Governance Institute of Australia

Digital Trust: Corporate awareness and attitudes to consumer data

August 2020

CSIRO DATA 61

Executive summary

Data Governance is key

Consumer data is swiftly becoming an asset that is central to the efficacy of the Australian economy.[1] Harnessing it effectively would create new economic opportunities, business outcomes, better informed decision making, policy development and innovation.[2] Taking advantage of data to these ends will require appropriate attention to matters such as privacy, security and intellectual policy.[3]

This report presents the results of a survey conducted through the collaboration between the Governance Institute of Australia (Governance Institute) and the Commonwealth Scientific and Industrial Research Organisation (CSIRO): *Digital trust: Corporate awareness and attitudes to consumer data*. This report comments on the findings of the online survey and provides insights from the complementary research that was undertaken, including a limited number of semi-structured anonymous interviews with Governance Institute members, and a review of the literature. The intent with these findings is to identify and discuss areas that boards and governance professionals might consider when embracing opportunities and managing risk with consumer data.

The research was conducted before the COVID-19 pandemic and associated lockdown, and as such, serves as a baseline of perception about organisational capability and relevant consumer data risks. As part of a proposed longitudinal study, the next survey would be interested in observations of any altered perceptions in the light of this event. In particular, it would be interesting to note whether corporate Australia has changed their data governance of consumer data as a result of COVID-19, and more specifically, whether this would be an ongoing future change.

The research underpinning this report should be seen for what it is; not representational, but rather an indication of the perceptions held in corporate Australia. Future research would seek to explore these indications more robustly.

[1] Productivity Commission, 2017, Data Availability and Use, p v.

[2] Ibid.

[3] Ibid.

Key findings

The valuation of data is contextual

The opportunities and value of data are highly contextual, making its valuation complex. Appreciating the value of data provides a useful context for considering the management of its risks. The value of data, however, changes over time, and the quantum of risk is also circumstantial.

Assessments of Data Governance capability and maturity are subjective

Organisations with a higher perception of the value of consumer data are more likely to report the integration of consumer data into their current and longer-term strategies or business models.

There is a disconnect between IT and business leaders

When it comes to appreciating the complexity of the risk and opportunity with consumer data, there is an apparent disconnect between technology and business executives.

Consumer data risks are relative

Organisations with a Data Governance Strategy are more likely to perceive risks involved in handling consumer data. In particular, they were significantly more likely to report that mishandling consumer data presented a high risk to their brand and reputation.

Reporting chains of Data Governance are inconsistent

Business executives are generally perceived as responsible for implementing the strategy for consumer data regardless of the organisation's Data Governance maturity. However, organisations with a higher Data Governance maturity are more likely to report their technology leaders as responsible for managing issues with consumer data.

> **Trust, specifically data trust, is poorly understood. Organisations need to prioritise developing an understanding of behavioural economics and the broader socio-political context they operate in. Without this deep understanding it's extremely challenging to develop a clear perspective about the type of future they want to contribute to designing. This stuff needs to become one of the highest order values for modern information businesses. These businesses need to be willing to be truly accountable. There's a heap of existing and emerging research out there to support [this].**
>
> **Digital Trust Survey Participant**

Acknowledgements

Governance Institute of Australia and CSIRO would like to thank all research participants for their time and insights.

Citation

Hanson RT, Rennie E, Lee J, Grobler MM, (2020) Digital Trust, an Australian Perspective: Corporate Awareness and Attitudes to Consumer Data, CSIRO, Canberra.

Copyright

Important disclaimer

CSIRO advises that the information contained in this publication comprises general statements based on scientific research. The reader is advised and needs to be aware that such information may be incomplete or unable to be used in any specific situation. No reliance or actions must therefore be made on that information without seeking prior expert professional, scientific and technical advice. To the extent permitted by law, CSIRO (including its employees and consultants) excludes all liability to any person for any consequences, including but not limited to all losses, damages, costs, expenses and any other compensation, arising directly or indirectly from using this publication (in part or in whole) and any information or material contained in it.

Letter from Andrew Stevens

Chair of Data Standards Body, Consumer Data Right Implementation, and Chair of Innovation and Science Australia

Leading organisations are very conscious of how they are, and should be, engaging with their customers and their data. As the competitive frontier becomes increasingly defined by intangible value-based attributes like trust, confidence and reliability; brands and reputations are being established amongst stakeholders, members, customers and employees in terms, not only by how they manage the data they hold about these communities, but how they use that data.

The digital world has enabled greater engagement with these individuals and businesses, and data analytics has enabled organisations to understand and even predict some of the decisions that we might make. Trust today revolves more and more around your openness about how you hold and use the data about your customers, employees, members or stakeholders.

Based on our customer experience research for the Consumer Data Right implementation, the 'gold standard' goes well beyond communication about holding and usage of this data. Demonstrating how your holding and use of data generates tangible benefits for the customer, employee, member or stakeholder is todays leading practice.

The concept of consent is a key thread here — does the employee consent to the data held about them being used to do this or that? Does the customer and member consent to this use or that disclosure? Consent, we have seen, is the key to trust in this new-normal world we live in.

The opportunity before us individually and collectively is to maximise the value of data flowing through our economy — and to do that, we must manage the risks and realise the opportunities through the application of effective governance.

Under the glare of increasing transparency, and highly informed stakeholders, our stewardship of data is as important to our brands as the value that we work to derive from it

Content

Research aim and process

This collaboration between the Governance Institute and CSIRO is aimed at better understanding the implications of the shifts occurring in the consumer data landscape. This understanding will better place corporate Australia in being more resilient in facing the impacts of having to innovate and adapt to the increasing risk and value of consumer data. The objective for this research is to understand the perceptions and opinions held by governance professionals for the risks, values, Data Governance and risk management of consumer data. This initial report is intended to serve as a catalyst to an ongoing dialogue about the implications of these changes.

Process

Step 1

In September and October 2019 invitations to participate in the survey were distributed through the Governance Institute's mailing list of approximately forty thousand email addresses who have subscribed to receive messages from the Governance Institute's. 117 participants completed the survey, taking on average nine minutes to do so. The participants provided insights into the risks related to consumer data, its value, relevant organisational accountabilities and responsibilities, and the capabilities of their organisations to manage data as an asset. Free text fields captured open-ended responses.

Step 2

The initial survey insights were outlined across most capital cities during a roadshow. At this point, invitations were offered to Governance Institute subscribers for qualitative interviews. A digital-ethnographist conducted nine semi-structured interviews with senior and experienced professionals from amongst the Governance Institute's email subscribers between October 2019 and January 2020. The insights gained from the survey was used to shape the interviews.

Step 3

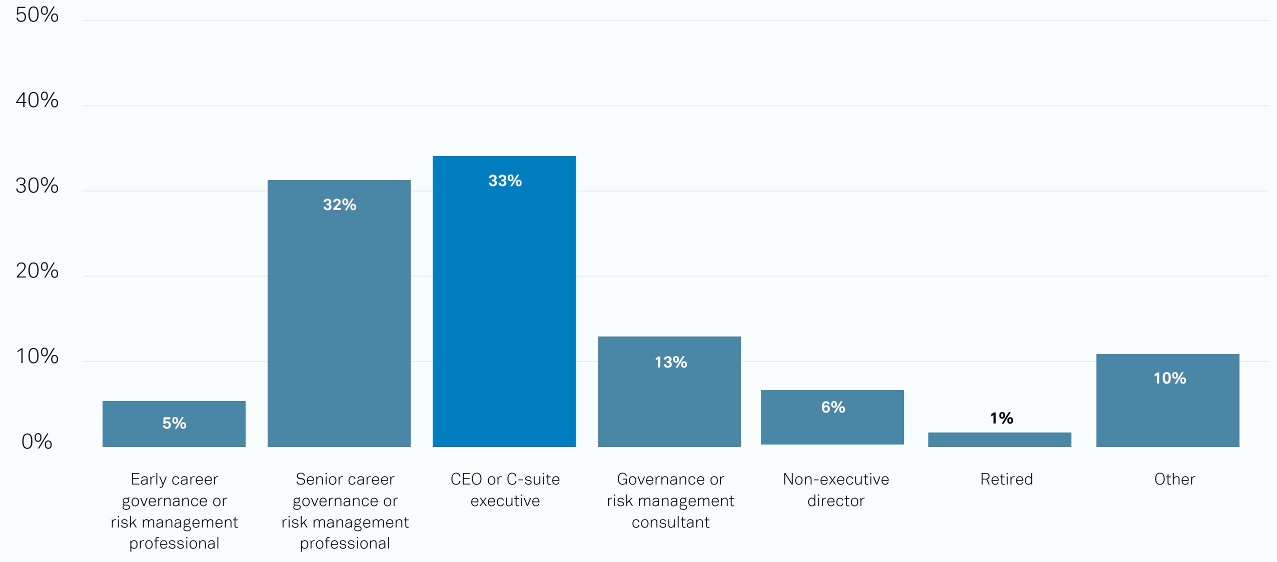
The results of the first two steps were analysed against a backdrop of a transdisciplinary literature review that considered the professional, academic and policy discourses related to data, privacy and trust. This analysis was shared and further developed amongst a transdisciplinary team of researchers.

> Trust, specifically data trust, is poorly understood… Without this deep understanding it's extremely challenging to develop a clear perspective about the type of future they want to contribute to designing. This stuff needs to become one of the highest order values for modern information businesses... There's a heap of existing and emerging research out there to support [this].
>
> **Digital Trust Survey Participant**

Snapshots about the online survey participants

Note: Percentages in survey graphs in this report have been rounded up.

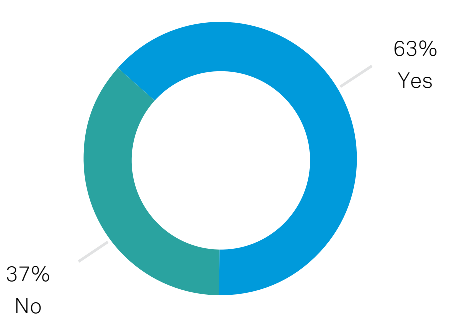
Where would you currently consider yourself in your career?



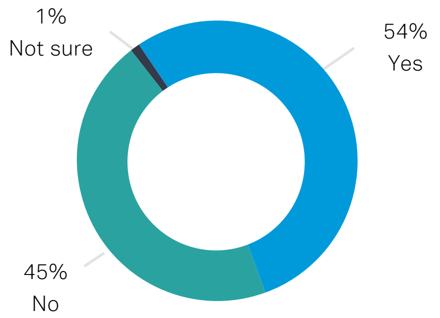
The majority of survey respondents were governance or risk management professionals (including both early career and senior professionals, and consultants of all levels) followed by C-suite executives. The interviewees were senior members who self-selected from amongst this same community, however they generally self-identified as having opinions, experience or expertise with regard to Data Governance, and/or cybersecurity.

Over a third of survey respondents were from the professional services sector, with the remainder mainly consisting of roughly equal shares from energy and utilities; health care; education; followed by a long tail from the remaining sectors.

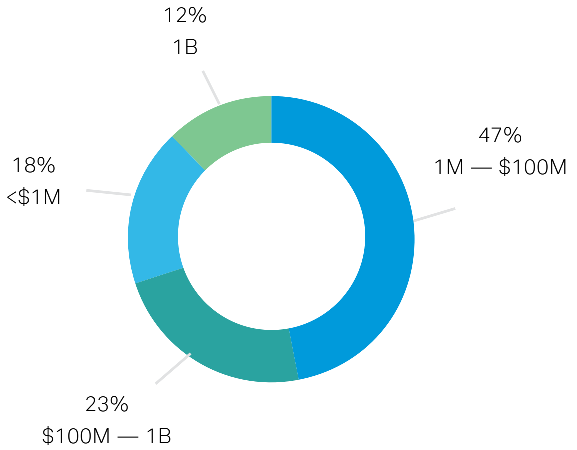
Are you a Governance Institute of Australia member?



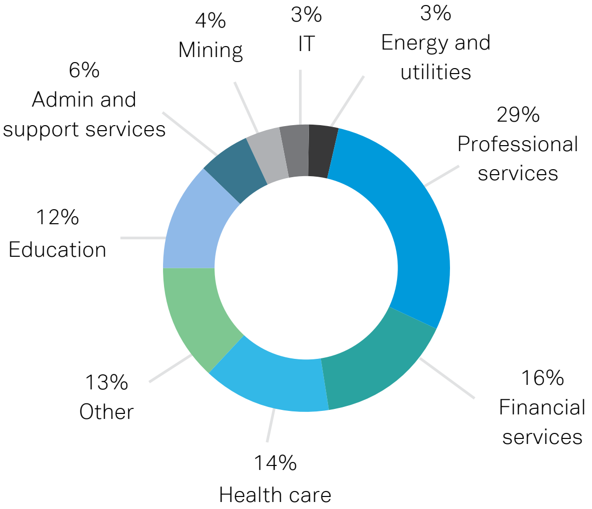
Do you have a Governance Institute of Australia formal accreditation?



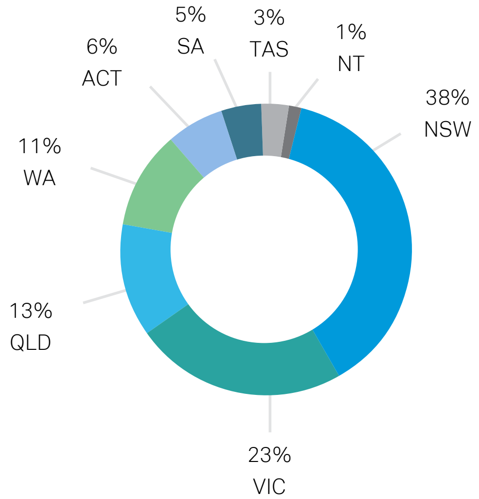
What is your organisation's annual revenue ($AUD)?



What sector do you work in?



Which state are you based in?



There was no statistical difference between the responses from members or non-members, nor was there statistical differences between accredited and non-accredited members.

Survey findings

Theme 1: The valuation of data is contextual

The opportunities and value of data are highly contextual, making its valuation complex. Appreciating the value of data provides a useful context for considering the management of its risks. The value of data, however, changes over time, and the quantum of risk is also circumstantial because different organisations and stakeholders attribute different meaning to the data. Their awareness and understanding of what is possible is altered by their experience and exposure to events.

Interviewees pointed to the challenges of data valuation, often recounting stories of organisations learning its sensitivity and value through an eventful experience. An interviewee involved in the fintech sector stated that larger companies are not always aware of the value of their data and 'tend to want to hoard as much data as they can without really understanding what they'll do with it.'

> **Trust is the number one currency for an organisation.**
>
> Principal Consultant

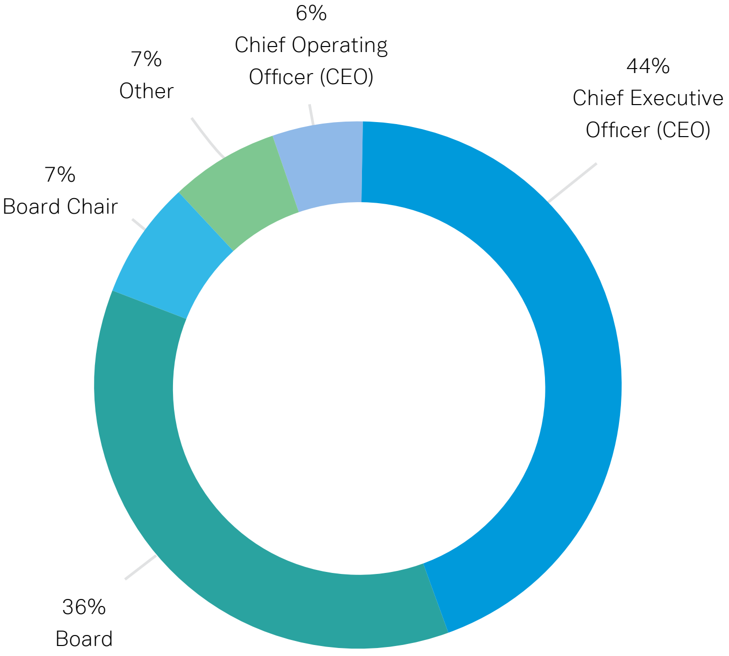
> **If we only ask our customers for data that they trust us with, then we're more likely to have a smooth interaction with them.**
>
> Company Director

'Landmines in the server room'

In one example provided by an interviewee, a company only discovered that their real-world consumer policies were not being appropriately reflected in their legacy systems after they upgraded the entire system. Consequently, the extrapolation was made that data quality is a significant business requirement, and ongoing Data Governance matter. Data decisions made years or decades before may quietly amplify into material issues, despite seeming of inconsequential risk or value at the time of the decision.

In order to assist the process of valuing data, recent research projects[4] have worked towards providing mental models to aid decision makers. Understanding and appreciating different stakeholder perspectives enables decision makers to better engage with the relevant threats and opportunities, especially when applying change management to consumer data. More specifically because, the mishandling and loss of data presents an emerging reputational risk that may materially impact a brand.[5]

Who is accountable for trust with your brand?



Positions identified under other:

- General Manager
- All Partners and staff
- Policy & Governance Manager
- Board & staff
- Managing Partner
- All of the above
- Franchisor
- Everyone / all

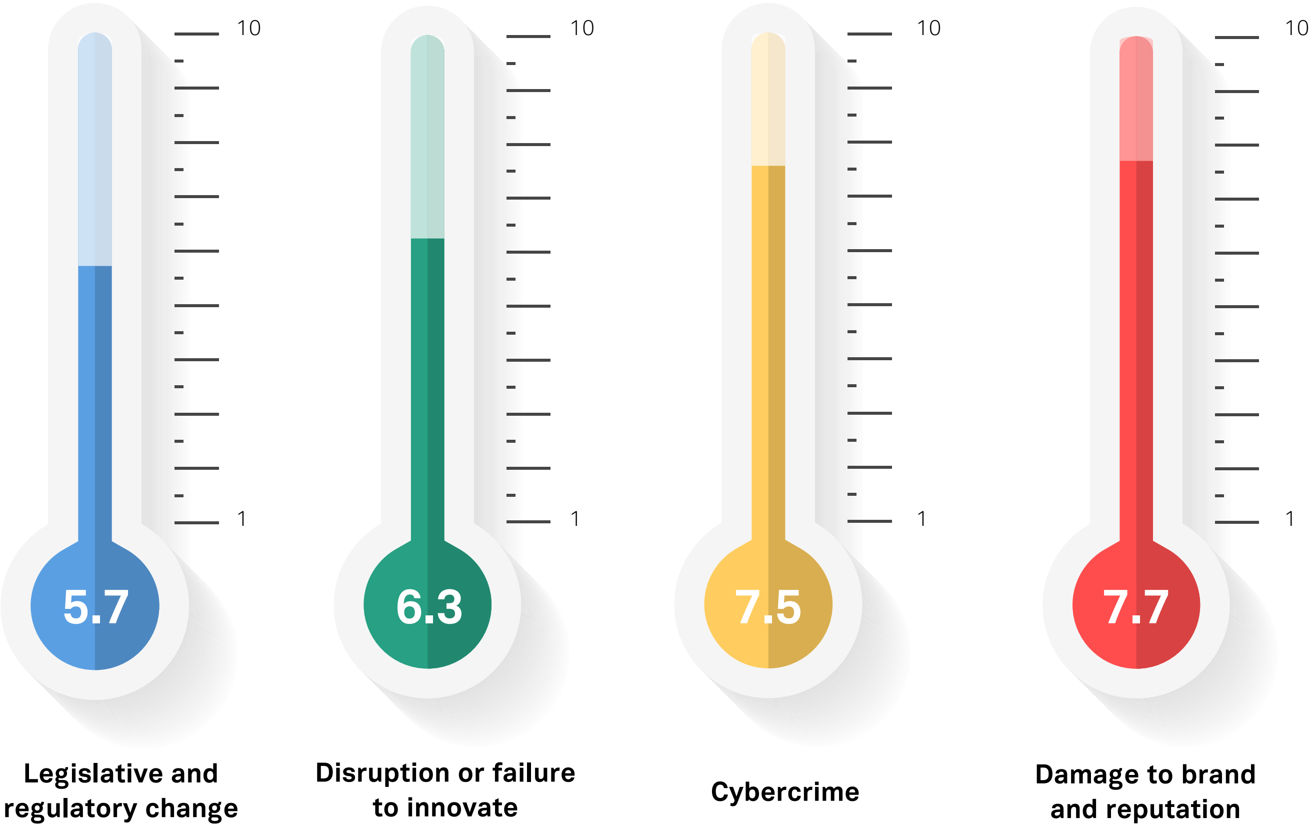
[4] Coyle D, Diepeveen S, Widowin J, Kay L, Tennison J, 2020, The Value of Data: Summary Report, Bennett Institute for Public Policy, Cambridge.
Widowin J, Diepeveen S, 2020, The Value of Data: Literature Review, Bennett Institute for Public Policy, Cambridge.
Coyle D, Diepeveen S, Widowin J, Kay L, Tennison J, 2020, The Value of Data: Policy Implications, Bennett Institute for Public Policy, Cambridge.

[5] Newton N, Statt N, Zelenkoo M, 2017, ‘The Verge Tech Survey, How American’s really feel about Facebook, Apple, and more’, The Verge www.theverge.com/2017/10/27/16550640/verge-tech-survey-amazon-facebook-google-twitter-popularity, online accessed 23 July 2020.

The accountability for trust with a brand includes the added complication that consumer data presents a reputational risk. In the online survey, the majority of respondents placed damage to brand or reputation as the highest potential impact of the four consumer data risks presented below. Perhaps this is not surprising as reputational risk is considered the '*risk of risks*'.[6]

A primary enabler for managing reputational risk has long been recognised as identifying it as a distinct category of risk and giving an individual unambiguous responsibilities for managing it.[7] The challenge now is to connect the governance of data and the governance of reputation with a chain of responsibility.

How would you prioritise the potential impact of these four issues with respect to consumer data?

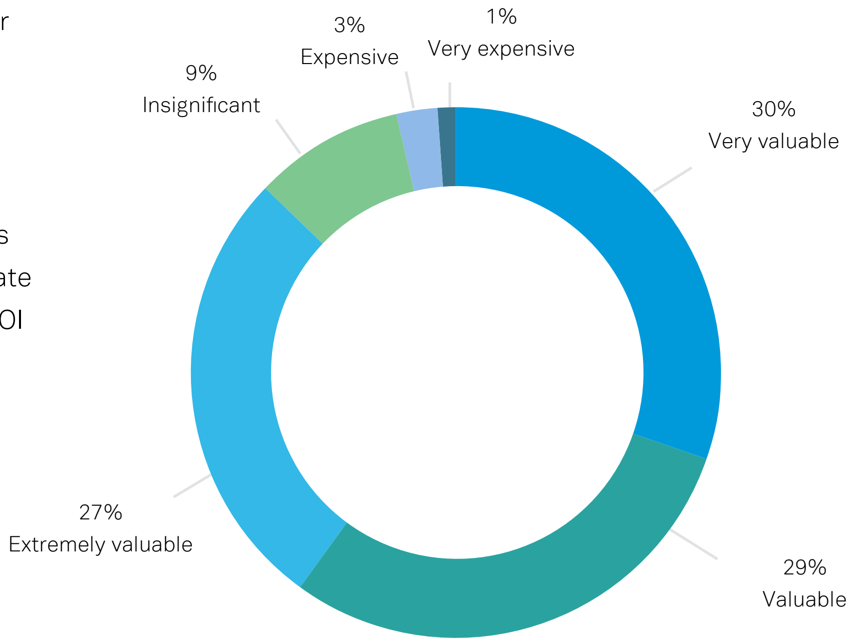


[6] The Economist Intelligence Unit 2005, *Reputation: Risk of risks*.

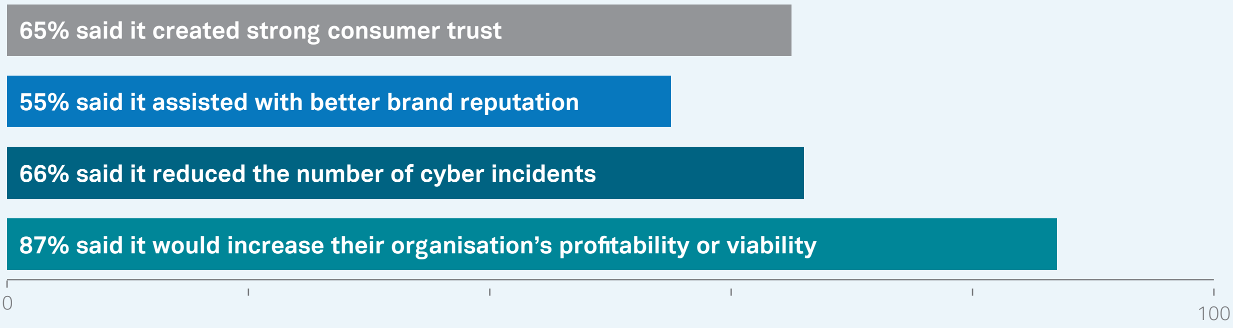
[7] Eccles R G, Newquist S C, Schatz R, 2007, 'Reputation and its Risks', *Harvard Business Review*.

Participants most often assessed consumer data as Very Valuable, with over 87% claiming consumer data ranged between Valuable and Extremely Valuable. Only a small minority claimed their consumer data was Expensive or Very Expensive. The question was designed specifically to necessitate that participants evaluate their ROI for consumer data.

Value of consumer data



In a 2018 survey,[8] North America enterprises reported that when it came to the benefits of a successful cybersecurity culture:



Just over 40 per cent of these North American enterprises reported 'executive champions speaking up for security' was a primary factor empowering a strong cybersecurity culture, and the primary inhibiting factor, according to just under a third of respondents, being 'a lack of senior buy-in or understanding'.

The logical extension of all this is that the Senior Executive accountable for managing reputational risk must empower technology leaders responsible for cybersecurity (including culture), in order to promote trust and enable effective Data Governance.

[8] ISACA and CMMI Institute, 2018, 'The Business Impacts of Cybersecurity Culture'

Theme 2: Assessments of Data Governance capability and maturity are subjective

The Data Governance challenge is in finding the optimal balance of risk and resource management for target capability maturity states. Services offering capability maturity baselines have become industrialised over the last couple of decades. Organisations such as the Capability Maturity Model Integration (CMMI) Institute provide capability baselining services and a Data Management Maturity (DMM) Model[9] to assist organisations in assessing their Data Governance capability and maturity.

Depending on the sector and the region, industry capability maturity averages and best-practice are often reported to be realistic at levels between 2-3 out of 5. Public versions of similar assessments for Commonwealth agencies in Australia, using the Portfolio, Programme and Project Management Maturity Model (P3M3) methodology, similarly demonstrate average current maturity states of 2–3 out of 5.[10]

According to a 2018 survey,[11] ninety-five per cent of North America enterprises reported there was a gap between their organisation's desired and actual culture of cybersecurity.[12] Cybersecurity unpins Data Governance, and this stated gap suggests they considered their current capability maturity states of Data Management to be below their target / desired states. This finding appears in contrast to the highly assessed maturity states found in the Digital Trust survey.

Self-reported assessments received in the Digital Trust survey appeared to deviate from the previously mentioned capability maturity baselines. The majority of survey results tended to fall across 3–4 out of 5, additionally there were much higher instances of assessments of 4–5 out of 5 than would be expected from the previous examples. The authors acknowledge, however, the main limitations of this study are based in the relatively small sample size of the participants, as well as the subjective nature of the answers provided by the self-selecting participants. Given the limitations of the study, the result could indicate that the participants completing the survey were perhaps somewhat removed from the technology functions, which would plausibly skew the results. This may suggest a disconnect in the perceptions of the respective capabilities by the respective functions. This scenario was further explored in the interviews.

Future research would harness existing and emerging capability assessment maturity methodologies in order to provide more objective capability maturity assessments. We hope future research activities will attract more engagement from corporate Australia.

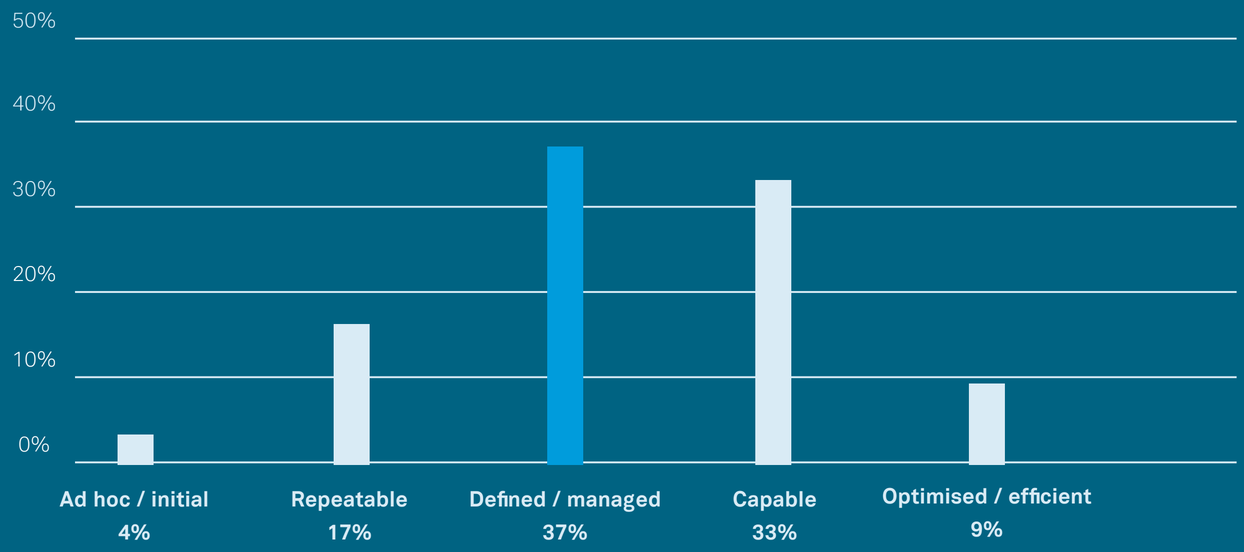
[9] DMM Model At-A-Glance cmmiinstitute.com/resource-files/public/dmm-model-at-a-glance, online accessed 23 July 2020.

[10] Young R, Young M, Zapat JR, 2011, 'A Critical Assessment of P3M3 in Australian Federal Government Agencies, Project, Programme and Portfolio Maturity Levels October 2011', University of Canberra, ANZSOG Institute for Governance.

[11] ISACA and CMMI Institute, 2018, 'The Business Impacts of Cybersecurity Culture'.

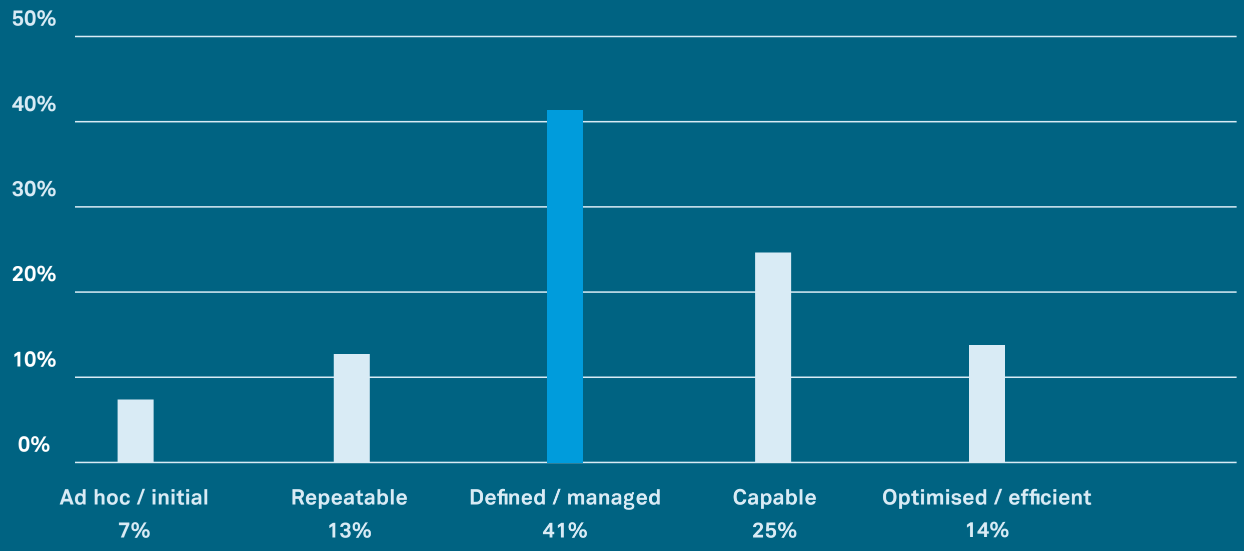
[12] Ibid.

Data Strategy maturity

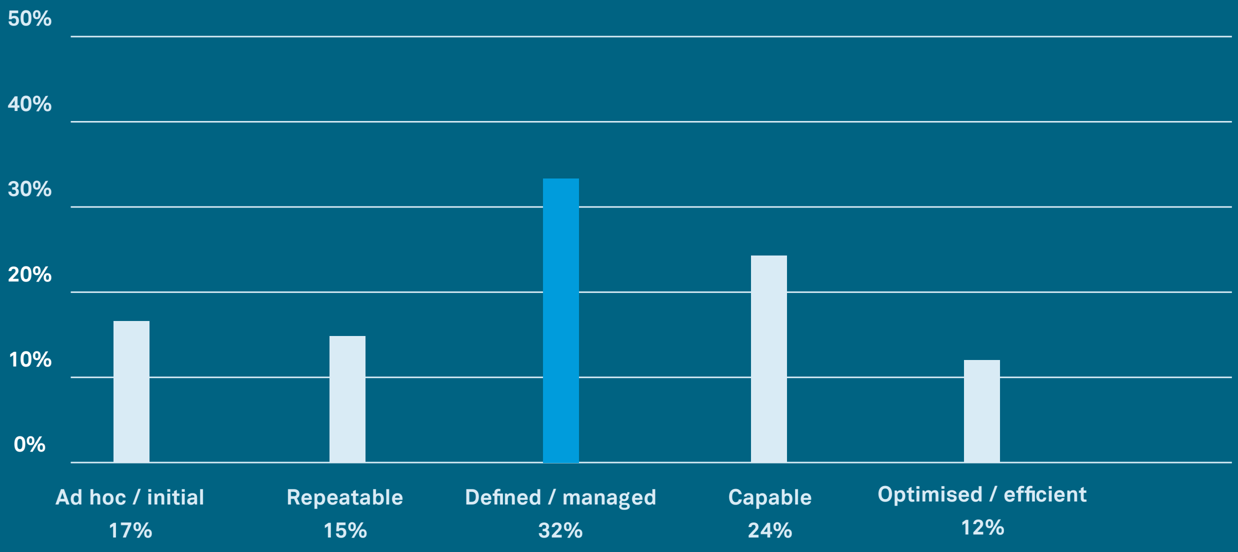


Organisations reporting a Data Governance Strategy were more likely to also report that consumer data was integral to their organisation's current and longer-term strategy/business model. Those organisations with a Data Governance Strategy were also more likely to report higher confidence in their ability to handle and share consumer data appropriately.

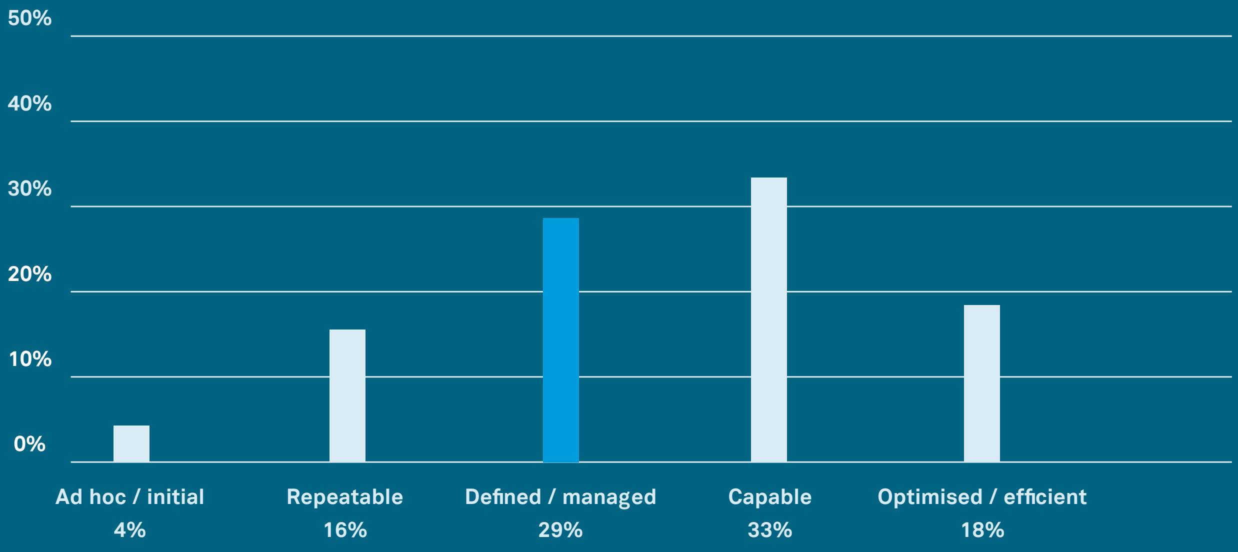
How well does your organisation manage the disclosure of consumer data (including derived data)?



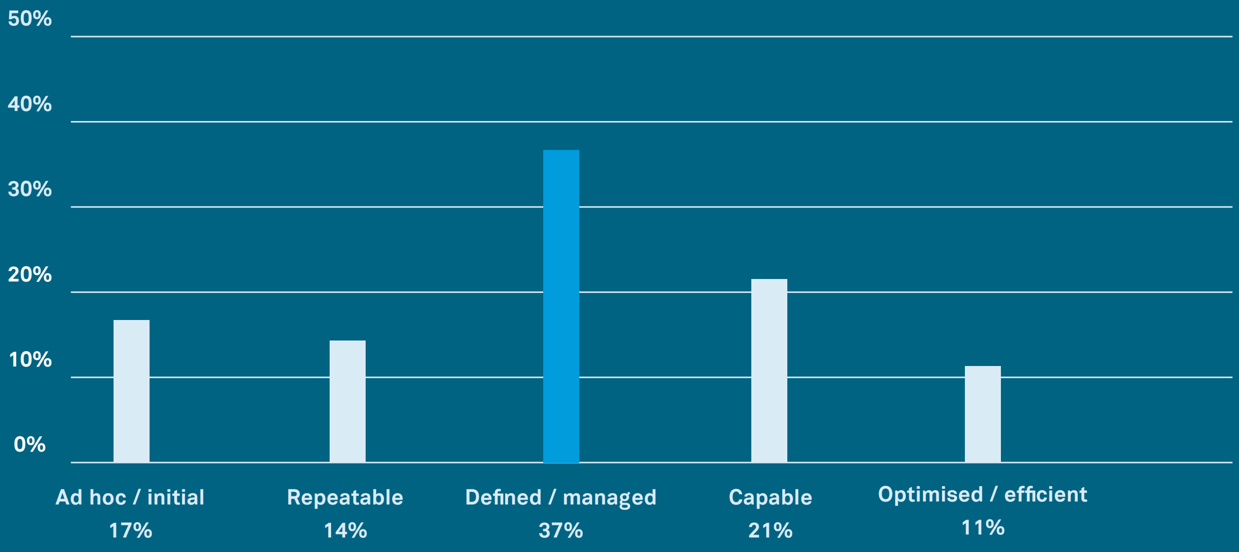
How well does your organisation manage the de-identification of consumer data?



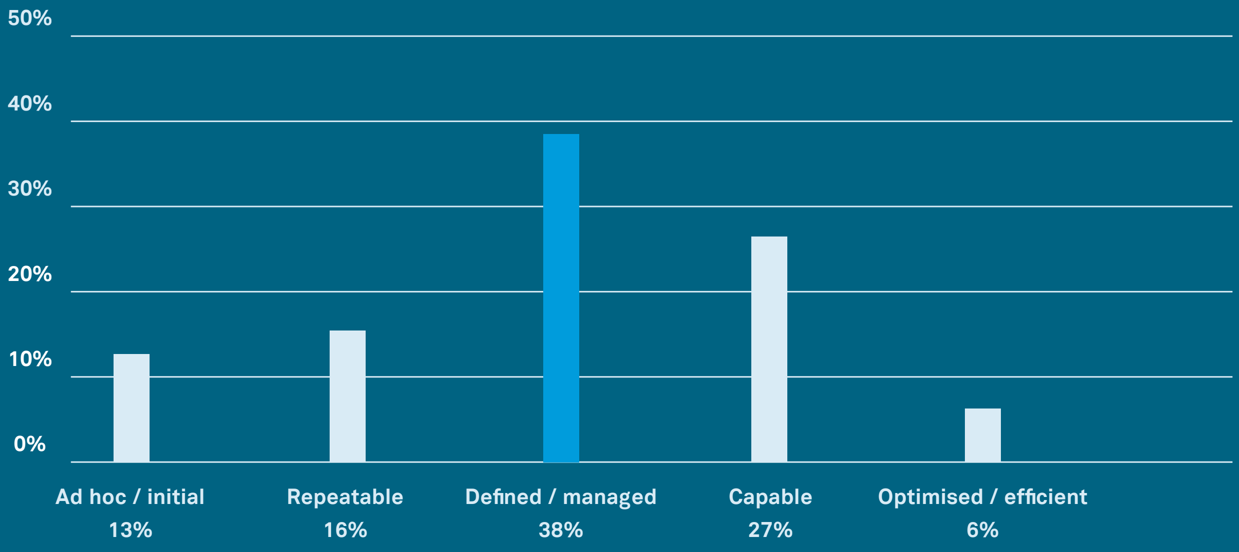
How well does your organisation manage the storage of consumer data?



How well does your organisation manage the deletion of consumer data?



How well does your organisation manage consumer data as an asset?



Theme 3: There is a disconnect between IT and business leaders

Our interview participants confirmed that there was a disconnect between the IT and business leaders. They described it in several ways:

- Those in technical positions felt problems are most likely to arise from **management not adequately identifying digital trust-related risks** and communicating risks with the board, or downgrading the risks because of potential cost issues. In some cases, clear Data Governance directions from the board were not effectively translating down into the organisation either. Interviewees identified the organisational challenges of boards receiving adequate assurances for Data Governance, including:
  - integrating Data Governance into new strategies and business models
  - assessing and communicating risk
  - providing appropriate visibility and reporting.
- The relative Data Governance competencies of directors and executives were suggested to be inconsistent across corporates, and sometimes within corporates. A consistent view was provided that **an appreciation for Data Governance is needed at all levels**, all the way through the Data Governance chain, including the board. Ownership and clarity of responsibilities along this chain where seen as amongst the most important conversations in establishing this capability.

> **Innovation is important but not as important as people's privacy and personal data. This must not be compromised. Until technology and the law catches up, digital innovation is losing the trust of consumers and will be at risk of failing.**
>
> Financial Services Director

- All interviewees agreed that **consumers have become more sensitive to how their data is used**. Although, some pointed out that consumers are contradictory and will use services despite the risks (privacy paradox), and there was a suggestion from some that the benefits consumers receive outweigh privacy concerns. Concerns were also raised over how the media may be negatively influencing consumer sentiment on Data Safety, which may impact Australia's ability to embrace innovation.
- Interviewees considered that organisations should get ahead of the Data Governance issues rather than simply complying with the law, especially as consumers might feel differently in the future. There was a view that organisations generally rely on regulations, although many survey respondents were sceptical about legislative and regulatory change, which they believed to be **ineffective and inefficient.**

The following quotes from the survey appeared to agree with and amplify the frustrations expressed with the regulatory environment, and the necessity to engage with it. This theme continued throughout the survey responses and the interviews.

“

The legislative landscape presents challenges and obstacles by ineffective regulation and under-resourced... regulators.

General Counsel

“

Regulatory change, both domestic and international, is evolving. [Consequently, there is an] ongoing requirement to investigate and assess consumer data privacy risks as the business enters new markets and adopts new systems and technologies to interact with clients.

General Manager, Corporate Governance & Risk

“

As governments and regulators ‘catch up’ to the current use/misuse of consumer data, they are likely to enact and enforce even more stringent rules and regulations.

Director

“

I am not sure that the regulators are up to the job.

Digital Trust Survey Participant

The future of the governance professional has been noted by the Governance Institute as a future 'with a different regulatory framework, greater complexity and technology shifts, each occurring at an increasingly rapid rate'.[13] The complexity of the business environment,[14] regulatory changes[15] and technology disruption[16] are all seen by the Governance Institute as key drivers to governance changes in the future.

[13] Governance Institute of Australia, 2019, 'The Future of the Governance Professional' p 5.

[14] Ibid, 48 per cent of respondents indicated environmental complexity was VERY IMPORTANT, and 31 per cent indicated it was VITAL.

[15] Ibid, 49 per cent of respondents indicated regulatory changes are VERY IMPORTANT, and 31 per cent indicated it was VITAL.

[16] Ibid, 49 per cent of respondents indicated technology disruption was VERY IMPORTANT, and 26 per cent indicated it was VITAL.

Theme 4: Consumer data risks are subjective

Organisations which have a Data Governance Strategy were more likely to perceive the risks involved in handling consumer data. In particular, they were significantly more likely to report that mishandling consumer data presents a high risk to their brand and reputation.

When asked about the risks and their rankings associated with consumer data, and 'what is the worst thing that could happen to consumer data?', there was, however, two main types of answers. One answer related to what could happen to the data, generally including descriptions of cybersecurity threats such as hacking or data breaches. The other answer provided much more detailed descriptions of the impact of those events, generally as part of a more well-articulated risk statement.

These descriptions appeared to build upon our theme of disconnection.

> **Australia needs to understand the changing risk appetite in relation to data as it pertains to our younger citizens. This needs to be supported by safe innovation**
>
> Financial Services Executive

'The break-down of cyber risk'

According to the international standard ISO 31000, risk is defined as, 'the effect of uncertainty on objectives'. Often this is articulated as an expression of likelihood and consequence. Professional bodies, such as the Institute of Internal Auditors,[17] describe risk using the following formula:

Risk = Threat x Vulnerability x Asset

Because of the threat of cyber criminals, and the value of consumer data being respectively reported as material, and increasingly so, the logical extension is that the protection of consumer data needs to be significant in order to appropriately manage the risk. Consequently, the controls that protect these vulnerabilities must not only be proportionate with the cybersecurity threat, but must keep pace with it, and be seen to be keeping pace with it, by all relevant stakeholders in order to be effective.

[17] Global Technology Audit Guide (GTAG), The IIA.

The threat

> There is **always a high level of risk from cyber criminals** — doesn't matter what sort of company you have and what sort of data you hold.

Company Secretary

> Their ability to undertake criminal activity outside national borders and protections, and the data is the new form of currency to hold businesses and people to ransom. These **criminals are 'professionals'** working out how to exploit vulnerabilities.

Chief Risk Officer, Banking and Finance

> **Cyber criminals are more innovative and faster moving than regulators and governments**; they have a strong profit motive, and little concern with ethics or fair practices. Recent media reports show the growing impact and scale of cybercrime.

Director

The impact

> Data stolen and consumers fall victim to identity theft, loss of trust in big organisations that fail to protect consumer data **causing systemic economic problems.**

Chief Risk Officer, Financial Services

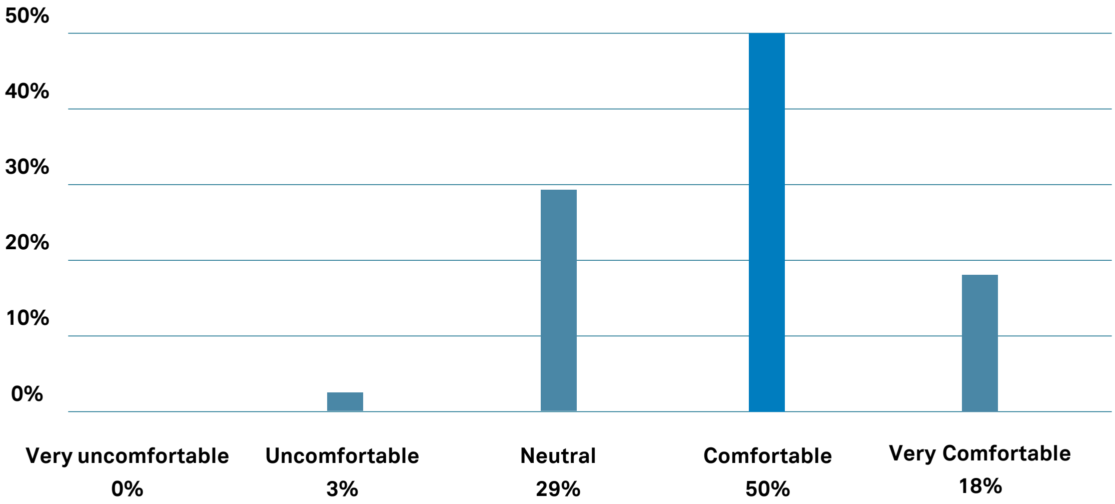
> Arguably **our entire country is at risk** here. If we cannot learn from mistakes and progress elsewhere, established an ambitious shared vision and execute collaboratively, we will be left behind.
>
> The **social, economic, emotional impact** of data leaks, identity theft and other cybercrimes.

Professional Services Director

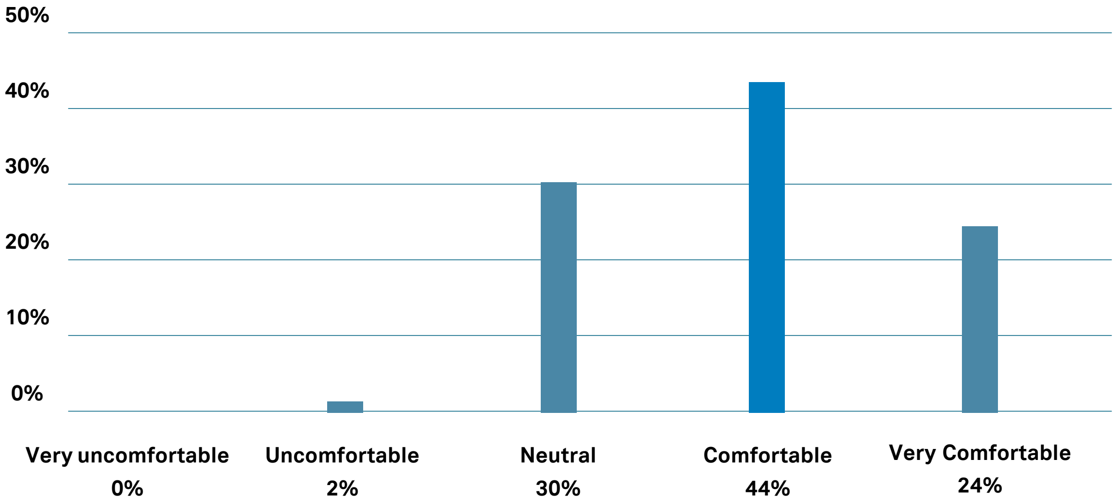
> The Australian Cybersecurity Centre defines the impact of a cybersecurity incident as including: 'direct costs of remediation activities, but also indirect costs such as downtime, lost productivity, and loss of reputation and consumer confidence[18] .
>
> **Trust is easily lost. Just one incident of reckless negligence would be devastating.**

Digital Trust Survey Participant

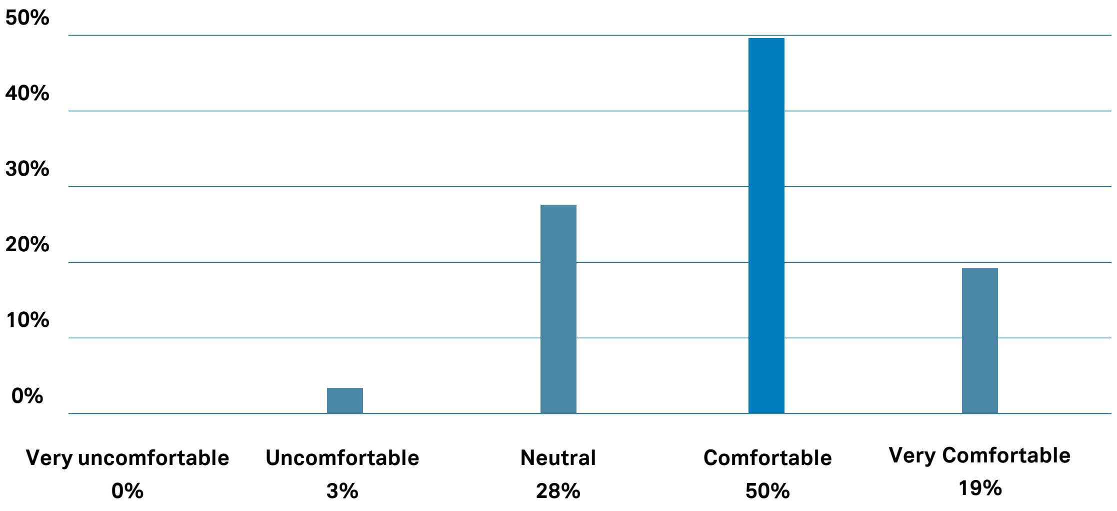
How would shareholders / members feel about how your organisation handles consumer data?



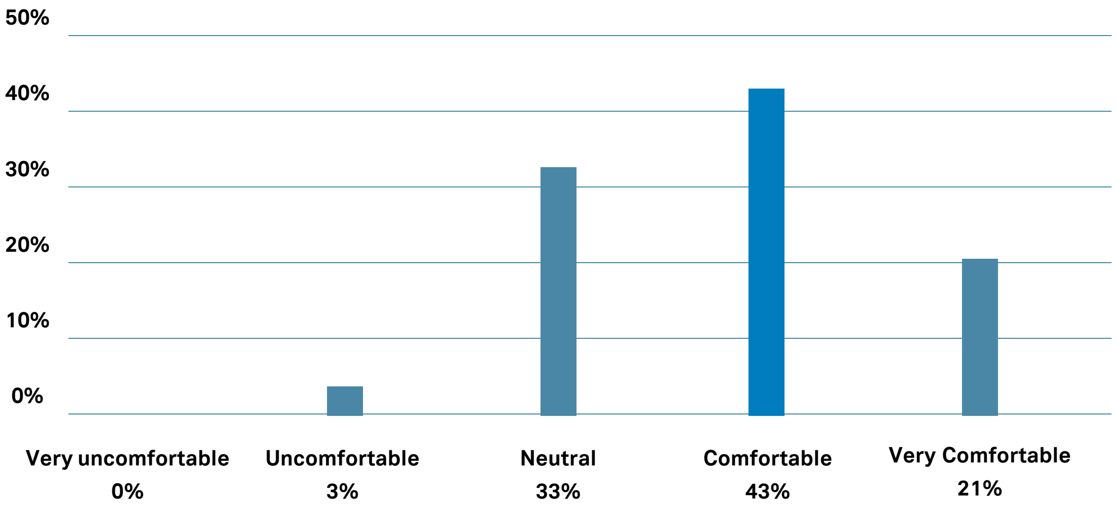
How would shareholders / members feel about who your organisation shares consumer data with?



How would consumers feel about how your organisation handles consumer data?



How would consumers feel about who your organisation shares consumer data with?



What sort of assurances are required in this high-threat environment with sophisticated cyber criminals, where the value of consumer data is increasing valuable, and the impact of its loss or mishandling is therefore increasingly material to the firm?

How do we make sure the controls are, and remain, adequate?

How do we know that consumers are comfortable with these approaches?

Theme 5: Reporting chains of Data Governance are inconsistent

In the survey, business executives were generally perceived as responsible for implementing the strategy for consumer data regardless of the organisation's Data Governance maturity. Organisations in the higher Data Governance maturity group, however, were more likely to report their technology leaders as responsible for managing issues with consumer data. This was the only instance where technology leaders were favoured.

Regardless of the effectiveness and efficiency of who is assigned these responsibilities, the finding was intriguing. There is the possibility that this suggests that when technology leaders are perceived to have enough business acumen and credibility, they are trusted to manage the complexities of these sensitive and significant issues; and that this type of technology leader is more likely to be present in an organisation with a higher Data Governance maturity. The structures of existing and optimal Data Governance chains present an interesting area for additional research.

Tools for measuring Data Governance maturity have been around in various forms for some time.[19] There is a recent emerging change in the landscape, however, with emerging data privacy frameworks providing similar types of maturity assessment tools[20]. Could data privacy regulatory reform initiatives help drive Data Governance maturity, and strengthen reporting chains?

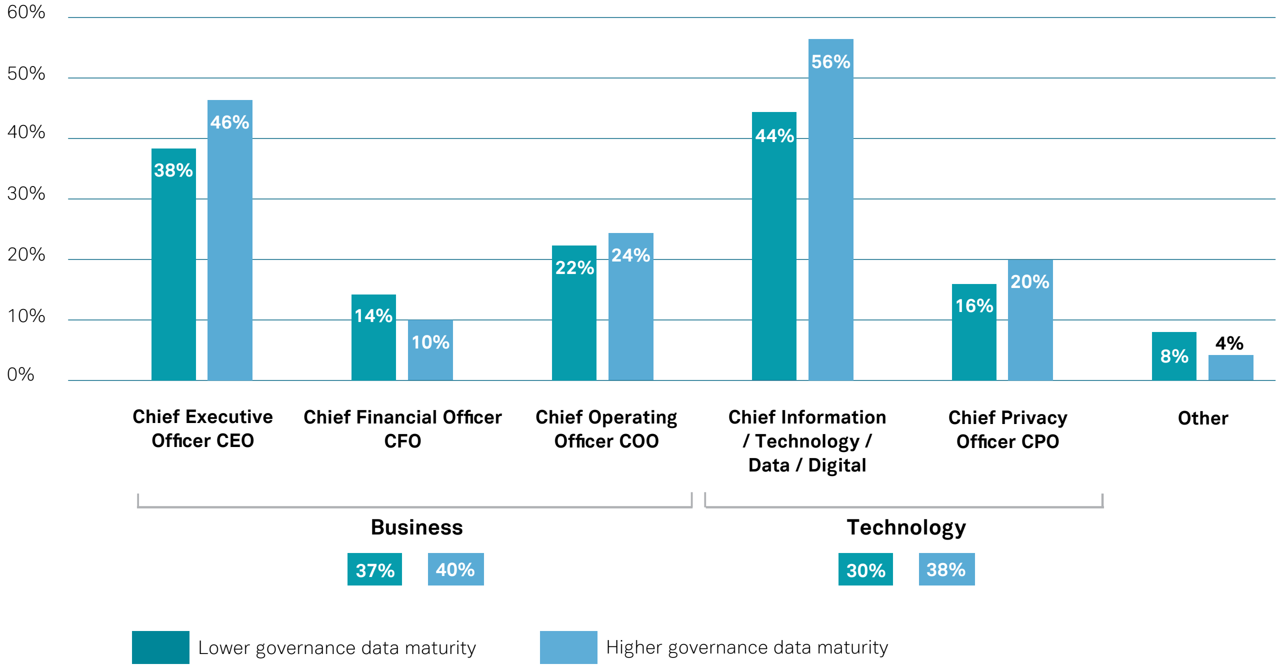
Understanding the identifiers and attributes for a mature Data Governance capability is one thing. However, credible reporting on capability maturity, by logical extension, is challenged in ways described by the interviewees when reporting on digital trust-related risks (Theme 3).

[18] Australian Cybersecurity Centre (ACSC), April 2019, 'What Executives Should Know About Cybersecurity.'

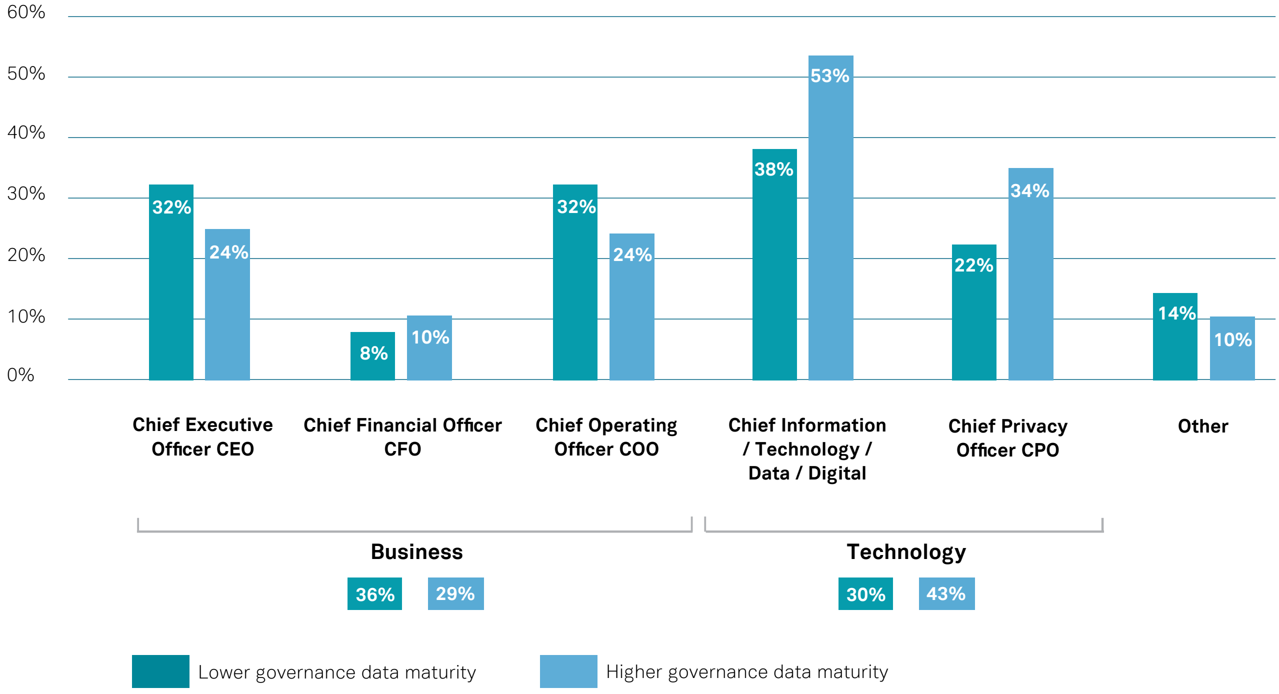
[19] CMMI Institute, Data Management Maturity (DMM) Model.

[20] NIST Privacy Framework, 2020, www.nist.gov/privacy-framework, online accessed 23 July 2020.

Implementing consumer data strategy

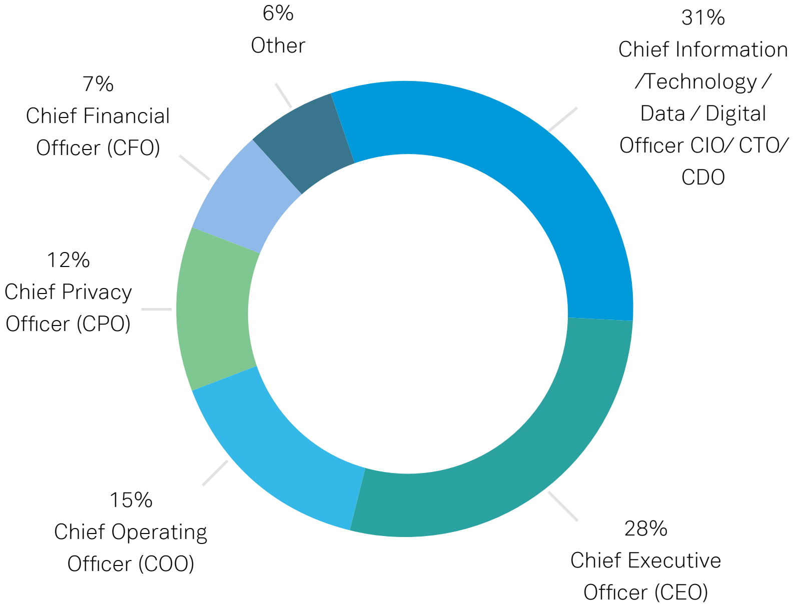


Managing consumer data issues



Please note the roles of Chief Information / Technology / Data / Digital Officers were combined for the purposes of the survey. Although combined technology leadership roles (including the CPO) were reported as holding responsibilities more often than the CEO in all cases, technology leaders were only predominate with responsibilities for managing consumer data issues in the higher maturity Data Governance cohort.

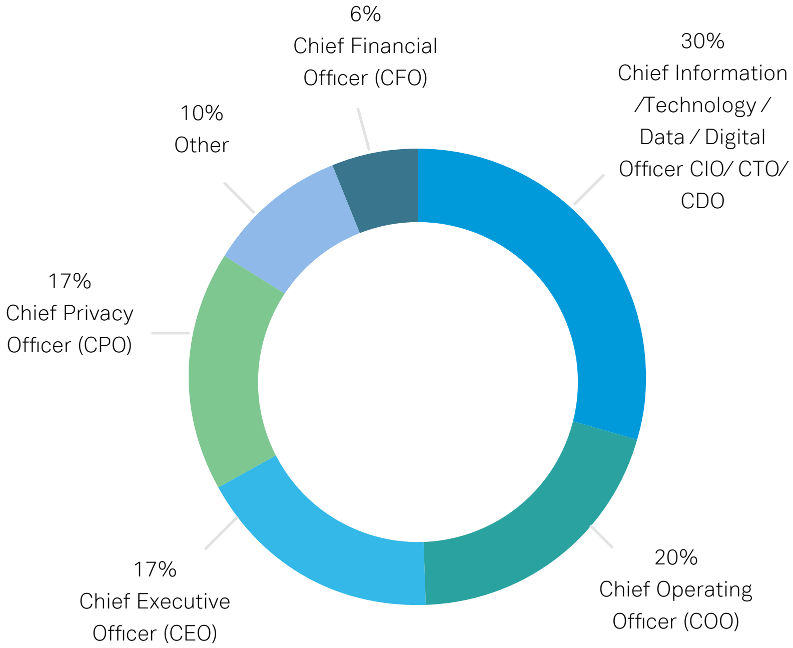
Who is responsible for implementing the strategy for consumer data?



Positions identified under other:

- ISMS Executive
- Administrator
- Director of Category and Consumer Marketing
- Managing Director
- Director (ie, GM) Quality & Innovation
- Policy & Governance Manager
- Managing Partner
- All of the above

Who is responsible for managing issues with consumer data?



Positions identified under other:

- General Counsel
- Director of Category and Consumer Marketing
- Director Quality & Innovation
- Internal Risk Committee
- Risk Manager
- Managing Director
- Technical Services Manager
- Policy & Governance Manager
- Company Secretary
- Managing Partner
- All of the above

Research directions

Participants were not extensively questioned about the environment they found themselves in, or what was on the horizon, other than to indicate why they had made certain assessments with respect to risk, capability or value. In continuing this conversation, future research would investigate further into perceptions about the shifting landscape.

Managing data as an asset

- How is corporate Australia evaluating the value and risk of consumer data?
- What is the capability maturity for corporate Australia's data management?

Data holdings that are unassessed present both a potential source of value, but also an unquantified amount of risk. Appropriate categorisation, classification and lifecycle-management would theoretically enable organisations to undertake appropriate stewardship. The question is, what is Corporate Australia doing, and where are the quick wins and next steps?

Assessing Data Governance

- What are the components of an effective Data Governance Strategy?
- Are traditional IT governance functions considering contemporary Data Governance issues?

A Data Governance Strategy appears to be a heuristic indicating a higher level of Data Governance maturity, but what makes for an effective Data Governance Strategy? What is industry best practice? What are the average respective maturity levels of these Strategies across industries?

Regulatory reform

- Is the contemporary international focus on data privacy assisting with bringing the right people, with the right skills together at the right time for Data Governance?
- What does the map of emerging data privacy requirements look like in Australia?
- How should self-assessments be undertaken, and what roles should be assigned, in these regulatory environments?

The requirements for managing data privacy is evolving globally. What does the emerging landscape look like in Australia, and how does this lay with the international context? What tools are available to assist with compliance, and how are they being adopted?

Interviewees described the challenges in the respective talent pipelines for technology and business leaders, and the resulting lack of staff who are connected to both sides of the organisation. Frameworks such as NIST's Privacy Framework[21], the Trusted Digital Identity Framework (TDIF),[22] and the General Data Privacy Regulation (GDPR),[23] all call for various data privacy roles. Are they assisting organisations to bridge this gap? Is corporate Australia harnessing the opportunities presented by this change?

[21] NIST Privacy Framework, 2020, www.nist.gov/privacy-framework, online accessed 23 July 2020.

[22] The Trusted Digital Identity Framework (TDIF) www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework, online accessed 23 July 2020.

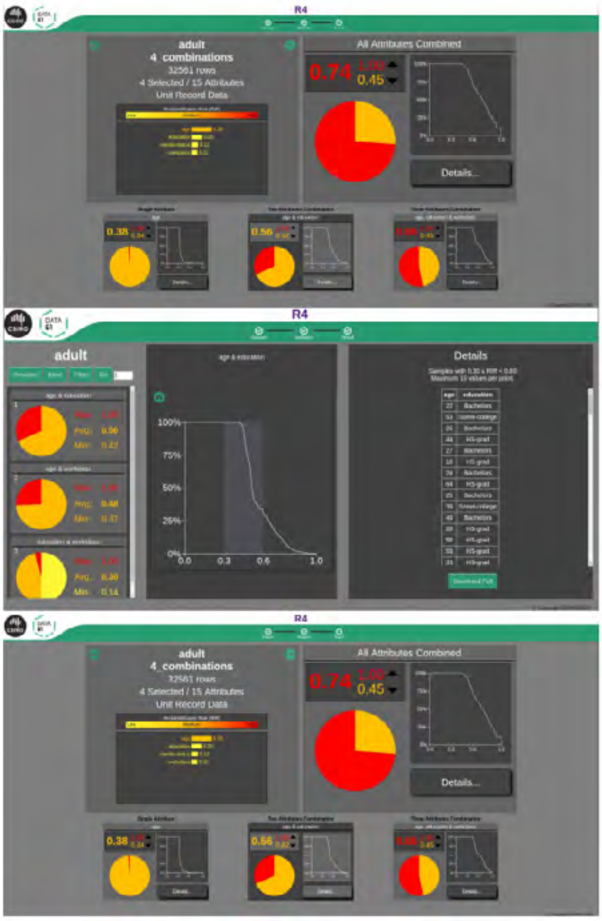
[23] The General Data Privacy Regulation (GDPR), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, online accessed 23 July 2020.

Trust-related research at CSIRO's Data61

Most businesses recognise the existence of privacy and confidentiality risks in collecting, using and sharing consumer data both within and outside their business in order to derive higher added value. There is no consistent and repeatable methodology or related tool, however, for a company to confidently measure and understand the level of such risks in its consumer data. Some ad-hoc guidelines propose qualitative methods exist to estimate these risks, but lack the quantitative tools to measure them. To efficiently control a risk, it first needs to be objectively measured.

The Information Security and Privacy group at CSIRO's Data61 has designed quantitative and qualitative privacy risk methodologies with appropriate formal metrics and assessment frameworks to understand the risks associated with sharing or releasing data within, or across businesses. These tools leverage scientific knowledge to provide accurate estimation of the residual risks associated with the sharing of sensitive data.

For example, one of our metrics allow the measurement of reidentification risks for an individual, event, or transaction. Another one of our metrics quantifies the risk of deducing non-reported values in aggregated data. Our assessment frameworks utilise these metrics to substantiate threat scenarios and provide comprehensive studies of risks.



We have developed software, such as our Re-identification Risk Ready Reckoner (R4), which implement these metrics and methodologies. R4 generates quantifiable risk assessments that display on a working dashboard to data custodians. It further provides data treatment options to help mitigate and re-assesses the risk in the treated data.

How Governance Institute can help you

Governance Institute of Australia oversees a strong program of thought leadership — publications, studies, and key analysis and research — to help advance the governance and risk profession as they grow in their roles from skilled individuals to innovative leaders.

With governance and risk issues in the spotlight like never before, we continue to add to and further the national discussion through the promotion of our thought leadership and guidance. This is a key focus for our policy and advocacy team, as our thought leadership initiatives tackle current and evolving issues. We ensure that the projects are relevant to our members, expertly informed and based on extensive and sound research and data.

Equipped with our expert thought leadership publications, we continue to proactively engage with the government, regulators, and peak organisations on behalf of our 7,500 members and broader network of over 38,000 company secretaries, governance leaders and risk managers.

Governance Institute of Australia