Strengthening Australia's cyber security regulations and incentives

REA Group

26 August 2021

Dear Sir / Madam

Strengthening Australia's cyber security regulations and incentives

REA Group Limited (**REA**) welcomes the opportunity to comment on the discussion paper, *Strengthening Australia's cyber security regulations and incentives,* released publicly on 13 July 2021 (**Discussion Paper**).

REA is a Melbourne-headquartered, multinational digital advertising company specialising in property. REA's core business involves advertising properties on behalf of real estate agents and allowing property seekers to search for properties by reference to criteria such as property type, price, location and features. In Australia, REA operates (among other things) the residential property website www.realestate.com.au and the commercial property website www.realcommercial.com.au as well as equivalent mobile sites and mobile device apps.

As one of Australia's largest and most innovative technology companies, REA invests heavily in the development of its products and services, and it is a substantial contributor to Australia's digital economy. Accordingly, REA has a strong interest in privacy and cyber security and is concerned to ensure that changes to Australia's cyber security framework foster an online environment that is transparent and safe.

REA wishes to make a number of observations regarding aspects of the Discussion Paper relevant to REA's business, as well as highlighting some areas of caution when considering how to incentivise business to invest in cyber security.

Key observations

1. Set clear expectations

(a) Blameless disclosure of cyber attacks

In order to learn from cyber attacks and improve security posture, organisations need to able to share technical details following security incidents with other organisations and industry groups without fear of retribution or exposure to further attacks. REA does not believe that there is currently a safe means to share this information and many disincentives exist to minimise information shared, such as fear of class actions, refusal of cyber insurance, blame-passing of liability through a supply chain or reputational damage. Put simply, talking about cyber-attacks is the digital equivalent of talking about mental health – it is difficult to make improvements and learn from experiences unless it is possible to exchange information safely and openly. REA believes that the Australian Cyber Security Centre could play an increased role in transparent information sharing. To date its role has been limited to sharing specific information only with companies directly involved in a cyber security incident rather than disseminating information more broadly.

A recent example of a company that shared information on a technology incident is Akamai, following a recent outage affecting Australian businesses. Their self-published report was seen as unusual—because it was transparent and detailed. While not related to a cyber-attack, the disclosures involving a global disruption are to be commended.

(b) Mandatory 2-factor authentication

A second suggested approach to raising minimum cyber security standards across business is through the mandatory use of two factor authentication (**2FA**). REA considers that 2FA is a basic yet significant control to mitigate many cyber attacks in industry. Use of 2FA raises the cost and effort for cyber criminals to access systems, is cost effective for businesses to adopt and has the potential to make a measurable difference to the security of a company. However, uptake of 2FA across business remains low at a global level, mainly through lack of awareness and also perceived poor user experience.

By educating businesses further about the benefits of 2FA from a cyber security perspective, REA believes that uptake of this measure will increase and in turn will improve Australia's cyber security framework.

2. Increase transparency and disclosure

(a) Minimum security standards for products

REA recognises the valuable role that cyber security vendors play in helping businesses protect themselves and their customers. However, REA has observed that security is now a premium product, often with premium pricing to match. Given that many small businesses (48% by the ACSC's own estimates)[1] are unlikely to spend more than $500 on digital protection, the premium pricing of security features in technology products represents a significant barrier across the ecosystem. In some cases, the pricing structure for security features stretches the budgets even of reasonably funded large organisations; in some cases, product security costs are manifestly excessive and put products or measures that may be beneficial to adopt out of reach of the organisations that ought to be able to benefit from them.

REA advocates for a baseline of minimum security features for security products, such that small business will have the opportunity to implement the best products for their ecosystems without having to spend more than they could afford on such products. This will go a long way towards ensuring an established baseline of security standards across all industry, for both smaller and larger enterprises.

(b) **Digital identity verification standards**

Public trust of digital identity remains low, in part driven by high profile cases, data breaches and a greater awareness of the importance of protecting personal information. Paradoxically, without digital identity verification standards, this means that businesses continue to collect and store copies of sensitive user identifier information such as drivers' licences, utility bills and other documents. The cost of protecting these documents is high and creates information honeypots that incentivise crime, including (but not limited to) extortion, ransomware, account takeover and fraud. Removing the need to collect copies of information that exists in already secure environments and is validated by electronic identify verification reduces the need to collect this information in the first place, and that effort should be placed building trust in these online verification systems.

[1] *Cyber Security and Australian Small Businesses – Results from the Australian Cyber Security Centre Small Business Survey*, Australian Cyber Security Centre, 1 July 2020, page 11.

3. Watchouts

REA urges caution in the following areas when considering future policy changes, regulation, or legislation:

(a) Limitations of maturity health checks / one-size fits all cyber security assessments.

It is unwise to reduce cyber security requirements to a checklist. There is significant complexity and nuance in every corporate network, supply chain and their connectivity across the internet. This means a uniform maturity assessment may not be a good indicator of risk.

There are many frameworks already in existence for businesses to assess their security posture, however the uptake is low in the small business sector. We believe this low uptake is due in part to the fact that the frameworks are complex and often lack specific guidance on measures that make a difference – rather many of these frameworks contain "shopping lists" of activities that are a disincentive to action. In addition to this, there is a risk that security scorecards may infer a posture that conveys false sense of security – either positive or negative to the true state – because they do not (and cannot reasonably) have regard to all relevant facets of a particular organisation's systems and circumstances. A parallel can be drawn to food labelling which has the potential to confuse buyers about the true health of a product, eg a food label may indicate that a product is low in fat and therefore may be deemed "healthy" even if the product may have a disproportionately high sugar content.

(b) Proper incentives for responsible disclosure in the security industry.

REA supports responsible disclosure of vulnerabilities and publishes a policy that encourages security researchers to report such vulnerabilities via our website. We do not offer monetary rewards for the finding of potential vulnerabilities, but we offer recognition of the individual through a "hall of fame". However, we recognise that the discovery of vulnerabilities is now a significant business model where vulnerabilities are monetised, and there is a risk that bug bounty programs have created perverse incentives to only disclose vulnerabilities to the highest bidder, or for a price that an organisation may not be prepared (or able) to make. There also are many examples of vulnerabilities being sold for exploit or remaining undisclosed for years, only to surface later in a compromise. REA urges consideration that future standards and regulations do not further reinforce a model that rewards only those that can afford to pay for vulnerabilities to be disclosed.

(c) Risks arising from cyber events are not static

Cyber security is not a binary goal, to be won or lost, but part of our technology landscape and a systemic risk to be managed on an ongoing basis. Experience shows that the controls to manage risks arising from cyber events erode over time and at different rates of decline as emerging technologies undermine what was previously deemed to be good practice/adequate controls. Examples include the deprecation of cryptographic hashes over time as greater levels of compute become more accessible, enabled by cloud infrastructure.

REA advocates for a method of continuous improvement to be built into standards and regulations, much like the ANCAP safety standards for motor vehicles which recognises improvements and raises the standards required to attain a five star rating over time.

(d) Aligned regulatory reporting timeframes

With increased regulatory scrutiny to address cyber security and privacy issues, we are observing the requirement for increasingly complex navigation through the required timeframes for regulatory reporting. Consider for example the 30 day window to assess whether a data breach is likely to result in serious harm under the *Privacy Act 1988* (Cth), versus the requirement to notify APRA within 72 hours of becoming aware of a notifiable information security incident under prudential standard CPS 234 Information Security.

Reporting has now become a complex framework within itself, and REA considers that the variability and complexity of reporting, and differences between reporting regimes, is likely to increase with the adoption of new cyber security standards and processes contemplated by the Discussion Paper. REA urges alignment of any new reporting timeframes with existing reporting timeframes, where possible.

REA is grateful for the opportunity to input its observations on the cyber security landscape, and looks forward to further discussion of these topics as the project progresses.