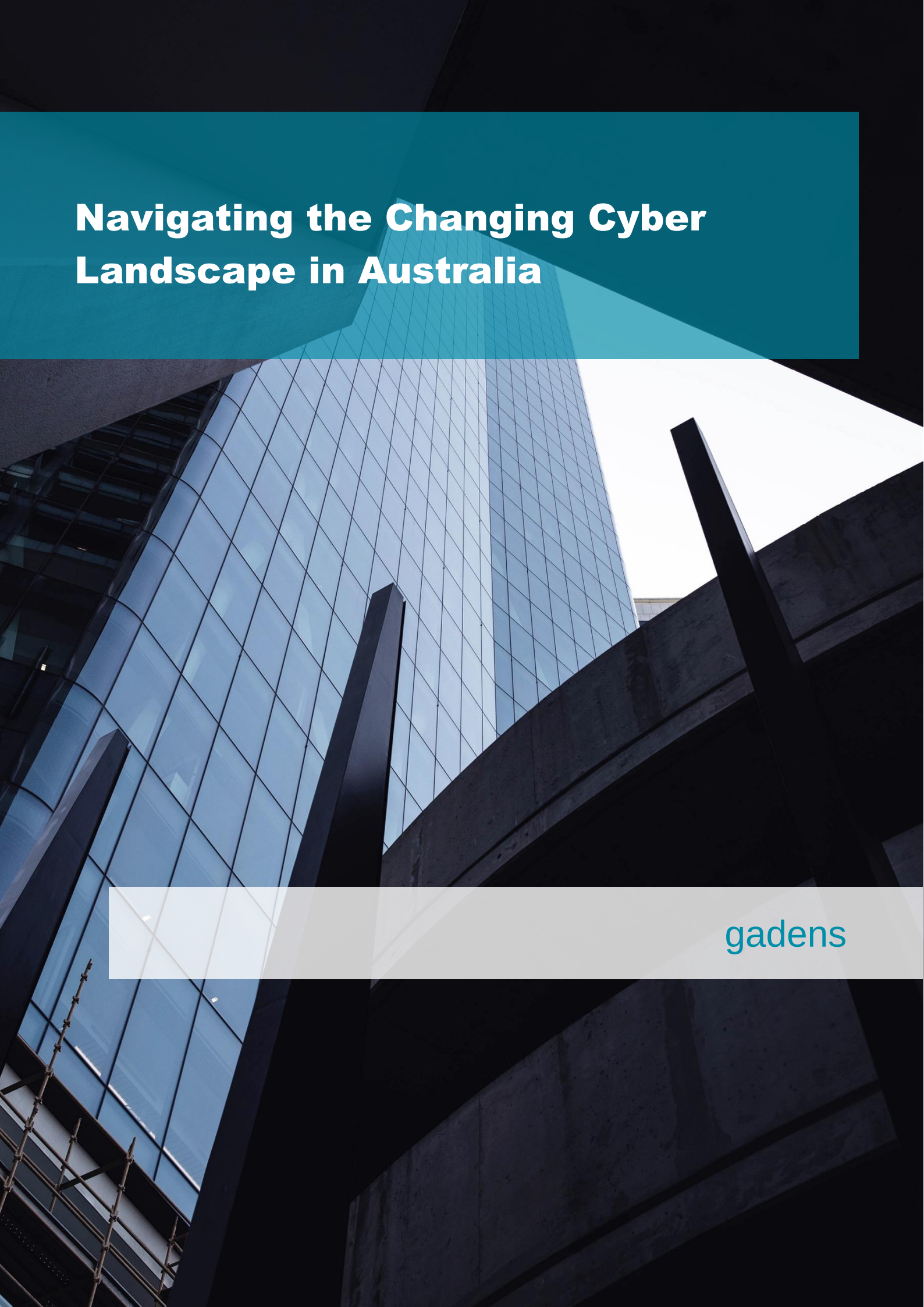
Navigating the Changing Cyber Landscape in Australia



gadens

gadens

Executive Summary

Both the Government and the Australian public reached a tipping point following a number of high profile data breaches in the second half of 2022.

This prompted much public debate on topics that included:

- whether people's personal information was being adequately protected
- responses to data breaches were too slow and fell below community expectations
- the amount of data that was being collected (particularly to identify people) and retained
- left to self-regulate, businesses were not doing enough to address cyber resilience
- boards were not taking cyber risk seriously enough
- supply chain risk is a serious threat when it comes to cyber attacks
- the existing penalty regime was seen as a cost of doing business
- Australian laws were lagging the rest of the world or considered poorly drafted.

Those high profile data breaches led to a swift response from the Government with the penalties for serious or repeated privacy breaches increased from $2.22 million to a minimum of $50 million at the end of December. Since then, the Government has released the Privacy Act Review Report and the 2023-2030 Australian Cyber Security Strategy that signpost a significant shift for Australia's cyber landscape. Critical infrastructure; personal information; cyber security; dealing with ransomware attacks – all are likely to be shaken up.

Change has already happened. More change is coming. The opportunity is here for all Australian businesses to get ahead of the next wave of laws and regulations. This white paper considers these changes and their likely impacts on Australian businesses in more depth.

THE MESSAGES ARE LOUD AND CLEAR

The messages from the Government and relevant regulators are loud and clear – change is needed, and businesses need to be listening and making sure they are prepared. The regulators have more powers and bigger sticks at their disposal, have already had some high profile successes in the courts (e.g., ASIC vs RI Advice) and will be looking for more successes to support its messaging. Here's what they are saying:

"*When Australians are asked to hand over their personal data they have a right to expect it will be protected.*

Unfortunately, significant privacy breaches in recent weeks have shown existing safeguards are inadequate. It's not enough for a penalty for a major data breach to be seen as the cost of doing business.
We need better laws to regulate how companies manage the huge amount of data they collect, and bigger penalties to incentivise better behaviour."

Mark Dreyfus, Attorney-General, 22nd October 2022

"*We went through Optus and Medibank, two of the biggest cyber attacks that Australia has experienced last year, and in those events we were meant to have at our disposal [a] piece of law … to help us engage with companies under cyber attack.*

And that law was bloody useless, like not worth the ink printed on the paper, when it came to actually using it in a cyber incident. It was poorly drafted."

Clare O'Neil, Minister for Home Affairs, 27th February 2023

"*For all boards, I think cyber resilience has got to be a No. 1 risk facing everyone. From my perspective, I see it as [a] top of the house, [a] board of directors level, issue*."

Joe Longo, ASIC Chair, 9th January 2023

"*We are well aware of these kind of issues [cyber-attacks not being disclosed by publicly listed companies in a timely fashion, or at all] and cyber is an enforcement priority that we are continuing to elevate and focus on*."

Sarah Court, ASIC Deputy Chair, 20th February 2023

CYBER ATTACKS ON THE INCREASE

Based on data from the Office of the Australian Information Commissioner for the second half of 2022, it should come as no surprise that cyber-attacks are on the increase. Large-scale breaches increased 67% in this reporting period. And this is only the breaches that were reported – it is likely that the majority of data breaches go unreported.

Source: Office of the Australian Information Commissioner - Notifiable Data Breaches Report: July to December 2022

Three large-scale breaches affected between 1 and 10 million Australians: Optus, Medibank and MyDeal. The data breach at Vinomofo affected between 500,000 and 1 million Australians.

Optus has provisioned $140 million in response to its data breach. Medibank is expecting to spend $40-45 million in the 22/23 financial year, not including litigation costs and regulatory penalties. Reputational impact is likely even more costly to these organisations than those stated sums.

In its most recent Annual Cyber Threat Report, the Australian Cyber Security Centre reported the following:

- an increase in financial losses due to Business Email Compromise to over $98 million - an average loss of $64,000 per report
- a rise in the average cost per cybercrime report to over $39,000 for small business, $88,000 for medium business, and over $62,000 for large business - an average increase of 14 per cent.
- over 76,000 cybercrime reports - an increase of 13 per cent from the previous financial year.
- almost 500 ransomware-related cybercrime reports, which represented an increase of nearly 15% on the previous financial year.

We can expect to see such numbers continuing to grow year on year.

THE GOVERNMENT RESPONDS – PRIVACY ACT REFORMS

"*The Privacy Act is no longer fit for purpose, and does not adequately protect Australians' privacy in the digital age*."

Mark Dreyfus, Attorney-General, 16th February 2023

Following the increase to penalties under the Privacy Act passed in late 2022, the Government tabled the Privacy Act Review Report (**Report**). The Report contains 116 proposals for reform of the Privacy Act, which in summary aims to achieve the following:

- recognise the public interest to society of protecting individuals' privacy
- clarify what information should be protected under the Privacy Act
- ensure de-identified information is protected from misuse
- require risks associated with holding and using information relating to individuals to be considered and protections applied accordingly
- regulate 'targeting' of individuals based on information which relates to them but that may not uniquely identify them
- enable privacy codes to be made by the Information Commissioner in certain circumstances
- ensure risks to privacy resulting from the small business, employee records, political and journalism exemptions are addressed in a proportionate and practical way.

The overall theme of the Report can be described as: more rights for individuals; more responsibility for all Australian businesses. If the majority of these reforms make it into law, then this will represent a step-change for how personal information is handled in Australia, more closely aligning laws here with Europe's General Data Protection Regulation (**GDPR**). Whilst the GDPR has its own criticisms, Australian privacy laws have clearly been lagging the rest of the world. This will change.

There is no timetable for when these proposed reforms will become law, or which of those reforms will make it through to a draft bill. Public feedback on the report is due by the end of March 2023 and then the Government will prepare a response based on that feedback. Whether the process takes 6, 12 or more months, the key message is that there are actions businesses can and should be taking now to prepare for Privacy Act reform.

The new higher penalty is already in place. Businesses should be acting now to review the risk of data breach, and looking at the three organisational pillars, be asking questions such as:

- People – are our people sufficiently trained and aware of cyber security threats? Does our organisation have a risk-focused culture that incorporates cyber security? Are our governance structures set up appropriately to incorporate due consideration of cyber risk?

- Process – in the event of a data breach, does our organisation have robust policies, plans, processes and procedures in place to respond? Have key processes been tested recently? Has our organisation mapped all of the data that we hold? Has our data retention policy been reviewed recently? Does our organisation have a cyber security or information technology management system in place?

- Technology – has our organisation invested appropriately in cyber resilience? Is our technology been managed in compliance with best industry practice and relevant laws and standards?

THE GOVERNMENT RESPONDS – CYBER SECURITY STRATEGY

On 27th February 2023, the Government released the 2023-2030 Australian Cyber Security Discussion Paper (**Discussion Paper**). Expert Advisory Board members had this to say:

"*Industry clearly has to do better in protecting customer data and implementing cyber security bestpractice and Government must lead by example and demonstrate its own commitment to hardening government systems and defending against cyber threats*."

Chair, Expert Advisory Board, Andrew Penn

"*Cyber attacks on government and on industry are only getting worse. The recent large-scale incidents have demonstrated to the community the very real risks online, are not going away and the real-world impacts they can have*."

Expert Lead, Expert Advisory Board, Rachael Falk

"*Cyber resilience requires a coordinated approach by governments, individuals, and businesses of all sizes*."

Expert Lead, Expert Advisory Board, Mel Hupfeld

The Discussion Paper poses a number of high-level questions, which give a good indication of the cyber roadmap ahead. Questions included:

- *What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?*

Currently only Federal and State Government agencies are required to adopt mandatory frameworks such as the Essential Eight. Could this mandate be extended to the private sector? Whilst the Essential Eight has its own limitations - people should be at the core of any strategy and is one missing piece from this framework – it can be considered a reasonable starting point. There are many other security frameworks to choose from, but it would not be a surprise for the Government to mandate and/or promote the Essential Eight (or even the Top Four, which rolled into the Essential Eight) for all Australian businesses.

- *Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?*

The Home Affairs Minister is clearly unhappy with how the Security of Critical Infrastructure Act is working in light of the Optus and Medibank data breaches, so as well as definition changes we may see proposals that strengthen the sharing of information between impacted organisations and relevant Government agencies in the wake of a cyber-attack, and potentially also see increases to the intervention powers of the Australian Signals Directorate.

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

Directors' duties are enshrined in section 180 of the Corporations Act, but these duties and the consideration to be given to discharge those duties are broadly stated. We could see section 180 specifically call out

directors' obligations for addressing cyber risk in the future therefore adding an additional compliance burden on directors and officers.

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

Cyber security legal obligations are spread across a patchwork of overlapping legislation and related instruments. There would be benefit to organisations in streamlining this patchwork and having a legal one-stop-shop for all cyber obligations.

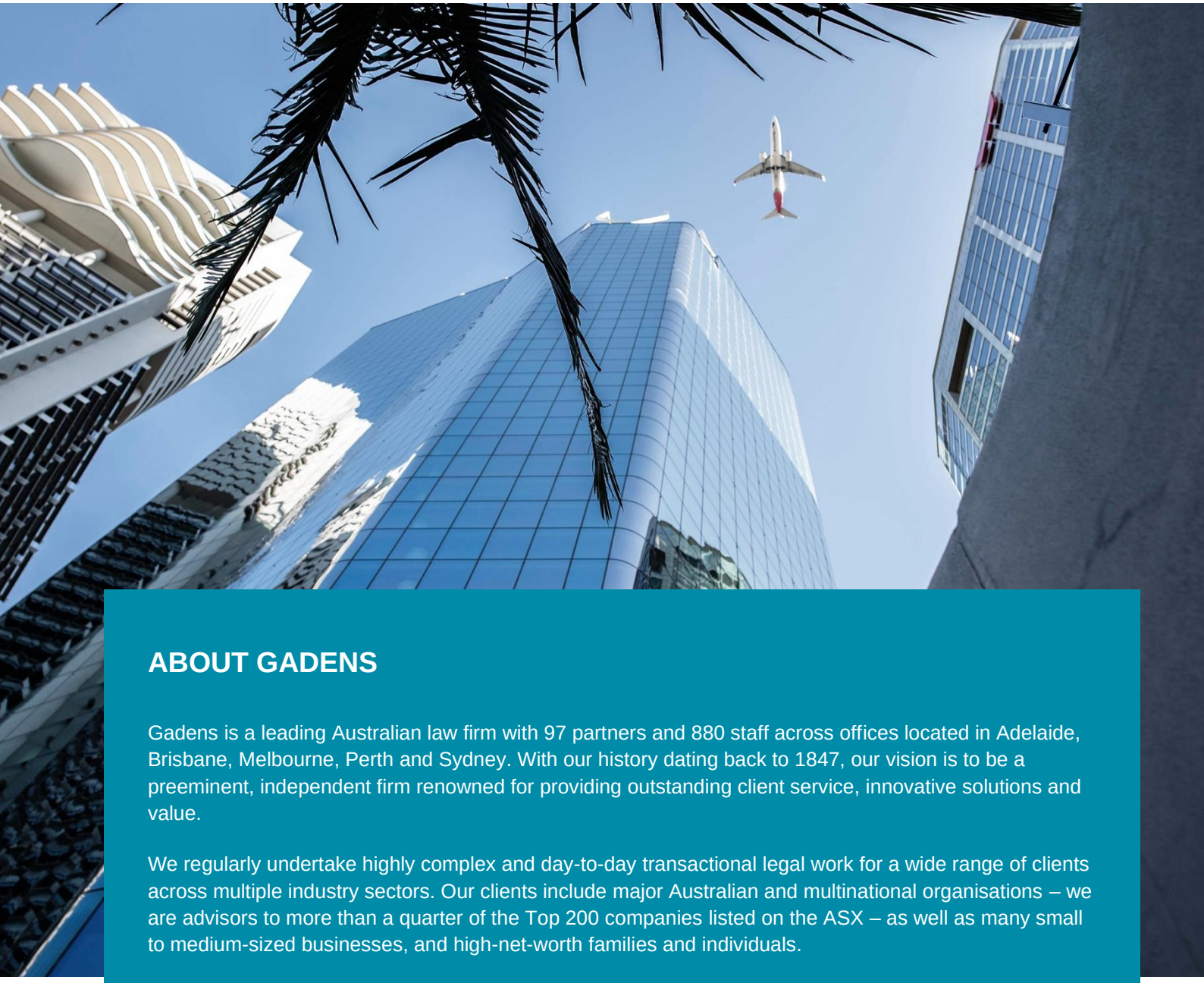
- *Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?*

There has been previous discussion on whether ransomware payments should be made illegal. The Discussion Paper poses a follow up question on what impact a strict prohibition of payment of ransoms may have on victims of cybercrime, companies and insurers. Looking at real-word data there is a trend in cyber criminals extorting, then extorting again – both the initial target organisation and impacted individuals. Will these criminals be deterred if such payments became illegal, or double-down on their extortion efforts? The Discussion Paper also asks whether the Government should clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law. This relates to potential breaches of Anti-Money Laundering and Counter-Terrorism Funding laws by making ransomware payments – where a paying organisation may not be able to identify who they are making payments to. It would be helpful if the Government clarified this position.

CONCLUSION

With so much change happening in the cyber landscape, businesses need to be up to date with the latest compliance requirements – both recent and upcoming. Whilst it's a matter of "when and not if" when it comes to the next cyber-attack, no-one wants to be the next Optus or Medibank, and it's likely that the next organisation to suffer a major data breach will be made an example of by the Government and the regulators. Businesses should be taking the opportunity now to review their people, processes and technology with respect to cyber risk and compliance. After all, security is everyone's responsibility.

gadens



ABOUT GADENS

Gadens is a leading Australian law firm with 97 partners and 880 staff across offices located in Adelaide, Brisbane, Melbourne, Perth and Sydney. With our history dating back to 1847, our vision is to be a preeminent, independent firm renowned for providing outstanding client service, innovative solutions and value.

We regularly undertake highly complex and day-to-day transactional legal work for a wide range of clients across multiple industry sectors. Our clients include major Australian and multinational organisations – we are advisors to more than a quarter of the Top 200 companies listed on the ASX – as well as many small to medium-sized businesses, and high-net-worth families and individuals.

Our aim is to help our clients achieve their objectives – providing an outstanding client experience for every client, every time. This is underpinned by our intense focus on understanding our clients, their needs and expectations and building meaningful, long-term relationships – a number of which span decades.

Our core values are the firm's foundation and reflect the essence and character of the firm – they define how we interact with one another and our clients.

Level 11, ONE ONE ONE
111 Eagle Street,
Brisbane QLD 4000

61 7 3231 1666

61 7 3229 5850

www.gadens.com