paymentsnz®

Consultation document – Risk management guidance on cyber resilience and views on information gathering and sharing

Payments NZ Limited submission

29 January 2021

Introduction

Payments NZ welcomes the opportunity to respond to the questions outlined in the Reserve Bank of New Zealand ("the Reserve Bank") Consultation document: Risk management guidance on cyber resilience and views on information gathering and sharing ("the consultation document").

The draft guidance on cyber resilience put forward with the consultation document will apply to all regulated entities of the Reserve Bank, including designated financial market infrastructures. While Payments NZ does not own or operate any infrastructure to enable payments to be made, Payments NZ manages the rules for both the settlement before interchange (SBI) and high value clearing systems (HCVS), both of which are likely to be designated under the Financial Market Infrastructures Bill, and it is on this basis that Payments NZ makes its submission.

Responses

Q1: In light of the nature of cyber risk and the range of observed international practices discussed in the previous section, do you support the Reserve Bank's policy stance of being 'moderately active' in promoting cyber resilience within the financial sector?

Payments NZ acknowledges the constantly evolving and rapidly changing information landscape and the need to understand and effectively manage cyber risk. It supports the Reserve Bank having a role in promoting cyber resilience within the financial sector, noting that the Reserve Bank's approach will primarily involve publishing risk management guidance and working with other public sector bodies in relation to information gathering and sharing arrangements. We understand that once the Reserve Bank has formed its initial views on these matters it will consult with stakeholders on a more detailed proposal, including enhanced incident response coordination.

The Reserve Bank has indicated its support for a moderately active role. At this stage, and given that the Financial Market Infrastructures Bill has not yet been enacted, it is difficult to know what a moderate approach would involve for Payments NZ if it were to be designated.

Q2: Do you agree with the Reserve Bank's general approach of sticking closely to international practice? Do you have any specific feedback on the draft guidance on cyber resilience?

Payments NZ agrees that international practice should be used in New Zealand, where it is appropriate and makes sense to do so.

It is noted that the principle of proportionality applies throughout the draft guidance and that the guidance is not exhaustive. However, there are elements of the draft guidance which appear to be quite prescriptive, particularly in relation to governance (e.g. the role of the board and the matters for inclusion in the cyber resilience strategy and framework). There are also parts of the draft guidance which suggest that approval or input from the Reserve Bank may be required,

particularly in relation to third party management (e.g. where entities should inform the Reserve Bank about outsourcing of critical functions to cloud service providers early in the decision-making process). It would therefore be helpful to understand the Reserve Bank's expectations in relation to how it sees the draft guidance being implemented.

Payments NZ also notes that there is both baseline and enhanced guidance and would like to better understand when the different thresholds will apply.

Q3: Do you agree that the guidance should be a set of high-level principle-based recommendations?

Payments NZ supports Reserve Bank guidance on cyber resilience being non-technical, principle-based and future-proofed. Payments NZ believes this is appropriate, rather than a prescriptive approach, and enables market participants to tailor their response to cyber risk within the context of the overarching framework. However, as noted above, there appear to be some parts of the draft guidance which may be too prescriptive in nature.

Q4: What's your view on the principle of proportionality and a risk-based approach adopted by the guidance?

The guidance is proposed to be used in a manner proportionate to the size, structure and operational environment of an entity, as well as the nature, scope, complexity, and riskiness of its products and services.

Payments NZ agrees with this approach. In particular (and as stated in the consultation document) regulated entities should be able to assess their own cyber risk tolerance and set their own cyber risk appetite. This will ensure that their cyber risk mitigation efforts are commensurate with the cyber risks that they face. However, some requirements in the guidance are prescriptive and appear to be more relevant to larger organisations. For example, the guidance requires a senior executive to be appointed to take care of cyber resilience issues who can act independently from the IT/operations department. Given that a smaller organisation may need to assign security roles and responsibilities as functions of broader roles, complete independence may not be achievable.

Q5: Do you agree that the guidance should apply to all regulated entities of the Reserve Bank?

Yes, we think it is logical that if the Reserve Bank is committed to issuing guidance on cyber resilience, then it should apply to the regulated entities that are mentioned (banks, non-bank deposit takers, insurance companies and financial market infrastructures).

Q6: What is your view on the Reserve Bank's collaborative and coordinated approach to information gathering and sharing?

Payments NZ regards information gathering and sharing as an important part of building cyber resilience in the financial system and minimising the impacts of incidents. Effective, and appropriate, information sharing can contribute to the development of effective detection, response and recovery strategies.

The approach to information sharing should be coordinated across other public sector bodies to ensure that this is as efficient, safe and broad as possible, without unnecessary duplication.

Payments NZ supports the purposes for information gathering and sharing outlined in the consultation document but notes that there must be adequate safeguards protecting the confidentiality of the reported information and it is pleasing to see the Reserve Bank recognises this, together with the need for appropriate controls in relation to sensitive information.

It is noted that the costs involved in establishing a trusted information sharing platform may be significant and it is important that careful consideration is given to balancing the costs of establishing an information sharing platform with the anticipated benefits of this.

As a key stakeholder in the governance of the New Zealand payments system, Payments NZ is in a position to facilitate and coordinate actions or responses at an industry level and has arrangements in place to respond to disruptions in the payments system. It is noted that these arrangements may have relevance to possible cyber disruptions and may assist in mitigating the impact of these.

Payments NZ also ensures that all participants meet the access criterion set out in the Payments NZ rules – namely that a participant will not adversely affect the integrity or reputation of the clearing system, or introduce significant risk into the clearing system. To satisfy this criterion, the Payments NZ rules specify prudential requirements, operational requirements and operational risk management requirements. These are extensive and serve to enhance the safety and integrity of the payments system.

Q7: Do you support the Reserve Bank's intention to broadly follow the international practices and establish a cyber data collection for all prudentially regulated entities? Do you have any particular concerns or issues that you would like the Reserve Bank to take into account when further developing its plan?

In principle, Payments NZ supports the Reserve's Bank intention to broadly follow international practices and establish a cyber data collection for all regulated entities, subject to better understanding what a moderate approach would involve for Payments NZ and how the detailed framework for information gathering and sharing will develop and be implemented. We note that a further consultation is proposed in the middle of 2021 in relation to this.

It may be helpful to look at how overseas jurisdictions have adopted international practices and the extent to which different approaches have delivered improved cyber resilience.

Summary

As the Reserve Bank continues to refine its views in relation to cyber risk management, Payments NZ makes the following observations:

- Guidance on cyber resilience should remain high-level and outcomes based;
- Obligations in relation to data collection and information sharing should be targeted, well defined and not unduly onerous for the regulated entities that are involved;
- In terms of reporting of cyber incidents, a materiality threshold and a time frame need to be considered;
- Appropriate safeguards to protect confidentiality and manage sensitive information must be in place and the costs of establishing an information sharing platform must be measured against the anticipated benefits of this;
- Data collection on cyber capabilities and resources within the context of the prudential regulation that is proposed by the Reserve Bank should be part of a coordinated approach across other public sector bodies. Regard needs to be had to what other agencies are doing when it comes to cyber to avoid duplication/having to report to a number of agencies, and having differing requirements between agencies. We note that currently there are a number of agencies that have an interest in cyber, including:
    - the National Cyber Security Centre, which is part of the Government Communications Security Bureau,
    - CERT NZ,
    - the Department of Internal Affairs,
    - the National Cyber Policy Office of the Department of the Prime Minister and Cabinet,
    - New Zealand Police,
    - Netsafe.

Contact details

If you wish to discuss the responses set out in this submission, please contact:

Steve Wiggins, Chief Executive: [redacted]