Boardroom Questions

Using your data ethically, efficiently, effectively and securely

Why trust in data is an important business consideration

KPMG Guardians of Trust Report, 2018

35%

of respondents say they have a high level of trust in their own organisation's use of data.

25%

of respondents admit they either have limited trust or active distrust in data.

92%

of respondents are worried about the impact the trust gap will have on their competitive advantage.

Research on consumers' behaviours and "desiderata" shows that while the value and price of products and services are still essential to customers' acquisition and retention, an increasing number of consumers are now expecting organisations to run and innovate their businesses ethically and in a way that inspires trust.

As businesses invest in their data capabilities to improve their services and invent new ones, trust in the way data is collected, stored, consumed, shared and disposed of is becoming a key priority for consumers.

In fact, nowadays most consumers expect data to be used by organisations that they trust in a way they understand and for a purpose they believe is valuable.

Additionally, strategic business decisions are now based on data and senior executives expect a high level of quality and reliability of the insights provided for decision-making.

As a result, trust in data is a non-negotiable business priority and C-suites are starting to question the trustworthiness of the processes and procedures that govern the data supply chain, from data collection to data analytics and disposal.

In this context, organisations need to adopt a consistent definition of "trust in data", as well as a clear view of who has primary responsibility for it.

Why Board members need to be "in the know" when it comes to "trust in data"

The breadth and depth of the "trust in data" debate means that the responsibility for identifying, preventing, managing and monitoring trust risks lies with multiple functions and teams across the organisation.

A shared understanding and view of the "data trust" foundations across C-suites and Board of Directors is key to enable executives to ask the right questions and to protect the trustworthiness of the organisation. Our approach articulates data trust in four pillars: data quality, data effectiveness, data resilience and data ethics.

Data quality: organisations need to ensure that the data collected and the way it is analysed are appropriate for the context in which the insights will be used. In many cases, this starts with questions about the quality of the underlying data.

Data effectiveness: effectiveness is about the extent to which the analysis and processing of data achieve the desired results, providing value to decision-makers who rely on the generated insights. When data-driven insights are thought to be ineffective, or are used in an inappropriate context, trust can quickly erode.

Data resilience: resilience is about optimising data sources and analytics models for the long term. Cyber security is a well known example, but executives should also think about the changing use of their data sources and digital infrastructure. This kind of resilience is particularly important as analytics become self-learning and reliant on one another.

Data ethics: data ethics refers to ethical and acceptable use, from compliance with data privacy laws to less clear areas such as the ethics of profiling and predicting behaviours. This anchor is of growing concern to consumers, and it is rapidly becoming a key focus for regulators and policy-makers, as they strive to assess the 'fairness' of analytical approaches.

Potential impacts and risks

1. The digital age creates opportunities as well as new concerns that can undermine trust across industries: constant news of data breaches, data misuse and inaccuracies is eroding public trust. Concern that the benefits of data-enabled innovation and transformation will not be evenly distributed is also growing amongst the public.
2. In this highly competitive, dynamic and data-driven environment, trust in data is a key element of business trust and ethics.
3. Organisations will need to develop a shared and consistent view of the foundations of trust in data, as well as of roles and responsibilities to protect the trustworthiness of data.
4. While three of the pillars of trust in data – quality, effectiveness, resilience – are fairly mature across organisations, the fourth pillar – data ethics – still represents an unknown territory for many organisations.
5. The lack of a unified point of view on "what good looks like" from a data ethics perspective as well as the limitations of the relevant data regulations (e.g. data privacy), mean that organisations will need to stay ahead of regulators and industry bodies and set the bar for data trust and ethics best practices in their respective industries.
6. Trust in data is likely to become one of the key strategic assets, as well as threats, to business success.
7. Defining and understanding the scope of trust in data as well as preventing, detecting and managing data trust risks within the data supply chain represents the new challenge for data scientists, business leaders, as well as risk management and assurance functions.

Boardroom Questions

1. Do we understand our customers' expectations as well as pain points from a "trust in data" perspective?
2. Does our organisation have a fit-for-purpose "trust in data" strategy and framework, which meets customers, stakeholders, public and regulatory expectations as well as national and international best practices?
3. Have we defined clear roles and responsibilities for management and monitoring of our "trust in data" strategy, framework and practices?
4. Are we comfortable that our governance, policies and processes governing "trust in data" are fit for purpose to drive trusted collection, analyses, storage, sharing and disposal of customers' data?
5. Do we understand the link between data trust and data ethics?
6. Do we understand data ethics and how to drive ethical practices, decisions and outcomes across the data supply chain?
7. Does our organisation adopt data ethics risk management practices that are fit for purpose for the management of ethical risks within the data supply chain?

Actions for Boards to consider

1. Listen to your customers to understand their expectations in relation to data trust.
2. Invest in new skills and capabilities and broaden the scope of collaboration within and outside the organisation to understand best practices and challenges in the space of data trust.
3. Develop a "trust in data" strategy and framework that meets best practices as well as expectations of relevant stakeholders.
4. Define and agree across the organisation where the primary and secondary responsibilities lie.
5. Understand the link between data trust and data ethics and ensure the organisation is equipped with adequate knowledge, governance, procedures and guidelines to manage data trust and data ethics risks.
6. Ensure the organisation adopts practical, customer-centric, outcome-focused and use-case driven approaches to managing data trust and data ethics risks.

Contact us:

Zoe Willis
Partner, Data and RegTech
zoewillis@kpmg.com.au