Submission No 19

INQUIRY INTO CYBERSECURITY

Organisation: Property Exchange Australia Ltd

Date Received: 18 September 2020

ABN 92 140 677 792
Property Exchange Australia Ltd

Tara Moriarty MLC
Chair
Portfolio Committee Number 1
NSW Parliament House
Macquarie Street
Sydney NSW 2000

18 September 2020

Re: Inquiry into Cybersecurity

Dear Ms Moriarty & Members,

PEXA (Property Exchange Australia) welcomes the opportunity to provide this submission. We note it cannot come at a more critical time given the current social and economic dislocation driven by the global pandemic.

While cybercrime knows no state borders, we welcome the diverse range of cybersecurity reforms introduced by the NSW Government. PEXA is keen to partner with the NSW Government to further support the industry in the delivery of ongoing cyber awareness programs and tools or products to mitigate the risks of cybercrime.

Digital innovation

As world leading early adopters of new technology, it's no surprise that Australia is also home to a growing number of innovative digital start-ups and success stories. Consumers are exercising enormous influence in how they want to transact. Today's digitally enabled customer leverages technology for everything. From how we bank to how we shop and how we communicate with each other. The property settlement experience should be no different but until the past few years, it was.

Investing in cybersecurity

Cybercrime is unfortunately an all-too familiar by-product of digital consumerism. Threats include new and evolving variants of ransomware that are becoming difficult to detect by typical signature-based antivirus solutions; and email phishing and business email compromise, which remains the most common entry vector for a cyber-attack. These attacks are mostly related to transactions of substantial amounts of money – such as property settlements, distribution of estates, and payment of settlement amounts in litigation matters. In this instance, law practices have been scammed into transferring funds into a fraudulent bank account.

Enhancing cybersecurity in the multi-ELNO Network

A move to a data exchange hub (ESB) or bilateral interoperability (Peer-to-Peer) market structure is currently being considered by the NSW Government. Under such a model, PEXA would be required to link its system with another ELNO (operated by Infotrack/Australian Stock Exchange).

Not only does this model risk entrenching a duopoly, but it also opens up property settlements to significant cyber security and operational risks. It also disadvantages other players wanting to enter the market, potentially stifling future innovations including cyber protections.

We note LexTech, which is seeking approval to operate as an ELNO, has also expressed its serious concerns about the model, claiming it was "unrealistic".[1]

While PEXA's concerns are well known in this space, this submission focuses on our commitment to protecting consumers and of the specific cyber security risks and threats we face should the current market structure proposal proceed in its present form.

The interoperability model introduces multiple, dispersed identity repositories and financial settlement paths. For example, it increases the risk of debits from unauthorised or unverified trust accounts as a result of the instructions being issued by one ELNO where signers and account details were verified by another.

Interoperability also risks introducing new vulnerabilities into the property settlement process. For example, a transaction can fail if one system has gone offline, even if the other remains stable. This has a broad impact for all industry participants, especially for the lawyers who serve as the 'frontline' for property transactions, dealing directly with customers in relation to their transactions. If the system goes down, or worse cyber-attacks are more frequent, vendors and purchasers will naturally turn to their respective conveyancers and banks for answers.

This does not lend itself to a positive customer experience and worse, ultimately undermines the trusted, proven system homebuyers and sellers across Australia rely on today. As noted earlier in the submission, to contemplate this at a time of heightened economic uncertainty raises concerns.

As an alternative to the interoperability model, PEXA believes there is potential to align with the Open Banking[2] framework.

We look forward to continuing dialogue with NSW on a national approach that facilitates competition while not introducing new or heightened cyber and operational risks into property settlements, and in turn the state-based land registries which are ultimately guaranteed by state taxpayers.

Issues for Consideration

As we continue to trade and conduct our lives in a more complex digital world, it is critical that before any policy, regulatory or rule changes are made to any sector, the cyber consequences are clearly understood and considered, actioned and accepted by all stakeholders.

While we acknowledge this Inquiry has a broad scope, we believe the PEXA experience has transferrable principles to consider during the Committee's deliberations. PEXA's recommendation for prioritisation to combat today's threats should ideally focus on:

- Alignment to at least one essential cyber security control framework;
- Clearly defined network policies and service configurations;
- Ongoing security awareness and training through email phishing tests, education sessions and communications; and
- Workforce and Skills.

Our recommended approach attached to this submission is broken into general observations and those related specifically to our sector.

[1] Jack Meredith, LexTech Head of Operations, The Australian Financial Review, 17 September 2020.

[2] The banking sector is transitioning to an open access model, with the first phase of Open Banking coming into effect on July 1 2020, requiring all financial institutions over time to participate with the big four banks live in phase one.

We look forward to working with you as you deliberate your response to this Inquiry and to play a practical leadership role in the continued investment and innovation in our industry. For further details on this submission, please feel free to contact me direct.

Kind regards,

Gary Howard
Chief Operations Officer (acting)
PEXA

Item no.	Recommendation	Commentary
General		
1	A simplified and harmonised regulatory environment with a minimum compliance standard.	Currently, industries face many different regulatory requirements depending on their business outcomes. These requirements can often overlap and complicate compliance for organisations while adding cost for no pragmatic cyber result. Ideally, the minimum compliance standards set for both Government and Industry should be measured against the Australian Signals Directorate (ASD) Essential 8 Strategies to provide a baseline for cyber security. Guidelines could be established and regulated by the Australian Cyber Security Centre (ACSC). Both State and Commonwealth cooperation is important for harmonization. Similarly, any individual industry requirement should align to centralised guidance from the ACSC and other regulatory bodies. In PEXA's case, the Australian Registrars' National Electronic Conveyancing Council (ARNECC) sets the standards. At the same time, they are providing the ability to easily map these to the ACSC or other requirements to enable prioritisation of controls to get the most value for individual businesses.
3	Require mandatory cost benefit analyses consistent with The Guide to Better Regulation for any regulatory reform impacting a certain sub-sector within the industry, and particularly the impact on cybersecurity.	In January 2019, the NSW Government released its laudable Guide to Better Regulation. These principles articulate what the NSW Government characterises as good regulation and minimisation of red tape. Critical, independent analysis of proposed regulatory or policy change that has ramifications for cyber security should be mandatory. It is possible that, in some instances, increases in cyber-risks are inaccurately weighed, resulting in potential unintended consequences. In our experience, regulation and regulators are not equipped to understanding the cyber implications of their decisions. This appears to be an increasing issue across governments and regulators, which can be addressed through enhancing government's cyber capability and through greater consultation with a broad range of industry experts.
4	Coordinated reporting regime.	Reporting guidelines across industries are presently complicated by differences in regulations for privacy and other standards. Current guidelines for government and industry should be reviewed to ensure they are scalable and potentially tiered depending on the agency implementing them. If not already completed, it may assist in reviewing the threat profile of each agency to determine potential priority targets and ensure more in-depth standards are applied appropriately. We note that the Commonwealth is also looking to enhance its view of cyber-risks and believe that greater Commonwealth-state cooperation in this space will ensure industry isn't saddled with unnecessary duplication of reporting requirements.
5	Provide a platform for industry and consumer input into regulatory and cyber reform to foster the spirit of collaboration.	Policy or regulatory decisions that may ultimately increase risk/alter risk tolerances should not be made unilaterally by one Department. Instead, PEXA would recommend engagement more broadly within the Government, including through its cyber security arm, and where necessary, including the involvement of third-party cyber security experts.
6	Build a cyber incident response framework.	Organisations require assistance when being able to detect and respond to a cyber incident. Most small to medium businesses have no individual body they can engage within the event of a significant incident to assist in forming a plan of action. Any framework here might consider how clear guidance is accessed. A centralised Security Operations Centre (SOC) that maintains security logging standards and incident response playbooks is advisable. The SOC should be on the frontline with those who it protects to ensure all involved parties understand their role in containing and responding to a cyber incident. We note that the Commonwealth is also looking at new capabilities and powers in this space and believe the optimal outcome for Australia would see greater Commonwealth-state cooperation and coordination in managing and responding to our cyber risk environment.

Item no.	Recommendation	Commentary
General		
7	Workforce and Skills.	Building depth and resilience within the cyber security workforce is dependent on nurturing cyber skills early (typically high school) and then through the provision of ongoing skills-building opportunities. As such, the NSW strategy should consider: • Focused cyber skills training as early as Year 9 to establish a future talent pool and create a cyber aware population; • Provide those who are undertaking education with clear cyber career pathways to help with their course selection. Cyber is rarely a one-size-fits-all industry; • Provide those who are undertaking education with job placement opportunities early in their studies. This will provide practical skills in their chosen cyber discipline beyond theory-based learning that may already be obsolete; • Encourage women to participate in cyber security education by engaging with and promoting key 'women in cyber groups; and • Ensure an ongoing skills development strategy to support the retention of key talent in the cyber security space. Cyber is a competitive labour market, and skilled resources can be easily coaxed away with rewards of more training and financial reimbursement.
8	Business Investment.	PEXA has found great value from investing in smaller start-up firms that augment its existing skillset. PEXA has experimented with the concept of providing a platform for others to provide 'Security as a Service' to our small to medium sized members. We believe this is an area in which we could partner with the NSW government to support the industry better. This could include providing simple uplift in cyber standards and education on cyber safeguards. Also, start-ups would benefit from a central register or directory of the types of services they offer, enabling other businesses to search for a provider based on particular needs. The NSW Government might also look at building a procurement register of NSW firms so that they can be notified of procurement opportunities. PEXA would be open to exploring how it could promote the availability of these third-party security service providers through its platforms and channels.
Recommendation specific to the eConveyancing sector		
9	Maintain the spirit of national cooperation in which eConveyancing was made possible to minimise cyber risk.	Cybercrime knows no borders. We should collectively ensure the consumer sits at the heart of any market structural reform. Within the eConveyancing industry this means advocating for a market structure that promotes sustainable competition while avoiding unnecessary cyber risk, cost, or complexity. The model could be drawn from the principles of the Open Banking model which came into effect on July 1, 2020.
10	Zero tolerance for using email to transfer banking and financial details business-to-business; and consumer to business/business to consumer.	Email fraud remains a significant threat. On September 7, 2020, the NSW Registrar warned law practices to be on high alert for email fraud, with an increase in recent weeks of cyber criminals targeting solicitors. It noted the attacks mostly related to transactions of substantial amounts of money – such as settlement of conveyancing transactions. There are free tools available such as PEXA Key which mitigate against this type of risk, safeguarding property transactions and consumers. There should be clear guidance for operators on managing user risks for their own staff and as appropriate their customers, such as recommending zero-tolerance for use of vulnerable channels like email for the transmission of sensitive information (i.e. banking details or credentials).