Southern Cross RBNZ Response

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?

While Southern Cross has invested in the development of its maturity and approach to information security resilience, we believe that our organisation and our members will benefit from RBNZ promotion of cyber resilience. Providing guidance on priority areas for cyber resilience capability uplift and risk remediation across the financial sector will hopefully result in a general uplift in the protection of the data and services we all provide.

We agree with the "moderately active" proposition, which avoids taking an overly prescriptive approach which we believe may not be appropriate, given the variance in maturity across the sector.

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 Do you have any specific feedback on the draft guidance on cyber resilience?

Much of the uplift in information security maturity over the last decade has been achieved by organisations settling on a small set of international standards developed by organisations such as ISO and NIST. These standards encapsulate agreed industry best practice and comprise a baseline for the assessment of control effectiveness and maturity. Use of standards allow organisations to benchmark themselves against other organisations with a similar risk profile, they also give confidence to customers and third parties transacting with an organisation.

Southern Cross is aligned to the international Centre for Information Security (CIS) Control Framework and is continually working to uplift our information security resilience as measured by this framework. While the RBNZ guidance provided is useful educational material for an organisation unfamiliar with risk or information security concepts, we agree that the RBNZ should guide regulated entities to align with an international standard that best suits their organisational requirements,

[redacted]

rather than an RBNZ-sponsored set of standard controls or forcing one specific standard across the industry.

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

Yes Southern Cross agrees with this proposition. Regulated entities need to understand their current information security resilience posture, and whether this is inside or outside of their organisational risk appetite.

We believe that stating “principle-based outcomes” might be a better way of describing this approach, rather than referring to “recommendations”. Although still subjective, outcomes describe results and can be measured where recommendations are able to be debated. With clear outcomes behaviours can be changed.

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

Southern Cross believes that information security resilience decisions need to be backed by a robust framework that recognises the operational environment and complexity of individual regulated entities. This ensures that the benefits of improved security resilience are justified. However, we’re not convinced that the size of a regulated entity should be a major factor in a risk-based approach. While the impact to the stability of the financial sector will be less if a smaller organisation is breached in an cyber security incident, we believe that customers are entitled to the same level of protection regardless of the size of an organisation. We are also conscious of the flow on impact that an organisation can have on its partners when effected by a cyber-attack. By ensuring all organisations lift their maturity we reduce the risk to the wider industry.

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

Southern Cross agrees that all regulated entities should be covered by the RBNZ guidance. Large NZ financial services organisations including Southern Cross generally have well-developed risk and information security functions. We believe that more benefits will be gained by increasing the resilience of smaller financial services businesses, and

RBNZ’s guidance will help to support these organisations in uplifting their information security capabilities and reducing the risk across the sector.

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

Southern Cross supports information gathering and sharing. We currently engage with NZ financial services organisations and the wider information security community via the New Zealand Internet Task Force (NZITF) and a number of other channels. We also engage with other health insurers internationally as part of an industry cyber security forum. Collaboration alerts us to “live” cyber threats, attacks, and indicators of compromise and allows us to understand the effectiveness of response options. Collaboration also serves to raise our understanding of information security trends and best practices.

We understand the National Cybersecurity Centre (NCSC) sponsor a number of sector-based information sharing forums, including in the banking sector. Southern Cross believes there are advantages to leverage these existing arrangements, rather than developing new arrangements hosted by the RBNZ. RBNZ could, of course, contribute to NCSC information sharing forums. We believe that this view aligns with RBNZ’s view as expressed in the Consultation Document.

We recognise that there is often a tendency for organisations to avoid sharing sensitive operational and technical security information that could be used to refine an attack if the information was leaked. Organisations are also reluctant to share details if they have been compromised if this would lead to professional embarrassment or customer reputational damage. Any information sharing arrangement will need to account for these factors, possibly by allowing organisations to share semi-anonymously through a threat intelligence platform.

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?

[redacted]

Southern Cross would like greater clarity on the benefits of the collection approach described in the Consultation Document before we can form a view on this issue. Input to support sector benchmarking and measurement would add considerable value, however the purpose would need to be well defined to ensure the information was used appropriately.

We are also conscious of the resource impact of data collection and ensuring the right cadence. For example, any requirement to report incidents will need to be backed up by a clear definition of material incident, since identifying and managing minor incidents are a frequent business-as-usual activity for most security operations teams.

[redacted]