AIA House,
74 Taharoto Road,
Takapuna,
Auckland 0622
-
Private Bag 92499,
Victoria Street West,
Auckland 1142

Phone (Int.) +64 9 487 9963
Freephone 0800 500 108
-
enquireNZ@aia.com
aia.co.nz

3 July 2023

Cyber data collection consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand – Te Pūtea Matua
PO Box 2498
Wellington 6140

By email: cyberresilience@rbnz.govt.nz
Copy to: S9(2)(a)

SUBMISSION ON THE DRAFT GUIDANCE FOR MANAGING CLIMATE-RELATED RISKS – AIA NEW ZEALAND LIMITED

This submission is made on behalf of AIA New Zealand Limited and its related entities (together, **AIA NZ**). It relates to the Reserve Bank of New Zealand - Te Pūtea Matua (**Reserve Bank**) March 2023 consultation paper on proposals for collecting financial entity related data to support cyber resilience (**Consultation Paper)** and the related material cyber incident report template (**Template**).

About AIA NZ

AIA NZ is a member of the AIA Group, which comprises the largest independent publicly listed pan-Asian life insurance group. It has a presence in 18 markets in Asia-Pacific and is listed on the Main Board of The Stock Exchange of Hong Kong. It is a market leader in the Asia-Pacific region (excluding Japan) based on life insurance premiums and holds leading positions across the majority of its markets.

Established in New Zealand in 1981, AIA NZ is New Zealand's largest life insurer and has been in business in New Zealand for over 40 years. AIA NZ's vision is to champion New Zealand to be the healthiest and best protected nation in the world.

AIA NZ offers a range of life and health insurance products that meet the needs of over 800,000 New Zealanders. AIA NZ is committed to an operating philosophy of *Doing the Right Thing, in the Right Way, with the Right People*.

AIA NZ is also a prominent member of the Financial Services Council (**FSC**).

Key submission points

AIA NZ is committed to protecting the interests of our customers, partners, employees and stakeholders, ensuring high standards of information security. AIA NZ has qualified staff who are members of the Information Systems Audit and Control Association (ISACA), the International Information System Security Certification Consortium (ISC2) and New Zealand Internet Task Force (NZITF). AIA NZ is bound by the AIA Group information security policies and standards that are consistent with those of leading companies globally to ensure that our systems, processes and information are secure.

Our full response to the Consultation Paper is attached to this letter. Our key points are summarised below:

1. AIA NZ appreciates the collaborative effort of the Financial Markets Authority (**FMA**) and the Reserve Bank and the proposed implementation of a singular Template that reduces regulatory burden, but do not believe Excel based reporting templates are a secure format to report cyber incidents. AIA NZ proposes that the Reserve Bank adopts a secure, online form of incident reporting to protect regulated entities and avoid the risk of the Reserve Bank making themselves a potential target for cyber-attacks by storing large amounts of cyber intelligence related data.

2. AIA NZ believes it is helpful that the proposed cyber incident reporting timeframe for the initial material cyber incident report is consistent with the reporting timeframes under the Financial Markets (Conduct of Institutions) Amendment Act 2022 (**CoFI**) and the Privacy Act 2020 (**Privacy Act**). However, a requirement to submit ongoing 24-hour reporting updates without any new information, or without clearly identifiable new information is resource intensive and has little added value. We favour a more pragmatic approach that would require updates to be provided if any further material information is discovered.

3. We propose the use of standard definitions and language. In our view, the proposed definition of materiality is open for interpretation and may lead to inconsistent reporting by different entities based on their internal assessments of harm and overall risk appetites. The Reserve Bank should clarify the definition of materiality and expand it further to include the material *effect* of a cyber incident. Furthermore, AIA NZ supports a closer alignment of the definition of materiality with other New Zealand regulators that impose similar cyber risk reporting obligations.

4. We recognise that there is a need for information sharing as proposed in the Reserve Bank's consultation document, provided information sharing is underpinned by an existing formally approved information sharing agreement with the receiving regulator or government agency, or where the information sharing is carried out in accordance with legislative authority, and / or subject to Principle 11 of the Privacy Act - Disclosure of Personal Information.

AIA NZ also contributed to and supports the submission from the FSC.

We would be pleased to discuss any questions you have on this submission and would welcome the opportunity to collaborate or consult further with the Reserve Bank as it considers the next steps.

Yours faithfully

S9(2)(a)

Question 1: Do you have comments on our proposed cyber incident reporting timeframe?

Overall, AIA NZ believes it is helpful that the proposed cyber incident reporting timeframe for the initial material cyber incident report is consistent with the reporting timeframes under CoFI and the Privacy Act. This timeframe is well understood by regulated entities and are already embedded in AIA NZ's privacy response processes.

However, we have concerns about the proposed timeframe for submitting a material cyber incident update every 24 hours until the incident is concluded (Part B of the Template). In our view, this would be overly burdensome and could create material unintended consequences, for example creating a 'rush to act' and detracting from level-headed incident resolution. Reporting every 24 hours is resource intensive and has little added value for reporting entities who should be focusing resources on responding to the cyber incident. In addition, the majority of the information requested in Parts A and B are only available following a full cyber incident assessment. Please see our further comments on the Template in our response to Question 3 below.

We favour a pragmatic approach to management of cyber resilience responses that encourage ongoing communications, when necessary, rather than burdensome point in time reporting.

Question 2: Do you have comments on our proposed definition of materiality?

AIA NZ believes that the proposed definition of materiality should be amended to provide more clarity and expanded to define the material *effect* of a cyber incident. We note that the Reserve Bank takes into account the extent to which a cyber incident had/has a negative impact on stakeholders but this does not sufficiently clarify what the material effect of a cyber incident is. In our view the materiality of cyber security incidents also depends on the range of harm that such incidents could cause. We further consider that the proposed definition of materiality in its current format is open for interpretation and may lead to inconsistent reporting by different entities based on their internal assessments of harm and overall risk appetites. For example, it is unclear whether it is intended for near miss events such as phishing attempts to be deemed as an incident that "had the potential to materially affect" the entity, or the interests of stakeholders, etc. Providing examples of incidents that would meet the materiality threshold would be helpful to further reduce potential subjectivity.

We note that the Reserve Bank adopted the Australian Prudential Regulation Authority (**APRA**) definition of materiality to accommodate New Zealand regulated entities with close ties to Australia. However, we disagree that the differences between the Reserve Bank's definition compared to the FMA's definition of materiality would not result in substantive differences in the types of incidents reported. We would prefer closer alignment across New Zealand regulators to avoid adding to regulated entities' regulatory burden of performing multiple assessments of the same cyber incident for the purpose of reporting to the Reserve Bank, FMA and the Office of the Privacy Commission (**OPC**). To mitigate the regulatory burden of reporting the same cyber incident to multiple regulators and subsequently responding to questions from multiple regulators we favour an approach

where either the FMA or the Reserve Bank should be identified as the single point of contact for a regulated entity.

Question 3: Do you have comments on our proposed cyber incident reporting template?

AIA NZ agrees that the Template provides clarity on the content of the report and ensures consistency of reporting regardless of the size or primary business of the reporting entity. We appreciate the collaborative effort of the FMA and the Reserve Bank and the proposed implementation of a singular Template that reduces regulatory burden. We do have the following comments to note:

Format

In our view, Excel files are not a secure format to report cyber incidents that may have a profound impact on a reporting entities' business, stakeholders and reputation, irrespective of submission through the Reserve Bank's BOX file sharing platform. Common issues when using Excel for data operations include inadequate encryption features for protecting sensitive business information, as well as the lack of error control as it is easy for any reader to inadvertently change a cell and therefore erode the data validity. Excel furthermore has problematic scalability, and collaboration is difficult where multiple users might otherwise have been able to submit data.

AIA NZ strongly proposes that the Reserve Bank adopts an online form of incident reporting similar to what CERT NZ, APRA and the OPC have in place for their regulated entities. In addition, we take note that the Reserve Bank will have appropriate safeguards in place to secure data provided as part of cyber resilience reporting, but welcome more specific information on the proposed measures the Reserve Bank will adopt to ensure data security and controlled access to the data. In addition, we propose the Reserve Bank consider including a disclaimer to the effect that securing the channels to transmit this data remains the accountability of the Reserve Bank and that the Reserve Bank would remediate any 'data-in-transit' and 'data-in-storage' breaches.

Repetitiveness

Parts A, B and C of the Template are tabs of the same Excel workbook and by default will be submitted together with each subsequent submission. However, this is highly repetitive as part B of the Template is a full restatement of the same information contained in part A *in addition* to any new information that may be included in part B. Part B of the Template does not differentiate between information already submitted in Part A and information that is new or amended. As noted in our response to question 1, part B is proposed to be submitted every 24 hours. It will be burdensome for the Reserve Bank to manually identify the new or amended information (if any) in every subsequent submission following the initial report in part A.

AIA NZ supports an alternative approach where part B is streamlined and reserved for reporting substantial new or different information until the cyber incident has concluded and has been fully mitigated and resolved. In addition, supervisors can request additional updates at any time.

Granular data

Further to our response to question 2, a cyber incident would trigger reporting to multiple regulators and government agencies, including the FMA, OPC, CERT NZ, and the National Cyber Security Centre (**NCSC**). We note that compared to the level of data required for reporting to the OPC, CERT NZ and NCSC the proposed cyber incident reporting template is much more detailed. The level of detail required may not be readily available within the reporting timeframe and further distract from response and recovery efforts. As noted in the Consultation Paper, the Reserve Bank cannot provide a technical response to an incident, therefore the proposed level of detail may not position the Reserve Bank to mitigate a cyber incident. In addition, part C of the Template requires detailed, sensitive information on the steps taken to resolve and mitigate a cyber incident and as this document is sent externally it poses a risk to regulated entities. We believe it would be more appropriate to discuss remediation activities directly with the supervisor.

Question 4: Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

Without first knowing the extent of the data that is proposed to be requested as part of periodic incident reporting AIA NZ is unable to comment on the impact on technological resources, training and the effort required to extract the data for this reporting. We would appreciate further detail on the Reserve Bank's planned measures to store and protect this information.

We encourage guidance on what constitutes in and out of scope incidents for annual periodic reporting. AIA NZ notes that financial institutions are under constant low level cyber security probing which includes events such as phishing attempts that are automatically stopped by the entities' cyber security measures. Including these types of cyber incidents will result in inflated number of instances being reported on and if each of these were considered an incident the overheads required to perform reporting would be unsustainable. Further it would detract resource from cyber resilience activities.

Question 5: Do you have comments on our proposed periodic reporting of cyber resilience capability survey?

AIA NZ supports the Reserve Bank's proposal to conduct periodic reporting of cyber resilience capability surveys. However, we note the basic and high-level responses required from entities and that it does not differentiate between the different size of entities and therefore question the usefulness of the surveys in the proposed format. We further note that some questions[1] require a response that covers the prior 24 month period, fitting for the frequency of reporting in respect of other entities, but not for large entities that require annual surveys. The Reserve Bank may want to consider separate surveys for the two different reporting entity

[1] Refer section A1, Q4 and Q5, as well as section B3, Q4 and Q6 of the cyber resilience capability survey.

types, or rewording the relevant questions to ensure relevance for both large and other entity types. In addition, we welcome further clarification of the definition of a large institution as it is unclear whether the $2b threshold relates to assets or revenue for example.

We note that the information being requested provides significant cyber intelligence on an entity and raises serious risk concerns if it is to be collated and then disclosed externally. Where the Reserve Bank stores and potentially share this information it should be anonymised and encrypted because the cyber resilience capability surveys in itself may cause a threat to cyber resilience. The RBNZ could consider an alternative approach of an online anonymous survey to collect the desired sectoral data.

Question 6: Do you have comments on our proposed frequency of reporting?

Please note our response to question 5 above.

Question 7: Do you have comments on how we propose to share information?

We understand that cyber security is a shared concern and part of the remit of multiple government agencies and regulators including the Reserve Bank, FMA, OPC, CERT NZ and NCSC along with being a priority theme for the Council of Financial Regulators (**CoFR**). We recognise that there is a need for information sharing as the vulnerability of one reporting entity can threaten the organisation's stakeholders, customers, partners, employees and wider industry.

AIA NZ is comfortable with the Reserve Bank's proposed sharing of cyber resilience data collected as part of the two periodic surveys where it is done under an existing formally approved information sharing agreement with the receiving regulator or government agency, or where the information sharing is done in accordance with relevant sectoral legislation, and / or subject to Principle 11 of the Privacy Act. We note that the CoFR members are currently working on information gathering and sharing arrangements. Entities are particularly vulnerable and exposed where they have disclosed information pertaining to their firewall or IT security measures. It is of utmost importance to AIA NZ that the data provided as part of Reserve Bank's cyber resilience data collection proposals are fully safeguarded and well protected. In addition, identifiable data relating to our customers, employees and other stakeholders must be safeguarded as set out in the Privacy Act. We expect that the Reserve Bank continues to safeguard and protect commercially sensitive information of AIA NZ and its partners.

Question 8: Do you have comments on our analysis on the financial policy remit?

AIA NZ does not have any comments on the Reserve Bank's analysis on the financial policy remit.

Question 9: Do you have comments on our prioritisation of our cyber data collection proposals?

AIA NZ considers that our feedback requires further discussion with the Reserve Bank, which would impact the proposed timeline for implementation.

RESPONSE ON THE RBNZ CYBER RESILIENCE DATA COLLECTION PROPOSAL

ANZ BANK NEW ZEALAND LIMITED

3 July 2023

Confidential

1. INTRODUCTION

1.1 ANZ Bank New Zealand Limited (**ANZ**) welcomes the opportunity to provide feedback to the Reserve Bank of New Zealand (**RBNZ**) on the Cyber Resilience Data Collection Proposal.

1.2 ANZ is aware that the New Zealand Banking Association (**NZBA**) and the Financial Services Council (**FSC**) have also provided an industry response on the Cyber Resilience Data Collection Proposal. ANZ has contributed to and supports the relevant aspects of those responses.

2. CONTACT DETAILS

2.1. Please contact [redacted] if you would like to discuss the contents of this response.

3. CONFIDENTIALITY

3.1. ANZ requests that the information identified in this response as requiring confidentiality are kept confidential on the grounds of protection of personal information and commercial sensitivity. If the RBNZ receives a request to release our response under the Official Information Act, we ask that the RBNZ consult with us, and our preference is that the information identified is withheld.

4. SUMMARY/GENERAL COMMENTS

4.1. ANZ supports the intent of the proposal. The purpose of this submission is to suggest improvements to some areas to better ensure the intent is achieved. Although we agree with the general intent, we consider that some information within the survey would be less relevant due to both the size and scale of organisations completing those metrics.

5. RECOMMENDATION OF SUBMISSION

1. Do you have comments on our proposed cyber incident reporting timeframe?

ANZ supports the proposed timeline of 72 hours, which is consistent with reporting timeframes under other regimes i.e., the Privacy Act 2020 and the Financial Markets (Conduct of Institutions) Amendment Act 2022, and we consider it goes some way to standardising the notification process between different regimes and regulators. ANZ also see value in expanding the definitions and reporting outcomes across regulators, particularly where New Zealand banks have additional responsibility to report the same data. ANZ seek clarity to align other RBNZ reporting timelines, particularly in relation to reporting operational material incidents (not as a result of a cyber-attack) and whether the Incident Response template could cater for both requirements to avoid the regulatory burden of performing multiple assessments over the same cyber incident for reporting purposes.

ANZ consider the completion of Part B every 24 hours to be impractical and we would support an alternative approach where a short form is created for immediate notification, and Part B is reserved for new or updated information as it becomes available. ANZ query the benefit of reliance on an excel spreadsheet updates vs. maintaining open channels of communication during an incident as previously enacted. For example, completing a template update could prompt further queries amongst impacted organisations and in this instance, open communication channels to co-ordinate cyber resilience actions could work better to improve the overall response to such an attack whilst fulfilling the RBNZ's objectivesof monitoring financial sector stability.

2. Do you have comments on our proposed definition of materiality?

Our view is that the definitions provide greater clarity on what constitutes a material cyber incident. However, we consider the proposed definition could be further clarified and expanded to define the material effect of a cyber incident. We note that the RBNZ considers the extent to which a cyber incident had or has a negative impact on stakeholders, but this does not sufficiently clarify what the material effect of a cyber incident is. In addition, the proposed definition of materiality is open for interpretation and may lead to inconsistent reporting by different entities based on their internal assessments of harm and overall risk appetites.

We note that the RBNZ has adopted the Australian Prudential Regulation Authority (APRA) definition of materiality to accommodate New Zealand regulated entities with close ties to Australia. However, we disagree that the differences between the RBNZ's definition compared to the FMA's definition of materiality would not result in substantive differences in the types of incidents reported. In addition, the RBNZ's definition is wider than the FMA's which, due to the sharing arrangements in place with the FMA, will effectively require entities to be pragmatic and report to both simultaneously. This may also be the approach taken to avoid responding to enquiries from one regulator who may have heard of the incident from the other and, detract resources from responding to the incident. ANZ supports the need for clear definitions for "Cyber Event", "Materiality", and "Cyber Incident".

3. Do you have comments on our proposed cyber incident reporting template?

ANZ supports completing the template in a secure (encrypted) application as opposed to utilising Excel securely transmitted through the RBNZ's BOX Facility, which could be prone to data quality errors. However, ANZ would provide the data regardless but propose the inclusion a disclaimer stating that securing the channels to transmit this data remains an RBNZ accountability and any 'data-in-transit' and 'data-in-storage' breaches would fall to the RBNZ for remedial action.

ANZ view Question A08 "Cyber Attack" as a cause and A09 "Internal outage/service failure" as an impact or consequence of that cause i.e., "an attack". It could also be that both could apply as a "cause" and accordingly ANZ seeks clarity as to whether this separation in the template is purposeful noting the requirements as they are drafted require material incidents impacting both core banking systems and cyber incidents to be reported. While the question heading indicates reporting of "cyber incidents", the requested data points seem to indicate a broader purpose of data collection.

Questions 9.1, 9.2, 11, 11.1, 11.2, 12, 12.1, 12.2, 13, 13.1 and 13.2 are tailored more towards operational outages to core banking systems and as stated above, further clarity on the definitions for "Cyber Incidents" and "Cyber Attack" is required to better assess the intended outcomes.

In response to Question 14.1 relating to selecting which customers have been impacted by the incident, we understand in some circumstances this could apply to "All".

4. Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

ANZ propose that PART A be reduced to focus on the minimum amount of information required to report a cyber incident as many of the questions would only be available through finalising the Post-Incident Review (PIR) process for many organisations. With reference to Question 1, similarly, the requirement to repeat this information in Part B every 24 hours is considered overly burdensome and ANZ query whether open channels of communication during the incident would be more effective to fulfil ongoing updates as they unravel.

5. Do you have comments on our proposed periodic cyber resilience capability survey?

Financial institutions are under constant low level cyber security probing which includes events such as phishing attempts and blocked requests that are automatically stopped by the entities' firewalls and other cyber security measures. Including these types of cyber incidents will result in inflated number of instances being reported on and if each of these were considered an incident the overheads required to perform reporting would likely be unsustainable. ANZ are unable to comment on the impact on technological resources, training and the effort required to extract the data for periodic incident reporting without clear understanding of the extent of the data that is being requested.

Manual reporting requirements may also require resourcing allocations and ANZ also would propose reviewing more robust automated processes to obtain data, for example, through API's where the information could be obtained with minimal overhead to any organisation.

In seeking numerical values through the survey response, we have concerns that the response would vary from organisation to organisation and given the differences in size and scale, and we question the usefulness of this information.

6. Do you have comments on our proposed frequency of reporting or the threshold for reporting more frequently?

We are comfortable with the suggested cadence of reporting.

7. Do you have comments on how we propose to share information?

ANZ expect that the RBNZ continues to safeguard and protect commercially sensitive information of reporting entities. ANZ recognises that the information shared pertains to vulnerabilities of the reporting entity, and a breach of such data could threaten the organisation's stakeholders, customers, partners, employees, and the wider industry. Therefore, it is of utmost importance that the data provided as part of RBNZ's cyber resilience data collection proposals are fully safeguarded and that identifiable data relating to customers, employees and other stakeholders are managed in accordance with the Privacy Act 2020. ANZ encourages the inclusion of a disclaimer stating that securing the channels to transmit this data remains an RBNZ accountability and any 'data-in-transit' and 'data-in-storage' breaches would fall to the RBNZ for remedial action.

ANZ would support a consistent approach whereby any information shared outside the RBNZ or FMA is anonymised or only provided at an aggregated level that would prevent an individual organisation being identified.

8. Do you have any comments on our analysis on the financial policy remit?

ANZ seek clarity to the first two components of the Financial Policy remit where the use of terms "with a low incidence of failure" have been utilised. Whilst the RBNZ states this is not of high relevance, ANZ's opinion is that without adequate Cyber Resilience control processes and procedures, a "low incidence of failure" would not be possible.

9. Do you have comments on our proposed prioritisation of our cyber data collection proposals?

ANZ would require a minimum of 6 months to fulfil the reporting requirements on a more sustainable basis due to its manual format and request of specific metrics that would need some level of coordination between our SME's, as well as alignment with our internal governance processes and timings.

RBNZ Cyber Resilience Data Collection Proposals (Step 2: Cyber Data Collection Requirements and Information Sharing Arrangements): BNZ response

3 July 2023

Introduction

1. Bank of New Zealand ("BNZ") appreciates the opportunity to provide feedback to the Reserve Bank of New Zealand ("RBNZ") on the consultation paper: Cyber Resilience Data Collection Proposals ("Consultation Paper"). BNZ recognises that prudential and privacy regulators globally are rightly responding to the evolution and pace of cyber-attacks and BNZ commends RBNZ for the steps being taken to increase the oversight of cyber resilience across regulated entities in New Zealand.

2. BNZ encourages RBNZ to adopt a highly active approach to bolster cyber resilience across the financial industry. BNZ also supports ongoing collaboration between regulators and regulated entities to build greater cyber resilience.

3. BNZ supports the separate response of the NZBA on this Consultation Paper and provides its specific feedback under the general headings below.

BNZ's responses to the questions in the Consultation Paper

Q.1 Do you have comments on our proposed cyber incident reporting timeframe?

4. BNZ agrees with the proposed approach to cyber incident reporting and the alignment with Australian requirements.

5. BNZ notes that the Consultation Paper proposes a 72-hour timeframe for regulated entities to provide Part A of the Material Cyber Incident Notification Report Template ("**the template**") to RBNZ. As a matter of course, BNZ would contact its prudential supervisors as soon as practically possible as an initial notification of a cyber related incident and expects the template would be in addition to this existing process.

6. BNZ considers that further clarification and guidance on the interpretation of "detection" would be useful to ensure the requirement is clear and appropriate. BNZ notes that it may take some time for an entity to identify that an incident has reached the threshold to be reportable. One way of ensuring that material incidents are appropriately reported might be to define "detection" as the moment the management of the entity become are briefed of the incident. This aligns with the current approach to data breach notifications involving third party or related parties.

Q.2 Do you have comments on our proposed definition of materiality?

7. BNZ agree with the materiality definition and aligning it with the existing APRA definition.

Q.3 Do you have comments on our proposed cyber incident reporting template?

8. BNZ is broadly supportive of the template.

9. It would be helpful for RBNZ to provide guidance on the purpose and intent of the "Low" severity classification under section A07.0 of the template, as this definition does not look to meet the materiality threshold for reporting.

10. Section A9.0 of the template, "*Internal outage/service failure*", includes operational resilience matters as well as cyber related incidents. BNZ submits that clarification on the definitions of "*cyber resilience*", "*cybersecurity*", "*cyber incident*" and "*information security controls*" would be helpful, to ensure that the intended and appropriate coverage is met.

11. The RBNZ Guidance on Cyber Resilience defines a "cyber incident" as one that "*jeopardises the cybersecurity of the (information) systems / information"* and "cybersecurity" as "*the preservation of the Confidential, Integrity, Availability of (information) systems."* The proposed definitions indicate that RBNZ would expect to receive notifications for material technology outages caused by threats that would not typically be considered "security" threats. BNZ believes that this would result in substantive differences in the types of incidents reported. For example, BNZ would consider a failed change management that brings down a critical system to be an operational resilience incident but, under the proposed definitions, BNZ would also be required to capture such incidents in the cyber incident template. BNZ submits that operational resilience incidents should be reported separately from cyber security related incidents.

12. BNZ understands and agrees that RBNZ should be kept up to date as cyber incidents unfold, however, BNZ considers that an updated template should only be required if there are sufficient updates to help inform RBNZ. BNZ submits that an email or phone call to the supervisor may be more appropriate to clarify minor/limited daily updates as the incident develops.

Q.4 Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

13. BNZ submits that annual reporting of all cyber incidents for all entities would be sufficient to provide all the relevant information to RBNZ. BNZ suggests that RBNZ may be able to obtain the appropriate information from other government organisations such as the National Cyber Security Centre or Computer Emergency Response Team NZ, which produces a quarterly report on the volume and scenario analysis of local cyber security attacks.

14. The definition of "cyber incident" in the context of periodic breach reporting could result in over reporting of cyber incidents. For example, a staff member clicking on a phishing email may fall into this definition as it is an incident that would potentially jeopardise the cyber resilience of an entities technology systems due to the regular occurrence of this event. BNZ submit that requiring entities to report this type of cyber incident would not assist in providing the outcome that the RBNZ is looking for as entities will have a comprehensive set of mitigating controls for this type of event.

15. Similarly, cyber incidents that "*violate(s) the security policies, security procedures or acceptable use policies; whether resulting from malicious activity or not*" does not account for mitigating controls within an entity. BNZ submits that requiring entities to report every single control failure would not assist the RBNZ to understand that the nature of cyber incidents impacting regulated entities.

16. BNZ is currently required to report information about cyber incidents that materially impact the cyber resilience of its technology systems to RBNZ and APRA. BNZ notes that potential material incidents and material control weakness that were assessed, but did not meet the threshold for formal reporting, would be available for RBNZ on request to assess and ensure a consistent approach is being taken to assessment and reporting. The calibration for this threshold could be clarified by individual bank supervisors.

Q.5 Do you have comments on our proposed periodic cyber resilience capability survey?

17. BNZ understands the intended outcome and supports the proposed approach to require entities to periodically provide data which provides insights into its cyber resilience capabilities.

18. BNZ suggest that, as a potential alternative or supplementary option to the periodic cyber resilience capability survey, could be to require entities to provide RBNZ with an independent assessment of an entity's capabilities against an industry-recognised Cyber Framework, such as

NIST CSF. This could offer a more comprehensive view of an entity's cyber resilience capabilities, and could be benchmarked both locally, regionally, and globally.

19. To ensure that entities are providing the most useful information to RBNZ, further clarification would be helpful in relation to the following capability survey questions:

    19.1. **B2. Protect Q4** "*How many times have you recorded breaches of security controls in the last 12 months*?". BNZ submits that further guidance is needed to ensure that RBNZ is provided with accurate and consistent information regarding security control weaknesses. BNZ suggests aligning this notification requirement to APRA CPS 234 in which an entity is required to notify after it becomes aware of a material information security control weakness which the entity expects it will not remediate in a timely manner. BNZ submit that "security controls" should be clearly defined to ensure RBNZ is provided with consistent and accurate information.

    19.2. **B2. Protect Q5** "*How many risk assessments have been undertaken*?" and **B2. Protect Q8** "*How many times in the last 12 months have you assessed for cyber security risk (include data loss prevention, data egress checking, data classification)*". BNZ undertakes a range of cyber security risk assessments for change (including Cyber Consulting assessments of new and material Business and Technology change), Internal Audits, External Audits, Third Party Supplier Testing, NIST, SWIFT CSP, etc. It would be helpful to understand the different types of information the RBNZ expects to receive under these two questions.

    19.3. **B3. Detect Q4** "*How many times were event, system, and data logs backed up to a secure location over the last 24 months*?". BNZ notes that this question focuses on an organisation's backup control to minimise the exposure and timely recovery from a Ransomware event. BNZ suggests a requirement to provide an evaluation of the extent of systems coverage and successful restore of critical system backups would be more effective in measuring an entities management of this risk.

Q6. Do you have comments on our proposed frequency of reporting?

20. BNZ supports the annual reporting frequency for larger institutions.

21. BNZ notes that the timing of reporting and scale of reporting requests need to be managed to ensure this can be completed in a consistent and timely manner.

Q7. Do you have comments on how we propose to share information?

22. BNZ supports the sharing of information provided with NCSC and encourages the RBNZ to work with NCSC on a crisis management framework that would help co-ordination of a response to a financial service provider cyber-attack.

Q8. Do you have any comments on our analysis on the financial policy remit?

23. BNZ supports the analysis set out in the RBNZ consultation paper. We note that one the learnings from the recent Silicon Valley Bank failure in the USA was that non systemically important banks can still have a disproportionate impact on financial stability across the sector where they are subject to failure or elevated risk. On this basis, BNZ urges the RBNZ to carefully consider proportionality settings in the context of cyber resilience.

Q9. Do you have comments on our proposed prioritisation of our cyber data collection proposals?

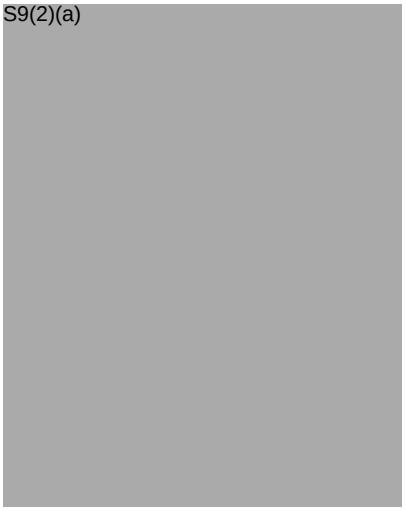
24. BNZ agrees that information sharing is an appropriate section of the RBNZ Cyber Resilience Guidelines to prioritise for sector wide reporting and alignment.

25. Consideration should be given to fast-track next steps of entity assessments regarding Governance; ensuring Boards and Senior Management are appropriately aware of cyber resilience expectations and are driving appropriate Capability and a cyber aware culture in their organisations.

26. BNZ's preference is for a highly active regulatory response to drive appropriate cyber resilience maturity across the industry. APRA, as a comparative example, first released guidance (CPG 234) in 2013 and implemented their mandatory standard (CPS 234) in 2019. New Zealand must progress faster given the recent volume of significant cyber events locally and regionally.

27. We look forward to the progression of the guidance to support the cyber resilience of the sector and all New Zealand. If you have any further questions in relation to this matter, please let me know.

S9(2)(a)



S9(2)(a)

From: S9(2)(a)
Sent: Friday, 23 June 2023 10:20 am
To: cyberresilience
Cc: S9(2)(a)
Subject: BANK OF CHINA - RE: Media release: Feedback sought on plans to build cyber resilience

To whom it may concern,

It's a great opportunity BOCNZ can participate in this consultation. The documents are very well organized and have a comprehensive consideration based on expertise and peer practice, however I do have some questions on Q2 and Q7 listed below,

Q2 Do you have comments on our proposed definition of materiality?

- Is it possible to provide benchmark samples of "material impact" in the guidance?
e.g.: *if 1% or 200+ customers were affected; or the cyber incident lasted more than 12 hours; etc.*. then it can be considered as "material impact".
It will help us to collect data from database and analyse the impact level based on a clear instruction.

Q7 Do you have comments on how we propose to share information?

- How RBNZ will share information among its regulated entities? Will there be more detailed information than regular trend reports so we can case study on them?
Will RBNZ consider warning its regulated entities about any potential attack if RBNZ received multiple attack reports from any internal or external channels in a short period or RBNZ discovered some significant incident itself? This will help us to prepare and get ready.

Thanks for your time.

Kind Regards,
S9(2)(a)
Bank of China (New Zealand)
Website: www.bankofchina.com/nz
S9(2)(a)
A: Level 17, Tower 1, 205 Queen Street, Auckland 1010

From: Reserve Bank of New Zealand <no-reply@lists.rbnz.govt.nz>
Sent: Monday, May 8, 2023 2:08 PM
To: S9(2)(a)
Subject: Media release: Feedback sought on plans to build cyber resilience

View this email in your browser

Feedback sought on plans to build cyber resilience

8 May 2023

The Reserve Bank of New Zealand – Te Pūtea Matua is seeking feedback on proposals for collecting financial entity related data to support cyber resilience.

The ability of cyber attackers to undermine, disrupt, and disable information and communication technology systems used by financial entities is a threat to financial stability. Service outages can affect individuals, businesses and organisations and lead to a loss of confidence where there is lack of alternative providers or disruptions between financial entities.

To improve our understanding of cyber risks and resilience in the financial sector, our consultation paper proposes the collection of data in three areas:

- a material cyber incident reporting requirement that mandates regulated entities to report all material cyber incidents to the Reserve Bank within 72 hours after detection;
- reporting of all cyber incidents, regardless of materiality, on a periodic basis; and
- a periodic survey on the cyber resilience of regulated entities based on the Reserve Bank's cyber resilience guidance.

Director of Prudential Policy Kate Le Quesne says "Collection of this information will improve our understanding of cyber resilience in the financial sector. It will also support industry engagement by sharing insights and ultimately enable

better responses to cyber incidents".

The Reserve Bank is working closely with the Financial Markets Authority on cyber data collection. We propose that our material incident reporting template can be used for reporting to both entities and that information gathered from the proposals will be shared. This would provide a joined up approach across regulators and minimise regulatory burden for our regulated entities.

On 1 May 2021, we published guidance for our regulated entities on cyber resilience. The Guidance sets our expectations (as the prudential regulator) on how our regulated entities can build cyber resilience to help promote a sound and dynamic financial system.

More information

- Consultation Paper - Cyber Resilience Data Collection Plan
- Guidance for our regulated entities on cyber resilience

Media contact:

S9(2)(a)

Read more

Our mailing address is:

Reserve Bank of New Zealand

2 The Terrace

Wellington, 6140

New Zealand

Add us to your address book

Want to change how you receive these emails?

You can update your preferences or unsubscribe from this list.

==========

此邮件已由 Deep Discovery Email Inspector 进行了分析。

Corporate Trustees Association

cta.org.nz

3 July 2023

Cyber data collection consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498 Wellington 6140

By email: cyberresilience@rbnz.govt.nz

Cyber Resilience Data Collection Proposals

The Corporate Trustees Association welcomes the opportunity to comment on your May 2023 Cyber Resilience Data Collection Proposals.

CTA is the industry association for New Zealand's five licensed supervisors. Collectively supervising over $500 billion assets under management, and licensed by the Financial Markets Authority under the Financial Markets Supervisors Act 2011, our members fulfil a statutory role under that Act to help enhance investor confidence in financial markets and retirement villages. CTA members supervise 14 Non-Bank Deposit Takers (NBDTs).

I attach our responses to your consultation questions. We address only the questions that relate to NBDTs.

Please contact me if you require any further information from CTA members.

S9(2)(a)

Q1 Do you have comments on our proposed cyber incident reporting timeframe?

We note that the RBNZ's proposed approach is that all material incidents (as defined) must be reported as soon as practicable after they are detected but no later than 72 hours. CTA suggests that the 72 hours should not commence from the time of detection, but from the point that the incident is considered material (by the management/board of the entity).

A minor issue may be detected and investigated and prove later to be material.

We note that NBDTs will report material cyber issues to their supervisors who in turn will report to the FMA and RBNZ under section 203 of the Financial Markets Conduct Act 2013 (FMC Act) and sections 25/26 of the Non-bank Deposit Takers Act 2013 (NBDT Act).

CTA members supervise small entities (all NBDTs are under $2b). The RBNZ may wish to consider a longer time period for small entities in recognition of their capacity and risk to the overall financial system.

Q2 Do you have comments on our proposed definition of materiality?

CTA supports the proposed definition.

In our view, any breaches of legislation or the NBDTs' governing documents (trust deeds), or legislation (FMC Act and NBDT Act in particular) would be material. We suggest guidance from RBNZ that contractual or legislative breaches would be the types of material cyber incident that would "more broadly raises prudential concerns".

Q3 Do you have comments on our proposed cyber incident reporting template?

CTA considers the proposed cyber incident reporting template fit for purpose.

However, as noted in Q1 above, NBDTs need to report material issues to their supervisors, and therefore this could be reflected in section A20.0.

We suggest that the form includes a section where the cyber incident can be described in a series of paragraphs by the entity submitting. While drop down options and short answers are important to ensure all the relevant information is captured, if these are used exclusively, important context and detail may be missed.

Q4 Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

Annual reporting is reasonable for NBDTs (all of which are not large).

Q5 Do you have comments on our proposed periodic cyber resilience capability survey?

No comment.

Q6 Do you have comments on our proposed frequency of reporting?

CTA considers biennially reporting of cyber resilience capability surveys would be appropriate for NBDTs.

Q7 Do you have comments on how we propose to share information?

No comment.

Q8 Do you have any comments on our analysis on the financial policy remit?

The RBNZ may wish to consider proportionality with regard to the cyber reporting timeframe (Question 1).

Q9 Do you have comments on our proposed prioritisation of our cyber data collection proposals?

No comment.

Financial Services Council NZ

Grow the financial confidence and wellbeing of New Zealanders

Monday 3 July 2023

Cyber Data Collection Consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

By email: cyberresilience@rbnz.govt.nz

Cyber Resilience Data Collection Proposals

This submission on the Reserve Bank of New Zealand (RB) Cyber Resilience Data Collection Proposals (the Consultation Paper), is from the Financial Services Council of New Zealand Incorporated (FSC).

As the voice of the sector, the FSC is a non-profit member organisation with a vision to grow the financial confidence and wellbeing of New Zealanders. FSC members commit to delivering strong consumer outcomes from a professional and sustainable financial services sector. Our 115 members manage funds of more than $95bn and pay out claims of $2.8bn per year (life and health insurance). Members include the major insurers in life, health, disability and income insurance, fund managers, KiwiSaver, and workplace savings schemes (including restricted schemes), professional service providers, and technology providers to the financial services sector.

Our submission has been developed through consultation with FSC members and represents the views of our members and our industry. We acknowledge the time and input of our members in contributing to this submission.

We welcome the opportunity to provide feedback on data collection proposals following on from the 2021 Cyber Risk Management Guidance to strengthen our industry against cyber incidents and risks. We also thank S9(2)(a) for attending the April FSC Regulation Committee to discuss this upcoming consultation.

Our members support the proactive approach being taken by both the RB and the Financial Markets Authority (FMA) in addressing this continual and substantive risk to our industry. Our feedback reflects our desire that the data collected is meaningful and useful in advancing cyber resilience without unduly significantly increasing regulatory burden and resource strain on our member organisations. As such we have recommended amendments to the proposals to assist in reporting being timely, consistent, accurate and therefore of value. We encourage standard definitions and language, starting with the definition of an incident and in turn a cyber incident. It is also valuable to align with existing notification processes and timeframes some of our members may deal with in other jurisdictions or those of their group or parent company.

We strongly encourage consideration of a short form being created for notification of material cyber incidents and agreeing with the RB additional information as required. We have concerns that the ongoing 24 hour reporting updates will not only potentially detract from addressing incidents but increase regulatory burden and resource strain on our member organisations and an increased workload for the RB.

We consider some of the information within the periodic survey, in particular information pertaining to organisation operational behaviours and some of the specific quantitative measures, will not be useful due

to differences in organisation context, size and scale. We propose alternatives to the periodic survey to ensure that the cyber resilience of regulated entities is protected and not unduly put at risk with large amounts of cyber intelligence being stored by RB making it a potential target itself for cyber attacks.

We welcome continued discussions and engagement and extend a further invitation to attend the FSC Regulation Committee if this would be helpful. I can be contacted on S9(2)(a) S9(2)(a) to discuss any element of our submission.

Yours sincerely

S9(2)(a)
Financial Services Council of New Zealand Incorporated

1. Do you have comments on our proposed cyber incident reporting timeframe?

The proposed cyber incident reporting timeframe for the initial material cyber incident report is pragmatic and consistent with the reporting timeframes under the Financial Markets (Conduct of Institutions) Amendment Act 2022 (CoFI) and the Privacy Act 2020. The coordination between the RB and the FMA to align the reporting timeframe of no later than 72 hours will help standardise processes for notifying regulators. However, we seek clarification and guidance on the interpretation and application of 'detection' of cyber incidents. We note the Australian Prudential Regulation Authority (APRA) requires the 72 hour clock to start ticking from the time an entity becomes aware that the incident has hit the materiality threshold.[1] If this is reported too early, it could create unnecessary costs and strain to a business. We also query whether the recommended 72 hours is over business hours or three consecutive days.

Our members concerns focus on the Material Cyber Incident Notification Report template (the Template) itself, which is considered excessive in terms of the information required, particularly within a 72 hour timeframe. The requirement to complete Part B every 24 hours from the previous submission of Part A or B until the incident is concluded is overly burdensome. Such reporting is resource intensive, adds to the regulatory burden on reporting entities and may have the unintended consequence of detracting from the resolution of the incident in question. In addition, the majority of the information requested in Parts A and B are only available following a full Priority Information Report.

We support an alternative approach where Parts A and B are streamlined, and a short form is created for notification within 72 hours and updates are provided as agreed with the supervisor. This also supports the purpose of collecting the data relating to cyber incidents being for better understanding of the nature of cyber incidents impacting regulated entities. Please see our further comments on the Template in our response to Question 3 below.

As it is possible that the full extent of a cyber incident may not be known within the reporting timeframe, any notifications provided to the RB, and other regulators, may be incomplete or continue to evolve over time as more information is obtained. We encourage a pragmatic approach to management of cyber resilience responses that encourage ongoing communications rather than burdensome point in time reporting.

If the impact of cyber incident results in other reporting requirements to the RB, then the RB should work with the entity to streamline the reporting to avoid the regulatory burden of performing multiple assessments on the same cyber incident for reporting purposes.

2. Do you have comments on our proposed definition of materiality?

The definitions provide greater clarity on what constitutes a material cyber incident, however, we consider the proposed definition could be clearer and expanded to define the material effect of a cyber incident. Using examples of incidents that would meet the materiality threshold would also be one way to reduce potential subjectivity. We note that the RB takes into account the extent to which a cyber incident had or has a negative impact on stakeholders, but this does not sufficiently clarify what the material effect of a cyber incident is. We encourage clear definitions of "Cyber Event", "Materiality", and "Cyber Incident".

We note that the RB has adopted the APRA definition of materiality to accommodate New Zealand regulated entities with close ties to Australia. However, we disagree that the differences between the RB's

[1] APRA Prudential Standard CPS 234, Information Security, paragraph 35 (a).

definition compared to the FMA's definition of materiality would not result in substantive differences in the types of incidents reported. In addition, this RB definition is wider than the FMA's which, due to the sharing arrangements in place with FMA, may effectively require entities to be pragmatic and report to both simultaneously. This may also be the approach taken to avoid responding to enquiries from one regulator who may have heard of the incident from the other and once again, detract resources from responding to the incident.

We would prefer closer alignment across New Zealand regulators to avoid adding to regulated entities' regulatory burden of performing multiple assessments over the same cyber incident for purposes of reporting to the RB, the FMA and the Office of the Privacy Commissioner (OPC). We also consider that one regulator should be identified as the single point of contact for a regulated entity so that the entity is not reporting to and responding to questions from multiple regulators. Alternatively, there could be consideration of a central agency as noted in response to Question 3 below.

3. Do you have comments on our proposed cyber incident reporting template?

We agree that a cyber incident reporting template that underpins the RB's cyber resilience data collection provides clarity on the content of the report and ensures consistency of reporting regardless of the size or primary business of the reporting entity. We appreciate the collaborative effort of the RB and the FMA and the proposed implementation of a singular Template that reduces regulatory burden.

It is beneficial to streamline report types, however we also encourage the RB to explore empowering a central agency for cyber reporting and to perhaps leverage off existing agencies. A central agency could then share any notifications with the other impacted regulators. Some of our members have previously supported this approach as a way to help reduce the number of reports that need to be submitted during a crisis, freeing up resources to focus on the incident.

Format

Our members have concerns that Excel files are not a secure format to report cyber incidents and that may have a profound impact on a reporting entities' business, stakeholders, and reputational risk, irrespective of submission through the RB's BOX facility. Common issues when using Excel for data operations include inadequate password sharing practices for protecting sensitive business information, as well as the lack of error control as it is easy for any reader to inadvertently change a cell and therefore erode the data validity. We suggest online incident reporting similar to what CERT NZ, the APRA and the OPC have in place for their regulated entities.

Given the sensitive nature of the proposed collection data and potential impact on reporting entities' businesses, we submit that the RB consider including a statement that securing the channels to transmit this data remains a RB accountability and any 'data-in-transit' and 'data-in-storage' breaches would fall to the RB for remedial action.

Template

Parts A, B and C of the Template are tabs of the same Excel workbook and by default will be submitted together with each subsequent submission. However, this is highly repetitive as Part B of the Template is a full restate of the same information contained in Part A in addition to any new information that may be included in Part B. It will be burdensome for the RB to manually identify the new or amended information, if any, in every subsequent submission following the initial report, noting this would be 24 hourly if this approach is progressed.

Overall, we consider the Template (Parts A, B and C) is too complex and could cause an unintended distraction for organisations experiencing a cyber incident. As noted in response to Question 1, the level of detail required may not be available within the reporting timeframe making it difficult to complete and distract from response and recovery efforts. We also question the level of detail being asked for given (as noted in the Consultation Paper) the RB cannot provide a technical response to an incident. We have further concerns that disclosing the information being requested would provide a high level of cyber intelligence which it itself is a risk as such information is highly protected with limited internal access.

Suggested amendments

Part A should be simplified and refined to support the provision of relevant information within the 72 hour timeframe. For example, the 72 hour notification timeframe for APRA, as noted in response to Question 1 above, requires a short form to be completed asking a small number of high level questions and a description of the incident and mitigating actions being taken. We also encourage consideration of webforms such as those used by the Australian Cyber Security Centre.[2]

Part B should not be required to be updated every 24 hours. This is not practical nor useful and would detract from using resources to deal with the incident itself. We consider Part B should be removed from the template. Instead, once a material cyber incident has been notified to the RB then it would be appropriate for the entity to determine next steps with its supervisor depending on the specific circumstances of the incident.

Part C requires the provision of information that is detailed and highly sensitive. Whilst we appreciate the RB would want information that the incident has been resolved and mitigation actions taken for future risks, providing such sensitive information in a document externally is in itself a risk to regulated entities. We consider other channels to provide appropriate post incident information to the RB are more appropriate, for example, discussions with the supervisor.

Feedback on specific questions

- A06.0 – These categories should be defined, for example, does 'Active' mean under active attack? What does 'Mitigated' mean?
- A07.0 – The 'Low' classification should be removed as anything that meets the 'Low' classification would be unlikely to meet the materiality threshold and would not be reported in the first place. To require material cyber incident reporting on matters such as 'failed attacks' would result in over reporting to the RB.
- A08.1 – Recommend changing "Distributed denial of service attacks" (DDOS) to "Denial of service attacks" which is a category the National Cyber Security Centre (NCSC) and CERT NZ use in their reports and would encompass DDOS.
- A08.0 and A09.0 asks for one to be selected when it could be both, for example, a cyber attack on an outsource provider resulting in a service failure.
- A0.90 has "internal outage/service failure" as one type of cyber incident. However, the definitions of cyber incidents versus IT outages/incidents are distinct and not to be confused. We suggest that IT outages unrelated to cyber should be excluded from incident reporting.
- A17.1 – This question should be removed. It is highly subjective, and the affected entity has no control over this.
- A18.0 – Given question A20.0 asks whether the incident has been notified to other regulators this question should be removed. It is not clear what is meant by 'regulatory impact' noting that the need to report the incident is in itself a potential regulatory impact.

[2] https://www.cyber.gov.au/report-and-recover/report/report-a-cyber-security-incident#no-back

Our banking members seek clarity as to whether the separation in the template is purposeful, noting the requirements as they are drafted require our banking members to report material incidents impacting both core banking systems and cyber incidents. Several questions are tailored more towards operational outages than core banking systems,[3] and as stated in response to Question 2, further clarity on the definitions of "Cyber Incidents" and "Cyber Attack" are required for all our members to better assess the intended outcomes.

4. Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

We consider it 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 have internal triaging processes and impact assessment processes to make sure energy and resource is spent on actual and high impact cyber incidents rather than non-material cyber incidents.

The proposal of reporting all incidents may also have the unintended consequence of reporting vulnerabilities rather than actual material cyber incidents. The proposal is suggesting businesses to report security events of interest and we submit that most events being triaged would not be deemed as a material incident.

Reporting of all cyber incidents, regardless of materiality, to the RB on a six monthly basis for large entities and annually for all other entities is broad and reporting volume could also be large. We do not see the value of the proposed periodic reporting and consider it should be removed. Financial institutions are under constant low level cyber security probing which includes events such as phishing attempts and blocked requests that are automatically stopped by an entities' firewalls and other cyber security measures. Including these types of cyber incidents will result in inflated number of instances being reported on and if each of these were considered an incident the overheads required to perform reporting would be unsustainable. Further it would detract resource from cyber resilience activities.

There is questionable value in the RB collecting and analysing information on non-material cyber incidents. It would require significant resource and is unlikely to provide insights that would better inform decisions on cyber resilience. We appreciate the desire to better understand the nature of cyber risk impacting the New Zealand financial sector, however in this regard, CERT NZ and the NCSC already collect such data and provide regular trend reports.

The regulatory burden and cost of such periodic reporting outweighs any potential benefit as it is difficult to see how it would further improve outcomes for the financial sector and its customers. We also question whether collection of this 'low-level' information is in alignment with international practice and established data collection practices for cyber resilience. Our understanding is that APRA does not have an equivalent requirement to report periodically on all cyber incidents.

We would like to hear further detail on how the RB would plan to use, store, and protect this information.

[3] Questions 9.1, 9.2, 11, 11.1, 11.2, 12, 12.1, 12.2, 13, 13.1 and 13.2.

5. Do you have comments on our proposed periodic cyber resilience capability survey?

Whilst we support the intent behind cyber resilience capability surveys, the information being requested provides significant cyber intelligence on an entity and raises serious risk concerns if it is to be collated and then disclosed externally. This in itself is a threat to cyber resilience, particularly if it is stored and potentially shared by the RB in a way that is not anonymised and encrypted.

Although it is referred to as a "Periodic Survey Questionnaire", the nature of the questions is akin to a compliance assurance review of the RBNZ's Guidance on Cyber Resilience. There is no such information sought by the RB on other obligations or expectations, for example, compliance with the Insurance (Prudential Supervision) Act 2010.

If the RB has concerns about an individual entity's cyber resilience, then we consider a preferable approach is to include cyber resilience as part of its regular prudential supervision with the entity, as each entity may differ in its cyber resilience maturity and approach. We note that a number of the RB regulated entities are also regulated by overseas supervisors, such as APRA, and will already be subject to their cyber reporting requirements. In addition, internal and external audits of cyber resilience are undertaken by entities.

The survey is very basic and high level. For example, the questions are one size fits all. The questions do not distinguish among businesses of low, medium, or high inherent risk. In addition, in seeking numerical values, we have concerns that the response would vary from organisation to organisation and given the differences in size and scale of reporting entities, we question the usefulness of this information. If the RB is seeking a view of cyber resilience at a sector wide level, we consider the proposed questions in the survey are too detailed for to achieve this. For example, knowing the number of internal staff trained to be able to identify anomalous activities and events does not provide any meaningful information on the sector because it depends on the size and nature of each organisation.

As an alternative to the proposed survey, we consider that an anonymous online survey with higher level questions that provide data that can be aggregated at a sector level would be a more appropriate way to obtain meaningful sector information. Manual reporting requirements may also require resourcing allocations so as much as possible the survey should allow the information to be obtained with minimal overhead to any organisation.

6. Do you have comments on our proposed frequency of reporting or the threshold for reporting more frequently?

Please note our response to question 5 above. We do not consider the proposed periodic survey to be the appropriate mechanism for obtaining information on the cyber resilience of an entity.

7. Do you have comments on how we propose to share information?

We understand that cyber security is a shared concern and part of the remit of multiple government agencies and regulators including the RB, FMA, OPC, CERT NZ and the NCSC. We also note that the Council of Financial Regulators (CoFR) is currently working on information gathering and sharing arrangements. We support sharing arrangements to minimise the reporting requirements imposed on our members.

We welcome the proposal that the material incident reporting template will meet the reporting requirements of both the FMA and the RB. We consider that either the RB or the FMA should be nominated as the single contact for the regulated entity. This will minimise confusion and duplication as the entity will not need to report to and answer questions from two different regulators. We would also

see value in expanding this type of coordination to include other agencies such as the OPC or consideration of a central agency as noted under Question 3 above.

However, our members have concerns with the RB's proposed sharing of the cyber resilience data it collects. This is due to information that identifies, or potentially identifies, a specific entity. We consider any information shared should be anonymised or only provided at an aggregated level that does not allow individual entities to be identified. Otherwise, the potential for exposure the vulnerability of one reporting entity can threaten the entity's stakeholders, customers, partners, employees and the wider industry. It is also of utmost importance that the data provided as part of the RB's cyber resilience data collection proposals are fully safeguarded and identifiable data relating to customers, employees and other stakeholders are managed in accordance with the Privacy Act 2020.

8. Do you have any comments on our analysis on the financial policy remit?

In reviewing the RB analysis on the financial policy remit, our members seek clarity of the first two components of the financial policy remit where the use of terms "with a low incidence of failure" have been utilised. Whilst the RB states this is not of high relevance, we consider that without adequate cyber resilience control processes and procedures, a "low incidence of failure" would not be possible.

Proportionality

We consider the cost of the current proposals are not proportionate to the expected risks and benefits to the financial system and society. The reporting requirements would incur significant compliance costs (diverting resource from cyber resilience activities) and increase cyber risk for entities which will ultimately impact on its customers.

Improving cyber resilience

The current proposals would require the RB regulated entities to collate and disclose large amounts of cyber intelligence. Such information is highly classified and has limited access even internally within entities. If the RB were to receive such collective information our concern is that it could make the RB itself a target for cyber criminals, a risk which is compounded further by the RB storing the information and sharing it with other parties.

The unintended disclosure of such information could substantially increase cyber risk to the RB regulated entities and potentially to the financial stability of New Zealand given the number, nature and size of the entities involved. As such, rather than improving cyber resilience, we are concerned the proposals could have the unintended consequence of significantly reducing cyber resilience.

We question the usefulness of many components of the information being requested and the feasibility of the RB reviewing the large volume of information to obtain meaningful insights. As such, we have concerns of large amounts of information being stored unnecessarily by the RB and the risks associated with such storage. If the RB were to analyse large volumes of non-material data, we consider this detracts from, and delays progress on, real issues that would help improve cyber resilience in New Zealand such as addressing the cybersecurity talent shortage and better cyber threat intelligence information and sharing.

We support the RB wanting to better understand cyber resilience in its regulated entities and welcome further engagement on ways this could be better achieved to strengthen our industry against cyber incidents and risks.

9. Do you have comments on our proposed prioritisation of our cyber data collection proposals?

The Consultation Paper notes implementing the incident reporting requirements as the first priority. We do not consider the proposal to implement as soon as possible this year is reasonable unless there are changes to the information being requested by the RB. The current proposals require significant processes to be put in place to be able to collate the information in the requested format. We welcome further discussion with industry to agree on a timeline of when the amended requirements will take effect to strengthen our industry against cyber incidents and risks.

We note that there is no proposed timing on when the cyber survey will be required. There would need to be a significant lead time to enable entities to put processes in place to collate the information being requested (noting that we do not support the cyber survey in the format currently proposed as the mechanism for ascertaining the cyber resilience of an entity).

Additional Feedback

Some of our members suggest that they would require a minimum of six to 12 months from when the reporting requirements are finalised to fulfil the reporting requirements on a more sustainable basis. This is due to its manual format and request of specific metrics that would need coordination between their subject matter experts, as well as alignment with internal governance processes and timings. As noted, we support ongoing engagement on all aspects of reporting, timeframes and the implementation of any proposals particularly given the high volume of new regulatory change and compliance implementation that our members are currently managing. Our members are keen to ensure that their resources are not distracted from cyber resilience activities and servicing their customers.

FINANCIAL SERVICES FEDERATION

3 July 2023

Cyber Data Collection Proposal
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand - Te Pūtea Matua
Wellington

By email to: cyberresilience@rbnz.govt.nz

Dear Madam/Sir,

Re: **RBNZ Cyber Resilience Data Collection Proposals Consultation**

The Financial Services Federation ("FSF") is grateful to the Reserve Bank of New Zealand ("RBNZ") for the opportunity to respond on behalf of our members to the consultation paper on Cyber Resilience Data Collection Proposals ("the Consultation").

By way of background, the FSF is the industry body representing the responsible and ethical finance, leasing, and credit-related insurance providers of New Zealand. We have over 90 members and affiliates providing these products to more than 1.7 million New Zealand consumers and businesses. Our affiliate members include internationally recognised legal and consulting partners. A list of our members is attached as Appendix A. Data relating to the extent to which FSF members (excluding Affiliate members) contribute to New Zealand consumers, society, and business is attached as Appendix B.

Introductory Comments

The FSF begins by stating that we understand the importance of cyber resilience and the impact that cyber attacks can have on financial stability in New Zealand. However, we believe there are a few points that require clarification in order to make the reporting regime more workable and less burdensome for regulated entities. In particular the FSF submits that RBNZ should define what constitutes a smaller entity and should have more consideration as to how this will interact with the mandatory reporting to the Office of the Privacy Commissioner (OPC) that is required under the Privacy Act 2020.

The FSF also indicates its strong support for the RBNZ and the Financial Market Authority's (FMA) joint approach to cyber resilience in an attempt to minimize additional compliance for entities. Due to the sheer amount of compliance in the industry this will help to mitigate additional regulatory burden on affected entities. However, we request clarification on whether entities will be required to file the same report with both regulators or whether the RBNZ and FMA's information sharing powers extend to this purpose.

Consultation Questions

1. Do you have comments on our proposed cyber incident reporting timeframe?

   Overall, the FSF and its members believe that the timeframe is acceptable. However, we believe there are some points that need to be clarified around the 72-hour materiality timeframe. The first is regarding the actual 72 hours/ 3 days timeline. Is that considered 72 actual hours or business hours?

   The second point is around the provision of updates about the cyber breach. Our members anticipate that they will get many updates over the course of the breach and understand that those updates must also be recorded within 72 hours. We would however like clarification around this timeframe in situations where the updates themselves are not considered material. Does the update still need to be made within the 72-hour timeframe in situations such as this?

2. Do you have comments on our proposed definition of materiality?

   The FSF and its members believe that the definition coupled with the elements listed by RBNZ is a workable definition of a materiality incident.

3. Do you have comments on our proposed cyber incident reporting template?

   We have no comment on the proposed cyber reporting incident template.

4. Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

   Depending on the content and extent of what entities must report this could be a huge compliance burden for smaller entities. It is difficult to tell without knowing the full scale of cyber risks that entities must report, for example must they report every phishing email they receive?

   Regarding the frequency of reporting, we submit that the RBNZ and the FMA should issue guidance around what is considered a smaller entity for the purpose of the reporting regime. This will allow entities to report in the correct timeframe relative to their size and ensure compliance with the proposals.

5. Do you have comments on our proposed periodic cyber resilience capability survey?

   We have no comment on the proposed periodic cyber resilience capability survey.

6. Do you have comments on our proposed frequency of reporting?

The FSF is very supportive of the proposed frequency of reporting provided some additional guidance is issued around what comprises a smaller entity versus a larger one.

7. Do you have comments on how we propose to share information?

   The FSF is extremely supportive of the sharing of information between RBNZ and FMA. However, as mentioned above we would like there to be some more consideration given to the overlap between the Privacy Act's mandatory breach reporting requirements and the required reporting to the FMA/ RBNZ.

8. Do you have any comments on our analysis on the financial policy remit?

   The FSF approves of the RBNZ's analysis, particularly in light of the RBNZ's comments around proportionality. We agree that a tiered approach is required in order to recognise that smaller entities have less resources than larger entities.

9. Do you have comments on our proposed prioritisation of our cyber data collection proposals?

   We have no comment on the proposed prioritisation of the RBNZ's cyber data collection proposals.

In summary, the FSF is supportive of the overall policy intent of the proposals however believes that a few points need to be clarified to ensure that the proposals are workable in practice and don't increase the regulatory burden for regulated entities.

Please do not hesitate to reach out if you wish for us to speak further on any of the points made in this submission.

Yours sincerely,

S9(2)(a)

Financial Services Federation

Appendix A

FINANCIAL SERVICES FEDERATION

FSF Membership List as at July 2023

Non-Bank Deposit Takers, Specialist Housing/Property Lenders, Credit-related Insurance Providers	Vehicle Lenders	Finance Companies/ Diversified Lenders	Finance Companies/ Diversified Lenders, Insurance Premium Funders	Affiliate Members	Affiliate Members contd., and Leasing Providers
XCEDA (B)	AA Finance Limited	Avanti Finance ➢ Branded Financial	NZ Finance Ltd	Buddle Findlay	Centrix
Finance Direct Limited ➢ Lending Crowd	Auto Finance Direct Limited	Basalt Group	Personal Loan Corporation	Chapman Tripp	Credit Corp
Gold Band Finance ➢ Loan Co	BMW Financial Services ➢ Mini ➢ Alphera Financial Services	Blackbird Finance	Pioneer Finance	Credisense Ltd	Debt Managers
Mutual Credit Finance	Community Financial Services	Caterpillar Financial Services NZ Ltd	Prospa NZ Ltd	Credit Sense Pty ltd	Debtworks (NZ) Limited
Credit Unions/Building Societies	Go Car Finance Ltd	Centracorp Finance 2000	Smith's City Finance Ltd	Experian	Equifax
First Credit Union	Honda Financial Services	Finance Now ➢ The Warehouse Financial Services ➢ SBS Insurance	Speirs Finance Group(L &F) ➢ Speirs Finance ➢ Speirs Corporate & Leasing ➢ Yoogo Fleet	Experieco Limited	Gravity Credit Management Limited
Nelson Building Society	Kubota New Zealand Ltd	Future Finance	Turners Automotive Group ➢ Autosure ➢ East Coast Credit ➢ Oxford Finance	EY	IDCARE Ltd
Police and Families Credit Union	Mercedes-Benz Financial	Geneva Finance	UDC Finance Limited	FinTech NZ	Illion
Specialist Housing/Property Lenders	Motor Trade Finance	Harmoney	Yes Finance Limited	Finzsoft	Quadrant Group (NZ) Limited
Basecorp Finance Limited	Nissan Financial Services NZ Ltd ➢ Mitsubishi Motors Financial Services ➢ Skyline Car Finance	Humm Group	Insurance Premium Funders	Happy Prime Consultancy Limited	Leasing Providers
First Mortgage Managers Ltd.	Onyx Finance Limited	Instant Finance ➢ Fair City ➢ My Finance	Elantis Premium Funding NZ Ltd	KPMG	Custom Fleet
Liberty Financial Limited	Scania Finance NZ Limited	John Deere Financial	Financial Synergy Limited	Lendscape Ltd	Euro Rate Leasing Limited
Pepper NZ Limited	Toyota Finance NZ ➢ Mazda Finance	Latitude Financial	Hunter Premium Funding	Loansmart Ltd	Fleet Partners NZ Ltd
Resimac NZ Limited	Yamaha Motor Finance	Lifestyle Money NZ Ltd	IQumulate Premium Funding	LexisNexis	ORIX New Zealand
Credit-related Insurance Providers		Limelight Group	Rothbury Instalment Services	Motor Trade Association	SG Fleet
Protecta Insurance		Mainland Finance Limited		One Partner Limited	
Provident Insurance Corporation Ltd		Metro Finance		PWC	
		Nectar NZ Limited		Sense Partners	
				Simpson Western	
				Credit Reporting, Debt Collection Agencies,	
				Baycorp (NZ)	Total 94 members

Appendix B

FINANCIAL SERVICES FEDERATION (FSF)

THE NON-BANK FINANCE INDUSTRY SECTOR - 2022

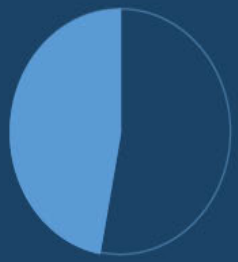
48%

of personal consumer loans are financed by the **non-bank sector** represented by FSF members.

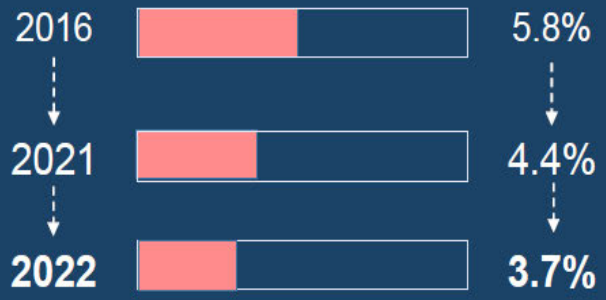
Setting industry standards for responsible lending, promoting compliance and consumer awareness.

Percent of Loan Requests Approved

46%



Percent of Loan Book in Arrears



KEY FACTS: THE NON-BANK FINANCE INDUSTRY SECTOR

FSF Members (as at 28 Feb 2022)

Number of Members	57
Number of Employees	3,561
Applications Processed	1,085,739
Loan Requests Approved	495,434
Percent of Loan Book in Arrears	3.7%

Bank Sector (as at 28 Feb 2022)

Value of Mortgage Loans	$329B
Value of Consumer Loans	$7.6B
Value of Business Loans	$118B

Non-Bank Sector Share (as at 28 Feb 2022)

% of Total Mortgage Loans	0.4%
% of Total Consumer Loans	47.7%
% of Total Business Loans	5.9%

Insurance Credit Related (as at 28 Feb 2022)

Number of Employees	237
Number of Policies	311,409
Gross Claims (annual)	$27.2M
Days to Approved Claim	20 days

Consumer Loans (as at 28 Feb 2022)

Total Value of Loans	$8.1B
Number of Customers	1,699,683
Number of Loans	1,584,984
Monthly Instalments:	$330M
Average Value of Loan:	
Mortgage	$171,932
Vehicle Loan	$12,393
Unsecured	$2,467
Other Security	$5,754
Lease Finance	$2,804
Average Monthly Instalment:	
Mortgage	$257
Vehicle Loan	$463
Unsecured	$144
Other Security	$302
Lease Finance	$241

Business Loans (as at 28 Feb 2022)

Total Value of Loans	$7.3B
Number of Customers	136,830
Number of Loans	264,827
Monthly Instalments:	$590M
Average Value of Loan:	
Mortgage	$443,784
Vehicle Loan	$28,869
Unsecured	$7,443
Other Security	$32,374
Lease Finance	$24,921
Average Monthly Instalment:	
Mortgage	$2,281
Vehicle Loan	$1,064
Unsecured	$799
Other Security	$11,044
Lease Finance	$939

IBM New Zealand Limited
12 Madden Street, Auckland 1010
PO Box 6840, Victoria Street West, Auckland 1142
New Zealand
Freephone 0800 801 800

3rd July 2023

Cyber data collection consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

To whom it may concern;

The Reserve Bank is the prudential regulator of banks, insurers, non-bank deposit takers and financial market infrastructures. The Reserve Bank's role as prudential regulator includes promoting the safety and soundness of our regulated entities as a part of its financial stability mandate. The growing cyber risks facing the financial sector mean that the organisation seeks to promote cyber resilience in regulated entities.

IBM Security is a global leader in cyber security software and services capability. We have over 8500 employees, operating in 130 countries with over 1000 people helping clients prepare for, and respond to data breaches. It is within this context that we feel compelled to share our experience in threat intelligence, sharing and incident response in the hope that it provides a perspective of value for the financial regulated industry within New Zealand.

Each year IBM publishes the Cost of a Data Breach Report in partnership with the Ponemon Institute, and the financial industry is always hear the top (often second to Healthcare). Our 2022 data showed costs of data breaches for Financial Industry reached USD5.97m and for ransomware it took organisations 277 days to identify and contain.

The future of cyber security is about delivering with speed, scale and accuracy. The ability to collect, analyse, extract context and share intelligence forms a key enabler to accelerate defence. In pursuing this resiliency program, the Reserve Bank will find itself in a position to bring renewed context to their regulated entities and with that an opportunity to accelerate collective defence.

IBM New Zealand welcomes the opportunity to respond to the consultation and would welcome the opportunity to engage more fully, perhaps with the new 2023 report findings due in July. Please feel free to reach out to IBM New Zealand, S9(2)(a)

Yours sincerely,

S9(2)(a)

Ref: https://www.ibm.com/reports/data-breach

IBM New Zealand Limited
12 Madden Street, Auckland 1010
PO Box 6840, Victoria Street West, Auckland 1142
New Zealand
Freephone 0800 801 800

Q1 Do you have comments on our proposed cyber incident reporting timeframe?

IBM commends the RBNZ view that cyber incident reporting needs to be timely. The IBM X-Force threat Intelligence report 2023 showed that attackers have reduced their ransomware attack completion from months to less than 4 days. This increases the urgency of organisations to detect and share valuable insight early in the attack sequence.

If the purpose of this data collection is to mitigate the risk of planned and simultaneous attack across multiple institutions, the language may need to be stronger to reflect of an 'immediate need' to report with a mean time expectation below 72 hours. In the case of a serious attack, the time to share initial indicators becomes crucial for other regulated entities to act with speed and accuracy.

RBNZ may also wish to mature this process once implemented to provide a more robust service level around notice periods compared to the proposed default notice period all incident classifications. For Example, a 'Severe' classification level may have a lower threshold timeframe to report to the regulator compared to a 'Low' classification. By focusing on a shorter/lower timeframe to report against the higher impacting classification of material cyber incidents it should focus organisation to clearly call out these events earlier than delay to the full SLA reporting period.

With the nature of cyber/security incidents and the complexities that surround these critical and important events, there is a strong emphasis on the reporting organisation to get this right first time. This maniacal focus may delay the reporting of the material cyber incident because of the complexity of classifications and severity may take time to profile, assess and report. Providing a mechanism for changing a classification (e.g. upgrade or downgrade the classification) once further information has come to light during these incidents may help to expedite the reporting (albeit with less accuracy in the reporting event).

Ref: https://www.ibm.com/reports/data-breach

IBM New Zealand Limited
12 Madden Street, Auckland 1010
PO Box 6840, Victoria Street West, Auckland 1142
New Zealand
Freephone 0800 801 800

Q2 Do you have comments on our proposed definition of materiality?

IBM agrees this definition captures the intent. There might be the risk that a particular low severity, somewhat mitigated threat at one institution may have a different material impact on others if not as well defended. This point does cover, in part that condition, but may be a little narrow in terms of the result being not exclusively financial consequences. A few additional points below:

- The extent to which the cyber-incident could result in financial consequences to the New Zealand financial system or to other financial entities.

    It may be worthy to provide a statement in terms of material impact on an individual client or entities affected by a breach (in addition to simply financial consequences). Data breaches that impact large numbers of users, e.g. identity, can lead to a material impact that may not just be financial.

- How long the cyber-incident lasted (if already remedied), or is expected to continue;

    IBM's Cost of a Data Breach Report indicates that most attacks (ransomware, destructive malware) take on average over 200 days to identify, and almost 100 days to contain attacks. IBM would recommend more granularity on both the identify and recovery phases, and a clearer definition of when a cyber incident begins. Attackers would consider an incident started the moment they executed a first phase incursion. Whilst this may go un-detected, it's important information that can be collected and used to form a better view worth sharing with other institutions.

Ref: https://www.ibm.com/reports/data-breach

IBM New Zealand Limited
12 Madden Street, Auckland 1010
PO Box 6840, Victoria Street West, Auckland 1142
New Zealand
Freephone 0800 801 800

Q3 Do you have comments on our proposed cyber incident reporting template?

With regards to the communication to the media (A17), given the potential for widespread alarm from a major cyber event being made known to the public, the regulator may nominate to become a key stakeholder prior to any engagement with the media. Engagement may result in the regulator providing material support in review of cyber material incident communication, collaboration and alignment when engaging and discussing media or public entities around a material cyber incident. Considerations could include stage gates for:

- Engagement including clear RACIs;
- Standardised media reporting templates to ensure consistency;
- Alignment between the regulator, government agencies and financial organisation involved in the cyber incident prior to reporting to media and public entities.

These measures may help to ensure that there is a coordinated (planned and practiced) effort to understand and remediate the event before public scrutiny causes escalation through media interest. The objective would be to ensure that communications do not inadvertently cause public concerns about other financial institutions, assuring the public that any major breach issues are being managed system wide.

IBM recommends, per above, finer granularity for time of known first detection (including a MITRE ATTACK reference if possible), including the method for determining, be considered for the template.

For completion, IBM's Cost of a Data Breach Report 2023 used the following initial attack vector classifications to map the overall cost and frequency of data breaches. It might be worth expanding the current list to consider these found within our survey responses.

- Business Email Compromise
- Phishing
- Vulnerability in third-party software
- Stolen/compromised credentials
- Malicious insider
- Cloud misconfigurations
- Social engineering
- Physical security compromise
- Accidental data loss/lost device
- Other technical misconfiguration.

Ref: https://www.ibm.com/reports/data-breach

IBM New Zealand Limited
12 Madden Street, Auckland 1010
PO Box 6840, Victoria Street West, Auckland 1142
New Zealand
Freephone 0800 801 800

The report also used the following definitions as the types of breach, perhaps helpful in expanding the list in the template:

- Ransomware
- Destructive attack
- Supply chain
- Human error
- IT failure
- Other malicious attacks.

Q4 Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

An automated and continuous feed of cyber incidents might bring greater benefits over periodic collection. With the range of technologies available, once established it may also be easier to implement and less costly than a larger periodic collection. This capability may increase speed and scale of threats being observed at single parties that may present themselves at others. Since the objective is to identify any signals that might lead to systematic failure, a mechanism to identify potential weaknesses or exposures exploited may provide early warning indicators.

Q5 Do you have comments on our proposed periodic cyber resilience capability survey?

The regulator should make it clear on if and how the reported information will maintain confidentiality if a breach becomes a matter of national interest attracting media comment from the regulator. This aligns with statements made above on how the regulator will offer its support, engagement, and influence during a material cyber incident to ensure clear processes can be aligned. This will provide alignment, consistency and the ability for the regulator to measure the ongoing maturity of material cyber incidents across New Zealand. As part of IBM's X-Force Incident Response exercises, executives and stakeholders are specifically trained on how to respond to media within the context of a cyber incident. It is therefore imperative that the regulator applies a consistent view of not just collection of information, but it's use under exceptional circumstances.

The following sections outline the elements of the NIST resiliency lifecycle outlined within the consultation:

B1. Identify

Within today's IT landscape, organisations are struggling to understand their attack surface. IBM would suggest that a periodic, or continuous assessment of external facing

Ref: https://www.ibm.com/reports/data-breach

IBM New Zealand Limited
12 Madden Street, Auckland 1010
PO Box 6840, Victoria Street West, Auckland 1142
New Zealand
Freephone 0800 801 800

services be performed at all institutions as part of exposure management programs, or at least whether this is being done (not just periodic penetration testing). Reports from IBM have shown that up to 30% of IT is not known to oganisations and that 70% of all attacks come through these applications.

B2. Protect

A more direct question is recommended for a wholistic data security program that encompasses discovery, classification, compliance, encryption, activity monitoring and threat detection.

IBM's Cost of a Data Breach report showed phishing as leading to the most expensive data breaches (USD4.91 million), and combined with lost/stolen credentials account for 35% of breaches. It's recommended that a question related to the widespread implementation of multi-factor authentication be added to the survey.

B4. Respond and Recover

IBM Cyber Range facilities operate in Boston, Bangalore and on a truck travelling around Europe. These facilities conduct range exercises aimed at executives, with an objective to equip business leaders with the muscle memory for responding to breaches when the heat is on. IBM recommends that the survey includes a question about readiness of incident response teams, but also inclusive of executives to ensure that everyone is prepared in their roles in case major cyber incidents disrupt the institution.

Q6 Do you have comments on our proposed frequency of reporting?

IBM does not have additional comments or recommendations.

Q7. Do you have comments on how we propose to share information?

IBM does not have additional comments or recommendations.

Q8. Do you have any comments on our analysis on the financial policy remit?

IBM does not have additional comments or recommendations.

Q9 Do you have comments on our proposed prioritisation of our cyber data collection proposals?

IBM does not have additional comments or recommendations.

Ref: https://www.ibm.com/reports/data-breach

Insurance Council of New Zealand
Te Kāhui Inihua o Aotearoa

Level 2 Asteron House
139 The Terrace
Wellington 6011

(04) 472 5230
icnz@icnz.org.nz
www.icnz.org.nz

3 July 2023

Cyber data collection consultation
Dynamic Policy
Prudential Policy Department
Te Pūtea Matua/Reserve Bank of New Zealand
Wellington

Emailed to: cyberresilience@rbnz.govt.nz

ICNZ submission on RBNZ cyber resilience data collection proposals

Thank you for the opportunity to submit on the RBNZ's cyber resilience data collection proposals (**proposals**).

ICNZ represents general insurers that insure about 95 percent of the Aotearoa New Zealand general insurance market, including about a trillion dollars' worth of Aotearoa New Zealand property and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, cyber insurance, commercial property, and directors and officers insurance).

This submission is in two parts:

- Overarching comments
- Responses to the questions in the consultation paper.

Overarching comments

A central repository of cyber security data creates risk

ICNZ welcomes the advancement of RBNZ's work on cyber resilience and notes that we have been consistently supportive of allowing for a greater ability to share information between entities about cyber incidents. This is particularly because from an underwriting perspective, cyber is an area which lacks the depth of material for assessing and quantifying risk available of other lines of insurance.

However, the proposals will not contribute to the ability to underwrite cyber risk, particularly as the proposals do not outline how the learnings from the proposed data collection might be fed back to the sector providing the information. Instead, and given the nature, detail, timing and frequency of what is requested, the proposals raise concerns for ICNZ about the creation of a single source of valuable security data about identifiable financial institutions such as insurers and banks.

The creation of such a risk is entirely foreseeable considering for example, the recent BlackCat attack on HWL Ebsworth in Australia, a law firm known to hold information on many clients, including government and large corporations. We would not support the possibility of the RBNZ becoming such a repository in Aotearoa New Zealand unless it can be shown with certainty that collection of

the proposed information will actively contribute to an increase in cyber resilience and/or threat reduction, and it would be done in a way that means information about identifiable entities cannot be accessed by threat actors.

Scope of the proposals

In relation to scope, we note the definition of large entities in paragraph 4.2 of the consultation paper is having assets in excess of $2 billion NZD. It would be helpful to know whether, when determining if an entity meets the definition of "large", this assessment should be based on the overarching position of the financial institution (i.e., including agency partners) and whether it would extend to any Australian operations of the entity.

Definition of cyber event

Paragraph 3 of the consultation paper defines a 'cyber incident'. Part ii of the definition states that a cyber incident is a cyber event that "violates the security policies, security procedures or acceptable use policies". There does not appear to be any threshold that must be met and therefore, all cyber incidents, no matter how minor, would be caught by the periodic reporting requirement. We caution that having to report every cyber incident, no matter how minor, could be onerous for an entity and question what value it would provide. While there is potential benefit in knowing the type and frequency of material events affecting the financial sector, we do not believe that the value gained from reporting all cyber incidents would outweigh the time and resources required to produce the reports.

Alignment with FMA requirements is positive

Notwithstanding our concerns about the nature of some of the information being sought and having extensive and potentially sensitive data concentrated within a single party, we welcome the proposed alignment between RBNZ and FMA and that the material incident reporting template will meet the reporting requirements of both regulators.

Overall, while ICNZ supports the principle of information sharing, we are not confident that the proposals are the safest or most efficient way of doing so. We urge the RBNZ to take ours and other feedback into consideration, and to engage further with regulated participants before advancing the proposals.

Responses to questions in the consultation paper

Q1. Do you have comments on our proposed cyber incident reporting timeframe?

ICNZ holds concerns about providing the requested information about a material cyber incident and the practicalities of doing so within a maximum 72 hour period. The reporting of an incident could be hindered by the nature and scale of the compromise if the systems that hold the required reporting data are impacted or the integrity of systems cannot be guaranteed (for example, if the email system is compromised, the entity would need to find an alternate way of communicating). We therefore believe that it would be more practical to consider a flexible timeframe for reporting the proposed detail.

We also have concerns about the proposal for all cyber incident reporting (regardless of timeframe) and question what benefit, if any, it would provide by entities being required to supply the information. We expand on these points in our responses to the questions below.

As already stated in the overarching comments to the submission, ICNZ is supportive of greater alignment between the RBNZ and the FMA in terms of reporting requirements and timing. It is important that where information is mandated in circumstances such as those proposed, regulators make all efforts to not duplicate reporting requirements for dual-regulated entities as this will impact both on their ability to report, as well as respond to the incident, so we consider this to be a positive move.

Q2. Do you have comments on our proposed definition of materiality?

ICNZ is supportive of the intent to align the proposed definition of materiality with that of APRA. However, we question whether including the words "potential to materially affect" brings into scope a wider range of cyber incidents than the RBNZ intends. The systemic and interconnected nature of IT systems means there is a risk that a seemingly small incident has the potential to become significant with material effects, but expecting reporting of all such small incidents would result in over reporting.

In addition to this, we believe that there is still room for many different interpretations of whether the threshold for materiality has been met. It may be useful to consider whether a tool such as the Office of the Privacy Commissioner's 'NotifyUs' could be introduced to help with triaging and to provide guidance on the need to report.

For completeness, we note that we are a particularly supportive of a definition that would also meet the FMA's requirements, reflecting the comments already made above about minimising duplication in reporting across different regulators.

Q3. Do you have comments on our proposed cyber incident reporting template?

Overarching comments

Before providing specific commentary on the draft incident reporting template, we make some general overarching comments about the information being requested:

- The collation and disclosure of information at this level of detail, especially if it can be attributed to a specific entity, provides a high level of cyber intelligence. This poses a significant security risk and providing it would be outside the risk appetite of RBNZ regulated entities. Incident details are highly protected, with access even being limited internally.
- The template requires a significant amount of information which is not practical to be gathered during an initial incident response and remediation. To focus on collating such information would materially limit the ability of incident response teams to perform their functions in relation to responding to and recovering from a material incident.
- ICNZ would like to understand: (a) how each data point requested is aligned to the role of RBNZ on receiving an incident report, (b) the purpose of collecting this information and (c) how this data will be used by the RBNZ. This is not clear from the consultation paper, and we are concerned that a wide net is being cast for highly sensitive information without clarity at the outset around why or how it will be used.
- We consider the data being requested will not position RBNZ to respond to and mitigate a cyber incident and note that this is not its role. It also does not contribute to the entity's nor RBNZ's understanding of the entity's cyber security posture. The severe risk of a successful cyber-attack relates mostly to the external environment and actors including their resources (especially nation state backed actors) and the lack of consequences.

- We consider that Part B should be removed from the template and once a material cyber incident has been notified to RBNZ the entity should instead be able to determine next steps with its supervisor based on what is appropriate in the circumstances.
- As noted in the consultation paper, RBNZ (and other regulators) cannot provide a technical response to an incident. The detailed information requested would be more relevant if an entity were seeking cyber expertise to manage the incident (for example, from CERT NZ or NCSC) however, even then, this extent of information would not be required to gauge the incident and inform next steps.
- The information being requested takes a different approach to what is required under APRA CPS234 notifications and may create complications for insurers with reporting requirements in Australia as well as Aotearoa New Zealand.
- The draft incident reporting template contains a lot of detail, more so than what is required by APRA. For example, A09.0, B09.0 and C09.0 each refer to an "internal outage/service failure". Consistent with the feedback already provided in the overarching comments, it is unclear what benefit reporting instances such as these as cyber events would provide and question whether such level of reporting is appropriate.
- "Cyber incidents" appear to potentially include outages that are not "cyber security incidents", for example, a major outage due to hardware failure would be captured. This is also beyond what APRA requires.
- RBNZ expects a Part A report to be submitted within 72 hours and then a Part B update submitted every 24 hours until the incident is resolved (with there being no indication that these timeframes exclude weekends and statutory holidays). It is not apparent from the proposals whether RBNZ has the capacity/and capability to analyse all the information requested, and if so, how the ongoing seven day a week provision of this information will contribute to its regulatory responsibilities and purpose. Such frequent and ongoing updates, which we note go well beyond what is required by the standard CoFI licence conditions, would be a distraction and source of undue pressure for an entity affected by a material cyber incident. This level of regulatory focus would detract from an entity's incident management resources subsequently risking the slowing down of containment and restorative processes.

<u>Comments on the template</u>

While overall, we do not believe that the proposed template in its current form is appropriate, we nevertheless set out commentary on each section below:

Instructions:

- If an incident is resolved within 72 hours, we believe that the entity should only have to submit Part A within 72 hours, and not Part C. Considerable time is required to carry out a post incident review and realistically, will take more than 72 hours.
- Requests for further information should be from either RBNZ or FMA and not both. For efficiency, there should be single point of contact for the regulated entity rather than answering questions from both RBNZ and FMA.
- As already noted above, Part B should not require daily updates. This is not practical or useful and would detract from using resources to deal with the incident itself.
- If an incident affects more than one regulated entity that is required to report to RBNZ, then the entities should have the option to elect for one entity to provide the report on behalf of all affected entities. This will reduce duplication/repetition of work for the regulated entities and RBNZ. It will also mean that affected entities can focus resources on providing information to the reporting entity rather than preparing individual reports that RBNZ will then need to collate to get the full picture.

Part A:

- Rather than requiring such a broad array of information, we believe that the RBNZ should look to the example of APRA and simplify and refine Part A. APRA has a 72 hour notification timeframe. Given the short timeframe, appropriately, a small number of high level questions and a description of the incident and mitigating actions being taken is asked for. This ensures that only relevant information is required at the first instance. Another example of an efficient initial notification requirement is the webform used by the Australian Cyber Security Centre (Report a cyber security incident | Cyber.gov.au).
- A06.0: to ensure that nothing is left to subjectivity at a time when an entity will already be under increased pressure, the status categories should have clear definitions. For example, would 'Active' mean under active attack, or the attack has ceased but the response plan is active?
- A07.0: the 'Low' classification is redundant and should be removed as anything that meets the 'Low' classification would be unlikely to meet the materiality threshold and would not be reportable.
- A08.1: we recommend amending "Distributed denial of service attacks" (DDOS) to "Denial of service attacks" to align with the categorisation used by the NCSC and CERT NZ in their reports. Using this categorisation would also then encompass DDOS.
- A17.1: we believe that this question is highly subjective and should be removed. Furthermore, we do not understand what bearing media attention should have on any response to an incident by the entity or RBNZ, rather the response should reflect the type and scale of incident.
- A18.0: this question appears to be surplus to needs as there is already a question about engagement with regulators in A20.0. It is also unclear what is meant by 'regulatory impact'.

Part B:

As noted above, we consider that Part B should be removed, and the affected entity should be able to agree update requirements with the supervisor that appropriately reflect the nature of the incident and the necessary response to it.

Part C:

We consider an alternative way to provide post-incident reporting to RBNZ would be more appropriate, such as discussions with the supervisor. The reason for this is the information required by Part C is potentially highly sensitive and collating it into one document and then sharing it externally is a risk to an entity. Entities will be able to provide information on the resolution of the incident and actions taken for mitigation of future incidents through discussions with their supervisor.

Q4. Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

ICNZ does not find the value of the proposed periodic reporting to be clear and notes that no rationale for this is outlined in the proposals. We believe the requirement for periodic reporting of cyber incidents should be removed for the following reasons:

- It is unlikely that entities report internally on low level and non-material incidents with no business impact. These incidents include attempted cyber-attacks that are automatically detected and blocked.
- This non-anonymised information would disclose a detailed picture of the cyber security of an organisation and should not be collated and shared externally.

- The resources required to collate this reporting and the risks of it being disclosed will have a negative impact on cyber resilience.
- Collection of such information relating to cyber resilience of entities such as banks and insurers will result in RBNZ having an inordinate amount of data making it an even more attractive target for malicious threat actors.
- We question the value in RBNZ using resources to analyse information on non-material cyber incidents and do not consider it will provide any meaningful insights or benefit to the financial sector and its customers.
- CERT NZ and the NCSC already collect data and provide regular trend reports on cyber risk impacting the Aotearoa New Zealand financial sector which RBNZ could utilise.
- Collecting this 'low-level' type of information does not appear to align with established data collection practices for cyber resilience internationally. For example, APRA does not require periodic reporting on all cyber incidents.
- We presume that the intended purpose of such information collection is to learn from experience but there is not any information in the proposals about how the learnings would be shared back with the organisations who provide the information.

Q5. Do you have comments on our proposed periodic cyber resilience capability survey?

Consistent with the feedback already provided, ICNZ believes that the information to be requested via the proposed survey provides significant cyber intelligence on an entity. The collation and external sharing of such information poses a serious risk to cyber security for an entity. Storage and further sharing of the information by RBNZ unencrypted and in a way that identifies (or potentially identifies) an entity further escalates the risks.

Proposed alternatives

Individual entity - Each RBNZ regulated entity will have differences in its approach to cyber resilience and the maturity level it has reached. For example, some will carry out internal and external audits of cyber resilience and/or be subject to overseas prudential cyber reporting requirements (such as APRA requirements). If RBNZ is concerned about an individual entity's cyber resilience, then we consider a more effective approach is for cyber resilience to be included in RBNZ's regular prudential supervision with the entity.

Sector view - If RBNZ wants to obtain a view of cyber resilience of the Aotearoa New Zealand financial sector we consider a more appropriate alternative would be through an anonymous online survey with higher level questions than those in the proposed survey. This would gather more useful data that can be aggregated at a sector level. Being an anonymous survey would encourage participation by entities.

Specific feedback

Despite the commentary above, and without resiling from our position that the proposed periodic survey itself creates cyber risk and is not the most efficient way to ascertain the financial sector's cyber resilience, we have the following specific feedback about the questionnaire in Annex A:

- The proposed questions are too detailed to provide a sector wide view. For example, without context of the size and nature of an entity, it is difficult to see what useful information can be ascertained from knowing the specific number of internal staff trained to identify anomalous activities.
- The intended scope of the survey must be clear. For example, should the responses cover all systems in the organisation, or only those relevant to NZ operations and customers?

- Any data type that is not a 'yes/no' or a numeric should be defined. For example, what would satisfy 'exceeds' or 'enhanced'?
- Many of the questions in the survey are about business risk management (such as B1, Identify, Q3: "What is the number of critical functions with unacceptable risk levels?"). Responding to these types of questions will require input from various business units across an entity which increases the human and time resources required to respond to the survey.
- In relation to A3, Culture and Awareness, Q11: to capture helpful information and to minimise the risk of different interpretations, this question ought to be more specific. For example, what does the RBNZ consider "relevant cyber training events/modules", or would that be left to the entity to determine?
- In aiming for consistency with the RBNZ Guidance, it would be helpful for the survey questions to reference specific sections or requirements.

Finally, we note that many of the questions in the survey are phrased as a measure of an entity's resilience in accordance with the RBNZ Guidance and therefore the exercise appears more akin to a compliance review. This raises the question of whether the guidance has become more of a mandatory cyber resilience requirement, than mere guidance on best practice. This would appear to go beyond the usual approach to guidance and we would appreciate the RBNZ clarifying whether this is in fact the intention.

Q6. Do you have comments on our proposed frequency of reporting?

We do not consider the proposed periodic survey to be the appropriate mechanism for obtaining information on the cyber resilience of an entity. However, without resiling from this position, if the survey is to be advanced, annually would be too frequent for large entities. We suggest RBNZ should consider every two years for large institutions and every three years for other institutions. This would also provide time to consider the information received from a survey, particularly the first one, its usefulness and whether changes would be required to the contents of the next survey. Additionally, requests for periodic reporting would align with APRA's timetable to lessen the regulatory burden.

We also note that this new survey would come on top of a rapidly growing list of regulatory returns required each year for insurers under a range of regulatory regimes.

Q7. Do you have comments on how we proposed to share information?

As noted above, ICNZ holds concerns regarding the nature and detail of the information proposed to be collected and stored by RBNZ. However, we recognise the benefits of sharing details of an attack with other regulated entities in near real time (such as Indicators of Compromise, and Tactics, Techniques and Procedures) to support detection and response activities, so long as it can be done in a way that does not identify, or potentially identify, an entity.

Please note that the following comments are made in relation to the principles of RBNZ sharing information and are subject to the nature and details of the actual information being shared:

- Paragraph 5.1: regarding the intention to share information with various forums and industry, it is not clear what is meant by "*after considering the need to protect privacy and commercially sensitive elements of the information*". We consider the entity that provided the information should be consulted before any such sharing but would appreciate further information on who else may be involved in this consideration other than the RBNZ and the FMA. We do not believe that information which identifies an entity should be shared with any other party, under any

circumstances, without first notifying the entity that provided the information.

- Paragraph 5.2: we support the proposal that the material incident reporting template will meet the reporting requirements of both the FMA and the RBNZ. To further simplify the process, we suggest that either the RBNZ or the FMA should be nominated as the single contact for the regulated entity. This will be more efficient than an entity having to report to and answer questions from multiple regulators.
- Paragraph 5.4: we would only support RBNZ sharing full details of its cyber resilience data collection with NCSC if it is done in a way which does not identify the entity that has provided the information. The survey contains highly sensitive information and could be from entities that do not have a direct relationship with NCSC.
- We note that NCSC will continue to seek further engagement with organisations independently. We agree that is appropriate for NCSC to use a more direct channel particularly given their focus on nationally significant organisations. Not all RBNZ regulated entities will necessarily be nationally significant and information collected for prudential supervision purposes will not necessarily be relevant for NCSC's purposes.
- The sharing of information would necessitate storage of information collected by the RBNZ. Information should only be stored for as long as it has an active purpose and should otherwise be deleted. In this regard, stored information should be reviewed at least annually to ensure that it is not being stored unnecessarily.

Q8. Do you have any comments on our analysis on the financial policy remit?

ICNZ does not believe that the proposals, as currently presented would effectively meet the objective of improving cyber resilience and there is the potential for them to increase cyber risk. At present, the proposals would require RBNZ regulated entities to collate and disclose large amounts of highly classified cyber intelligence which has restricted access even internally within entities. The receipt and storing of such information from entities in the financial sector raises concerns of whether it could make the RBNZ a target for cyber criminals. Any unintended access to, or disclosure of, such information would significantly increase cyber risk to RBNZ regulated entities and potentially to the financial stability of Aotearoa New Zealand given the number, financial nature and size of the entities involved.

As already noted in our responses above, we also question how useful many aspects of the requested information are and how practical it is for RBNZ to review it all and ascertain insights that would be of practical use to RBNZ and the financial sector in increasing cyber resilience. Instead, there will be a significant volume of information being stored unnecessarily by RBNZ and this will carry associated risks. Rather than RBNZ potentially analysing a substantial amount of non-material data we consider resources would better be spent on issues that would help improve cyber resilience in Aotearoa New Zealand, for example, improving cyber threat intelligence information.

In terms of the proportionality component (which we agree is of importance), we consider the current proposals would impose significant regulatory and supervisory costs which are not proportionate to the expected benefits to the financial system and society. Significant resources from RBNZ regulated entities would be needed to meet the proposed reporting requirements. This would divert resources from cyber resilience activities and increase cyber risk for entities and their customers.

Q9. Do you have comments on our proposed prioritisation of our cyber data collection proposals?

Incident reporting

Unless there are changes to the information being requested by RBNZ (which our submission advocates there should be) we do not consider implementing the incident reporting requirements "as soon as possible this year" is reasonable or workable. Significant work would be required to put processes in place to gather the information and to put it in the required format within the required timeframes.

Cyber survey

While there is not currently any proposed timing on when the cyber survey will be required, we ask the RBNZ to be mindful that this would also require substantial work by its regulated entities and therefore needs a significant lead time. Because of the classified nature of the information, there will need to be processes put in place to collate, encrypt and transfer the information in accordance with internal security and data protection policies.

We reiterate again our view that we consider the proposed cyber survey is not the most effective mechanism for gaining a view of the cyber resilience of an entity or the financial sector.

Finally, we would appreciate further information about the next steps in this process once the RBNZ has received submissions. For example, is it anticipated that the RBNZ will hold workshops which would allow interested parties to raise questions and gain clarity on the proposals and why the RBNZ has chosen to take a particular direction.

Conclusion

Thank you again for the opportunity to submit on the proposals. If you have any questions about our submission or require additional information, please contact S9(2)(a)

Yours sincerely,

S9(2)(a)

S9(2)(a)

From: S9(2)(a)
Sent: Monday, 8 May 2023 2:41 pm
To: cyberresilience
Subject: Cyber resilience consultation

Thank you for the opportunity to provide feedback on these proposals:
I am an individual / interested bystander and so my comments are brief.

1. Cyber incident reporting

A requirement to report all material cyber-incidents to the Reserve Bank as soon as practicable, but within 72 hours (see Annex A in the consultation paper for the reporting template) and to report all cyber incidents (material and non-material) periodically.

I **SUPPORT** this proposal which seems obvious to me. I see it as entirely consistent with the Banks' mandate to ensure financial stability and as overall regulator and supervisor of the New Zealand financial system. In order to properly fulfil those functions– the Bank must be across any threat to the system it monitors.

Currently no one seems to have an overall picture on cyber threats which results in an ad hoc response.

2. Cyber capability survey

A periodic cyber resilience survey about organisation capabilities (see Annex B in the consultation paper for the draft questionnaire).

I **SUPPORT** this proposal which seems obvious to me. I see it as entirely consistent with the Banks' mandate to ensure financial stability and as overall regulator and supervisor of the New Zealand financial system. In order to properly fulfil those functions– the Bank must be across any threat to the system it monitors.

Currently no one seems to have an overall picture on cyber threats which results in an ad hoc response.

COMMENT: My only ancillary comment is around standards and expectations of the organisations to which this practice will apply. Will there be minimum software / hardware requirements for example ? Technical I know but I assume this is also in the pipeline ?

Thank you

S9(2)(a)

Reserve Bank of New Zealand

By email: cyberresilience@rbnz.govt.nz

3 July 2023

MICROSOFT'S RESPONSE TO THE RESERVE BANK OF NEW ZEALAND'S CYBER RESILIENCE DATA COLLECTION PROPOSALS

1. Thank you for the opportunity to provide a response to the Reserve Bank of New Zealand's (*RBNZ*) Cyber Resilience Data Collection Proposals (the *Consultation*). We consider the Consultation to be an important and timely step in addressing and building resilience across New Zealand's financial services sector.

2. Microsoft provides this response as a major provider of online (cloud) services, software and other technology products and services to RBNZ-regulated entities. Our industry leadership in data security and privacy protection has been recognised for over two decades, beginning with the establishment of our Trustworthy Computing principles in 2002, and continuing today with our Microsoft Trusted Cloud initiative. Microsoft cloud services provide a broad set of security and privacy compliance offerings, including third-party certifications and attestations.

3. We are supportive of the proposals contained in the Consultation, but wish to make a submission in respect of Question 1, relating to the proposed cyber incident reporting timeframe.

Question 1: Do you have comments on our proposed incident reporting timeframe?

4. At section 3.1 of the Consultation, the RBNZ proposes that all material incidents "must be reported as soon as practicable after they are detected but no later than 72 hours." As further emphasised in our response, Microsoft suggests that the timing for a regulated entity to notify should commence only **after it becomes aware** of the material cyber incident.

5. Persons who obtain unauthorised access to information systems work hard to disguise that fact and may, in fact, obtain unauthorised access indirectly, for example through outsourced service providers' systems. Accordingly, the nature of many regulated entities' business and informational technology arrangements is such that many information security events are often detected initially by a third-party service provider and subsequently advised to the regulated entity. Accordingly, in our view, time should start to run from the point at which the RBNZ-regulated entity becomes aware of the incident and has had time to review the incident and its effects to determine whether it meets the materiality threshold.

6. We believe that, in any event, the approach proposed by Microsoft in paragraph 4 is the RBNZ's intended approach, noting that Part A of the reporting template included as Appendix A to the Consultation specifically states that detection may occur by way of "outsourced provider notification" or "customer notification" to the regulated entity. This suggests that "detection" of the incident in this context occurs at the point at which the outsourced provider or customer makes the regulated entity aware that it has occurred. However, we suggest that the language used in the RBNZ's final policy document is clarified in further guidance, for the avoidance of doubt.

7. We welcome the value the RBNZ places in the Consultation document on closer alignment with Australia, noting that this approach may minimise the compliance burden for regulated entities who also operate, or are part of a broader group that operates, in Australia. To this end, we note that the approach proposed at paragraph 4 above would align with language used by the Australian Prudential Regulation Authority (*APRA*) in CPS 234 Information Security. CPS 234 requires regulated entities to "…notify APRA as soon as possible and, in any case, no later than 72 hours, after **becoming aware** of an information security incident"[1] (emphasis ours). We believe it would be helpful to make that even more explicit in the language adopted by the RBNZ in its final policy document.

8. Microsoft thanks the RBNZ for the opportunity to make this submission and is committed to increasing cyber resilience and helping industry participants protect themselves and their customers. We would welcome the opportunity to further discuss with the RBNZ the points made in this submission and to provide any additional input that may be of help in developing the Proposals or their practical implementation within financial institutions.

Kind regards,

S9(2)(a)

[1] See APRA's CPS 234 at paragraph 35.

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:

S9(2)(a)
[redacted]
[redacted]

[redacted]
[redacted]
[redacted]

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.

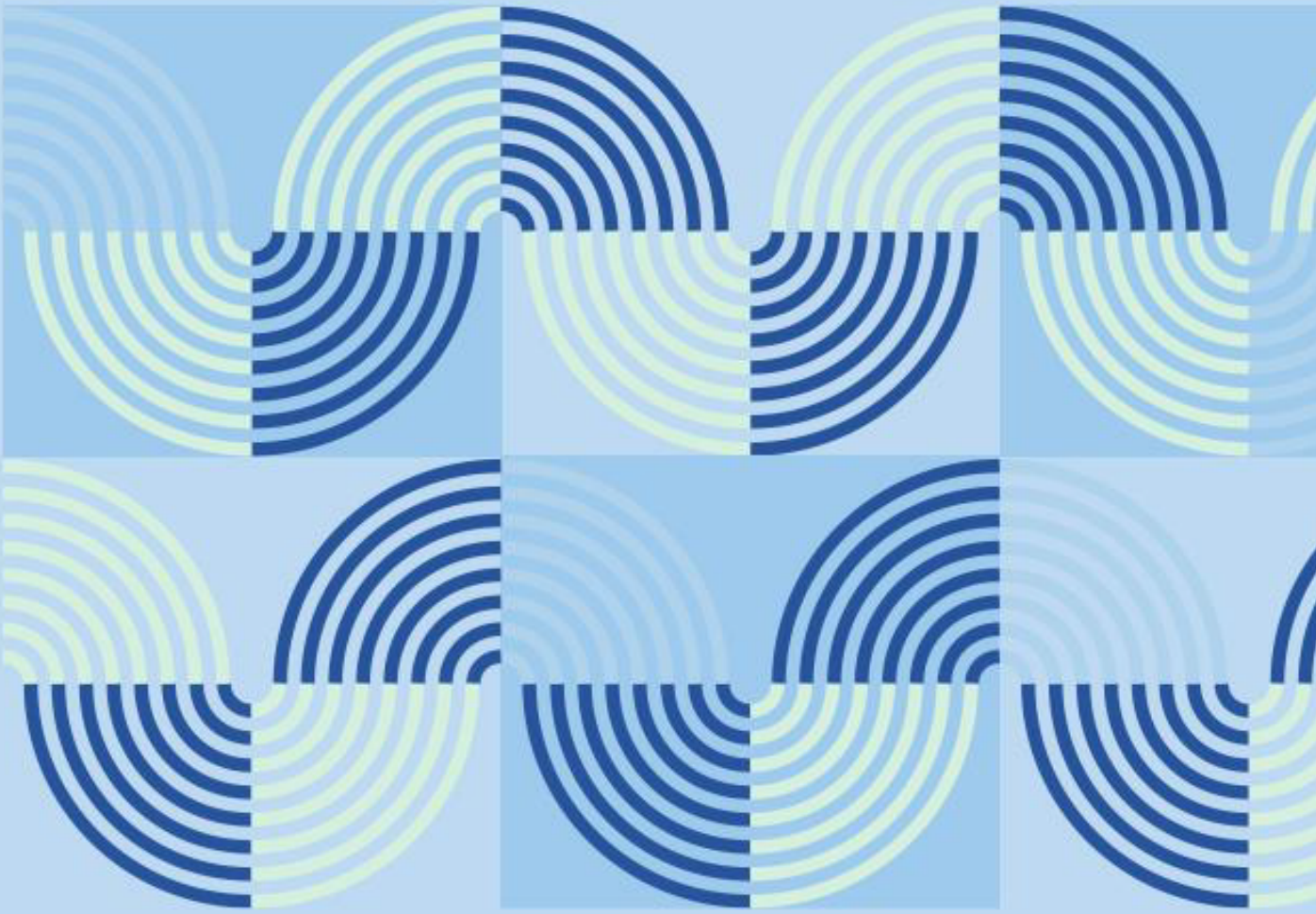
38. We would also request further information as to the timeline of when the requirement will take effect. It would likely take banks at least six months to prepare to satisfy their reporting requirements on a regular and sustainable basis.

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.



Cyber Resilience Data Collection Proposals

Reserve Bank of New Zealand

03 July 2023

Cyber Data Collection Consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
Wellington, 6140

By email: cyberresilience@rbnz.govt.nz

Cyber Resilience Data Collection Proposals

Thank you for the opportunity to provide a submission on the Reserve Bank's Cyber Resilience Data Collection Proposals, 08 May 2023. This submission is on behalf of Union Medical Benefits Society Limited (Trading as UniMed).

UniMed is an Incorporated Society registered under the Industrial and Provident Societies Act 1908 in November 1979. Its principal product and service is health insurance within New Zealand. The Society is domiciled and incorporated in New Zealand and is a Public Benefit Entity.

The Society was granted a licence by the Reserve Bank of New Zealand on 23 May 2013 to operate as an insurer subject to the Insurance (Prudential Supervision) Act 2010 (IPSA). The Society is also licensed by the Financial Markets Authority to operate as a Financial Advice Provider and will be subject to licencing requirements under the upcoming Conduct of Financial Institutions (CoFI) regime.

UniMed provides health insurance products to more than 100,000 Members throughout New Zealand. While UniMed's key market segment is 'Group' workplace schemes, employees and their whānau, UniMed also provide direct to retail health insurance products and continuation options for group leavers.

I can be contacted on S9(2)(a) to discuss any element of our submission.

Yours sincerely

S9(2)(a)

Union Medical Benefits Society Limited

Q 1 Do you have comments on our proposed cyber incident reporting timeframe?

The proposed 72-hour timeframe for reporting material cyber incidents is consistent with the notification timeframe to the FMA, under the upcoming CoFI regime, of any event that materially impacts the operational resilience of a financial institutions critical technology systems. It makes sense to streamline these notification times.

While UniMed supports 'notification' of a material incident within the proposed 72 hour timeframe (clarity is sought on whether this includes out of business hours, such as weekends), we consider the detailed reporting within this timeframe (through Part A of the Material Cyber Incident Notification Report), and the ongoing reporting (through Part B of the Material Cyber Incident Notification Report) every 24 hours, to be overly burdensome. UniMed's critical concern is that the proposed detailed and ongoing reporting will be resource intensive, especially for smaller entities with limited internal technical resources, necessitating skilled resources to detract from incident response and remediation in order to attend to reporting. This could foreseeably prolong resolution of the incident, with an increased negative impact on affected persons.

We suggest that further consideration be given to the proportionality of response. For example, if the 'reasonable outlook' from an initial triage is that the incident is both not malicious and isolated (i.e only one system is effected, or, it appears to be an internal incident / affecting the entity only), an initial notification could be made to the Reserve Bank (and FMA for CoFI licenced entities), with the subsequent completion of Part A within 5 business days. For these isolated and non-malicious incidents, weekly updates (through Part B) could be provided to the Reserve Bank until resolution. A more immediate update should be required if the incident is later realised to be more widespread than first thought, or the investigation uncovers malicious intent.

Where an entities initial triage indicates the incident is widespread and / or a result of malicious activity, we acknowledge this will create a heightened level of interest from the Reserve Bank and accept that an increased level of reporting would be appropriate. However, in such an event, particularly in a smaller entity with limited technical staff, the skilled resources will already be under immense pressure investigating and containing the incident, liaising with and managing vendors, keeping the operation teams and management informed, potential PR input, activating BCP responses etc. Pausing from these critical activities to provide detailed reporting every 24 hours would be impractical.

To ensure that the Reserve Bank is provided the information necessary to assess the potential for wider industry risk, whilst enabling the entities skilled resources to primarily focus on containment, we suggest, in the instance of a widespread of malicious cyber incident, that the entity provides the Part A response within the 72 hour timeframe and then engages with the supervisor to agree the form and frequency of updates (which may or may not be through the completion of Part B).

Q 2. Do you have comments on our proposed definition of materiality?

We strongly support a clearly defined and unambiguous definition of what constitutes a material incident.

As this will be heavily relied on by entities to determine which cyber incidents are subject to the significantly involved material incident reporting, and which may be incorporated in the far less time critical and resource intensive periodic reporting, it is of utmost importance that the definition does not contain language which is subjective, or which could lead to over or under reporting.

We have concerns with the inclusion of the phrase '*or had the potential to materially affect*'. We consider this should be removed from the definition.

As drafted, this definition would appear to include attempted cyber incidents which have been successfully blocked by the entity's controls (ie firewalls). It would be difficult to determine, especially within a period of less than 72 hours, whether any of these blocked attempts would have had the potential to materially affect the entity. That the attempts were successfully blocked, proves the effectiveness of the control which, in our opinion, eliminates these incidents from being considered material.

Including incidents which had the 'potential to' but did not actually affect (materially or otherwise) the entity, would result in over reporting, with no real value to the Reserve Bank (this information would still be provided in the periodic reporting), but would impose a significant compliance burden to the entity.

Through removing the words '*or had the potential to materially affect'*, the definition would more closely align with the reporting requirements to the FMA under CoFI standard condition *5:*

> *You do not need to notify us of minor events, such as receiving a 'phishing' email* ***that is not successful*** *i.e. has not materially disrupted or affected the provision of your financial institution service, and* ***has not had a material adverse impact on consumers****."* (Emphasis added).

The '*potential to materially affect'* phrase also appears inconsistent with the definition of cyber incident on page 9 of the consultation paper, which we note is the definition contained in the glossary of the Reserve Banks Guidance on Cyber Resilience.

We consider the FMA's emphasis, (under CoFI standard condition 5) on the incident having an actual 'material adverse impact' is a more appropriate definition for 'materiality'. We are otherwise in support of the definition as drafted.

We also support the inclusion of the additional guidance points (adapted from the Reserve Banks framework for breach reporting for registered banks) to help entities consider how a cyber incident could present material impacts and raise prudential concerns.

Including some examples of hypothetical, but not unlikely, incidents that would and would not be considered 'material' against this definition, would be a pragmatic and useful additional guidance tool for entities.

Q 3 Do you have comments on our proposed cyber incident reporting template?

The cyber incident reporting template is easy to follow as a submitter and we appreciate the efficiencies of utilising the incident notification template for notification to the FMA as well as the Reserve Bank, where appropriate.

In the current proposal, if there has been 'any updates or changes' since the previous reporting, Part B must be (re)completed in full. While this should be easy for the entity to update only the relevant fields, it may be difficult for the Reserve Bank to readily identify what has changed, particularly if the update or change is limited to one or two fields only. We suggest consideration be given to how any changed fields can be more readily drawn to the Reserve Banks attention.

The categories listed at A09.0 extend beyond security related incidents, to include 'failures'. Occasional IT outages can happen for many reasons and arguably should be exempt from cyber incident reporting unless the outage itself is a result of a breach.

Q 4 Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

An effective managed security provider may block somewhere in the region of 6,000 – 10,000 attempted breaches in any given month. Obtaining, or manipulating, this data to fit in a specified format may be cumbersome as standardised reporting produced by various monitoring & detection tools will deliver outputs in different formats.

The periodic reporting proposes to collect information on 'all cyber incidents that have occurred'. We encourage greater clarity on what is and is not in scope for this reporting.

The 'cyber incident' definition (page 9 of the consultation paper) would indicate that the periodic reporting should only capture an event which:

i. *jeopardises the cybersecurity of an information system or the information the system processes, stores or transmits; or,*
ii. *violates the security policies, security procedures or acceptable use policies.*

However as noted in question 2, this appears to be inconsistent with the proposed definition of materiality.

Section 3.2 of the consultation paper is unclear as to whether any non-material events would be excluded from the reporting, such as phishing attempts, IT outages, or blocked requests that are automatically stopped by the entities' firewalls and other cyber security measures.

With highly sensitive data being collected from entities it would be reassuring to understand what storage and security protections will be in place to protect the incident data, particularly as this data may contain customer information (including PII) and direct or indirect details of an entity's vulnerabilities or risks. To mitigate the risk of any unintended exploitation of the entity's vulnerabilities, and to protect customer information, we suggest that both customer information and information which could identify the entity should be anonymised in any stored reports.

Q 5 Do you have comments on our proposed periodic cyber resilience capability survey?

We support the proposed periodic survey as a tool for the Reserve Bank to better understand the cyber resilience capabilities of regulated entities.

The data that will be collected through this survey will include significant cyber intelligence on an entity, including the entity's potential vulnerabilities. There could be severe outcomes if the security of this information were to be compromised and the information accessed by a malicious party. Alongside extremely robust security provisions, we strongly recommend that any information which could identify the entity be anonymised to mitigate the risk of the entity's vulnerabilities being exploited.

We support the publication of trends, key lessons or insights to help inform a broader industry and public understanding of cyber resilience in the financial sector. We would encourage the Reserve Bank to explore whether there is an additional opportunity to provide some form of comparative analysis (anonymised or aggregated) to entities from which they can benchmark themselves and aim to improve against.

Q 6 Do you have comments on our proposed frequency of reporting?

We support the annual reporting frequency for large entities and every two years for others.

Q 7 Do you have comments on how we propose to share information?

Section 5 of the consultation paper states *certain information that 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.*

We consider there could be more clarity around the intentions for information sharing, particularly clarity around when the information would be shared on a non-anonymised / aggregated basis. It would be reassuring to understand the types of circumstances where the Reserve Bank may collaborate and coordinate with agencies such as NCSC, CERT.

Section 3.3 notes '*We will use the information gathered through cyber incident reporting to support any necessary regulatory response and to ensure that there is co-ordinated communication and engagement from financial regulators. Our proposal will ensure that details of cyber threats are communicated in near real time to improve situational awareness, prevent attacks spreading and preserve confidence in the economy.'*

It would be reassuring to have clarity on what types of incidents may be shared 'in near real time', to which possible forums, and in what circumstances this would include identifiable information.

While we appreciate that information will only be shared 'after considering the need to protect privacy and commercially sensitive elements of the information', we would encourage the Reserve Bank to provide advance notice to an entity before sharing its identifiable information with another party. We would further suggest that the entity be given reasonably opportunity to contest the sharing of non-anonymised information.

We strongly consider that any identifiable customer data should be anonymised at all times.

We appreciate the opportunity for streamlining the incident notification to both the Reserve Bank and the FMA. Clarity would be helpful on whether this would be expected for Part A only, or whether the FMA would expect the same updates and conclusion reporting through Parts B and C.

While incident notification to both regulators is required for CoFI licenced financial institutions, we strongly recommend that the Reserve Bank and FMA commit to only one regulator making enquiries of the entity while the incident is ongoing, so that resources are primarily focussed on resolution, without the distraction of reporting and responding to enquiries from multiple regulators.

Q8 Do you have any comments on our analysis on the financial policy remit?

The current proposal has appropriately recognised the greater cyber risk attached to larger financial institutions. We agree with the classification of a large institution as having assets in excess of $2 billion.

As noted in question 1, we consider that the proportionality should be extended with regard to the detail and timeframes of material incident reporting, especially with consideration of the impact on smaller entities.

The consultation notes the Reserve Banks view that 'the proposals in this paper are not expected to impose significant costs that could provide barriers to entry and inhibit competition'. While the anticipated costs to

entities will not reach the extreme level of causing entry barriers or departure from market, the costs to entities will not be insignificant, particularly on smaller entities, with the frequent and detailed reporting demands having a significant IT and compliance resource impact.

We do agree generally that the intention behind the proposals will have a significant impact on improving cyber resilience of regulated entities and improving the Reserve Bank's understanding of cyber resilience within the financial sector.

Q 9 Do you have comments on our proposed prioritisation of our cyber data collection proposals?

We agree with the commencement of incident reporting as a first priority, with the information gathering cyber survey to follow.

An appropriate lead in time will be crucial, especially for smaller entities. In addition to the development or enhancement of internal processes and systems, entities will also need to validate the requirements and develop or refine processes with managed security service providers. At a time when Financial Institutions are experiencing an abundance of new and upcoming regulatory requirements, demand on internal resource is a real challenge. The proposal to implement the incident reporting 'as soon as possible this year' may be impracticable. We encourage the Reserve Bank to reconsider the implementation timeframe with regard to the wider regulatory reforms affecting Financial Institutions.

100 St Aubyn Street East
PO Box 431, Hastings 4156
0800 229 943
unitymoney.co.nz
enquiries@unitymoney.co.nz

26 June 2023

Cyber Data Collection Consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

Unity Submission on Cyber Data Collection Consultation

Kia ora sir/madam,

Thank you for the opportunity to provide a submission on the RBNZ consultation on the **Cyber Data Collection Consultation.**

Unity is generally supportive of the direction the RBNZ is taking to understanding the sector's cyber security risk profile, and to introduce mandatory material cyber incident notification. However, we are very conscious of the sensitivity of this information and how its security will be managed by both the RBNZ and FMA. For example, secure collection of data, limited and secure access to raw data, limited/anonymous sharing of incident information with other agencies, and general security measures in place around storage of sensitive information must be carefully considered, managed and monitored. The RBNZ has identified the importance of safeguarding the information it collects in Section 5 its submission paper. It is critical that measures are in place before any information is sought from the sector.

We have considered the consultation questions, as well as the content of the Cyber Incident Reporting / Cyber Capability survey. Our responses on the questions are outlined below.

1. Do you have comments on our proposed cyber incident reporting timeframe?

For material cyber incidents, notification to RBNZ / FMA 'as soon as practicable…but with 72 hours' seems reasonable. Also, six-monthly reporting of all cyber incidents seems reasonable, but further information is needed on this:

- What format will the reporting take? How much detail would be required? A balance needs to be struck between understanding the level of incidents vs becoming onerous for businesses to complete.
- 'Cyber events' definition is broad, especially when including 'acceptable use policies'. Are these acceptable use policies those that are defined by individual businesses' suite of policies?

2. Do you have comments on our proposed definition of materiality?

The definition of material incidents is good, no further comments to add on this.

3. Do you have comments on our proposed cyber incident reporting template?

Yes:

- 'Cyber Attack' (A08.0) should be renamed to 'Cyber Incident', as not all cyber incidents are 'attacks'.
- The drop-down list options in A08.0 should also include "Inappropriate use" to capture incidents as a result of internal human error and/or employee malicious behaviour.

4. Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting?

Only the comments made above in terms of the detail. E.g. clarity is needed on what format will the reporting take and how much detail would be required. This reporting should not be onerous.

5. Do you have comments on our proposed periodic cyber resilience capability survey?

Generally, the questions asked are in line with the *Guidance on Cyber Resilience*. However, the RBNZ should provide flexibility around responses to capture the different maturity of compliance businesses may have with various systems the business uses. We are also interested to understand what, if any, resulting action or followup the RBNZ intends to do upon receipt of survey information, particularly where businesses may be at a relatively lower maturity of cyber resilience. We would welcome the RBNZ's direction on their longer-term future plans on this.

6. Do you have comments on our proposed frequency of reporting?

Unity, as a smaller business, is comfortable with the frequency of reporting against the survey to be conducted every 2 years, and for annual reporting requirements for large businesses.

7. Do you have comments on how we propose to share information?

As noted above, sharing information on cyber incidents and maturity needs to be carefully managed due to its sensitive nature. The RBNZ and FMA should share generic information where possible, noting that should businesses experience a material cyber incident, they will be engaging directly with the relevant parties (e.g. Police, CERT NZ, insurers).

8. Do you have any comments on our analysis on the financial policy remit?

No

9. Do you have comments on our proposed prioritisation of our cyber data collection proposals?

No

Please contact me via email should you have any further questions on our submission feedback.

Ngā mihi,

S9(2)(a)