ICNZ 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.

<u>Scope of the proposals</u>

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.

<u>Definition of cyber event</u>

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.

<u>Alignment with FMA requirements is positive</u>

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.

Comments on the template

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 Jane Brown (jane@icnz.org.nz).

Yours sincerely,

Tim Grafton

Tim Grafton
Chief Executive

Jane Brown
General Counsel