New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Reserve Bank of New Zealand

on the

Consultation Paper: Cyber Resilience Data Collection Proposals

3 July 2023

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following eighteen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - KB Kookmin Bank Auckland Branch
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

NZBA welcomes the opportunity to provide feedback to the Reserve Bank of New Zealand (**RBNZ**) on the Consultation Paper: *Cyber Resilience Data Collection Proposals* (**Consultation Paper**). NZBA commends the work that has gone into developing the Consultation Paper.

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Associate Director, Policy & Legal Counsel
sam.schuyt@nzba.org.nz

Introduction

4. NZBA is supportive, in principle, of the introduction by the RBNZ of some level of cyber reporting and appreciates the continued efforts of the RBNZ in building cyber resilience against the evolving threat landscape. We believe this will assist the RBNZ in better understanding cyber threats to New Zealand's financial system.

5. However, NZBA would like to ensure that the time and effort regulated entities put into complying with reporting requirements are worthwhile in providing the outcomes that the RBNZ is looking for.

6. In the current proposal, we have concerns that some of what is asked for goes too far for the purposes for which the RBNZ is collecting the information, and would create a disproportionate and onerous burden on banks. This is of particular relevance when factoring in the similar reporting that is being requested by other regulators. In the absence of a central agency for cyber reporting, alignment of reporting methodology and definitions between regulators should be a priority.

7. In summary, our key submissions are that:

    7.1. further clarity on what constitutes "detection" of a material cyber incident is essential to ensuring that it is clear from when the RBNZ's proposed 72-hour deadline for reporting starts to run;

    7.2. the reporting of all non-material cyber incidents (as currently defined) should be narrowed so that it does not detract from the RBNZ's first step of focusing on material incidents;

    7.3. the definition of "materiality" leaves room for subjectivity and there is scope to improve the definitions of "Materiality", "Incident" and "Potential" materiality by using examples of incidents that would meet the materiality threshold;

    7.4. the proposed Cyber Resilience Survey is currently too detailed, and we suggest alternative methods of data collection (such as engaging with banks to access pre-existing data collated for NIST assessments), are considered by the RBNZ; and

    7.5. cyber security is a highly sensitive area and collected data must be securely stored and its use carefully considered. We would request that further, more detailed information is provided on who the information will be shared with, how it is shared, for what reason, when it is disposed of and what happens if there is a data breach at the collecting organisation.

8. This submission is supported by the Financial Services Security Information Exchange (FSIE) industry cyber security forum, which is comprised of information security professionals as representatives from across the sector and is hosted by NCSC.

9. Our specific feedback is set out under the general headings below.

Timeframes for Cyber Incident Reporting

Material Incident Reporting

10. NZBA submits that the proposed 72-hour deadline for the reporting of all material cyber incidents is reasonable and aligns with the FMA's Standard Conditions for Financial Institution Licences and international standards.

11. However, clarity on when that 72 hours begins to run is important and the guidance is currently unclear. Further clarification and guidance on the interpretation of what constitutes "detection" of material cyber incidents is required. While a bank will know when an event has hit its system, it may take some time to determine whether that event is material.

12. We submit that the 72-hour timeframe should commence from the time that a regulated entity becomes aware that the incident has hit the materiality threshold, rather than any initial detection of a cyber incident on a bank's systems when the materiality of the incident may not yet be known.

13. NZBA also requests clarity on how the reporting requirements will align with other RBNZ reporting timelines (for example, in relation to reporting operational material incidents that are not a result of a cyber-attack). There is potential for the Incident Response template to provide for both requirements, thereby eliminating the need for a bank to perform multiple assessments of the same incident to comply with reporting requirements.

Periodic Cyber Incident Reporting

14. In relation to the requirement that all entities report all cyber incidents to the RBNZ (with large entities required to report on a six-monthly basis and other entities annually), NZBA has some significant concerns around the practical complexity and resource intensity of reporting all incidents, particularly in relation to defining what constitutes an "incident" for the purposes of reporting. There is concern that including the reporting of all non-material cyber incidents (as currently defined) goes too far, is disproportionate and could detract from the RBNZ's first step of focusing on material incidents.

15. We submit that it is impractical to report all incidents from a prioritisation and resourcing perspective, especially for incidents relating to IT outages versus cyber incidents. The volume of IT outage incidents could be high. Businesses usually internally have a triaging process and impact assessment process to make sure energy and resources are spent on actual and high impact cyber incidents rather than non-material cyber incidents.

16. The current definition of “cyber incident” (on page 9 of the Consultation Paper) could result in potentially large numbers of incidents, many of which could be considered insignificant, being reported (for example, insignificant events such as an internal policy breach). It would require significant operational process and effort to manage, and we question how this information would assist RBNZ in building cyber resilience against the evolving threat landscape.

17. NZBA therefore submits that, if the periodic reporting does not focus solely on material cyber incidents, there should be a narrower definition of “cyber incident” than is currently proposed. We understand from paragraph 3.3 of the Consultation Paper that the RBNZ’s collection of the information will “round out” financial regulators’ understanding of cyber risk impacting the financial sector beyond material incidents. We submit that a narrower definition can still achieve this goal. We would be happy to engage further with RBNZ on the detail of that revised, narrower definition.

18. We would also request clarity on whether the reporting requirement applies to incidents outside of New Zealand, for entities that operate in more than one jurisdiction.

Materiality Threshold Definition

19. NZBA believes that the definition of materiality used in the guidance gives greater clarity on what can be considered a material cyber incident, and notes that it generally aligns with existing APRA requirements.

20. The definition does however leave room for subjectivity and there is scope to improve the definitions of “Materiality”, “Incident” and “Potential” materiality by using examples of incidents that would meet the materiality threshold. By way of example, it is unclear how a bank would assess the potential damage that could have been caused by a phishing email if a staff member detects it, reports it, and does not interact further with it.

21. Further, we submit that the differences between the RBNZ’s and the FMA’s definitions of materiality may result in substantive differences in the incidents that entities will report. The RBNZ’s definition is in our view wider, and due to the sharing arrangements in place between the two regulators, entities will pragmatically need to report to both simultaneously.

22. Further and more specific feedback on the definition is set out at Appendix 1.

Cyber Incident Reporting Template

23. NZBA understand that only the material incidents template has been prepared so far. We are broadly supportive of the use of a template in principle, but have set out below some concerns with the proposed drafting.

    23.1. There seems to be an expectation of daily updates mentioned in the report template instructions. Given the nature of some material cyber incidents, daily updates may not always be appropriate where these occur over an extended time period with little material change on a day-to-day basis (for example, in the context of phishing campaigns involving multiple sites which may be identified over time as the investigation progresses). The requirement to provide updates could be adjusted to situations where the incident "materially changes".

    23.2. The information required may go too far, particularly given it would be required at a time of stress and in a tight timeframe. We would welcome a template that either asks only for key information, or clarification from RBNZ that financial institutions can fill out the fields to the best of their knowledge (therefore balancing the need for RBNZ and relevant other agencies to be aware of an incident with the importance of the reporting bank being able to focus on responding to the incident itself).[1]

    23.3. It is not clear whether the reference at question A08 to an "internal outage / service failure" refers to a type of cyber incident or the impact / consequence of a cyber incident. Further clarity of whether this refers to a cause or effect would be appreciated – the definitions of cyber incidents versus IT outages / incidents are distinct and should not be confused.

    23.4. We would like to bring the Financial Stability Board's (**FSB**) work on a common Format for Incident Reporting Exchange (FIRE) to RBNZ's attention, and recommend that RBNZ wait for the final template from the FSB before introducing its own template. The FSB has found that there is a high degree of commonality in the types of information that authorities require financial institutions to report under existing cyber incident reporting frameworks, and alignment with this format may allow reporting entities to streamline the information they are required to provide to various regulators.

    23.5. Further to the above, the RBNZ may want to explore the utility of a central agency for cyber reporting (for example, NCSC). The central agency could then share any notifications with other impacted regulators, and will help to reduce the number of reports that need to be submitted during a crisis, freeing up resources to focus on the incident.

[1] The FSB's "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report" notes that "In the early stage of the incident, the information available to the affected FI could be rather limited. Nevertheless, the FI should still provide, to the best of its knowledge, an overview of what happened, which could include when the incident was detected, possible cause(s) of the incident, immediate impact (e.g. the services affected) and initial incidents taken to manage the incident."

23.6. Definitions of “Active / Under investigation / Mitigated” should be included in section A06.0 (and elsewhere it features).

Cyber Resilience Survey

24. NZBA submits that the draft survey in Annex B of the Consultation Paper is currently too detailed, would require a high level of detail in its responses and would be a time- and resource-intensive task to complete. We question why the RBNZ are proposing to seek this amount of information and for what purpose. We note that no response time is provided outside of the suggested annual / biennial frequency of reporting. That timeframe would place an onerous burden on banks, particularly if the current level of information sought is in addition to the proposal for periodic cyber incident reporting.

25. We suggest that alternative methods of data collection should instead be considered by the RBNZ. For example, the RBNZ could explore:

25.1. engaging with applicable banks to access relevant and agreed data already collected within existing external independent assessments that banks already have to prepare (for example, NIST assessments) instead of creating a separate survey; and

25.2. whether some information can be obtained by the RBNZ from other Government organisations, such as the GCSB, CERT NZ, and NCSC.

26. As currently drafted, we also note that the questions in the survey are drafted as a ‘one-size-fits-all’. They do not distinguish between businesses of low, medium or high inherent risk. We submit that RBNZ should ensure the survey provides the information it needs to assess the level of cyber resilience.

27. We are interested in whether the RBNZ will provide a benchmark of what “good” resilience looks like. The RBNZ may wish to consider an entity’s cybersecurity investment as a percentage of overall technology investment, as this is a widely used benchmark in industry.

28. We note, in relation to paragraph 25.2 above, that the consultation paper acknowledges that the NCSC has previously surveyed the financial sector’s resilience, is planning future surveys, and that both the RBNZ and NCSC entities are working together to identify where collaboration may be possible to reduce duplication. We welcome coordination between the RBNZ and other relevant entities to help reduce the compliance costs incurred by banks in providing multiple, mostly identical responses.

29. NZBA supports the RBNZ’s approach of following international practices, and the guidance on cyber resilience published in 2021 follows the same approach and recommends a list of frameworks for entities to refer to. We note that the NIST

Cybersecurity Framework (**CSF**) is currently being developed to v2.0 and further alignment with the new version would increase global regulatory harmonisation.

30. In particular, the Cyber Risk Institute Cybersecurity Profile (**CRI Profile**) builds upon NIST CSF and is specifically tailored to the financial sector by integrating various regulatory expectations and best practices from international standards. We submit that use of the CRI Profile could elevate the sector's cyber resilience and welcome opportunities to further discuss this with the RBNZ.

31. As to the frequency of reporting, we support the proposed frequency. We would suggest that, rather than categorisation by way of revenue, the RBNZ categorises banks in terms of Domestic Systemically Important Banks (**D-SIB**s) and non-D-SIBs, which is more consistent with how the RBNZ typically categorises banks in other areas. We submit that D-SIBs would be required to provide periodic cyber reporting every six months and a cyber survey annually, and non-D-SIBs to provide the report and survey annually and biennially, respectively.

Information Sharing

32. NZBA supports, in principle, the RBNZ's proposal to share data. However, we have some concerns about the potential extent of the RBNZ's use of the data. Cyber security is a highly sensitive area and collected data must be securely stored and its use carefully considered. We would request that further, more detailed information is provided on who the information will be shared with, how it is shared, for what reason, when it is disposed of and what happens if there is a data breach at the collecting organisation.

33. For example, on page one of the Consultation Paper, the RBNZ refers to the collection of information as supporting a number of functions which it lists and one of which is, for example, "*providing insights and intelligence on the cyber threat landscape that could be shared with industry, public sector agencies or others.*" At paragraph 4.3, the RBNZ refers to exploring how to "*publish trends, lessons or insights*", and at paragraph 5.1 that "*certain information we are proposing to collect is intended to be shared with various forums, including public sector agencies with an interest in cyber resilience and industry itself.*"

34. The information shared will relate to vulnerabilities of the reporting entity, and it is essential that data collected by the RBNZ is fully protected. Any data that may identify customers, employees or other stakeholders will need to be managed in accordance with the Privacy Act and requisite confidentiality considerations.

35. NZBA would support an approach where information shared outside the RBNZ or FMA is anonymised, or otherwise aggregated so that no individual organisation would be at risk of being identified.

Financial Policy Remit

36. NZBA requests clarity on the use of the term “with a low incidence of failure”. Our position is that without sufficient cyber resilience control processes and procedures, it would be very difficult to achieve a “low incidence of failure”.

Prioritisation of Cyber Data Collection Proposals

37. NZBA recommends that the RBNZ takes a risk-based approach towards cyber data collection as there is risk that the rich information collected may become the target of malicious threat actors.

38. We would also request further information as to the timeline of when the requirement will take effect. It would likely take banks at least six months to prepare to satisfy their reporting requirements on a regular and sustainable basis.

New Zealand Banking Association
Te Rangapū Pēke

Appendix 1

Proposed definition by RBNZ	Comments
Materiality definition	
A material cyber incident is one which materially affected, or had the potential to materially affect…	We propose removing "potential" incidents from the materiality definition. Unmaterialized threats have no impact and, therefore, should not be scoped in. Resources should be focused on actual incidents. The scope of cybersecurity incident should be limited to situations when there is evidence of a cybersecurity safeguard failure that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.
…financially or non-financially, the entity or the interests of its stakeholders such as depositors, policyholders, beneficiaries, other customers, system participants, or more broadly raises prudential concerns.	System participants and prudential concerns are not part of the APRA CPS234 materiality definition. For banks operating in both Australia and New Zealand, this broader definition may lead to dual compliance processes and potentially inconsistent reporting. It should be clarified whether the RBNZ is intending to extend the duty of care beyond its stakeholders to third parties in the broader financial system – if yes, then what are the limits around who a "system participant" may be?
	We propose clarifying the term "prudential concerns" and whether it pertains to cyber incidents with potential systemic impact or broader macro-prudential concerns. The former is more aligned with industry practices while the latter is determined by prudential regulator rather than FIs. As noted by RBNZ in the consultation paper, given that many FIs have close ties to Australia, there is value in aligning to APRA's approach. We also request clarification on whether the standard is intended to link to the sub-considerations of 'carry on business in a prudent manner" per s 78 of the Banking (Prudential Supervision) Act, or whether a different set of considerations are intended.

In assessing materiality, we consider that the following elements should be taken into account: • The impact of the cyber-incident on the entity's ability to carry on business in a prudent manner; • The extent to which the cyber-incident could result in financial consequences to the New Zealand financial system or to other financial entities; • The extent to which the cyber-incident had/has a negative impact on stakeholders such as customers, investors or system participants; • The extent to which the cyber-incident could have a significant adverse impact on the entity's reputation; • How long the cyber-incident lasted (if already remedied), or is expected to continue; • Whether the cyber-incident is an isolated incident, or part of a recurring pattern of cyber incidents; • The extent to which the cyber-incident indicates that the entity's internal control frameworks to ensure compliance with the conditions of registration are inadequate; and • The nature of the underlying cyber-incident.	The impact of a cyber-incident on an entity's ability to carry on business in a prudent manner could be assessed differently by different entities. As a result, what one entity views as material may not meet the threshold of materiality for another. Aligned with our comments above, we propose removing the line "the extent to which the cyber-incident could result in financial consequences to the New Zealand financial system or to other financial entities" from the guidance. It is difficult for FIs to ascertain the impact on the financial system or other financial entities as FIs may not have access to their information. This is an assessment that regulators may conduct in close collaboration with FIs. We propose removing "How long the cyber-incident lasted (if already remedied), or is expected to continue" because there may be instances where the immediate disruption of the cyber incident is mitigated and ongoing impact is minimized even if the effected entity continues to remediate the incident. If RBNZ wishes to retain this requirement, we seek clarity on how to calculate the length of incident and suggest that the time taken do not take into account post-incident efforts, such as root-cause analysis, controls uplift, and others.