Box C

Building Resilience to Cyber Risks

Cyber incidents can have systemic implications

Cyber risk is the potential for the disruption or destruction of information technology (IT) systems that results in the interruption of businesses and financial loss. In the case of banks, such incidents could lead to financial distress within an institution and have flow-on effects to its lending and deposit-taking business, with implications for the wider economy. This disruption could be due to an error or a malicious cyber-attack. It could affect a financial institution's IT operations directly or indirectly through a third party, such as a software service provider. Cyber risk resembles other operational risks, but is particularly challenging for institutions and regulators because it is difficult to identify, constantly evolving, borderless and often started by malicious actors.

While cyber incidents have, so far, mostly been contained within an institution, a key concern of authorities is that a significant incident could be broad in impact and affect the functioning of a large part of the financial system.[1] An incident is systemic if it disrupts or disables critical functions of the financial system, such that it cannot operate effectively.[2] Cyber-attacks are more likely than other types of incidents to be systemic: a well-resourced and sophisticated adversary seeking to cause widespread distress will actively exploit cyber vulnerabilities to maximise the impact of their attack (including by affecting multiple institutions). Cyber-attackers could be motivated by financial gain or a desire to disrupt – the latter is more concerning because it is harder to defend against such attacks. Incidents that reduce the integrity or availability of IT systems or data could have systemic implications. Cyber incidents that impair the confidentiality of IT systems seem less likely to cause systemic stress, but they could lead to severe reputational damage for the institutions affected.[3]

Whether a cyber incident could become systemic is often characterised by three transmission channels summarised in Table C.1: confidence; interconnectedness; and lack of substitutability.[4] An incident could propagate through one or more of these channels, and through the financial system or broader IT systems.[5]

The risk of a major incident occurring has increased …

Cyber-attacks have become more frequent and sophisticated. Publicly available data are incomplete, but the number of known cyber incidents globally has tripled over the past decade and various reports suggest that the number of serious cyber-attacks has been trending higher.[6] In Australia, there has been an increase in the number and severity of cybersecurity incidents of late; around 55 per cent of reported data breaches of Australian financial institutions over the past two years have been malicious.[7]

The financial system has become more exposed to cyber risk over time because of a number of factors. The importance of digital platforms and service channels has increased, and innovation in these technologies continues at a rapid pace. Often, this further

Table C1: Cyber Risk Transmission Channels

	Confidence	Interconnectedness	Lack of substitutability
Description	A loss of confidence could cause market participants to be reluctant to transact and seek to reduce their exposures to others, thus spreading the impact to other participants. Confidence is likely to erode more the longer an incident lasts.	The links within the financial system and/or between IT systems could expose them to a common vulnerability or rapidly transmit the impact of a cyber incident from one institution to another.	The unavailability of critical infrastructure or a key institution could mean that market participants are unable to, or have sufficient difficulty in being able to, switch to an alternative provider.
IT example	Concern that key infrastructure will not be able to recover (e.g. payments system), that funds or transactions will be lost, or that other institutions have similar vulnerabilities.	Direct attack that spreads via IT links between institutions (e.g. supply chain attacks that make use of malware, phishing or ransomware).	Disruption at a key third-party service provider (e.g. cloud services).
Financial example		Disruption to liquidity/solvency of large institutions resulting in financial spillovers (e.g. loss of data integrity of account balances at a key institution).	Disruption at a financial market infrastructure (e.g. payment or settlement systems).

increases the complexity and interconnectedness of these systems, as well as potential vulnerabilities (such as from legacy systems). Although the Australian Prudential Regulation Authority (APRA) directly supervises around 680 financial institutions, the financial system has around 17,000 interconnected entities, including third-party service providers.[8] Further, many key IT services such as cloud computing and storage are provided by a small number of providers, and while their scale can help to bolster their IT security, it also contributes to a lack of substitutability and has the potential to connect financial institutions to a common vulnerability.[9] In addition, the shift to working-from-home during the COVID-19 pandemic has created potential vulnerabilities as organisations further open their systems to computers outside their networks. At the same time as these exposures have been increasing, the knowledge and skills required to conduct a cyber-attack have become more accessible and the tools available to malicious attackers have become more sophisticated.[10]

There have been a number of high-profile incidents in recent years:

- Recently, the financial sectors of Ukraine and Taiwan have been disrupted by significant cyber-attacks; liaison indicates that Russia's invasion of Ukraine has further increased the perceived risk of a sophisticated attack.
- From 2019 to 2021, the Solarwinds, Microsoft Exchange and log4j incidents allowed attackers to potentially access hundreds of thousands of IT systems.[11]
- In 2020, the New Zealand stock exchange suffered a distributed denial-of-service attack that resulted in a trading halt for a number of days.[12]

- In early 2021, a data breach involving a legacy file-sharing service run by Accellion (a third-party technology provider) affected a wide range of entities, including the Australian Securities and Investments Commission and the Reserve Bank of New Zealand.[13]
- The Australian Federal Parliament has faced multiple cyber disruptions in recent years, including in a malicious intrusion by a 'sophisticated state actor' in 2019.[14]
- In 2020, Service NSW experienced a cyber-attack that resulted in the theft of the personal information of 100,000 people.[15]
- In mid-2021, an outage at a web services provider resulted in a temporary outage for the websites of three major Australian banks and the Reserve Bank of Australia.[16]

The direct costs of cyber incidents are difficult to establish but they can be significant. The average annual cost of cybercrime to firms in the banking and insurance industries in 2018 was estimated to be US$18 million and US$16 million, respectively.[17] One estimate put the average annual expected loss for cyber incidents in New Zealand's banking and insurance industries at 2–3 per cent of net profits per year and found that there was a 5 per cent chance that costs could exceed 25 per cent of net profits.[18] These costs also refer to publicly known incidents, which have been contained. By their nature, costs associated with a potential systemic cyber incident are likely to be much higher. Unsurprisingly, research has found that firms which invest in IT skills and incorporate cyber resilience into their business practices generally experience smaller losses from cyber incidents.

… but ongoing actions aim to bolster the resiliency of the financial system

To date, the financial sector has demonstrated greater resilience to cyber-attacks than other sectors.[19] In recent years, the financial system has significantly improved its cyber defences, in part by developing compliance frameworks, as well as regulators and institutions devoting more resources to cybersecurity. Having established this foundation, financial institutions and regulators are increasingly focusing on cyber resilience – that is, the ability of an institution to anticipate and adapt to cyber threats and to withstand, contain and rapidly recover from a cyber incident.[20]

Institutional resilience

Banks have increased their investment in managing cyber risk, including by establishing crisis management teams to respond to cyber-attacks and engaging in simulation exercises to test and improve their ability to identify, respond to and recover from attacks.

In Australia, the agencies that comprise the Council of Financial Regulators (CFR) continue to support financial institutions' efforts to strengthen cyber resilience.[21] The CFR agencies have developed a domestic cyber-attack protocol so as to better coordinate their efforts during a significant threat or attack affecting one or many regulated entities.

The CFR recently completed its Cyber Operational Resilience Intelligence-led Exercises (CORIE) pilot program to test and demonstrate the cyber maturity and resilience of institutions within the Australian financial services industry.[22] The CORIE framework was used to help prepare and

execute cyber resilience exercises, and utilised intelligence gathered on institutions to simulate targeted attacks. These exercises mimicked the tactics, techniques and procedures of real-life adversaries, using tools and techniques that may not have been anticipated and planned for. They measured the ability of an institution to detect, respond to and recover from the operations of a real adversary. While many financial institutions already carry out simulated cyber-attacks against their own infrastructure, CORIE brings a fresh perspective, enabling cyber resilience to be benchmarked across institutions. The attacks were also performed on live production systems and targeted institutions' staff. This ensured the attacks reflected real-world conditions as closely as possible.

The CORIE pilot identified common strengths among the participating institutions, as well as weaknesses that could present a risk to the integrity and stability of Australian financial institutions. It also provided data and reports to help Australian regulators and financial institutions to identify actions needed to uplift their cyber resilience. The CFR has endorsed further enhancing the CORIE framework, its use as an ongoing assessment tool and a rollout of the testing program to other financial institutions over the coming years.

As the primary regulator for banks, insurance companies and superannuation funds, APRA has taken a number of steps to strengthen the cyber resilience of regulated entities. Building on its Prudential Standard CPS 234 Information Security that came into effect in July 2019, APRA launched its Cyber Security Strategy in November 2020. A key focus of the strategy is to establish a core set of cyber controls for financial institutions. The strength of these controls will be independently assessed against APRA's information security requirements. As part of this strategy, APRA has collected data from financial institutions on their cybersecurity practices, which has helped to inform priority areas for improving resilience; this knowledge has been shared to facilitate entities' self-assessments and industry benchmarking. As a result of these exercises, along with insights from its supervisory activities, APRA highlighted that boards must strengthen their ability to oversee cyber resilience,[23] and expects them to have the same level of confidence in reviewing and challenging information security issues as they do when governing other business issues.

Financial market infrastructures (FMIs)

The cyber resilience of FMIs – such as high-value payment systems, central counterparties and securities settlement facilities – is critical given the central role that FMIs play in the smooth functioning of specific parts of the financial system. As a result, the Australian Government and regulators are working on additional initiatives to further increase their resilience.

The Reserve Bank oversees a number of FMIs that operate in the Australian financial system, and regularly assesses their cyber resilience and identifies areas for improvement. This process takes into account guidance on cyber resilience from international bodies that set standards, and includes working with home regulators of overseas entities that operate in Australia, as appropriate.[24] In the case of the Reserve Bank Information and Transfer System (RITS) – Australia's real-time gross settlement system – the Bank has dual roles as overseer and operator, with these roles conducted by

separate departments in the Bank. Its operator role means that the Bank also supports broader initiatives that engage RITS members, including contingency exercises with industry participants.

Likewise, the Bank has dual roles with respect to SWIFT – a global provider of the critical messaging and connectivity services for the financial system. As a member of the SWIFT Oversight Forum, Bank staff oversee the ongoing work to ensure SWIFT members' defences against cyber-attacks are up to date and effective. As a user of the SWIFT network and RITS operator, the Bank is compliant with SWIFT's Customer Security Controls Framework.

Global regulatory coordination

The borderless nature of cyber risks requires a coordinated effort across jurisdictions to identify risks, to promote resilience of all systems and to respond to international disruptions. Examples of this work include:

- The Cyber Security Working Group is producing a joint response protocol with agencies in New Zealand.
- The Financial Stability Board has been developing further guidance for oversight of financial institutions' reliance on critical service providers.
- The World Bank has been working to strengthen the resilience of payment systems in developing and emerging economies through its Financial Inclusion Global Initiative, and has launched a new global fund to improve cybersecurity development and offer technical assistance.
- The Bank for International Settlements, the World Bank and the International Monetary Fund have participated in simulated cyber-attack exercises on the global financial system to improve cooperation across countries.
- Bank staff members have taken part in various other international working groups promoting industry coordination in managing cyber risks and related contingency measures.

Endnotes

[1] For discussions of bank and systemic risks, including cyber risks, see Kearns J (2021), 'Evolving Bank and Systemic Risk', Speech to the 34th Australasian Finance and Banking Conference, 16 December; Byres W (2021), 'Banking On an Unpredictable Future', Speech to the 2021 AFR Banking Summit, 30 March.

[2] European Systemic Risk Board (2020), 'Systemic Cyber Risk', February.

[3] RBA (2018), 'Box D: Cyber Risk', *Financial Stability Review*, October.

[4] Adelmann F, I Ergen, T Gaidosch, N Jenkinson, A Morozova, N Schwarz and C Wilson (2020), 'Cyber Risk and Financial Stability: It's a Small World After All', IMF Staff Discussion Note No 2020/007.

[5] For example, an attack on a cloud service provider could provide access to many institutions (IT interconnectedness) or could take down the key service provider (lack of IT substitutability), or both. A ransomware attack could become systemic by spreading to multiple institutions through the internet (IT interconnectedness) or by disrupting the liquidity of a key financial institution and causing financial stress (financial interconnectedness).

[6] See Australian Cyber Security Centre (2022), '2021 Trends Show Increased Globalized Threat',

Joint Cybersecurity Advisory from Cybersecurity Authorities in the United States, Australia and the United Kingdom, 9 February; RBNZ (2021), *Financial Stability Report*, November; Sveriges Riksbank (2021), *Financial Stability Report*, May; Aldasoro I, L Gambacorta, P Giudici and T Leach (2020), 'The Drivers of Cyber Risk', BIS Working Paper No 865.

[7] See Australian Cyber Security Centre (2021), 'ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021', September; Office of the Australian Information Commissioner (2022), 'Notifiable Data Breaches Report: July-December 2021', February.

[8] Summerhayes G (2020), 'Strengthening the Chain', Speech at the Financial Services Assurance Forum, 26 November.

[9] Healey J, P Mosser, K Rosen and A Tache (2018), 'The Future of Financial Stability and Cyber Risk', Brookings, October.

[10] Adelmann *et al*, n 4.

[11] Government Accountability Office (2022), 'Federal Response to SolarWinds and Microsoft Exchange Incidents', January.

[12] Financial Markets Authority (2021), 'Market Operator Obligations Targeted Review – NZX', January.

[13] See ASIC (2021), 'Accellion Cyber Incident', 25 January; KPMG (2021), 'Reserve Bank of New Zealand Incident Assessment', May.

[14] Brangwin N and H Portillo-Castro (2019), 'Cybersecurity', Parliamentary Library Briefing Book, Parliament of Australia.

[15] Legislative Council (2021), 'Cyber Security', Report to Portfolio Committee No 1 – Premier and Finance, 26 March.

[16] Chalmers S and M Janda (2021), 'Akamai Says a Technical Problem Not Cyber Attack Was Behind Mass Bank, Corporate Web Outage', *ABC News*, 17 June.

[17] Accenture (2019), 'The Cost of Cybercrime', Research Report, 6 March.

[18] Collins R, C O'Connor-Close and A Zhang (2020), 'Cyber Incident Cost Estimates and the Importance of Building Resilience', RBNZ *Bulletin*, 84(2).

[19] Aldasoro *et al*, n 6.

[20] Financial Stability Board (2018), 'Cyber Lexicon', 12 November.

[21] The CFR agencies are the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission, the Australian Treasury and the Reserve Bank of Australia.

[22] Similar such initiatives exist in other jurisdictions, which many foreign financial institutions and FMIs that operate in Australia have been subject to for a number of years. See, for example, the United Kingdom's CBEST <https://crest-approved.org/schemes/cbest/index.html>.

[23] See APRA (2021), 'Improving Cyber Resilience: The Role Boards Have to Play', Insight, 23 November.

[24] RBA (2021), 'Box B: Assessing the Cyber Resilience of FMIs', *Payments System Board Annual Report*.