RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

The Reserve Bank, cyber security and the regulatory framework

A speech delivered to the Future of Financial Services (10th annual) conference in Auckland

On 19 July 2017

By Toby Fiennes, Head of Prudential Supervision

2 The Terrace, PO Box 2498, Wellington 6140, New Zealand
Telephone 64 4 472 2029 Online at www.rbnz.govt.nz

"Better be despised for too anxious apprehensions, than ruined by too confident security."
- Edmund Burke

Introduction

Concern about cyber risks is everywhere. Pick up a newspaper or read a news site and the chances are there'll be a prominent item on cyber risks. It is frequently a topic raised with us by CEOs of firms we regulate. But how worried are we, as a financial sector regulator, and what can and should we do about it? Is the greater risk being "over anxious" or "too confident"?

Today I will share with you the Reserve Bank's observations on the cyber security landscape, our response to the emerging risks, and what this all means for the institutions that we regulate and supervise – these institutions being banks, non-bank deposit takers (NBDTs) insurers and Financial Market Infrastructures (FMIs).[1] "Is cyber risk a unique risk and does it require a change in mind-set?"

The answer to this question is likely to shape how we approach cyber risks and try to ensure that entities we regulate manage the risks appropriately. Financial technology, or 'fintech', and the concept of 'digital disruption', will also affect our supervision of financial institutions, and I will share our perspective on the risks and opportunities.

The traditional focus of prudential supervision

Prudential regulations require financial firms to adequately identify, measure, and control the risks they face – that is, to be more prudent. Historically, prudential regulators have looked at risks through what can be called a balance sheet lens. The risks that received most attention were those of a more quantifiable nature – credit risk, liquidity risk, and market risk. Credit risk is the potential that a borrower or counterparty will fail to meet its obligations in accordance with agreed terms. Liquidity risk is the risk that a financial institution cannot meet its short term financial demands. This usually occurs because the financial institution cannot convert an asset into cash without taking a large haircut (loss) on the asset's value. Market risk is defined as the potential for losses arising from movements in market prices. These risks and their mitigants can be priced and reported on balance sheets.

Operational risk is different. Until finally more broadly defined by the Basel Committee for Banking Supervision in the early 2000s, operational risk was a term mostly used as a catch-all for the 'residual' or unquantifiable risk facing a financial institution – that is, any risk that could not be categorised as credit, liquidity or market risk and therefore captured by line items on a balance sheet.

[1] NBDTSs include building societies, credit unions and other deposit-taking finance companies.

FMIs provide channels through which payments, securities, derivatives or other financial transactions are cleared, settled or recorded. An example of an FMI is the Reserve Bank Exchange Settlement Account System (ESAS) which along with Real-Time Gross Settlement (RTGS) allows individual transactions between financial institutions to be settled as the transactions happen.

The Basel framework[2] explicitly includes operational risks in minimum capital requirements, along with credit and market risks.[3] The Basel Committee defined operational risk as:

> *"The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk"* [4]

This definition of operational risk captures cyber risk, though it does not yet have a specific, globally accepted definition. When one does emerge, it is likely to be similar to that adopted by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) in their 2015 guidance on cyber resilience for Financial Market Infrastructures:

> *"The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for the organisation"* [5]

The rising risk of cyber attack

It almost goes without saying, particularly to a forum like this, that cyber-attack poses a significant threat to the global financial system and broader real economy. In recent years, there has been a steady increase in cybercrime around the world, with various surveys of private and public industry participants showing attacks are now an everyday occurrence, as indeed are media stories about the phenomenon.[6]

The 'WannaCry' ransom ware attack that is estimated to have affected over 200,000 systems around the world – including systems at Britain's National Health Service, is still

---

[2] Basel Committee on Banking Supervision (2011), 'Basel III: A global regulatory framework for more resilient banks and banking systems', Bank for International Settlements, Basel, http://www.bis.org/publ/bcbs189.pdf, accessed 4 July 2017.

[3] The Basel framework's 'Pillar one' refers to requirements, imposed by prudential regulators, on banks to hold minimum levels of capital against credit, market, and operational risk. In contrast, pillars two and three include requirements for sound risk management and supervision at banks, and disclosure requirements respectively.

[4] Basel Committee on Banking Supervision (2003), 'Sound Practices for the Management and Supervision of Operational Risk', Bank for International Settlements, Basel, http://www.bis.org/publ/bcbs96.pdf, accessed 4 July 2017.

[5] Committee on Payments and Market Infrastructures and Board of International Organization of Securities Commissions (2016), 'Guidance on cyber resilience for financial market infrastructures', Bank for International Settlements and International Organization of Securities Commissions, http://www.bis.org/cpmi/publ/d146.pdf, accessed 26 June 2017.

[6] Recent examples of such surveys include: PricewaterhouseCooper's annual Global State of Information Security Survey; the Australian Prudential Regulation Authority's (APRA's) Information paper on their 2015/2016 Cyber (available here: http://www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Cyber-Security-2016-v4.pdf); and the UK government's 2017 cyber security breaches survey (available here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf). Three-in-ten of firms in the UK survey reported having a breach or cyber-attack within the last twelve months. Just over half of the twenty firms regulated by APRA and surveyed had experienced a cyber-incident within the last twelve months.

vivid in many of our minds.[7] And WannaCry has already been succeeded by more sophisticated forms of ransom ware such as 'notpetya' – although these attacks appear to have been less disruptive.[8] Looking back to just last year, the robbery cyber-heist of the Central Bank of Bangladesh by hackers shows that even central banks and international payment systems can be vulnerable. Nearly USD81 million remains unaccounted for after this attack and, if it had not been for a few spelling errors which caught the eye of officials, the amount stolen could have been closer to USD1 billion.[9]

The World Economic Forum's 2017 Global Risks report lists a "Massive incident of data fraud/theft" as a top five global risk in terms of likelihood for 2017, alongside large-scale terrorist attacks and major natural disasters. [10] This report also notes that cyber-attacks were first identified as a top-five global risk in terms of likelihood in 2012, and then again in 2014. [11]

Scope of the Reserve Bank's responsibility

The Reserve Bank of New Zealand is here to promote the soundness and efficiency of the New Zealand financial system and the insurance sector. Unlike many other prudential regulators around the world, we chiefly have a systemic focus, rather than a focus on customers or individual institutions. Certainly, we have powers for ensuring that individual firms are carrying on their business in a prudent manner, but we use these powers to promote the safety and soundness of the system as a whole: we do not pursue a zero failure regime. We would allow a regulated entity to fail under circumstances where the negative impacts on the rest of the New Zealand financial system were limited. This stance helps support accurate pricing of bank deposits, wholesale funding and equity by market participants, because there is incentive for them to accurately price-in the risk of a financial institution's default. This in turn supports efficiency of the financial system (as investment decisions will be based on less distorted fundamentals) and encourages financial institutions to take actions which reduce their risks.

---

[7] Schwartz M (16 June 2017), 'British Security Services tie North Korea to WannaCry', Bankinfo Security, http://www.bankinfosecurity.com/british-security-services-tie-north-korea-to-wannacry-a-10005, accessed 26 June 2017.
[8] Schwartz M (3 July 2017), 'Ransomware Smackdown: NotPetya Not as Bad as WannaCry', Bankinfo Security,http://www.bankinfosecurity.com/ransomware-smackdown-notpetya-as-bad-as-wannacry-a-10077,accessed 4 July 2017.
[9] Quadir Serajul (11 March 2016), 'Spelling mistake stops hackers stealing $1 billion in Bangladesh bank heist', The Independent, http://www.independent.co.uk/news/world/asia/spelling-mistake-stops-hackers-stealing-1-billion-in-bangladesh-bank-heist-a6924971.html, Bankinfo Security, accessed 26 June 2017.
[10] World Economic Forum (2017), 'The Global Risks Report 2017', http://www3.weforum.org/docs/GRR17_Report_web.pdf, World Economic Forum, Geneva, accessed June 26 2017.
[11] Ibid.

Applying this approach to cyber means that our focus is on mitigating the systemic risks. The risks include:

- a cyber-attack on one or more banks, NBDTs, FMIs or insurers that leads to a broad loss of confidence in the financial sector;
- an attack on one or more firms or FMIs that disrupts their provision of critical banking and financial services and economic functions; and
- an attack that leads to the outright failure of a large, systemically important financial firm or FMI that would have wider, systemic impacts.

Consumer protection and guarding against isolated incidences of cyber-attacks that affect banks' profits or leave them open to legal risk around breach of data privacy are not a direct responsibility of the Reserve Bank. Our role is clearly separated from those of other agencies involved in New Zealand Cyber Security Strategy, such as the recently launched Computer Emergency Response Team (CERT NZ) that supports business and individuals against cyber-attacks[12] [13]. Nonetheless, the New Zealand Cyber Security Strategy does link into the Reserve Bank's financial stability objective by building overall system resilience, so we have been engaging with other agencies on this.

A cyber-attack on an insurer is less likely to affect the functioning of the broader financial market than an attack on a bank, but we have a statutory objective of promoting confidence in the insurance sector and an attack that caused large-scale loss or theft of policyholders' data could undermine confidence. For non-bank deposit takers (NBDTs) the risks posed to the financial system from possible cyber-attack are similar in nature to those faced by banks. Given the smaller size of the sector, our response is proportionally smaller. However, smaller firms with less internal IT expertise may be more susceptible to cyber-attack and the impact of a cyber-attack could still be transmitted through the New Zealand financial system.

Cabinet has recently agreed that a Bill will go to Parliament that would provide for a comprehensive prudential and market conduct regulatory framework for FMIs.[14] The proposed legislation would give the Reserve Bank and the Financial Market Authority (FMA) powers to set regulations on how a range of prescribed risks are managed by FMIs. Cyber risk, as a type of operational risk, will be captured here.

[12] http://www.dpmc.govt.nz/dpmc/publications/nzcss
[13] https://www.cert.govt.nz/
[14] http://www.rbnz.govt.nz/news/2017/05/enhanced-oversight-framework-for--financial-market-infrastructures

The Reserve Bank's response to the risk of cyber-attacks

There are two avenues which already allow us to respond to the threat of cyber-attack on the institutions we regulate.

1. Supervised institutions are expected to manage operational risks — and cyber is covered indirectly in high level management, disclosure and attestation requirements as well as business continuity planning. IT and cyber security risks are implicit in our existing regulatory framework. Cyber risk planning is incorporated into supervisors' regular engagement with regulated firms on prudential matters. This engagement mostly focuses on firms' high level strategy to manage information technology and security threats. For example, they inform us about the types of attacks they might be experiencing and we explore their broader situational awareness (i.e. are they keeping up with cyber trends nationally and globally), and the processes they have in place for preventing, detecting, and responding to threats. This last point includes whether they have incident response plans in place, whether cyber threat is part of their business continuity planning, and the resilience of arrangements with critical third-party service providers like communications and IT suppliers and – for example, "Are requirements in place for the security arrangements and incident response plans of these third party providers?".

   As has been noted by many experts in this area, the nature and incidence of cyber risk is unique, meaning that typical approaches to risk management and disaster recovery planning may not be appropriate. Anyone in the organisation with a computer and access to the network is a possible point of entry for cyber-attack. No matter how robust an IT department's controls, if there isn't a strong culture of cyber awareness across the whole of the organisation then vulnerabilities will remain at every potential point of entry. With cyber 'you are only as strong as your weakest link'. Furthermore, while vulnerabilities can be mitigated, they can never be eliminated: the potential sources of cyber threats and the attack footprint are just too broad. So, in the event that a risk crystallises and an attack is successful, it is essential to have rapid and effective response and recovery capabilities. Particularly, because unlike other operational risks which might hit haphazardly, cyber-crime is intelligent, motivated and focused.

2. Our Capital Adequacy Framework (BS2A/2B) is designed to ensure banks are adequately capitalised against the risks they face, including cyber risk. Banks that face greater operational risk, including higher risk of cyber-attack (or where the impact of an attack is greater, including because of weak operational resilience planning) should have higher capital requirements. However, in practice cyber risks are hard to quantify. It is difficult and expensive to generate a complete map of cyber weaknesses, and even more challenging to keep it up-to-date in a rapidly changing environment. Banks may underestimate the amount of capital they need to hold against cyber risk. There is a more general point too: that for cyber risk, and similar types of operational risk, capital may not be an effective mitigant. It can absorb final losses but it cannot solve the presenting technology problem.

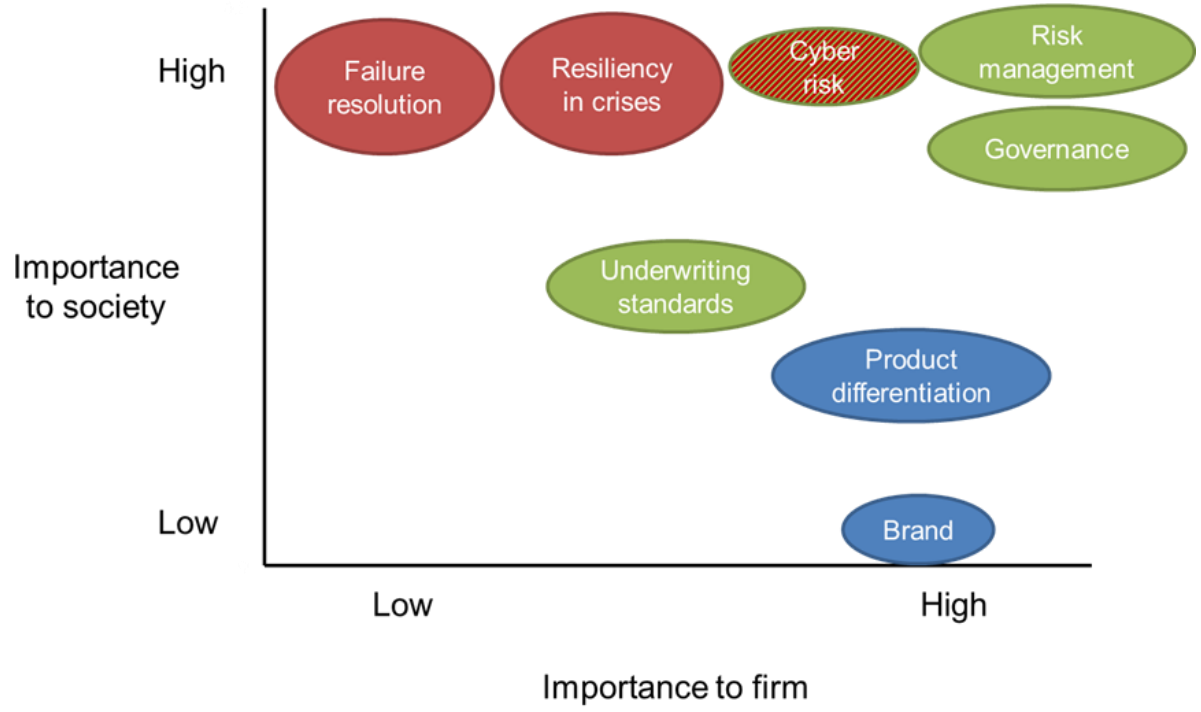
So the Reserve Bank needs other ways to think about the challenge.

Last year, we considered whether to introduce more prescriptive requirements related to cyber security. We know that firms have strong reputational and financial incentives to address the cyber risks they face, but they may not consider the wider systemic effects of cyber-attacks. That is our job.

It is also difficult for market participants to judge whether a financial institution's own cyber risk management strategies are effective and therefore ensure that the institution's debt and equity products are properly priced. Compared to, say, credit or market risk faced by a bank it is much harder to gauge a bank's cyber risks from its disclosure statements.

We at the Reserve Bank are not the technical cyber experts. Given our systemically-focused objectives, the existence of industry guidelines and our consideration that public and private incentives are relatively well aligned (see figure 1), to date we have not imposed prescriptive cyber security regulations on the financial sector. We doubt that doing so now would appreciably improve the outcome, when both the technology and threat landscape is changing so rapidly. We will, however, review this policy stance from time-to-time to ensure that it remains appropriate.

Figure 1[15]



The dynamic cyber environment means organisations have to be nimble in their approach to cyber security - focused on outcomes, rather than prescriptive compliance exercises. They need to be always abreast of their internal vulnerabilities and the external threat environment, and stay up to date with ways to protect and manage these. This is where

[15] For a full explanation of the Reserve Bank's supervisory approach and figure one please refer to: Fiennes T (2016), 'New Zealand's evolving approach to prudential supervision', speech to the New Zealand Bankers' Association, Auckland, http://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Speeches/2016/NZs-evolving-approach-to-prudential-supervision.pdf, accessed 17 July 2017.

international standards and best practice guidance can help financial firms to develop appropriate cyber-risk management frameworks. There are certainly many players in both the private and public sector who have the resources and expertise to provide up to date guidance on cyber, and I specifically note here the usefulness of the recent guidance from CPMI on cyber resilience for FMIs. It provides principles-based, supplemental guidance to the internationally recognised standards contained in the Principles for Financial Market Infrastructures (PFMIs), which broadly form the basis of the Reserve Bank's approach to FMI oversight.[16] I think most industry participants would acknowledge that some of the CPMI's cyber resilience standards are aspirational at the moment, but it is nonetheless a useful standard to work towards. No similar globally accepted set of standards exists for the banking or insurance sectors but there are a myriad of industry self-assessments and best practice guidance available.

The US National Institute of Standards and Technology's (NIST) Cyber Security framework is a widely recognised and respected approach for organisations to assess and improve their ability to prevent, detect and respond to cyber-attacks.[17] The UK's CBEST framework is another approach to cyber threat modelling that has become a de facto industry standard, helping organisations identify the objectives, capabilities, and approach of cyber threats.[18] On an international level, the International Organisation for Standardisation publishes guidelines for internet and cyber-security best practice.[19] Closer to home, the Australian Signals Directorate's Top 4 and Essential 8 set out risk mitigants that are easy to understand and apply across the whole of an organisation.[20] In New Zealand, the Government Communications Security Bureau's Information Security Manual (NZISM) and the Protective Securities Requirements (PSR) - while targeted at government organisations and publicly accessible information systems, offer some valuable guidelines for cyber security best practice for all organisations.[21] [22]

The Reserve Bank expects the entities it regulates to draw on guidance like this to develop cyber resilience practices that are appropriate for their business models and robust to the risks that they face. Obviously, there is no 'one size fits all' guide out there: firms will have to consider what parts of the various guidance materials are most appropriate. We encourage this approach in our regular bilateral engagement with regulated entities, as well by supporting forums for cooperation and coordination across the industry. Working together to build compatible resilience frameworks, rather than in isolation, will help promote the soundness and efficiency of the overall system.

Coordination across industry is also important in terms of keeping on top of the threat environment. It is crucial that firms share information about the threats they have identified, or attacks they have been subject to. Despite the tension around sharing commercially sensitive information, it is important that industry approaches cyber risks in the spirit of

---

[16] Committee on Payments and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, (2012) 'Principles for financial market infrastructures', Bank for International Settlements and International Organisation of Securities Commissions, http://www.bis.org/cpmi/publ/d101a.pdf, accessed 26 June 2017.
[17] See https://www.nist.gov/cyberframework
[18] See http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
[19] For example, see https://www.iso.org/isoiec-27001-information-security.html
[20] See https://www.asd.gov.au/publications/protect/top_4_mitigations.htm and https://asd.gov.au/publications/protect/essential-eight-explained.htm
[21] See https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/
[22] See https://www.protectivesecurity.govt.nz/

collaboration rather than competition. The Reserve Bank is aware of some such collaboration already taking place but encourages greater inclusion where possible.

In addition to the expectations that we place on firms, the Reserve Bank, as the owner and operator of payments systems and participant in the financial system more generally is also taking its own cyber-risks seriously. Protection from cyber security attacks is a high priority for the Reserve Bank. We have a programme underway to improve the capability and maturity of our security practices. It includes a cyber-resilience self-assessment and review of the Bank's key information assets, critical functions, threat exposures, vulnerabilities and appropriate mitigants. This process is drawing on some of the best practice guidance I mentioned earlier: the PSR's 'maturity assessment', which we adopted as a reference for our current and desired level of maturity; the GCSB's NZISM and the SWIFT Customer Security Programme.[23] The Reserve Bank's senior management team is highly engaged, right up to the level of the Governor and his deputies - where ownership of the project lies. Once completed, it will allow us to better track our cyber risk exposures and consider appropriate mitigations.

Observations on fintech

I would like to take the opportunity to share some thoughts on the related area of "fintech", which is expected to have a significant impact on financial markets and how firms provide financial services.[24] A recent paper by the Committee on the Global Financial System (CGFS) and Financial Stability Board highlights that financial risk in fintech platforms may be higher than at banks due to greater exposure to digital processes.[25] Some new fintech platforms rely on investor confidence for new business, so are particularly vulnerable to a significant operational risk event, including cyber-attack that may result in a loss of investor confidence.

The Reserve Bank is closely watching the emerging wave of 'digital disruption' affecting the banking sector, as banks and other firms outside the traditional banking sector react to customer demand for a more digital banking experience. Non-bank 'digital disruptors' include peer-to-peer lending services; electronic wallets; and block-chain related technology such as crypto-currencies and distributed ledgers[26]. Another emerging trend is that of 'open-banking' - where third-party providers use a bank customer's data to offer them additional services such as the ability to view accounts with multiple banks in once place, or track spending across different categories of goods and services to create budgeting advice.

An important question for us here at the Reserve Bank is: How will fintech change the traditional role that banks and existing payment systems play in the economy? Our interest is in the impact this might have on the New Zealand financial sector and the economy more

[23] See https://www.swift.com/myswift/customer-security-programme-csp
[24] Committee on the Global Financial System and Financial Stability Board (2017), 'Fintech Credit', Bank for International Settlements and Financial Stability Board, http://www.bis.org/publ/cgfs_fsb1.pdf, accessed 26 June 2017.
[25] Ibid.
[26] A distributed ledger can be described as a ledger of transactions or contracts that is not maintained centrally by a single entity. Instead, it is maintained across multiple persons and or locations. Distributed ledgers may be less prone to fraud or cyber-attack as fraudulent changes need to be made to multiple copies of the ledger simultaneously to be successful. Block-chain refers to a specific form of the public distributed ledger first used by bitcoin.

broadly, and the implications for monetary and financial policy – notably the soundness and efficiency of the New Zealand financial system. Historically, banks have been the intermediaries between depositors and borrowers and provided payment services. In fulfilling these roles, banks provide security and convenience to depositors and access to credit for borrowers. The banking system also has established roles in the creation of money, providing physical notes and coins to the public, and in the transmission of monetary policy.

A recent Reserve Bank *Bulletin* article found that digital disruption is currently focused on 'customer-facing' banking services rather than the back-end, but it also could result in more fundamental changes to the banking system. Profit concerns are motivating banks to respond in order to remain competitive.[27] Notable examples of this strategy include pursuing mobile banking strategies, and building partnerships with disruptors. However, a fundamental barrier for many banks is the current state of their core systems. Many banks, both globally and in New Zealand, are faced with dated, sprawling and complex technology systems, although so far banks in New Zealand and Australia appear to be active in modernising their systems in response to digital disruption.

In the short term, digital disruption may result in new risks and increased instability in the financial system. For example, peer-to-peer lenders do not take on credit risk in the same manner as a bank, but they do undertake decisions on behalf of lenders and so may introduce different operational risks to the borrowing and lending process. Likewise, payments innovations may introduce new operational risks to the payments system. Other risks include the potential for fintech credit to be pro-cyclical (relative to traditional bank lending); a loss in investor confidence during times of stress may be more likely, leading to a pullback in the availability of credit. That said, innovations like 'regtech' — the use of technology to help providers meet their compliance obligations — may have the potential to enhance soundness in both the short and long term.

In the long term, digital disruption of the banking sector may improve the efficiency of the financial system. For example, new payments providers increase the speed and ease of initiating payments for consumers, and the application of new technologies (such as block-chain) could increase the speed and reduce the cost of making cross-border payments. In addition, peer-to-peer platforms may carry lower overheads and so reduce the cost of matching borrowers with lenders.

The long-term impact of digital disruption on financial system soundness is less clear. Soundness may be reduced if existing banks' profitability buffers are reduced due to increased competition from digital disruptors. The FSB has noted, among other potential negative impacts, the possibility of an 'unbundling' of bank business lines by specialised fintech credit platforms which could erode banks' revenue bases, making them more vulnerable to losses.[28] However, digital disruption may also improve financial system soundness if it results in a greater diversity of competitors and fewer systemically important banking entities. This may reduce the impact of a single entity failure. Further, this may alleviate the 'too-big-to-fail' risk where authorities may feel pressured to prevent large banks

[27] Watson A (2016),'Disruption of distraction? How digitisation is changing New Zealand banks and core banking systems' *Reserve Bank of New Zealand Bulletin*79(8) , http://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2016/2016may79-8.pdf, accessed 26 June 2017.
[28] Committee on the Global Financial System and Financial Stability Board, (2017), 'Fintech Credit', Bank for International Settlements and Financial Stability Board, http://www.bis.org/publ/cgfs_fsb1.pdf, accessed 26 June 2017.

from failing due to systemic concerns. This would, in turn, reduce the probability of banking entities taking on risks that they are not willing to bear. The FSB refers to this potential benefit of fintech credit as a 'spare tire' for the economy in situations where problems are idiosyncratic to banks.[29]

In New Zealand, fintechs engaging in lending practices are subject to regulation by the FMA and Commerce Commission. Disruptors that participate in or provide a payment system in New Zealand are subject to the Reserve Bank's information gathering powers. Under the proposed new legislation for FMIs, any disruptor in the payments space that grows enough to be considered systemic would be subject to prudential and market conduct regulation jointly by the Reserve Bank and FMA. Other fintechs may fall outside the current regulatory perimeter. Looking forward, The Reserve Bank and other regulators will need to make sure the regulatory regime in New Zealand is adaptive should any new business models become systemic, while not unduly harming innovation.

Therefore, we are working with other agencies, such as the FMA and Ministry of Business, Innovation and Employment (MBIE), to ensure that New Zealand presents an environment where new digital innovations can flourish, provided they are done safely. In our view, New Zealand's financial market regulatory settings support innovation and industry-based solutions and we see no need to actively steer potential solutions from industry by providing a concessionary environment for new entrants (a "sandbox").[30] Some other jurisdictions have prudential regulators with a greater focus on individual firms. Our system-level focus means that entrants such as digital financial service providers that are not yet large enough to be considered systemic are not subject to particularly strict regulatory requirements by the Reserve Bank.

Conclusion

At the start, I posed the question —'Is cyber risk a unique risk and does it require a change in mind-set?' The answer, I think, is a guarded no.

The risks are certainly new and the potential impact on the whole financial system is enormous. And these are not the sort of risks that are amenable to quantification and modelling techniques.

Although we are not well placed to add technical expertise, as the prudential regulator, we can explore whether financial institutions appear to be taking cyber risks seriously and we collaborate where possible. We look to self-discipline and market discipline to provide the defences, agility and crisis preparedness that are required. As elsewhere, strong risk governance remains key. Put another way, human behaviour remains the weak link.

Fintech poses some similar challenges in that it is rapidly evolving and regulators and other authorities need to work together; we need to permit valuable innovations to flourish, and also to be alert to systemic risks emerging.

[29] Ibid.

[30] For example, Chartered Accountants Australia and New Zealand rated New Zealand as a 'fintech friendly regime'. See: Chartered Accountants Australia and New Zealand (2017), 'The Regulator of 2030: Regulating our digital future'.

In the final analysis, there is no simple silver bullet. Firms, regulators, and other authorities all need to play a part and remain alert to emerging risks and opportunities. As Edmund Burke said “No man made a greater mistake than he who did nothing because he could do only a little.”