29 January 2021

Dynamic Policy Team
Financial System Policy and Analysis
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

By email: cyberresilience@rbnz.govt.nz

RBNZ – Risk Management guidance on cyber resilience and views on information gathering and sharing

About Fidelity Life

Fidelity Life is New Zealand's largest locally-owned life insurer and the 2017, 2018 and 2019 ANZIIF New Zealand Life Insurance Company of the Year. We've paid more than $1.1 billion in claims since we were founded in 1973. We distribute our products through a network of 2,000+ independent financial advisers, as well as through strategic alliance partners, and employ around 250 people.

Less than 40 per cent of New Zealanders have a life insurance policy[1] which means under-insurance remains the burning issue our industry needs to address. Evolving consumer and regulatory expectations, legacy technology constraints, rising claims costs and increasing pressure on profitability and solvency are other challenges facing life insurers.

That's why we're transforming our business to reimagine what life insurance can be for New Zealanders. Our aim is to deliver sustainable growth, build trust and continue delivering on our promise of protecting New Zealanders' way of life.

Introduction

Thank you for the opportunity to provide feedback on the above consultation. We understand that cyber incidents continue to be a growing risk for all New Zealand entities and there is a need for regulators to promote and raise awareness of cyber resilience for all those involved in the financial sector.

We welcome further discussion on the scope of information gathering and sharing on cyber resilience, to ensure what is being proposed is appropriate due to the sensitivity of some information and to ensure any adverse consequences of collecting and sharing information is well considered. A fundamental component of cyber security is limiting the disclosure of information about the security an entity has in place.

[1] Financial Services Council: Moments of Truth – Key Insights into the New Zealand Life Insurance Industry, September 2019.

We also ask that there is clarity and consistency across regulators (and relevant legislative requirements) with regards to risk management guidance on cyber resilience and reporting, to reduce duplication of reporting and in turn compliance costs.

Specific Questions

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

We agree with the Reserve Bank's (RBNZ) approach to take a 'moderately active' policy stance in order to achieve its aim to raise awareness of and promote cyber resilience of the financial sector. The publication of risk management guidance on cyber resilience (Guidance) will help ensure there is a baseline-level of cyber resilience applied across all entities who can then tailor them to their own specific needs and technologies. Any Guidance should be reviewed to ensure it remains relevant.

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

We agree with the RBNZ's approach of aligning to international practice in developing Guidance. This enables entities to get up to speed with international practice and provides a more consistent approach to cyber management. We do note the following:

- A1.8. We are of the view this recommendation needs to be practical with regards to the size and nature of an organisation. Firstly, it may not be practical in all circumstances that a Board be included in the appointment process of a senior executive. While we support the appointment of a senior executive to be responsible for cyber resilience issues, this may be just one aspect of their role. This means it may be difficult for that person to act completely independent from the IT/operations department. Due to the technical nature of this role and size of New Zealand there may also be a shortage of resources to carry out this function.
- A2.1.1 to A2.6. We agree with the importance of an entity having a cyber resilience strategy and framework that is regularly tested and updated. It is our view that the requirements set out at A2.1.1 are too prescriptive and should be more high level. The detail of a cyber resilience strategy and framework should not be shared outside of an organisation to reduce the risk of it being accessed by a third party. Further to this, it may not be appropriate to disseminate the actual cyber resilience strategy and framework to all staff as set out at A3.1.1 but instead disseminate relevant elements of it which support risk mitigation.
- B2.2. There are many ways to mitigate against cyber incidents and attacks, segmentation being one option. This recommendation is therefore too prescriptive and needs to allow for other options that may be more appropriate.
- B2.3 and B2.3.2. We have concerns about these recommendations. See our feedback to question 3 below.
- B4.3. We believe that it could be clarified that staff responding to a cyber incident or breach may outsource the skills required to address the situation.
- B4.8. We would like further clarification about when a common response and recovery plan is suitable for the financial sector. Because we have a fuller understanding of our circumstances, we feel that we are best positioned to develop our own plan to respond to our own unique circumstances. We want to ensure that developing and sharing response and recovery plans for

cyber incidents across the financial sector, does not expose or increase the risk of further cyber incidents.

- D3.1. We agree with the sentiment proposed but negotiation with large international third-party entities may be difficult. We suggest that this requirement be softened slightly to "use their best efforts".
- D8.1 We ask the RBNZ to clarify what 'critical functions' means so we can better understand what outsourcing needs to be notified to the RBNZ.

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

We agree that Guidance should be based on a set of high-level principle-based recommendations. We ask that a further review of the Guidance is undertaken to ensure that the recommendations are sufficiently high-level and principle-based to avoid unintended consequences for some industries and consumers.

In particular, B2.3 states an "entity should regularly monitor its systems… and ensure all available updates are installed and sufficient support is maintained" and further, B2.3.2 'legacy systems that are outdated… should be decommissioned and replaced.' Legacy technology constraints are an issue for some industries. There are potential challenges with ongoing support and maintenance in a legacy systems environment. We suggest that B2.3 should include the words 'as appropriate'. There could also be significant costs and resource associated with such a recommendation to decommission and replace legacy systems, which would likely impact customers. A better approach would be to ensure that the 'appropriate security is applied to support legacy systems and protect information.'

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

We agree with the RBNZ's view on the principle of proportionality and a risk-based approach being adopted by the Guidance especially given the number of different entities who will apply it, some having more mature cyber resilience practices in place than others. It allows entities with a baseline level of cyber resilience to continually improve cyber resilience as they mature. We also agree with the RBNZ's statement that 'regulated entities should not use this Guidance as a checklist for cyber resilience minimum requirements' and 'instead, entities should design and develop their own cyber resilience frameworks that adequately address the specific cyber threats they face.'

We do note however that having the two levels of recommendations (baseline and enhanced) allows entities to apply the minimum only and ask if further context can be given as to when it may be more appropriate for entities to adopt enhanced-level practices. We think further review should be done of the items within baseline and enhanced. In some cases, items should possibly be changed from one classification to the other.

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

We agree that the Guidance should apply to all regulated entities of the Reserve Bank.

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

We understand the RBNZ's objectives regarding information gathering and sharing on cyber resilience to support risk management guidance and practices and to help build cyber threat awareness across the stakeholder community.

As acknowledged by the RBNZ, certain cyber related information can be highly sensitive, and it is our view that information gathering and sharing should be handled extremely cautiously. As such, it is important that the RBNZ follow consistent guidelines and apply the same level of security controls to ensure the safety of such sensitive information. This also applies to the other public sector bodies the RBNZ intends to share information with. It may be more appropriate that any sharing of information is done in person. This may also encourage entities to have more open conversations about their experiences.

We ask that further discussion is held on the purpose and development of a shared information resource to ensure there is no duplication of similar exchange forums that already exist. Given this is a specialised subject it is important that the RBNZ has the relevant expertise to enable a collaborative approach. We look forward to seeing a more detailed proposal on the RBNZ's information gathering and sharing concept.

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

We understand the RBNZ's view to follow international practices in collecting information and establishing a cyber data collection. We welcome further discussion on the details of what information will be collected, how it will be shared, and how it will be securely stored by the RBNZ.

In our view further consideration is needed of the potential adverse consequences of reporting certain information. For example, in some circumstances it may not be appropriate to report cyber incidents as soon as reasonable after they are detected. This is to ensure that any investigation or steps undertaken to mitigate the breach are not compromised and the focus remains on dealing with the affected information and those impacted. We also want to be mindful that any reporting of information to third parties right away does not expose any risk of further cyber incidents. There is also a significant risk of exposing commercial and or operational matters.

In progressing the information and sharing plan, we agree that maximising the value of reporting and minimising the reporting burden for organisations is paramount and ensuring there is no duplication of information being collected across public bodies. Consideration of other types of breach reporting that already exist (such as under the Privacy Act) needs to be considered so that there is limited reporting overlap.