RESERVE BANK OF AUSTRALIA

Cyber Security Legislative Reforms

Submission to the Government's Consultation Paper

March 2024

Introduction

The Reserve Bank of Australia (RBA) welcomes the Government's efforts to strengthen cyber security laws and help citizens and businesses engage confidently in the digital economy.

The RBA is the principal regulator of Australia's payments system with a mandate to promote the safety, efficiency, and competitiveness of the payments system. The RBA is also the relevant Commonwealth regulator under the *Security of Critical Infrastructure Act 2018* (SOCI Act) in respect of 'critical payment system assets' – that is, assets used in connection with the operation of a payment system that is prescribed under the rules as being critical to the security and reliability of the financial services and markets sector. [1]

Financial market infrastructures are critical to the smooth functioning of the financial system, and retail payment services play an important and growing role in supporting economic activity. As the reliance on electronic payments increases and use of cash declines, consumers and businesses increasingly expect payment services to be fast, convenient and reliable.[2] This is reflected in consumers shifting to electronic payment methods, including online and more convenient payment methods (e.g. tapping their phone or cards).[3]

The Bank supports further clarifying the SOCI Act and the proposed initiatives supporting the cyber resilience of the financial sector. The issues below are centred around the key areas where the Bank considers that measures proposed in the consultation paper could be improved to make the legislative framework for cyber resilience more cohesive and efficient.

Expanding and clarifying the scope of regulatory powers

Cyber risk management is an area where many government agencies share and complement one another's powers to achieve the best outcome for the resilience of the Australian economy. As such, the RBA welcomes the initiatives targeted at closing the gaps in regulatory coverage and improving the efficiency of regulatory interventions. However, in implementing these initiatives, due consideration should be given to:

1 Currently, each of the Mastercard and Visa debit and credit card systems, the EFTPOS card system and the New Payments Platform is prescribed as such - see s10(5) of the Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021.

2 See A Strategic Plan for Australia's Payments System (treasury.gov.au) (2023).

3 See Consumer Payment Behaviour in Australia | Bulletin – June 2023 | RBA.

(a) the reasons behind the respective mandates and powers of relevant agencies; and

(b) addressing any unintended consequences that the introduction of new powers could have on the efficient exercise of current powers.

With these objectives in mind, the RBA:

- supports, in principle, the proposed amendments to the SOCI Act and relevant rules to explicitly cover data storage systems holding business critical data related to the operations of critical infrastructure (CI) assets in sectors outside the data storage and processing sector (Measure 5). This recognises the growing reliance of many industries on outsourced services.

- welcomes the proposals to impose the ransomware reporting obligations (Measure 2) and the introduction of 'no-fault' and 'no-liability' protection principles. However, as noted in the consultation paper, it will be important to clarify that affected entities must still continue to meet their legislative and regulatory obligations, including any reporting obligations to relevant sector regulators. It should also be clear that any 'no-fault' and/or 'no liability' protections would not prevent other relevant authorities from investigating the root cause of the incident and issuing recommendations pursuant to their respective regulatory functions and powers.

- encourages careful consideration of the potential impact of the work of the Cyber Incident Review Board (CIRB) proposed in Measure 4 on the powers and obligations of other relevant sector regulators; it should be made clear that the work of CIRB does not impact other regulatory or law enforcement actions – in particular, CIRB investigations should not preclude a regulator from being able to use their regulatory powers in relation to the incident (including to conduct an investigation or require the production of information relating to the incident), nor exempt an entity from continuing to meet reporting obligations.

- emphasises the need to establish clear consultation, cooperation and governance arrangements surrounding the use of the extended emergency Government consequence management powers (Measure 6); such arrangements should help minimise inconsistencies with any actions being taken by the RBA, or other regulators, and avoid unintended consequences that may hamper the broader crisis management response of the relevant regulator.

Improved and secure information sharing for more efficient regulatory interventions

It is essential that regulators have timely and efficient information gathering powers, and the ability to securely share relevant information with other agencies, where appropriate. Having adequate information should be a necessary condition for introducing enforcement powers. The proposed critical infrastructure risk management program (CIRMP) review and remedy powers

(Measure 8) appears to be a meaningful addition to the regulatory suite under the SOCI Act. However, a number of areas warrant further consideration.

The proposal contemplates a new directions power to address seriously deficient elements of a CIRMP when certain conditions are met. One of the proposed conditions is that the Secretary of Home Affairs or relevant Commonwealth regulator has, following consideration of certain matters, formed a reasonable belief that an entity's CIRMP is 'seriously deficient'. This assumes that the RBA, as the relevant Commonwealth regulator in respect of critical payment system assets, has reviewed and considered the relevant responsible entity's CIRMP.

However, the entities responsible for the operation of critical payment systems are only required to provide an annual report, including an attestation of compliance of their CIRMP with the SOCI Act and rules. Responsible entities are not obliged to, and the RBA currently has no powers to require the responsible entity to provide, the CIRMP itself to the RBA.[4]

Accordingly, the RBA submits that the Government should either introduce an obligation for a responsible entity to provide a copy of its the CIRMP to the relevant Commonwealth regulator (where there is one), or include a specific provision which enables the relevant Commonwealth regulator (and not only the Secretary of Home Affairs) to require a responsible entity to produce a copy of its CIRMP.

Further, responsible entities and regulators require clarity over their respective abilities to share information. The RBA welcomes the proposed improvements to the information sharing provisions of the SOCI Act (Measure 7) but submits that the proposed amendments may need to go further in order to achieve their intended objective. In particular:

- it is unclear how the definition of 'protected information' under the SOCI Act will be revised to reflect a 'harms-based approach' where, in the context of the consultation paper, the latter appears to relate to an entity's consideration of whether to *disclose* protected information. It is also unclear whether any implementation of a 'harms-based approach' would be based on a subjective or objective assessment of 'potential harm' by an entity. In any case, the RBA submits that any proposed amendments to the definition of 'protected information' and/or provisions authorising disclosure of 'protected information' under the SOCI Act should be carefully drafted so as to achieve the stated objective of providing greater clarity for both industry and government.

- the changes should go further and eliminate the existing limitations and uncertainty relating to the sharing of protected information concerning CI entities' security and resilience between Home Affairs and other relevant Commonwealth regulators to the extent possible. This would enable Home Affairs and the relevant Commonwealth regulator to discharge their respective obligations more efficiently and contribute to the reduction of unnecessary regulatory burden

4 Under section 37 of the SOCI Act, only the Secretary of Home Affairs can require a reporting entity or an operator of a critical infrastructure asset to provide information and documents.

- to protect the confidentiality of information exchanged by the agencies, the information sharing provisions should require secure data storage and preventing multiple copies of information being held by several agencies.

Minimising unnecessary regulatory burden

While improving the coverage of the regulation helps mitigate additional risks, it imposes additional burden on the regulated entities. The RBA welcomes the consideration of minimising unnecessary regulatory burden being one of the key features of the ransomware reporting proposal (Measure 2), and encourages the Government to:

- consider the existing cyber incident reporting obligations, e.g., of the entities responsible for the operation of critical infrastructure assets under the SOCI Act, to enable them to submit a single report covering different regulatory obligations, and
- further enhance the Single Reporting Portal for cyber security incident reporting to enable the responsible entities to use it as an actual reporting tool for all relevant obligations, including the proposed ransomware incidents reporting.

Reserve Bank of Australia
1 March 2024