Box D

Cyber Risk

Over recent years regulators and financial institutions have increasingly focused on cyber risk. Cyber risk refers to the threat of financial losses, disruption and/or reputational damage from a malicious breach of an entity's information systems. It is one component of operational (or technological) risk more broadly. The potential for cyber attacks is rising due to the growing use of information technology among businesses and consumers. The increasing presence and sophistication of cyber adversaries is also contributing to the growing threat.

Globally, the financial services and energy sectors account for the largest share of cyber incidents involving nationally important systems.[1] The risk of cyber attacks in the financial system has increased due to a rapid rise in the digitalisation of services and use of third-party providers has increased the sector's online footprint. Increased use of technology and digital records in banking, such as the introduction of open banking over the coming year, could raise additional cyber risks. As a result, cyber security will be a core challenge for the financial system for years to come.

There are different types of cyber attacks

Perpetrators of cyber attacks are usually motivated by financial gains or a desire for notoriety. Malice can also be a driver. Attacks generally occur in one of four ways:

- data breaches – where attackers aim to steal sensitive data. An example was an attack on Equifax where sensitive information from 147 million customers was obtained
- system disruptions – where attackers disrupt the availability of critical systems or websites, most commonly using a denial-of-service attack, such as during the 2016 Australian Census
- integrity of data attacks – when attackers modify information, often with the aim of rendering critical information unusable. Examples include the attack and release of altered medical records stored by the World Anti-Doping Agency in 2016
- financial attacks – where adversaries attack for financial gain and/or sabotage, either through fraud or ransom (often using ransomware). An example was the theft of US$81 million from Bangladesh Bank by an attack on their Society for Worldwide Interbank Financial Telecommunication (SWIFT) connected systems.

The incidence of cyber attack is rising

There is a lack of comprehensive data on cyber attack incidents or costs, in part because institutions and governments are reluctant to share this information. However, it is clear that financial institutions have increased their focus on cyber risk over recent years. One simple measure of this is that mentions of 'cyber' in the Australian major banks' annual reports have risen

1 For an Australian perspective on this, see ACSC (2016), 'Threat Report', October. Available at <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf>.

rapidly. Surveys of financial institutions show that cyber risk was considered one of the highest risks they faced in 2017, having not even been considered a top ten risk four years earlier.

There are some estimates of the extent of cyber attacks. An Accenture cybercrime report, based on a sample of 254 companies (across all industries) in seven advanced economies (including Australia), found a 27 per cent increase in successful breaches of company information security infrastructure in 2017 compared with a year earlier. This report also estimated that the average annual cost for each financial services entity to manage and recover from cyber attacks was US$18 million. The International Monetary Fund has estimated that direct losses from cyber attacks could be as large as 9 per cent of total bank net income globally.[2] It estimated that this cost could rise to about one-third of income if the frequency of attacks and interconnectedness among institutions were to rise as per its 'severe' scenario. These estimates exclude indirect costs, such as the loss of reputation, which could make the potential losses even larger.

In Australia, no financial institution regulated by the Australian Prudential Regulation Authority (APRA) has yet recorded a significant financial or data loss from a cyber attack. However, half of the financial institutions surveyed by APRA in 2015/16 reported at least one cyber security incident that was material enough to report to executive management over the prior 12 months.

Some types of attacks could have financial stability impacts …

Globally, successful cyber attacks have generally only affected a specific institution, but an attack could potentially spread to have systemic implications. While the likelihood of an attack with severe financial stability implications is very low, the costs could be very large. The channels through which an attack on one institution could become systemic include operational dependencies (such as third-party providers), financial interconnectedness and the impact on confidence (including consumers and creditors).

The direct financial costs from a cyber attack can arise from fraud or ransom attacks and include the costs of lost data and/or the need to investigate and repair assets affected by the attack. However, it seems unlikely that an attack would have a large impact on the capital positions of Australia's major banks.[3] It is unlikely, for example, that a fraudulent attack that is large enough to directly threaten a bank's viability could be disguised. Further, it is not credible to demand a ransom large enough to force a bank to fail.

A cyber attack that disrupts the payments system, particularly the wholesale payments network, could have more systemic implications. Disruption to the Reserve Bank Information and Transfer System (RITS) – which settles real-time high-value payments across Exchange Settlement Accounts held at the Reserve Bank – could prevent or delay a wide range of economic activity from occurring by stopping the final settlement of interbank payments. These include payments by governments (such as pensions and social security payments), corporations and between major banks and the Reserve Bank. Significant economic and financial stability consequences could develop if the disruption were not resolved in a timely manner.[4] An outage of RITS could also result in a build-up of credit risk in the financial system until interbank obligations were settled.

2 Lagarde C (2018), 'Estimating Cyber Risk for the Financial Sector', IMF Blog, 22 June. Available at <https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/>.

3 These banks have around $170 billion in CET1 capital.

4 International guidelines indicate that such systems should aim to be operating again within two hours, and should complete settlement by the end of the day, even in extreme (but plausible) scenarios.

A significant disruption to a retail payment system is likely to have a broad impact and could prevent customers from paying bills and/or transferring funds. This could create difficulties for some households. But unless it widely restricted access to, or damaged the perceived security of, deposits, it would be unlikely to adversely affect financial stability. The potential disruption caused by such an attack has risen as consumers have switched to digital payment methods, but cash is still a viable means of conducting most retail transactions.

A cyber attack involving a breach of data integrity in the financial system could have the most severe financial stability implications. For example, an attack that had implications for the integrity of banks' record of their assets and liabilities could impede their ability to disburse funds to customers or collect on monies due. In the extreme it could raise questions about the institution's solvency status. This could force directors to withdraw the bank from trading while investors may pull back on capital market funding.

Any type of material attack is also likely to have an impact on customers and creditors' confidence that could amplify the shock. For example, there could be a marked deterioration in financial stability if creditors (both depositors and wholesale funders) lost confidence in the accessibility or security of the funds they have placed with banks. Australian banks could face liquidity issues if this resulted in creditors withdrawing funds or refusing to roll them over. In these circumstances, alternative funding sources would need to be accessed by banks, including as a last resort from the Reserve Bank's liquidity provision mechanisms. A loss of confidence could also see consumers pull back from electronic transactions and towards cash.

… so supervisors and institutions are working to increase resilience

Supervisors and central banks globally have been increasing their focus on the growing threat from cyber attacks. The issue has been raised as a key risk in financial stability reports in numerous countries and is a focus for several international standard setters.

A key challenge for regulating cyber risk is accurately quantifying it, particularly given the rapidly evolving nature of cyber threats. Standard analytical tools cannot easily be used to quantify vulnerabilities, unlike in other parts of banks' risk frameworks. In addition, cyber threats are dynamic in nature, meaning that current requirements may quickly become insufficient. For these reasons, regulators usually take a principles-based approach to regulating cyber threats.

The response by regulators to manage cyber risk varies and is at early stages compared with other risk frameworks (such as credit). A small number of jurisdictions have specific regulatory measures for managing cyber risks at banks, including Singapore, the United Kingdom and the United States.[5] Cyber risk regulatory requirements in these jurisdictions are typically based on the framework set by the CPMI-IOSCO.[6] This framework encourages entities to focus on strengthening five risk management categories: governance; identification; protection; detection; and response and recovery. It also encourages entities to continually test their systems and evolve their frameworks as key lessons are discovered. This requires firms to stay informed

5 For more information, see Crisanto J C and J Prenio (2017), 'Regulatory approaches to enhance banks' cyber-security frameworks', FSI Insights on Policy Implementation No 2. Available at <https://www.bis.org/fsi/publ/insights2.pdf>.

6 The Committee on Payments and Market Infrastructure (CPMI) and the International Organization of Securities Commissions (IOSCO). While this framework was established for FMIs, its application is general enough to be extended to other financial institutions. For more details, see <https://www.bis.org/cpmi/publ/d146.pdf>.

of developments in cyber security and to enhance their ability to pre-empt and manage cyber threats.

As supervisors strengthen guidance around cyber security, one consideration is ensuring that guidance is broadly harmonised across jurisdictions. In addition to reducing costs for banks that are active across several jurisdictions, harmonisation would recognise that cyber attacks affect financial institutions without regard to location and usually have cross-border implications. However, a mandated harmonised approach to cyber risk could also mean that vulnerabilities are common across countries and institutions. These issues are currently pertinent as over 70 per cent of supervisors expect to announce cyber security initiatives in the coming year.[7]

In Australia, APRA announced earlier this year that it will introduce its first prudential standard for information security management.[8] Key objectives of the proposed prudential standard are for all APRA-regulated institutions and industries to maintain information security management controls that are commensurate with their size and the extent of the threat to information assets, and to have appropriate mechanisms in place to detect and respond to breaches in a timely manner. These principles-based proposed standards are expected to be finalised later this year and implemented by mid 2019.

Through their roles as supervisors of financial market infrastructures (FMIs), the Reserve Bank and the Australian Securities and Investments Commission (ASIC) have powers to ensure that FMIs have effective controls to manage cyber threats and that they report cyber breaches to their supervisors in a timely manner. Indeed, cyber security has been a priority in the Reserve Bank's supervision of FMIs and RITS in recent years. As part of this, the Reserve Bank recently reviewed the ASX against international guidance on cyber resilience, concluding that the ASX's practices are consistent or broadly consistent with the guidance. A similar review of RITS in 2017 found no significant issues with its cyber security arrangements. As part of its continuous review of security practices, the Reserve Bank has in recent years made enhancements that further strengthen the resiliency of RITS to cyber attacks and its ability to recover from a successful attack within a short time frame. In recognition of this, RITS has recently been assessed as being compliant with various international standards. More broadly, ASIC has been strategically reviewing the cyber resilience of the financial sector firms it regulates, using standards-based surveillance tools, structured self-assessments and targeted interviews and follow ups.

The financial services sector is also responding to increasing cyber attack threats. SWIFT has introduced a 'customer security program' that establishes mandatory controls for security, guidelines for monitoring network breaches, and a protocol for sharing information on attacks. Private sector reports on cyber security also suggest that large financial institutions are investing heavily to strengthen defences against attacks. However, cyber security will need to continue to evolve as attackers increase their sophistication and ability.

7 See Financial Stability Board (2017), 'Summary Report on Financial Cybersecurity Regulations, Guidance and Supervisory Practices', October. Available at <http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/>.

8 For details, see APRA (2018), 'APRA to introduce first prudential standard aimed at tackling growing threat of cyber attacks', Media Release No 18.10, 7 March. Available at <https://www.apra.gov.au/media-centre/media-releases/apra-introduce-first-prudential-standard-aimed-tackling-growing-threat>.