



**SUBMISSION**  
**Cybersecurity Strategy**  
**Discussion Paper**


14 APRIL 2023


**Real Estate Institute of Australia**


PO Box 234


DEAKIN WEST ACT 2600

Ph: 02 6282 4277

 @REIANational

 @REIAustralia

 @reiaustralia

 Real Estate Institute of Australia

## REIA Comments on the 2023 Cyber Security Strategy Discussion Paper

Thank you for the opportunity to contribute to the 2023-2030 Australian Cyber Security Strategy (the Strategy) and the 2023 Cyber Security Strategy Discussion Paper (the Discussion Paper).

The Real Estate Institute of Australia (REIA) is the professional body for Australia's real estate sector and was established in 1924.

Today, REIA represents real estate practitioners and agencies through our work across policy and political action, media advocacy, market research and evidence, industry excellence and national leadership and networks.

Real estate is the backbone of Australia's economy and businesses sector, as agencies represent 46,793 Australian businesses, 99 percent of which are small businesses.

Agencies employ 130,000 Australians and the Australian property industry is worth \$300 billion to the Australian economy as a measure of GDP.

### Cyber security is a front of mind issue for real estate businesses

Cybersecurity in Australian real estate businesses is a growing economic and reputational threat. This has always been the case with awareness heightened with high profile businesses like Optus and Medibank being hacked in October 2022.

In a survey conducted to our membership – representing over 85% of Australian real estate businesses – in December 2022, cybersecurity ranked third of 27 total key business issues identified.<sup>1</sup>

Deeper insights research show that 78% of real estate business owners continue to be concerned by the threat of cyber-attacks with real estate companies of all sizes suffering over the past 12 months at an average cost of \$33,442 to medium sized enterprises. At the same time, 30% of agencies surveyed nominated issues relating to data privacy and security as a barrier to implementing new technology.<sup>2</sup>

Suffice to say cybersecurity is a front of mind issue for the real estate business sector. Real estate is a relatively unique sector as it's a large segment of the Australian economy servicing nearly all Australians almost exclusively by small businesses.

To put this in perspective, there are 44,000 Australian real estate agencies Australia wide with 99% of these being small businesses.

At the same time our consumer base is considerable, with our outreach estimated to be:

- 6.9 million Australians helped into home ownership or rentals each year.
- \$350 billion in home sales settled the last recorded financial period.
- \$78 billion in rent receipts collected annually.
- \$3 trillion in rental assets under management.

---

<sup>1</sup> Source: REIA Evaluation Survey 2022. Internal Document.

<sup>2</sup> Source: Optus Business – Real Estate Industry Pulse 2022. Available: [Optus Business Real Estate Industry Pulse 2022 - Optus](#)

- Combined residential real estate asset value of \$9.3 trillion.
- Combined commercial real estate asset value of around \$1 trillion.

Be it home sales, residential or commercial rents or large scale commercial and residential transactions real estate businesses have both a large financial role; as well as a very substantial Personal Protected Information (PPI) role across buyers, sellers, tenants, investors, and any other parties to a deal.

As an industry we recognize more needs to be done to in relation to cybersecurity and that an ongoing way of working needs to be established within the real estate workforce, so cybersecurity is 'everyone's responsibility.'

It is our pleasure to provide some initial commentary to the Expert Advisory Panel (the Panel) on the 2023-2030 Australian Cyber Security Strategy against some applicable questions posed by the Cyber Security Strategy Discussion Paper Questions.

Please note our comments are made in relation to those Discussion Question relating to our business sector over those of national security.

### Specific responses to discussion questions

1. **What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?**

As outlined above, given the unique challenges of cybersecurity threats specific to the Australian real estate industry, REIA would like a sector specific strategy for real estate which includes an industry wide adoption and capability plan funded and rolled out on a national scale.

This would benefit consumers, businesses, and regulators.

2. **What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?**

REIA recommends rather than focussing on regulatory frameworks and reform that working with the real estate business sector on **adoption** and **establishing an ongoing way of working** across our workforce would be a better use of the resources of the strategy.

Cyber threats and cybersecurity capability will by nature evolve, in some instances minute by minute. The slow process of law-making process in Australia should not be seen as the desirable first line of protection.

REIA would like to highlight to the Panel the current parallel processes being pursued by the Australian Government that provides contradictory messages and confusing signals in relation to cybersecurity, financial transactions, and PPI:

- The Privacy Act Review Report which could see small businesses with a turnover of \$700,000 or less on the line for millions of dollars in penalties for breaches.<sup>3</sup>
- The proposed but to be disclosed process in relation to Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime which could require real estate businesses to become a quasi-workforce for AUSTRAC and the

---

<sup>3</sup> Source. REIA. Available: [Submission \(reia.com.au\)](https://reia.com.au)

Australian Federal Policy<sup>4</sup>. If a model, for example, from New Zealand was applied this would require agencies to handover large tranches of financial information and PPI direct to authorities and be another major cybersecurity vulnerability for our sector.

**c. Should the obligations of company directors specifically address cyber security risks and consequences?**

REIA opposes this responsibility being assigned legally to Directors and argues that the Strategy should focus on a 'cybersecurity being everyone's business' approach rather than top-down regulation.

**d. Should Australia consider a Cyber Security Act, and what should this include?**

As above.

**e. How should Government seek to monitor the regulatory burden on businesses because of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?**

It is recommended that an annual regulatory impact report is funded and produced by the Strategy that outlines sector-by-sector impacts, particularly on small businesses.

In addition, no laws or reform processes should proceed without a regulatory impact analysis on business.

**7. What can government do to improve information sharing with industry on cyber threats?**

It is REIA's observation that current Australian Government engagement in relation to cybersecurity appears for the most to be limited to the 'big business' sector and highly corporatized sectors.

It is recommended that a Cybersecurity Small Business Stewardship Group is established immediately that meets monthly/ quarterly and on as needed basis to disseminate key confidential, as well as public good industry wide information.

Membership of this forum should be limited to national bodies that have extensive outreach back to industries that suffer from cybersecurity vulnerabilities.

The Modus Operandi does not need to be complex and can be borrowed from the long standing and effective Small Business Stewardship Group managed by the ATO.<sup>5</sup>

**8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?**

---

<sup>4</sup> Source. Australian Financial Review. Available: <https://www.afr.com/politics/federal/labor-considering-tougher-anti-money-laundering-laws-20230412-p5czss>

<sup>5</sup> Source: ATO. [Small Business Stewardship Group | Australian Taxation Office \(ato.gov.au\)](https://ato.gov.au/Small-Business-Stewardship-Group)

Yes.

**11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?**

Yes. The nine industry Jobs and Skills Councils need to be engaged and funded to develop skills plans, including roll out plans, for their respective sectors.<sup>6</sup>

This should be funded by the Strategy.

**12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?**

To establish an ongoing way of working across all of Australia's workforce and make cybersecurity everyone's business, accessible and available micro-credentials should be made available. This should extend from the tertiary system through to the VET sector.

Cybersecurity is not simply the issue of an IT department or 'person', and our collective capability will only be achieved as a business sector if we take this approach.

The Jobs and Skills Councils would be the appropriate bodies to design and deliver tailored, timely and industry-specific training and should be funded to do so under the Strategy.

**15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?**

Many ideas have been tabled throughout this submission in relation to a 'better way of working,' however to summarise this should include at a minimum:

- **Day-to-day:** Regular program of engagement, tailored funding opportunities for industry, templates, checklists, free government support and counselling on cybersecurity for small businesses. Additional regulation only where necessary, costed and justified.
- **Crisis:** Simulations with key industry sectors should be undertaken annually or biannually to test capability and provide continued learning opportunities.

**a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?**

Many ideas have been tabled throughout this submission in relation to a 'better way of working,' however to summarise this should include at a minimum:

- Regulatory consistency and clarity based on risk and without regulatory overreach.
- Regular engagement and two-way information sharing with authorities.
- Training and adoption funding and support.
- Real estate specific strategy with a particular Adoption and Capability Plan funded and implemented.
- Identification of best practise modules, products, and ways of working. The current marketing place is saturated with 'cybersecurity experts' and quick fix products.

---

<sup>6</sup> Source. DEWR. Available: [Jobs and Skills Councils – Stage One Outcomes - Department of Employment and Workplace Relations, Australian Government \(dewr.gov.au\)](https://www.dewr.gov.au/jobs-skills-councils-stage-one-outcomes)

**21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?**

The Strategy should ultimately be about influencing Australians to change their behaviour and make everyone responsible for cybersecurity.

A baseline and bi-annual report outlining how the Strategy is achieving practise-change (i.e., impacts rather than tabling an annual report listing a series of government activities) should be a critical metric in ensuring the Strategy is being shared by all stakeholders and all are responding in a meaningful and agile way.

**Thank you**

REIA thanks the Panel for the opportunity to contribute our thinking in relation to the Strategy which should put people at the centre and make cybersecurity everyone's business.

Sector specific engagement, programs and funding will be critical success factors for real estate, and we encourage you to take this feedback on board on behalf of both real estate businesses and customers.

REIA would welcome further engagement with the Panel and is available for further meetings.

**ENDS**