RESERVE BANK OF NEW ZEALAND
TE PŪTEA MATUA

Consultation Document

Risk management guidance on cyber resilience and views on information gathering and sharing

20 October 2020

Submission contact details

The Reserve Bank invites submissions on this Consultation Paper by 5pm on 29 January 2021. Please note the disclosure on the publication of submissions below.

Address submissions and enquiries to:

(E-mail)

cyberresilience@rbnz.govt.nz

(Hard copy)

Dynamic Policy Team

Financial System Policy and Analysis
Reserve Bank of New Zealand

PO Box 2498

Wellington 6140

Publication of submissions

All information in submissions will be made public unless you indicate you would like all or part of your submission to remain confidential. Respondents who would like part of their submission to remain confidential should provide both a confidential and public version of their submission. Apart from redactions of the information to be withheld (i.e. blacking out of text) the two versions should be identical. Respondents should ensure that redacted information is not able to be recovered electronically from the document (the redacted version will be published as received).

Respondents who request that all or part of their submission be treated as confidential should provide reasons why this information should be withheld if a request is made for it under the Official Information Act 1982 (OIA). These reasons should refer to section 105 of the Reserve Bank of New Zealand Act 1989, section 54 of the Non-Bank Deposit Takers Act, section 135 of the Insurance (Prudential) Supervision Act 2010 (as applicable); or the grounds for withholding information under the OIA. If an OIA request for redacted information is made the Reserve Bank will make its own assessment of what must be released taking into account the respondent's views.

The Reserve Bank may also publish an anonymised summary of the responses received in respect of this Consultation Paper.

Contents

Executive summary

Cyber risks are rising alongside an increasingly digital economy and the role for public bodies in promoting resilience is becoming clearer. In its *November 2019 Financial Stability Report*, the Reserve Bank outlined its intention to become more proactive in promoting cyber resilience in New Zealand's financial sector. Developing high-level risk management guidance and an information gathering and sharing plan were noted as likely areas of policy work.

The consultation document presents draft cyber risk management guidance which applies to all regulated entities of the Reserve Bank, including registered banks, licensed non-bank deposit takers, licensed insurers and designated financial market infrastructures.

The consultation paper also seeks feedback on the Reserve Bank's initial views on how information gathering and sharing can help build cyber resilience. In addition, the consultation document outlines a future area of policy work to establish protocols among public and private sector bodies to effectively share information and respond to cyber incidents when they do occur. A key overarching objective of the Reserve Bank's programme of work on cyber risk is to raise awareness on how to build resilience and set appropriate expectations on the industry.

Consultation is open for 14 weeks and closes on 29 January 2021. We will hold a workshop for the industry after publishing the consultation. Please advise of your interest to participate in the workshop.

Introduction

The cyber world has long been recognised as a significant source of operational risk for financial institutions. As cyber risk continues to rise alongside an increasingly digital economy, there is growing awareness that cyber incidents could present risks to the stability of the financial system as a whole. While a commonly agreed 'best practice' framework to address cyber risk has yet to emerge, the role for financial sector regulators has grown clearer in recent years as documented by the Bank for International Settlements.[1] Cyber risk management practices and information reporting requirements are now fairly common elements in the range of observed international practices. The need for a high degree of coordination among various public and private sector bodies is another key feature of international practices.

In February 2020, the Reserve Bank published a *Bulletin* article that estimates cyber incident costs for the New Zealand financial sector and discusses the importance of building resilience. The *Bulletin* article builds awareness that cyber risk is a growing concern in New Zealand and helps inform decisions around the management of these risks. In light of rising cyber risk and growing clarity on a suitable role for financial sector regulators, the Reserve Bank outlined its intention to become more proactive in promoting cyber resilience in New Zealand's financial sector in the *November 2019 Financial Stability Report*.

The core element of the Reserve Bank's approach to helping build the cyber resilience of the financial system is the development of cyber risk management guidance for all of its regulated entities. The guidance draws heavily from well-recognised international frameworks but is tailored to New Zealand circumstances. This tailoring includes a focus on high-level principles and makes an effort to minimise the use of highly technical terms. These types of adjustments reflect the fact that directors and senior management are the target audience for the risk management guidance. Raising awareness of the importance of cyber resilience and setting clear expectations on the industry are key objectives of the guidance.

The Reserve Bank cyber resilience framework includes two additional elements that build on the risk management guidance that we are now consulting on in this document. They are 1) information gathering and sharing, and 2) enhanced incident response coordination. This consultation paper presents our initial views on the scope of cyber information gathering and sharing, and seeks stakeholder feedback. We intend to then refine the information gathering and sharing concept and consult stakeholders with a more detailed proposal around the middle of next year.

There is already a fairly high degree of coordination among public bodies when responding to cyber incidents. The third element of our cyber framework – enhanced incident response coordination – is aimed at operationalising and getting the best value out of cyber information gathering and sharing by the Reserve Bank collaboratively with relevant public sector bodies. The work of building enhanced incident response coordination will progress alongside the development of information gathering and sharing plans.

[1] www.bis.org/bcbs/publ/d454.pdf.

The consultation paper is organised as follows:

- Part 1 outlines the basic rationale for regulatory interventions to help promote cyber resilience;
- Part 2 describes the Reserve Bank's policy approach relative to a range of international practices;
- Part 3 explains the design of the draft cyber risk management guidance that will apply to all regulated entities of the Reserve Bank; and
- Part 4 provides initial views on the scope of cyber information gathering and sharing.

1. Rationale for regulatory intervention

While regulated entities have a clear interest in maintaining cyber resilience, the nature of cyber risk has evolved to the point where there is now widespread acknowledgement that public bodies have a useful role to play alongside industry. Indeed, cyber resilience is increasingly recognised as having the properties of a public good like education, public health and national defence.[2,3] This indicates that private interests alone may tend to under-invest in cyber resilience and not achieve the outcomes that are desirable from a societal point of view. Importantly, this does not mean the public sector bodies will replace the efforts of private industry. Rather, close coordination between public and private sector bodies is called for at the national and international level to effectively build resilience and address the growing number of cyber threats. In New Zealand, the establishment of the National Cyber Security Centre (NCSC) and the Computer Emergency Response Team (CERT NZ) are good examples of the growing presence of public sector bodies joining the effort to build cyber resilience in New Zealand. The rest of this section describes some particular features of cyber resilience that contribute to the need for close coordination among public and private bodies.

Highly technical and rapidly changing information landscape

The cyber world is a complex technical creation that is constantly evolving and rapidly changing. Considerable specialist IT knowledge is typically needed to understand cyber risk and how to effectively build cyber resilience. This feature of the cyber world poses a significant challenge for the board and senior management of financial institutions, who typically have limited knowledge in the cybersecurity field.[4] This gap in knowledge at the decision-making level can hinder a firm's effectiveness in identifying and dealing with cyber risk.

Increasing reliance on third-party service providers (including cloud computing service providers) further compounds the gap in cyber knowledge between decision-makers and technical specialists.[5] Similarly, important external stakeholders of a firm, such as investors, customers and journalists, may also lack the necessary knowledge or expertise to understand cyber risks. This diminishes the important disciplining force that these stakeholders have on firms.

---

[2] B Coeure, " Cyber resilience as a global public good", speech, 10 May 2019

[3] The Cyber Incident Landscape, Nikil Chande and Dennis Yanchus, Bank of Canada (2019)

[4] Identifying How Firms Manage Cybersecurity Investment, Tyler Moore, Scott Dynes and Frederick Chang; *Economics of Information Security* (2016)

[5] Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018, Financial Conduct Authority (2018)

Difficulties in coordinating information sharing

Information sharing about cyber incidents and response coordination among private and public sector bodies are both crucial to minimising the impacts of incidents and promoting the resilience of the financial system. However, individual firms may be reluctant to voluntarily disclose cyber incidents in a timely fashion because they face adverse reputational costs if the incident becomes common knowledge before it has been remedied[6]. There are also high costs involved in establishing a trusted information sharing platform, which further demotivates information sharing.

Public sector bodies have a role to play in helping to fill information gaps and coordinating the efforts of multiple stakeholders towards building cyber resilience in New Zealand. The Reserve Bank's initiatives outlined in this paper are designed and calibrated to support the wider effort in building cyber resilience.

Range of international practice

Prudential regulators worldwide are increasingly making cyber resilience a top policy priority. A recent report by the Bank for International Settlements has usefully documented the range of practices used among prudential authorities to address cyber risk.[7] The range of observed practice includes elements like risk management guidance; legally-binding standards covering cyber resilience governance; enhanced supervision of cyber readiness; development of information gathering and sharing frameworks, and protocols for the management of cyber risks associated with third-party service providers. It is fairly common to see policy approaches becoming more proactive and more stringent over time.

At a high level, the range of international practices can be viewed as falling into the two broad categories of *risk management frameworks* and *information gathering and sharing arrangements.* In each category, the level of intervention by prudential authorities ranges from low, medium to high. Table 1 sets out this framing of the range of international practices for improving cyber resilience by prudential authorities.

Table 1. Spectrum of regulatory activities for improving cyber resilience

	Low activity	Moderate activity	High activity
Cyber risk management framework	Recommendations to use established international frameworks.	Publication of risk management guidance.	Legally binding requirements. Regulator-led penetration testing.
Information gathering & sharing arrangements	No role for prudential regulators. Rely on 3rd party information.	Prudential regulator partners with other public sector bodies.	Prudential regulator acts alone.

[6] Cyber risk, market failure, and financial stability, Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, IMF working paper (2017)

[7] www.bis.org/bcbs/publ/d454.pdf.

2. Reserve Bank policy stance

In considering its own role in promoting cyber resilience, the Reserve Bank has taken stock of the domestic landscape and the relevant international context as outlined in Table 1. The Reserve Bank recognises that there is a trade-off that needs to be made when choosing its policy settings. On one hand, taking a more active policy stance can be expected to improve cyber resilience; on the other hand, being more active is associated with resource costs and a potential increase in moral hazard risk. An important feature of the domestic landscape is that public sector bodies like NCSC and CERT NZ are centres of technical expertise but also have a system-wide focus, which means there is space for financial sector regulators to add value to the areas they regulate.

In November 2019, the Reserve Bank announced[8] an evolution in its policy thinking towards taking a more proactive approach in helping to build cyber resilience in the financial sector. When measured against the range of international practices, the Reserve Bank considers that taking a 'moderately active' policy stance is appropriate and represents a suitably balanced approach. The Reserve Bank's approach includes three elements which are interconnected and built on each other. They are: developing risk management guidance, establishing information gathering and sharing arrangements, and building enhanced incident response coordination protocols among public and private sector bodies. Figure 1 illustrates the three elements.

Figure 1 Reserve Bank's three steps to promoting cyber resilience

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?

Part 3 introduces the design of the risk management guidance and Part 4 discusses the Reserve Bank's views on information gathering and sharing. The third element of our cyber framework – enhanced incident response coordination – is aimed at operationalising and getting the best value out of cyber information gathering and sharing. The work of building enhanced incident response coordination will progress alongside the development of information gathering and sharing plans.

[8] See Financial Stability Report, November 2019 (RBNZ, Nov 2019)

3. Risk management guidance on cyber resilience

The risk management guidance on cyber resilience is designed to provide greater clarity for regulated entities around the regulatory expectations from the Reserve Bank on cyber resilience. The guidance is principle-based and draws heavily from leading international and national cybersecurity standards and guidelines. This broadly follows the approach that prudential regulators in other jurisdictions have taken when developing their cyber frameworks and avoids duplication or conflicting expectations, particularly where the Reserve Bank's regulated entities also have parent entities in other jurisdictions.

The international cyber resilience frameworks that we have drawn from are:

- CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (FMI);
- Guideline and standards published by National Institute of Standards and Technology; and
- ISO guidelines for cybersecurity.

We have also drawn from the approaches taken by prudential authorities in Australia, U.K., EU, Hong Kong and Singapore.

3.1 Structure and contents

There are four parts in the draft guidance: (1) governance, (2) capability building, (3) information sharing, and (4) third-party management. The preamble in front of each section elaborates on the importance of the relevant content and how it fits into the holistic cyber resilience framework. Good governance is the foundation of good cyber risk management; Capability building is structured around the five functions in the NIST Cybersecurity Framework (identify, protect, detect, respond and recover); Information sharing promotes a trusted environment that will benefit all entities, and; Third-party management is an area of growing importance and the guidance includes a special subsection on the use of cloud computing services in light of the rapid adoption of cloud services by financial sector firms.

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?

3.2 Granularity (level of detail)

Best practice recommendations are designed to be non-technical, principle-based and future-proofed. The guidance aims to strike a balance between being concise and sufficiently informative. The guidance is technology and methodology agnostic, which means the Reserve Bank does not favour any specific tools or methods regarding cyber risk management. Regulated entities are expected to improve cyber resilience by utilising a robust process suited to their situation and requirements. Entities that require more detailed guidance on specific aspects of cyber resilience should refer to the New Zealand Information Security Manual (NZISM) developed by the Government Communications Security Bureau (GCSB) and other well-recognised frameworks (e.g. those published by NIST).

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

3.3 Principle of proportionality and a risk-based approach

The principle of proportionality applies throughout the guidance and should be employed in a manner proportionate to the size, structure and operational environment of an entity, as well as the nature, scope, complexity, and riskiness of its products and services.

The guidance aims to provide the baseline level of cyber resilience recommendations for entities. However, where necessary, the guidance also provides recommendations for enhanced-level practices. This list of practices is not meant to be exhaustive. The intention is to illustrate current best practice and encourage continual improvement beyond these practices into all areas where entities can further strengthen their cyber resilience.

In most cases, the guidance does not specify the frequency of actions that an entity should take: for example, the recommended frequency for response plan testing or updating the cyber resilience strategy. Entities should choose the frequency according to their own tailor-made cyber resilience frameworks.

Regulated entities should assess their cyber risk tolerance, set their cyber risk appetite and ensure their cyber risk mitigation efforts are commensurate with the cyber risks they each face.

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

3.4 Scope

The guidance applies to all regulated entities of the Reserve Bank, including banks, non-bank deposit takers, insurance companies and financial market infrastructures.

Regulated entities should decide which level of recommendations of the guidance is relevant to them, according to the nature of their business and the products and services they provide.

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

3.5 Rationale for not having a prescriptive checklist

Regulated entities should not use this guidance as a checklist for cyber resilience minimum requirements. Instead, entities should design and develop their own cyber resilience frameworks that adequately address the specific cyber threats they face.

One of the shortcomings of a checklist approach is that it does not lend itself to thinking critically about the specific cyber risks faced by each entity. A uniform approach does not allow for flexibility to address the vulnerabilities unique to an entity, and may leave it exposed to threats. A checklist achieves compliance, but does not ensure risks are properly managed. This is because entities may only implement the bare minimum of requirements, as they check the required boxes, but fail to protect themselves further when they have been so explicitly advised of what is needed.

Conversely, a less prescriptive, principles-based guidance can encourage entities to adopt the most effective solutions to suit them and strengthen their cyber resilience, which is vital in staying on top of an ever-changing cyber risk environment.

4. Views on information gathering and sharing

The Reserve Bank regards information gathering and sharing on cyber resilience as a crucial element in its three-step approach to building cyber resilience in the financial system. This section discusses the purposes of information gathering and sharing, outlines our plans to take a collaborative approach with other public sector bodies, and provides a high-level overview of international practices.

4.1 Purposes

Information gathering and sharing are intended to serve several purposes:

a. Enable system risk monitoring and reporting;
b. Support risk management guidance and practices by establishing industry benchmarks;
c. Support incident response practices; and
d. Build cyber threat awareness among stakeholder community through information sharing.

The Reserve Bank recognises that certain cyber related information can be highly sensitive and is committed to ensuring that all appropriate controls are applied to sensitive information.

4.2 A collaborative approach

The Reserve Bank encourages participation in reliable domestic and international cyber information exchange forums but also recognises that there are limits to the effectiveness of existing forums. For instance, the voluntary nature of existing industry information sharing forums may not be ideal in all circumstances, such as when an entity chooses not to share its experience for fear of reputational loss or if it leads to smaller and more vulnerable entities being excluded from such networks.

Therefore, as a complement to these forums, the Reserve Bank sees value in developing a shared information resource for public sectors bodies that is comprehensive. In doing so, the Reserve Bank will aim to coordinate and collaborate (to the extent possible) with other public sector bodies with an interest in cyber resilience. Specifically:

- NCSC, which provides cyber incident response support to nationally significant organisations;
- CERT NZ, which works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents; and
- The Financial Markets Authority (FMA), as the national conduct regulator with a strong interest in promoting cyber resilience in the financial sector.

Consistent with its recent *Statement of Intent (2020-2023)*, the Reserve Bank will pursue enhanced collaboration with other public sector bodies on building cyber resilience through information gathering and sharing "in the best interest of all New Zealanders".

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

4.3 International practices

It is common practice for prudential authorities in other jurisdictions to collect two broad types of information: cyber resilience capabilities and cyber incidents.

Information on cyber resilience capabilities is generally collected through periodic surveys and typically includes financial institutions' practices in fields that are relevant to building cyber resilience (e.g. governance, contingency plans, etc.). It may also include some quantitative information about the resources (staff and financial inputs) regulated entities have placed towards cyber resilience.

In many jurisdictions, but not all, it is mandatory for financial institutions to report cyber incidents to regulators. Sharing information on cyber incidents involves more consideration on protecting the privacy of affected entities and is often anonymous or in an aggregated format.

The incident reporting frameworks adopted in different countries range from formal communication (following a pre-set template) to informal communication. Incident reporting also involves the requirement of a reporting time frame and pre-defined threshold that triggers reporting on a "significant" or "material" cyber incident.

4.4 Reserve Bank's view on establishing cyber data collection

The Reserve Bank considers that there are merits in following the broad pattern observed in the international practices of establishing a cyber data collection. At a very high level, this includes:

- A regular but fairly infrequent data collection (perhaps annually or once every few years) on cyber capabilities and resources dedicated to building cyber resilience;
- Establishing an obligation to report cyber incidents to the prudential authority, perhaps with a materiality threshold for reporting incidents as soon as reasonable after they are detected.
- An information collection plan that is applicable to all regulated entities of the Reserve Bank.

In progressing our work to develop an information gathering and sharing plan, the Reserve Bank will be working closer with other public bodies to maximise the value and to minimise the reporting burden. As a principle, the Reserve Bank will tailor reporting requirements to ensure they stay relevant and minimise the reporting burden.

There are certainly many details that will need to be worked through. We welcome feedback on this high-level plan.

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?

5. Next steps

Submissions are welcome by 29 January 2021. We will publish a submissions and a summary of submissions and final guidance in March/April 2021.

We are developing a detailed framework for information gathering and sharing, and will consult stakeholders in the middle of 2021.