers not having internet access.
- Freedom of access to the internet – which does include issues of trust – does not always extend to commerce. At USD 2.8 trillion in ecommerce sales in 2021, China is worth over three times the next largest ecommerce market (the US, at USD 840 billion).[6] Trust in the commercial value of the internet in China is clearly not affected by the tight government control of digital channels.

Box 2: Access to data and digital can mutually benefit insurers and customers

Floow is a telematics provider that transmits driver risk data directly from a policyholder's vehicle to their motor insurer.[7] During the COVID-19 pandemic, many frontline workers had difficulty in commuting due to the shutdown of public transportation systems. A UK-based car sharing company Car & Away had car owners willing to donate their cars but wanted reassurance that their vehicles were in safe hands. Floow designed an app to monitor driving behaviour to bridge this trust deficit between car owners and users. Car users were happy to share this data as a good trust score meant credibility. This is one example of how access to digital and data can result in trust to conduct a transaction between unknown parties.

[6] *E-commerce sales by country in 2021*, Emarketeer, 2021
[7] *https://www.thefloow.com/*.

Reliability
Ease of use

Key takeaway: Digital design and customer experience are important factors in building consumer trust. Test, refine, test again and repeat to create an attractive, accessible and easy-to-use platform to develop digital trust.

Digital design, led by behavioural science, can engender trust and nudge users to make more informed choices. Research shows that carefully designed digital front ends are crucial in shaping positive financial behaviour, including increasing the propensity to save. One example includes a study by the Universities of Pennsylvania and London, together with a financial services provider, which showed that changes in the wording of online retirement savings plans can have a major impact on the rate of enrolment. Notably, the wording option "I do not want to save" elicited fewer rejections of a proposed retirement plan than "I do not want to enrol".[8]

It is not just language. Studies indicate that multisensory factors such as visual aesthetics and sound effects can also play a role in implicitly driving digital trust. For the banking and insurance industries specifically, research reveals that certain colours (dull hues of white and blue), shapes (symmetrical, angular or circular) and sound features (low pitch and low volume) are associated with higher degrees of digital trust.[9]

Digital platforms are becoming increasingly important in the insurance journey, in many cases complementing or even replacing the traditional agent-driven model. Being persuaded to buy insurance digitally is one thing; making sure individuals have sufficient information to judge coverage needs appropriately is another. A rich digital user interface and high-speed digital interaction may initially impress consumers but accelerated purchase journeys also risk individuals not fully understanding what they are buying and what they are covered for. This protection gap may reveal itself only downstream when claims are filed.

It is important to balance sharing relevant information with the need to simplify the purchase journey. Previous research from Swiss Re Institute shows that behavioural design plays an important role in finding the balance between how much information insurers want to extract versus how much consumers are comfortable to disclose. However, digital platforms must be designed with ethical rigor in order to ensure that products benefit both companies and consumers alike.[10] Research clearly shows that the key to strengthening trust between insurers and policyholders lies not in asking more and more questions but in asking relevant ones. Insurers must avoid extremes – one study suggested that a university-level education would be required to properly understand policy terms and conditions.[11]

Finally, digital design that is layered with empathy is crucial at claims settlement, particularly if there are disputes.[12] Claims made digitally (or otherwise) are often emotionally charged interactions. This makes digital trust paramount. The digital platform must prove trustworthy not only at the point of purchase – but also later in the journey, such as when delivering unexpected or unpleasant news.[13] Digital trust between insurers and policyholders for claims can also be strengthened by designing simplified parametric solutions. For example, Swiss Re has designed an easy-to-use platform for real-time, trigger-driven, pre-determined pay-outs in the event of flight delays.[14]

Box 3: Digital design to improve accessibility and aid decision making in online insurance

The sheer amount of online information may overload online insurance customers. Typical decision biases can be magnified when online. Understanding this behaviour is critical to digital success. For a customer, an instant aesthetic perception of a website can carry more importance than the actual usability of the site. While many hesitate to look at insurance plans online due to their perceived opacity, use of behavioural science in trials has yielded positive results. Changes in digital design have resulted in higher email click rates, improvement in straight through processing of electronic underwriting, and higher online sales due to a clarified decision-making process. Aside from behavioural variances in the ways individuals absorb information, an online environment also makes a difference in how they provide information. Internal Swiss Re research indicates that people tend to reveal more sensitive information, such as health problems, drug use, medical symptoms and negative behaviours, via computer surveys rather than when answering to another human being.

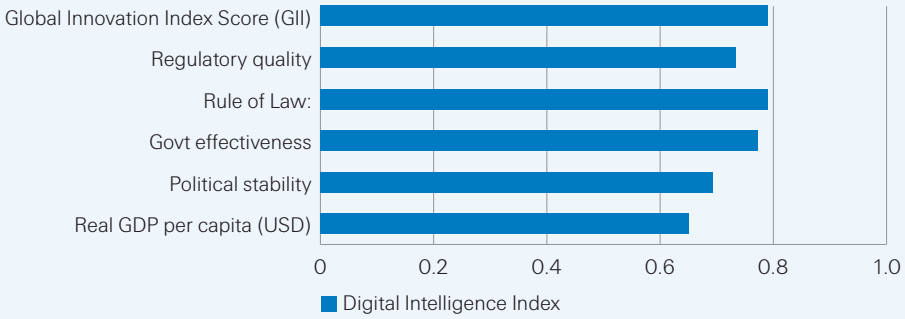
[8] S. Benartzi and S. Bhargava, "How Digital design drives user behavior", Harvard Business Review, February 2020.
[9] *Enhancing digital trust in banking and insurance*, Asian Institute of Finance, 2017.
[10] *To BE or not to BE*, Swiss Re Institute, November 2021
[11] Ibid.
[12] *Technology and insurance: themes and challenges*, Swiss Re Institute, June 2017.
[13] J. Hageman, "The Empathetic Bot", Lemonade.com, https://www.lemonade.com/blog/the-empathetic-bot/
[14] *Real-time flight delay insurance*, Swiss Re.

Reliability
Cultural / generational attitudes

Key takeaway: Digital trust is influenced by our surroundings and circumstances – it typically correlates with wealth and political stability, but some countries are exceptions to the rule.

Societies may have certain inherent characteristics that either fuel or inhibit digital trust. These could be linked to political structures, socio-economic factors, cultural identities or other values. Swiss Re Institute analysis (Figure 4) reveals that countries with higher levels of digital trust usually exhibit one or more of the following cultural characteristics: they tend to have more innovative populations, enjoy higher incomes, and exhibit better governance.

Figure 4:
Greater internet openness and digital trust have positive externalities for trade, innovation and entrepreneurship, macroeconomic performance, and social wellbeing.[15]



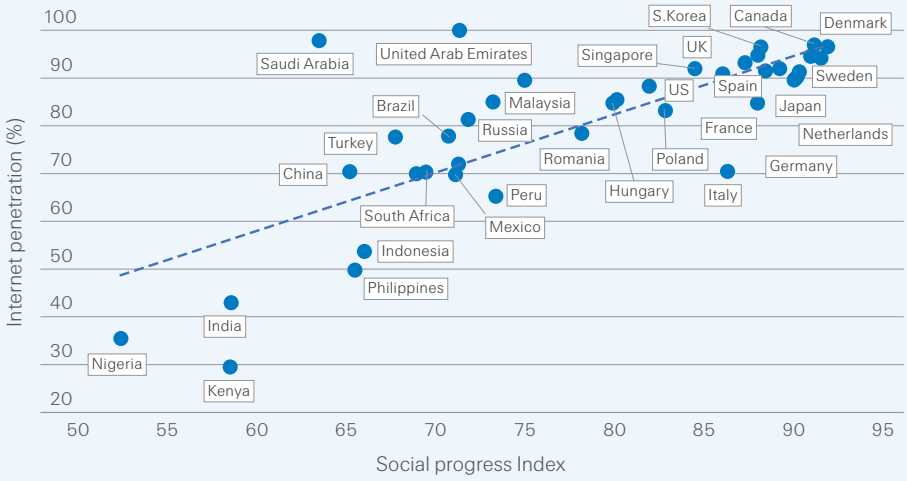
Source: Swiss Re Institute (SRI), Tufts University, World Bank, and Global Innovation Index (GII)

Note: We use the Digital Intelligence Index (DII) constructed by Tufts University as a proxy of digital trust levels across countries. DII is measured as an interplay between trust givers (citizens and consumers, exhibited through the pillars of attitude and behaviour) and trust guarantors (businesses and institutions, exhibited through the pillars of environment and experience).[16]

Countries that have made greater strides socially are usually willing to trust the digital space more. Using the Digital Intelligence Index (DII) published by the Tufts University and the Social Progress Index 2021, we find that there is a moderately high degree of correlation between the two indices (0.61).[17,18] Social progress is also positively associated with the degree of internet penetration (correlation coefficient of 0.88) – countries with a high degree of social progress have a greater internet penetration. Figure 5 highlights this association. Some outliers (such as Italy) highlight our earlier point that digital access and trust do not track against any single variable. Progress on social issues does not automatically accompany economic development. While the Nordic countries are some of the best performers in the SPI, countries like Fiji, Sri Lanka and the United Arab Emirates have recorded the most significant progress in the last ten years.[19]

[15] "Economic and Social Benefits of Internet Openness", OECD Digital Economy Papers, 2016.
[16] Each of these four pillars are individually scored across countries and their average represents the Digital Intelligence Index for the respective countries. For more, see *Digital Intelligence Index*, Tufts University, 2019.
[17] *Digital in the time of COVID*, Tufts University, 2019.
[18] The Social Progress Index (SPI) takes into consideration 53 social and environmental indicators across three themes – basic human needs, foundations of wellbeing, and opportunity to measure progress of nations on the quality of lives of their citizens. See *Global Index: Overview*, socialprogress.org, 2021.
[19] *2021 Social Progress Index*, Social Progress Imperative, 2021.

Figure 5:
Greater internet openness and digital trust have positive externalities for trade, innovation and entrepreneurship, macroeconomic performance, and social wellbeing.



Source: Swiss Re Institute (SRI), ITU, and Social Progress Imperative

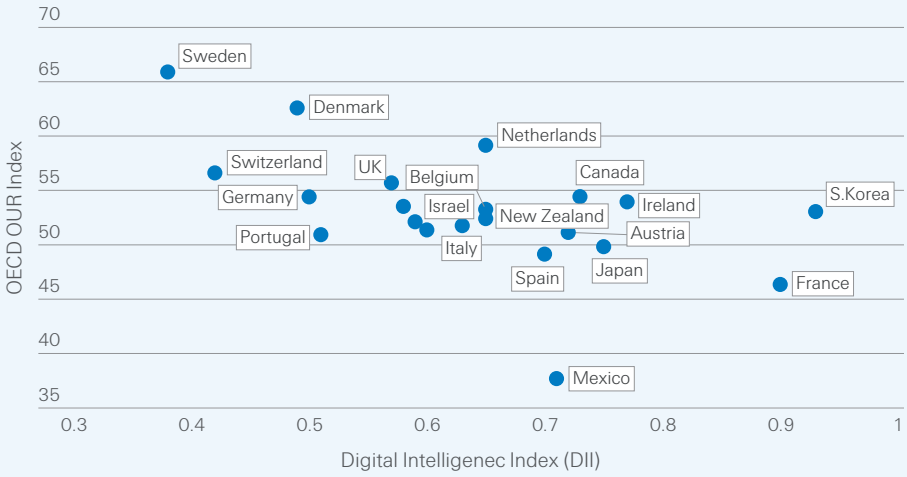
Cultural and generational attitudes are also an important determinant of how citizens choose to interact with local and national governments. With changes in demographic patterns, urbanisation and technological advances, there is a marked shift from offline to online engagement between the state and its citizens in many countries. The extent to which such a transition is successful largely depends on the historical attitudes of a country's population towards change and innovation and the perceived trust levels of that population in both the government and digital platforms.

At the beginning of the section, we had hinted at how certain parameters related to the political structure of the country – such as stability and governance – could impact the level of digital trust by citizens. Other political drivers of digital trust include data protection and privacy regulations, anti-discrimination and insurance laws, election and voting manipulation and misinformation, the threat of cyber extremism and multilateral cyber cooperation.[20] These indicate to what extent people can trust government preparedness and resilience in the digital context. We will explore elements of privacy, security and ethics below but it is important to emphasise how the perception of the government in this context is itself an important deciding factor on the quantum of digital trust.

Measuring political will in bringing about effective digitalisation is difficult. Could the nature of public sector data be a proxy? The OECD OURdata Index measures the availability, accessibility and re-use of government data.[21] Open government data forms the basis of transparency, accountability and value creation by making government data available to all. Could this in turn encourage people to trust the government and any digital initiatives and data-backed AI strategies they choose to pursue? Simple correlation between the OUR Index and the Digital Intelligence Index shows that this does not seem to be the case for the set of OECD countries in the sample (Figure 6). Thus, digital trust is more driven by the political stability and effective governance of a country rather than extent of public sector data openness.

[20] *Future of Digital Trust: Driving forces, trends and their implications on our digital tomorrow*, Deloitte, 2021.
[21] *OECD Open, Useful and Re-usable data (OURdata) Index: 2019*, OECD, 2020.

Figure 6:
Government data openness and digital intelligence



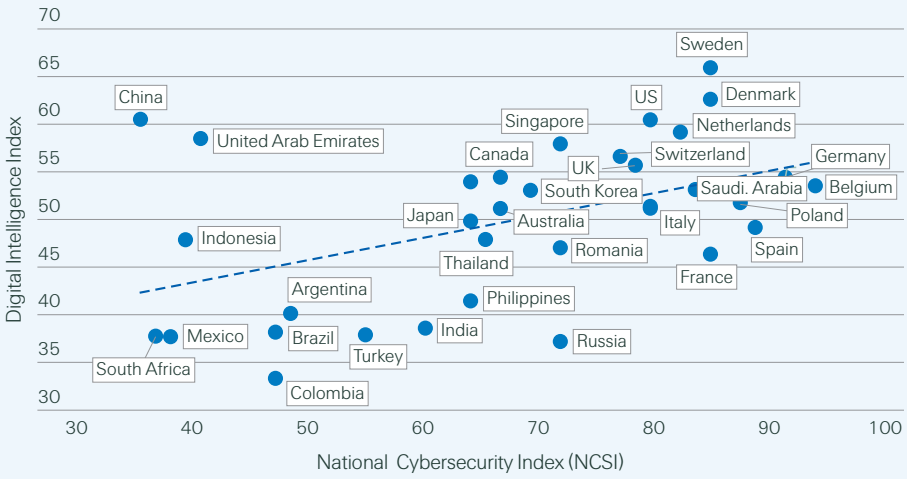
Source: Swiss Re Institute (SRI), Tufts University, and OECD

Security
Data/cyber risk

Key takeaway: Insurers can help in the adoption of better "cyber hygiene" among organisations and institutions through sharing best practices and encouraging the use of third-party security firms. This in turn will make cyber risk more insurable.

Cyber resilience is an important step towards establishing digital trust. Swiss Re Institute analysis finds that there is a strong positive correlation between cyber preparedness and digital trust, suggesting that countries that invest in cybersecurity policies, legislation and outcomes do experience greater levels of digital trust within their economies. Figure 7 highlights this cross-sectional relationship.

Figure 7:
Positive association between digital trust and cyber resilience



Source: Swiss Re Institute (SRI), Tufts University, and e-Governance Academy Foundation

However, given the rapidly evolving nature of these risks, legislative policies should be accompanied by an updated understanding of threats by end users. Executives may still not fully appreciate the true nature of cyber risks for their businesses – the PwC Global Digital Trusts Insights 2022 revealed that as many as 60% of C-suite executives had less than a thorough understanding of the risk of third-party data breaches.[22]

Given the ever-changing nature of these threats, insurers are offering innovative coverage in the cyber and digital space. Some examples may be found in Box 4. Insurers can incentivise "cyber hygiene" within organisations and among individuals, share best practices and encourage the use of third-party security firms. Enhancement of cyber hygiene will improve insurability and make cyber risk more underwriting-friendly.

Cyber risk insurers must continue to develop strong underwriting practices and a solid accumulation risk framework.[23] Market assessments indicate that the cyber insurance market is growing rapidly. In the United States alone, it has almost doubled in size since 2015.[24] However, prices are increasing sharply as well, in part fuelled by higher ransomware-driven claims. Market participants also fear that cyber risk is not very different from natural catastrophes – losses can be huge and there is significant threat of aggregation risks.

[22] *2022 Global Digital Trust Insights*, PwC, 2022.
[23] *Advancing the societal benefits of digitalisation*, Swiss Re.
[24] *Cyber Insurance Market: Growth Potential attractive but profitability uncertain*, J.P. Morgan, December 2021.

Box 4: Insurers can catalyse digital trust

- Smaller businesses, traditionally underserved, now have the opportunity to better protect their digital assets by partnering with firms that combine comprehensive insurance and proactive cybersecurity tools to help manage and mitigate cyber risk.
- Insurers can leverage the plethora of new data sources to design and offer parametric products that pay out in case of disruptions such as internet outages. They could also provide downtime cover for critical cloud apps.
- Individual consumers too can benefit from solutions for personal digital risks such as online financial fraud, identity theft, social media liability, cyber bullying, and smart home malware attacks. Such products cover financial losses, legal and restitution costs, counselling expenses and IT consultation costs.

Security
Data ethics/privacy

Key takeaway: Data is useful. Target the specific datasets you need, explain carefully to consumers how you will use those datasets and frame ethics policies in terms of being mutually beneficial.

A key imperative to establishing the circle of digital trust between governments, businesses, customers and employees is the protection of personal data and preventing its unethical use. People were wary of sharing their personal information, even during the height of the pandemic, when governments and organisations were seeking health information from citizens and employees using digital means. Cisco's Consumer Privacy Survey in June 2020 revealed that 31% of respondents were concerned that their data would be used for unrelated purposes, while 25% were worried that their data may be shared with third parties.[25] Concerns over data privacy are prevalent not just at work or when sharing information with public agencies, but also when interacting and communicating via social media. There are fears of data abuses and predatory profiling as well as privacy violations.[26]

Insurers are increasingly asking themselves how they should collect, curate, analyse and process the growing flows of relevant data coming from their personal and commercial policy holders (see Box 5). However, they will also need to assuage the concerns of data owners, especially with the growing use of black-box machine learning and AI approaches. Choice sets on websites and mobile apps can be designed in a way that is not beneficial to users. These so-called "dark patterns" and "sludges" can result in unethical design practices and can also cause reputational damage to businesses and impede trust. In 2019, for example, a British online travel retailer made headlines when customers complained that the checkout process was so confusing, they inadvertently bought travel cancellation insurance that they did not want.[27]

Box 5: The ethical conundrum in e-health

Capturing new and personalised data sets, such as real-time monitoring of fitness and exercise data, has clear benefits for helping individuals maintain a healthy lifestyle. It marks a shift in approach from disease treatment to prevention.

Capturing such large real-time data sets would also benefit life and health insurers. Ongoing data analysis could enable an insurer to spot upcoming problems and advise clients to consult a doctor or adopt a healthier lifestyle. People who were hitherto considered uninsurable might receive cover if their data revealed full treatment compliance and positive lifestyle factors.

However, the exciting potential of big data also raises ethical questions that go beyond data protection and privacy challenges. Making sure that no individuals or groups are disadvantaged by the information coming out of big data algorithms will be very important. The benefits of better results using big data and smart analytics cannot be at the cost of infringing privacy rights. Leading healthcare provider UnitedHealthcare leverages big data without compromising on privacy by aggregating large volumes of de-identified unstructured medical data of patients into data lakes and using big data analytics to better detect fraud, waste, and abuse in claims.[29]

However, this does not imply that organisations (including insurers) and governments must stop collecting data altogether. Much of the data collected by insurers, for instance, is used to analyse consumer needs and preferences, and design better solutions that can ultimately go a long way to creating greater trust. The insurance industry needs to balance between expanding its digital footprint and using data transparently and responsibly. This can be done by adding layers of privacy to ensure availability and fair usage of sensitive and personal data. Independent third-party digital privacy management solutions such as Pryv (see below, Box 6) have been developed for ethical data sharing.[29]

Similarly, Human API collects and aggregates data from more than 40,000 unique sources (including hospitals, clients, pharmacies, labs, health information exchanges, wearables and others).[30] Only permissioned health data is then shared with health insurers. Insurers benefit from access to patient health records in a structured, normalised format that is easy to ingest. However, policyholders stand to benefit as well: By sharing their data they could be receiving more personalised and higher-quality service. They could also be saving time and effort on medical tests that may otherwise be needed for health underwriting. The core proposition that makes this

[25] Cisco June 2020 survey of more than 2600 respondents across 12 countries – See *Protecting Data Privacy to Maintain Digital Trust*, Cisco, 2020.
[26] C. Veliz, "Privacy and digital ethics after the pandemic", Nature, January 2021.
[27] *Ethics in digital nudging*, Swiss Re Institute, June 2021.
[28] https://www.itproportal.com/features/five-big-data-trends-in-healthcare/ , https://www.uhc.com/.
[29] *Privacy management to drive outcomes from data aggregation*, Swiss Re Institute, February 2018.
[30] *Navigating The Digital Decade: 25 Emerging Technology-Led Businesses Well Placed To Help Insurers Succeed*, Oxbow Partners, 2021.

system work is the fact that customers can trust that only the data they wish to share with their insurers is actually being passed on, adding a much-needed layer of privacy.

Ethical considerations must be incorporated, not just post-implementation, but at the discussion and development stages of complex investments like artificial intelligence projects. Gartner predicts that the growing importance of data ethics and privacy is likely to drive spending on data protection and compliance beyond USD15 billion every year.[31]

Box 6: Privacy management solutions for sharing data responsibly

Rather like a bank acts as a middle-man between counter-payees, Pryv is used by businesses as a layer to apply custodial rights and provide selective access to data while building trust with individuals.[33] Just as individuals can see their bank accounts with confidence and assurance, so they also want to see their data, who is accessing it, why, and with what consent.

Gaining detailed information while being compliant with regulations such as the General Data Protection Regulation (GDPR) or the E-Privacy EU directive is not always straight forward. Pryv makes this easy by providing its customers with a novel data-model and privacy-by-design software layer for granular consent management so they can further provide their own consumers with sufficient assurance that they will use no more data than necessary. Thus, the companies are assured that they will have compliant access to data and do not have to worry about how the data is collected, structured, and stored.

[31] *Gartner Says Digital Ethics is at the Peak of Inflated Expectations in the 2021 Gartner Hype Cycle for Privacy*, Gartner, September 2021.
[32] https://www.pryv.com/.

Security
Trust by proxy: Laws, self-policing

Key takeaway: Laws and industry standards build digital trust to a certain point. However, past that point, the relationship may not be linear.

The previous two security sections focused on the bilateral relationship between customer and supplier or service provider, be that in data not being lost or stolen or data being treated fairly and ethically in any given transaction. In security by proxy, we look at environmental factors that might affect digital trust, notably laws and common standards.

Digital legislation

The basis of digital law, consumers will be grateful to hear, is an extension of inalienable rights embodied in international conventions such as the United Nations Universal Declaration of Human Rights. Article 19 of the Declaration allows everyone the "right to freedom of opinion and expression." Subsequent recommendations detail how this freedom should be applied to internet use.[33] The right to internet access is also included within the Sustainable Development Goals of the United Nations, which has been signed by 193 signatories.

The next layer of digital legislation is set by nation states or quasi-sovereign bodies. Widely regarded as best-in-class – at least from a consumer standpoint – is the EU's General Data Protection Regulation (GDPR). Implemented in 2018, and running to 99 articles, the GDPR's focal point is personal data. Companies should hold no more data than necessary and cyber security should be appropriate to the size of the organisation.[34] GDPR is not without critics, largely in its implementation.[35] China has followed elements of the GDPR in its three-pillar data security legislation but with important differences around supervision, individual rights, and international data transfer. Critics believe Chinese legislation increases political control; checks the power of internet giants; and considerably extends the reach of the government off-shore. The US, by contrast, lacks a comprehensive federal data protection law. Tired of waiting, some states, including California, have implemented their own. Elsewhere, countries range from lacking entirely in data protection legislation (much of the Middle East); to implementing criticised or flawed data protection regimes (India); to establishing relatively strong data laws (several South American states).[36]

One might expect a good correlation between digital trust and the strength of digital security legislation – a win-win for legislators determined to implement strong data protection laws. It may not be the case. McQuinn and Castro suggest no linear relationship between legislation and trust: "No regulation can mean very little trust and some reasonable baseline level of regulation increases trust but trust does not measurably increase beyond that baseline level."[37] The authors cite increased use of social media and internet shopping in the US (lacking federal codified data protection) against lower usage in the EU (with the GDPR). They suggest a 'goldilocks' level of regulation is best to maintain trust. Excessive legislation may even erode trust (as well as investment) by creating 'overregulation', a path the EU may already be on.

Self-policing

Where companies may see data legislation as being insufficient to create trust, they can sign up to standards codified by a third party. This codification can be much broader in its remit than just data protection, encompassing the ethical use of data.

This form of standards-setting is well known from other industries. Most developed economies have some form of accreditation mark for products to demonstrate compliance with health and safety standards. These include the CCC in China, the CE mark in the European Union or the FCC in the US.

Most of these trust-building labels are applied to manufactured goods. Such labels are in their relative infancy within the digital sphere. The original Kitemark – first established to meet British Standards' specifications in 1903 and covering everything from crash helmets to smoke detectors – has also been extended to secure digital banking and credit card transactions.[38,39] Swiss Re has recently participated in pilots for the Swiss Digital Trust Label (see Box 7).[40]

[33] C. Howell and D. M. West, "The internet as a human right", Brookings, 7 November 2016.
[34] M. Burgess, "What is GDPR? The summary guide to GDPR compliance in the UK", Wired, 24 March 2020.
[35] *Three Years Under the EU GDPR*, Access Now, May 2021.
[36] E. Masse, "The best and the worst in 2022: data protection laws across the world", Access Now, 27 January 2022.
[37] A. McQuinn and D. Castro "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use", ITIF, 11 July 2018.
[38] *For confidence when you bank, look for the BSI Kitemark for secure digital banking*, bsi.
[39] https://alwaysfinance.co.uk/2021/12/03/barclaycard-app-becomes-first-credit-card-app-to-achieve-bsi-kitemark-for-secure-digital-banking/.
[40] *Cross-Industry Coalition Advances Digital Trust Standards*, Trust Over IP Foundation, 5 May 2020. .

Other initiatives are underway within the tech sector to enhance digital trust. The Trust over IP Foundation – with a number of participants, including Accenture and IBM Security – "will use digital identity models that leverage interoperable digital wallets and credentials and the new W3C Verifiable Credentials standard to … enable consumers, businesses and governments to better manage risk, improve digital trust and protect all forms of identity online".[41] UK-based InsurTech start-up TrustLayer partners with insurers and brokers to provide a risk management tool that can help verify whether business partners have the right insurance and compliance documentation in place or not.[42] The tool uses robotic process automation (RPA) to scan paper- and PDF-based insurance documentation of vendors, tenants, and borrowers to track the sum insured, expiration and exclusion-related aspects, in the process adding a certified trust label for these business partners.[43]

Box 7: Swiss Digital Trust Label

Swiss Re is one of the pilot companies participating in the Swiss Digital Trust Label Initiative. The Swiss Digital Trust Label, which is owned by the independent foundation Swiss Digital Initiative and is the product of a partnership between the Swiss government, academia and business, can be applied to a specific digital product or service deployed by an individual company. Swiss Re has completed the pilot certification for Magnum Go automated underwriting solutions, which many primary insurance clients integrate into their sales platforms to efficiently and accurately underwrite their consumers' life insurance policies.[44]

[41] *Ibid.*
[42] https://trustlayer.io/
[43] *Risk management*, TrustLayer.
[44] "Swiss Re one of two pioneers to receive the Digital Trust Label – world's first label for digital responsibility launched by the Swiss Digital Initiative", Swiss Re, 18 January 2022.

Reassurance
AI/Automated decision making

Key takeaway: AI will be transformative across industries. Consumer reactions to machines making decisions currently appears equivocal.

Trust and transformation

Looking through the literature, two themes quickly coalesce around AI. The first is game-changing. Across a wide vista of activities, AI will be transformative. It will create efficiencies, enable discoveries and facilitate automation. This is very much the case within the insurance industry. As IBM predicted in 2021: "In the coming years, automation and AI solutions will roll out across every domain in the insurance industry".[45] AI will be able to provide insurance customers with a more personalised journey across the insurance value chain, while empowering insurers to perceive new insights into both their customers and the risks their customers face. AI will allow insurers to overcome the inefficiencies of legacy systems, consolidate consumer data and breach previously held silo walls.

Box 8: Superhog[46]

Superhog is a product targeted at property management companies with multiple lettings enabling hosts and guests to demonstrate to each other their trustworthiness by stepping through an identity and biometric verification process. Artificial intelligence, predictive analysis, and machine learning are utilised to help verify information across a multitude of platforms in real-time building a complete picture and understanding of an individual's short-term rental history.

In the unlikely event that the tech fails, Guardhog's insurance product is embedded into Superhog's solution and provides up to USD7m in cover for accidents, guest damage and liability.

The second theme is trust. IBM devotes a whole subsection of its AI website to the theme of trust.[47] For IBM, the matter of trust around AI is relatively clear: "When people understand how technology works and we can assess that it's safe and reliable, we're far more inclined to trust it". Trust, then, is a matter of opening up the black boxes and shining a light on the underlying algorithms. Those algorithms have to be explainable, be fair and maintain accountability. AI can even be designed to recognise its own limitations and quantify uncertainties in its decision making. Countries around the world are realising the need to strengthen internal governance related to the application of AI and the responsible use of data. For instance, the Veritas initiative, developed by the Monetary Authority of Singapore (MAS) and part of the Singapore National AI Strategy, aims to enable financial institutions to evaluate their AI-driven solutions against the principles of fairness, ethics, accountability and transparency (FEAT).[48]

Trust and understanding

An IPSOS survey for the World Economic Forum in 2022 explored attitudes to AI in 28 countries.[49] It reported a positive correlation between a perceived understanding of AI among respondents and trust in companies using the technology. However, understanding may not have been the only driver of trust. Both levels of trust and levels of understanding were higher among emerging markets than developed markets. Figures for trust and understanding of AI were significantly lower, for example, in Japan – hardly a stranger to digital technology – than India or China, which suggests cultural factors at play. Also distrustful of companies using AI were respondents from Germany, Canada, the US and the UK.

A KPMG survey on trust and AI in 2020 stated that there were four drivers behind trust in AI. (1) the regulatory structure around it; (2) its impact on jobs; (3) familiarity and understanding; and (4) perceived societal impact.[50] Less optimistic than the IPSOS survey, only 21% of the respondents from five countries approved or embraced AI, although 70% accepted or tolerated the technology. There was greater trust in the use of AI in healthcare; less in human resources. Trust was greater in younger age groups.

[45] *From underwriting to claims management, artificial intelligence will transform the insurance industry*, IBM, 13 September 2021.
[46] www.superhog.com.
[47] Trusted AI, IBM.
[48] *Veritas Initiative*, Monetary Authority of Singapore, 3 March 2021.
[49] J. Myers, "*5 charts that show what people around the world think about AI*", World Economic Forum, 5 Jan 2022.
[50] *Trust in Artificial Intelligence*, KPMG, March 2021.

Trusting the robots

The most tangible contact individuals are likely to have with AI may come in the field of automation – and self-driving cars could be the largest single market for such technology.

In 2018, a pedestrian was hit and killed by an Uber vehicle in driverless mode, with the human driver, supposed to be monitoring the car, distracted. The pedestrian emerged from the dark at a spot where there was no crossing, but the Uber took no avoidance action. Two days later, Uber suspended its autonomous vehicle testing for a period that lasted two years. A handful of other fatal accidents have been attributed to cars in self-drive mode and there have been many minor crashes.

Proponents of autonomous vehicles make two points: Firstly, no technology has yet been developed that it is completely accident free; and secondly, technology is many levels better at driving than humans. Both points have to be understood by potential consumers. It is a tragic figure, but around 100 people die on any given day on US roads, with the vast majority of accidents the result of human error.

It makes for an interesting juxtaposition. Individuals routinely underestimate the risk of human driving and overestimate the risk of autonomous driving.[51] However, trust is a subjective expression that escapes objective measurement. Smart device developer Xperi undertook a survey of 2,000 drivers in 2021.[52] Only 13% of respondents would currently trust journeying in an autonomous car. However, 44% of those surveyed believe that they will end up using a self-driving car in the next 10 years (although 39% believe they will never use an automated car). Notably, 41% of those questioned believe autonomous cars will eventually be the safest way to travel (31% reject this statement). Self-driving cars were seen as a particularly attractive alternative for older drivers.

Box 9: Using emerging technologies in underwriting and claims

InsurTech start-up Photocert uses computer vision and AI to scan through evidence of damage and assert its authenticity.[53] Policyholders can register and submit a motor claim with image proofs - AI validates the extent of the damage and estimates value. Trusted timestamping servers legally certify the verify date, time, source device, and GPS location while Ethereum blockchain store the image certifications. Photocert's solutions can not only make claims more efficient, but speed up underwriting as well. On sharing images and relevant documentation, policyholders can get customised quotes for their insured items on a mobile app powered by image recognition.

[51] One analogy here can be flying. In the wake of the 9/11 attacks. Nervous of air travel, many drove on journeys they would have previously flown. The accident rate went up accordingly – car travel is far riskier than flying. See J. Ball, "*September 11's indirect toll: road deaths linked to fearful flyers*", The Guardian, 5 September 2011.
[52] *The 2022 Vehicle Predictions Report*, Xperi, 2022.
[53] https://oxbowpartners.com/insurtech-bitesize/photocert-2021/.

Reassurance
Empathetic/social AI

Key take out: Customers appreciate empathetic AI – but it does not come cheap and the closer it gets to humans, the more it may alienate some.

The jump between AI and emotionally literate or sensitive AI is a significant one. Smart machines can learn from data sets. The data set of human interactions is a hugely granular and complex undertaking. Moreover, human interactions are executed through many levels of sensual perception, including language, facial response, body language and even smell. To become more challenging still, human relationships are also undertaken through the lens of particular languages and cultures. The field is an established one, dating back at least to the 1990s and the Affective Computing Group at MIT Media.[54]

The points of potential emotional exchange between AI and insurance customers are several. Perhaps the most obvious place to start is chatbots. Chatbots allow customers access to their insurance company 24/7 in a manner of their choosing. Insurers save on labour costs and can control and monitor calls highly effectively. In a Swiss Re publication, "The future is bright; the future is humanoid chatbots?" (2021), we discuss extensively the levels of maturity required to develop chatbots to an emotional level.[55]

Figure 8: Development of emotional bots

Maturity level	Details	Preconditions
4 **Own personality**	▪ The bot develops its own identity and personality over time based on accumulated interaction experiences ▪ The company must continuously 'calibrate' the parameters of its own identity and values and adapt them to the times	▪ Situational recognition of context and personality ▪ Adapted linguistic-subject personalised bot-personality response ▪ Personality traits and values are defined and adapted
3 **Empathic interaction**	▪ Identifies and reproduce empathic interactions ▪ Communication can be very situationally adaptive to empathic response ▪ Company manages, regulates and controls empathic response	▪ Detection of additional emphatic and situational context ▪ Continuously adapted linguisticsubject personalised empathic response
2 **Emotional interaction**	▪ Identifies and reproduce emotional interactions ▪ Communication can adapt situationally to emotional response ▪ Company manages, regulates and controls emotional response	▪ Understanding of additional emotional context ▪ Continuously adjusted linguisticsubject emotional-supportive response
1 **Functional interaction**	▪ Simple, factual interaction ▪ Communication is strongly controlled and steered by professional expertise ▪ Company controls, regulates, and monitors functional response	▪ Understanding of professional context ▪ Correct linguistic-subjective responses in terms of syntax and semantics ▪ Continuous adaptation of factual knowledge

Source: Swiss Re Institute

[54] M. Sommers, "*Emotion AI, explained*", MIT Management Sloan School, 8 March 2019.
[55] *The future is bright; the future is humanoid chatbots?*, Swiss Re Institute, 8 December 2021.

The requirement of emotional support and conditions of mental illness can have considerable repercussions for insurers. The numbers are large; Swiss Re Institute estimates that around 45 million people suffer mental conditions in six key insurance markets.[56] In the light of these findings, Swiss Re is collaborating with leading AI-powered mental health platform, Wysa, to create an insurance-specific app.[57] The new app will include improved monitoring and mental health tracking, curated pathways to signpost consumers to relevant offline support and better reporting for insurance clients.

Bots to robots

AI-driven apps and bots can provide emotional interaction at the level of a computer interface. The next level of challenge to engage engineers is reproducing emotional AI with movement in a 3D casing – the emotionally intelligent robot.

This is no longer the stuff of science fiction. Anthropomorphic robots already have a high level of cultural acceptance in Japan. These robots are not necessarily AI-powered but have found emotional connection. Robots are – and have been for some time – common in nursing homes, producing positive results with dementia patients.[58] Perhaps also worth mentioning here: humans have been shown capable of forming at some level emotional bonds with technology that is in no way trying to be empathetic, such as in the case of robotic vacuum cleaners.[59] This could be of interest in the Internet of Things world – might individuals form at some level a relationship with their self-driving car, for example, and what might that mean for the commercial space around the car?

The prospects of empathetic AI can swiftly lead to discussions of cyber consciousness, our relationships with robots, boundaries between man and machine, and prospects of singularity. All are endlessly fascinating topics in their own right, but outside the scope of this paper.

The key takeaway from this brief excursion is that consumers will show greater trust in empathetic AI, tempered by cultural and possibly generational perspectives. However, emotional training of AI currently consumes time and investment and there are concerns that providing a service that becomes overly realistic but not-quite-human could conversely erode trust.

Box 10: Uncanny valley

The term was first used by Japanese robot designer Masahiro Mori. Mori suggested humans respond positively to increasingly empathetic and human-like technology until the technology reaches a point of near-realism, where the attraction can suddenly switch to revulsion. It can occur in films, in game design or in robots. The feeling of uncanny valley can be prompted by ambiguity; cultural expectations; mismatching; inconsistency; and even a survival response. Some films have even been reshot to make them seem less realistic, after negative reactions from test audiences. Uncanny valley is most likely to occur in the insurance context with chat bots, particularly if customers initially believed they were talking to humans.

[56] *Head first: supporting consumers' mental wellbeing through insurance*, Swiss Re Institute, 7 October 2021.
[57] *Mayden and Wysa collaborate on Mental Health etriage*, Wysa, 16 March 2022.
[58] B. Lufkin, "What the world can learn from Japan's robots", BBC, 7 February 2020.
[59] J. Mourey, J. Olson and C. Yoon, "Products as Pals: Engaging with Anthropomorphic Products Mitigates the Effects of Social Exclusion", Journal of Consumer Research, 21 January 2017.

Reassurance
Human-to-human interactions

Key take out: Building an effective digital trust strategy should respect limitations and retain services still best delivered by humans.

In 2015, Richard Susskind and his son, Daniel, published "The Future of the Professions." Their conclusion was that digitalisation, and AI in particular, would bring sweeping changes to the world of white-collar work. Processes currently undertaken by professionals, in fields such as health, law and financial services, would be increasingly automated, rendering many jobs, as we currently understand them, obsolete. Daniel Susskind's 2020 follow-on publication "A World without Work" goes the extra mile in imagining a post-work landscape.

The Susskinds are not alone. The Second Machine Age (2014), by Erik Brynjolfsson and Andrew McAfee, paints another picture of the march of automation. To quote the authors:

"Now comes the second machine age. Computers and other digital advances are doing for mental power — the ability to use our brains to understand and shape our environments — what the steam engine and its descendants did for muscle power."[60]

AI-induced changes to working practice in the insurance sector could be dramatic. By 2030 – a mere eight years away at the point of writing – McKinsey predicts the number of insurance agents will have "substantially reduced" and their role altered to "product educators". Underwriting, as we currently know it, will "cease to exist" and more than half of claims activity will be "replaced by automation".[61]

A revolution to come

The revolution may come, and the technology certainly suggests it can; but statistics imply it is not here yet. Approximately 1.1 million people were employed in the financial services sector in the UK in 2020, down from 1.19 million in 2001.[62] This modest fall was largely the result of bank and building society branch closures. In part, that can be attributed to digitalisation, although branch consolidation in the sector pre-dates online banking by some decades. A more anecdotal comparison might be found closer to home: at the time of writing, a major international job site has postings for around 400 underwriters in the greater London area. If underwriters are indeed headed the way of the dinosaur, not all employers have seen the memo.

David Autor[63] provides some corrective to those commentators – including John Maynard Keynes, William Morris and Lyndon B. Johnson – who have repeatedly warned that the coming of higher productivity automation will cause, for good or ill, worker obsolescence. Autor suggests that despite some polarisation between employees, complementary effects of technology on labour and the ability of humans to provide "problem-solving skills, adaptability, and creativity" suggest that mankind is more than capable of adapting to machines.

The human factor: trust

We will add one factor to this mix: trust.

Humans are highly nuanced social creatures. That homo sapiens overcame bigger-brained, physically stronger Neanderthals in the evolutionary race was in large part due to their higher level of socialisation.[64] They worked better together. We are a species built on trust.

One sector that has considerable potential for automation is education. Courses could be designed specifically to certain attainment levels; children could progress at a speed suited to their needs; systems could be standardised; the risks of poor teaching navigated; and swathes of admin, from testing to marking, automated. One reformer has suggested building a 'school in the cloud'.[65]

[60] E. Brynjolfsson, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton Company, 2016.
[61] Insurance 2030 — The impact of AI on the future of insurance, McKinsey, 12 March 2021.
[62] *Number of employees in the financial services sector in the United Kingdom from 2001 to 2021*, Statista, 6 April 2022.
[63] D. H. Autor, "Why Are There Still So Many Jobs? The History and Future of Workplace Automation", *Journal of Economic Perspectives*, 29 (3) 2015, p 3-30.
[64] "We [homo sapiens] were — and clearly still are — adept social networkers." https://www.livescience.com/20798-humans-prevailed-neanderthals.html
[65] S. Mitra, "Build a School in the Cloud", TED, 2013.

Yet relatively few, even post-pandemic, are ready to take learning out of schools. As well as teaching academic subjects, schools are places where children learn socialisation skills both in the structure of the classroom and in the jungle of the playground. These build the mechanics of human trust. Even automation enthusiasts McKinsey suggested in 2018 that, while teaching will be greatly supported by digital technologies, demand for teachers will not fall, but rise, by "5 to 24 percent in the United States between 2016 and 2030." [66]

At the heart of this debate is a question: is there a natural limit to the extent of our trust in digital? And based on our experiences thus far in the education sector, the answer would appear to be that there might well be. Are you ready for a robot to break to you the news of your malignant tumour? Even one trained in empathy? Would you board a plane without a pilot, even if I told you that well over 90% of a typical flight is already performed by autopilot?

Does this translate to the more prosaic world of insurance? The natural limit of digital trust is probably more extended than for teaching or health, but a limit may nonetheless exist. Insurance products support some of the largest decisions and most significant events of our lives. I might be willing to buy car coverage or travel insurance from a bot, maybe more so if the bot is emotionally trained. But when it comes to life insurance – for the average consumer a relatively complex product to cover the provision for descendants in the event of their death – is it not reasonable to expect that individuals might want the reassurance of an experienced agent? IBM endorses this approach, suggesting AI can be used to automate impersonal parts of the human process, allowing "knowledge workers… [to] focus more on 'human touch' tasks that make customers feel valued".[67]

Our conclusion: Building an effective digital trust strategy also necessitates understanding where human trust may be necessary and complementary.

Box 11: Digital + Human trust in the insurance value chain

Digital is an important component along the journey of a typical insurer's value chain. For example, iptiQ- the digital B2B2C insurance company powered by Swiss Re, is delivering multi-channel[68] customer experiences through an advanced end-to-end digital platform. Below are some examples on how digital can be integrated at each step along the insurance value chain.

Digital underwriting

With advanced underwriting processes today, insurers can dynamically tailor the underwriting questionnaire to the customer and intelligently pose the most relevant questions as the process progresses. The result is a much-improved understanding and assessment of the customer when insurance is purchased. This allows insurers to offer improved insurance coverage to even more customers and with less unexpected surprises at claim time.

Digital claims and policy updates

Customers can not only make more informed decisions during insurance purchase with the help of data and digital channels, but they can also access, track and manage their transactions, claims and policy updates at any time at the click of a button. Ultimately, trust and transparency are both two-way streets that would require customers sharing data on aspects such as health, exercise or driving habits. While initially such an exchange can be incentivised (through lower premiums), ultimately these relationships would be based on a foundation of digital trust. Once gained, digital trust should not be lost due to use or abuse of personal data.

Digital + human to boost trust

As discussed earlier, the promise of technology backed by appropriate human intervention and input will give customers a critical level of reassurance that may be lacking with a fully automated process or a human-only process. Automation should minimise the risk of human bias and mistakes at more basic levels of the insurance journey and provide instant feedback to customers. However, for more complex products and processes relating to such products, human input is invaluable when making those critical decisions. This combination of digital and human engagement will bolster transparency and build a higher level of digital trust. As a new model for digital interaction emerges, we can expect more engaged customers and that usually equates to better products, service, and satisfaction.

[66] *How artificial intelligence will impact K-12 teachers*, McKinsey, 14 January 2020.
[67] *From underwriting to claims management, artificial intelligence will transform the insurance industry*, IBM, 13 September 2021.
[68] *How insurers can pave a path to digital trust with greater transparency*, iptiQ by Swiss Re, 10 November 2021.

Conclusion

The digital trust pyramid and the case of insurance

This secondary literature review of the drivers of digital trust does not reveal neatly aligned data sets. The drivers of digital trust are many. We have attempted to work our way through nine stages in this report to provide us with some structure to our thinking.

Equally, we are not capturing all the factors that must be present. Digital trust is a subset of the wider notion of trust. The factors that affect trust across nations, cultures, language groups, class, genders – indeed any subdivisions of people – are numerous and not easily reconciled. The foundations of trust do not necessarily correspond. In one survey, only Sweden, the Netherlands and Norway had more positive respondents to the statement "most people can be trusted" than China.[69] Needless to say, the cultural, societal, and political differences – inclusive of digital governance – between the first three countries and China are significant.

Watch for negative correlations

In this review, we have largely been looking at positive drivers of digital trust. It may, however, be that there are negative drivers. We would like to associate open and more transparent political cultures with greater levels of digital trust. Yet trust in digital, be it in terms of transactions, interactions, information or social media, may actually be higher because trust in government and governance structures is low. Digital is a better alternative. This phenomenon is not confined to politically unstable developing markets; many Americans trust the shadowy corners of internet conspiracies more than their own government.[70] Filter bubbles are a real thing and have contributed to a polarisation in US politics.[71] A similar point can be made for financial institutions. Those in countries that have suffered repeated financial crises may show more trust in digital payment systems because the alternative – banks – are distrusted.

This negative association can also be made in terms of development. In this report, we have suggested that higher levels of digital trust can be achieved with greater levels of infrastructure development. It may also be that digital leapfrogs bureaucratic infrastructure development – that digital is so strong because the analogue alternatives are weak, lagging, corrupt or expensive. Some large and rapidly emerging markets may fall into this category.

Beyond the determinants of digital trust, one may ask why digital trust is needed in the first place. It may be easier to explain with another question: what would happen in the absence of digital trust? What price would be paid for a lack of digital trust by individuals, societies and businesses? Box 12 highlights the costs of digital misinformation in the absence of trust.

[69] E. Ortiz-Ospina and M. Roser, "Trust". Published online at *OurWorldInData.org*, 2016.
[70] Trust in the US government was77% in 1964. It fell to 17% in 2019; See *Wellcome Global Monitor 2020: Covid-19*, Wellcome, November 2021.
[71] A point made by Eli Pariser back in 2011: *Beware online "filter bubbles"*, TED, March 2011.
[72] *Digital News Report 2021*, Reuters Institute, 2021.
[73] *Economic cost of climate change could be six times higher than previously thought*, UCL News, 6 September 2021.
[74] Refer to Appendix.
[75] *Non-communicable Diseases*, World Health Organization, 13 April 2021.
[76] The YLLs for a cause are calculated as the number of cause-specific deaths multiplied by a loss function specifying the years lost for deaths as a function of the age at which death occurs
[77] Refer Appendix

Box 12: Digital misinformation and its costs

Where the internet is available, it is available – barring censorship – to all. It creates a 'too-much-too-little' scenario – too much information is available, but only a small proportion may be relevant and accurate. The Reuter's Institute Digital News Report 2021 shows that while 82% of survey respondents read news online (including social media), only 34% trust search engines for news whilst 24% trust the news they read on social media.[72]

We can estimate the quantitative cost of misinformation. To do so, we took two case studies of climate change and non-communicable diseases (NCDs). We used a funnel approach of a total population of 18 countries using social media as their primary news source. We then estimated the share of social media users with an interest in climate change and the probability of those viewing inaccurate or misinformation on climate change. Studies suggest that the economic cost of climate change per person (accounting for both cost to humanity as well as impact of climate change on economic growth) could be as high as USD15,000.[73] Swiss Re Institute (SRI) analysis revealed that digital misinformation-driven climate change inaction could cost the world USD37.5 billion, or roughly 0.05% of global GDP.[74]

NCDs are driven by poor diet, nutrition, and lack of exercise. They result in 41 million premature deaths annually.[75] We wanted to estimate the mortality and morbidity cost associated with digital misinformation on diet, nutrition, and exercise. Research shows that almost 60% of younger consumers refer to digital media for news related to health and nutrition. Further analysis reveals that up to 40% of the most frequently shared links often contain fake news. Using a combination of this data along with figures on NCD years of life lost (YLLs)[76] from the Global Burden of Diseases database,[78] we arrived at an estimate for NCD YLLs due to misinformation– 26.26 million years of lives lost in the selected sample of countries. Using per capita income as a proxy for per capita YLL cost for the same set of 18 countries, we arrived at the huge figure of USD962.81 billion in costs to the world (or 1.1% of global GDP) resulting directly from digital misinformation relating to the premature mortality cost of NCDs.[77]

These findings, combined with a plethora of research associating misinformation with the COVID-19 pandemic, suggests that digital trust, reliability, and authenticity come not only with significant economic but also human costs.

Insurers as a catalyst for trust

The final point of this paper is that insurers are not passive bystanders in questions of digital trust. Insurers know about the trust game. They provide financial cover for many of the major events in our lives, right up until death. Purchasing a house, driving a car, manufacturing a widget, being treated for a health condition – these all need insuring. Insurance provides reliability and peace of mind. Insurers can be active players in creating and supporting digital trust.

Insurers have made their first incursions into the digital world. Global cyber insurance coverage amounted to USD7.4 billion in 2020, with forecast average compound growth of over 25% in coming years, so that the market could be over USD25 billion by 2026.[79] Cyber is the most obvious point on the digital value chain where insurers can seek to create trust. Swiss Re recently teamed up with Hitachi to provide a parametric cover in automated manufacturing processes.[80] Self-driving cars may well prove safer than human-driver cars, but they will still need insurance to take to the road. Insurers will have to assess risks associated with hardware, software and connectivity. There are already insurers specialising in covering partially automated cars[81] – just as there are insurers covering risks facing robotics.[82] Insurers are further thinking about how to provide protection for digital assets.[83]

Creating digital trust is a puzzle of many pieces. Some parts will fit together easily, some will be much harder to integrate and manage. Insurers should not just seek digital trust in themselves – they should think how they can facilitate it in others. Transparency and openness will both be key, particularly so that consumers understand where they have coverage and feel in control of all aspects of their digital journey.[84]

If re/insurers cannot generate digital trust they will miss out on one of their most important future resources – data. That is why insurers should see facilitating digital trust as important as developing and investing in new digital technologies/solutions.

[78] Institute for Health Metrics Evaluation. Used with permission. All rights reserved.
[79] Global cyber insurance market size in 2020, with forecasts from 2021 to 2026, Statista, 11 January 2022.
[80] Hitachi and Swiss Re Corporate Solutions announce strategic partnership to offer industry first 'digital risk' solutions, Hitachi, 6 October 2020.
[81] *Let's insure a safer road.* Avinew.
[82] *Insurance for Robotics Companies*, Founder Shield.
[83] *Digital Asset Insurance*, BitGo.
[84] *How insurers can pave a path to digital trust with greater transparency*, iptiQ, 10 November 2021.

Appendix – Digital misinformation and its costs

I Cost of digital misinformation on climate change

1. We consider 18 countries – United States, United Kingdom, Thailand, Switzerland, Spain, South Korea, Singapore, Russian Federation, Mexico, Japan, Italy, India, Germany, France, China, Canada, Brazil and Australia.

2. Population estimates (from World Bank) and social media penetration rates (from Statista) help us arrive at an estimate of total social media users across these countries.

3. Reuter's Institute Digital News Report 2021 gives us the share of adults who use social media as a source of news.

4. Survey research from Reuter's Institute[85] indicates that about 9% of respondents refer to social media for news related to climate change.

5. Swiss Re Institute analysis, based on secondary literature, estimates that approximately 20% of climate change-related news on social media is driven by misinformation.

6. For the purpose of this analysis, based on secondary literature, we peg the probability of getting influenced by climate change-related fake news at 30%.

7. The multiplicative impact of steps 4, 5 and 6 on total social media users helps us arrive at an estimated number of people persuaded to climate inaction due to fake news, for each country.

8. Studies suggest that the economic cost of climate change per person (accounting for both cost to humanity as well as impact of climate change on economic growth) could be as high as USD15,000.[86]

9. For each country in our analysis, we multiply the number of people driven to climate inaction with the per person economic cost of climate change (adjusted for purchasing power parity) to arrive at a dollar value of climate inaction.

10. Since the countries in our analysis comprise 85% of the global GDP, the sum total of the cost of climate inaction across the 18 countries can be extrapolated to arrive at a global cost of digital misinformation-driven climate inaction – USD 37.5 billion, which is about 0.05% of global GDP.

II Cost of digital misinformation on non-communicable diseases

1. We consider the same set of 18 countries as before.

2. Population estimates for the age group 30–70 (from World Bank) and social media penetration rates (from Statista) help us to arrive at an estimate of total social media users in the target age group across these countries.

3. Based on secondary literature and our own understanding, we make the following assumptions for this analysis: namely, that 60% of the population uses social media for information on diet and exercise; that 40% of the social media content on these topics is driven by misinformation; and that the probability of influence is 30%.

4. The multiplicative impact of assumptions in step 3 helps us to arrive at an estimated number of people influenced by fake news on diet and exercise, in each country.

5. We factor in the NCD years of life lost (YLLs) for each country from the Global Burden of Diseases database and, using the assumptions in the previous step, arrive at the proportion of NCD DALYs due to misinformation.

6. We assume per capita income of a country to be a proxy for the loss associated with each DALY. Multiplying the total NCD DALYs driven by digital misinformation with the per capita income provides an estimated opportunity cost (premature mortality) for digital misinformation driven NCDs for a country.

7. Since the countries in our analysis comprise 85% of the global GDP, the sum total of the economic cost of NCD driven DALYs across the 18 countries can be extrapolated to arrive at a global cost of NCDs driven by digital misinformation – USD 87.4 trillion, which is about 1.8% of global GDP.

[85] S. Andi, "How People Access News about Climate Change", Reuter's Institute, 2021.
[86] *Economic cost of climate change could be six times higher than previously thought*, UCL News, 6 September 2021.

Published by
Swiss Re Management Ltd
Swiss Re Institute
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 3095
Email institute@swissre.com

Armonk Office:
175 King Street
Armonk, NY 10504

Hong Kong Office:
18 Harbour Road, Wan Chai
61th floor, Central Plaza
Hong Kong

Authors
Mitali Chatterjee
Simon Woodward

Contributors
Jonathan Anchen
Daniel Ryan
Francesca Tamma

Editor
Paul Ronke

Managing editor
Christoph Nabholz
Chief Research Officer, Swiss Re Institute

The editorial deadline for this study was 26 April 2022.

The internet version may contain slightly updated information.

Graphic design and production:
Corporate Real Estate&Logistics /Media Production, Zurich

Order no: 1507720_0522_EN

Swiss Re Management Ltd.
Swiss Re Institute
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 3095
swissre.com/institute