Box B

Assessing the Cyber Resilience of FMIs

Cyber security threats are currently ranked by the Council of Financial Regulators (CFR) as one of the top five risks to the Australian financial system. Consistent with this, cyber resilience has been a focus area over recent years for all FMIs (see below for entity-specific information). The Bank has assessed the FMIs' practices and procedures to be broadly aligned with the relevant regulatory requirements, but as cyber threats are continuing to evolve, the Bank is closely monitoring developments.

The approach of regulators to assessing an FMI's compliance with cyber risk management standards has evolved significantly in recent years. Cyber risk was previously considered to be a subcategory of operational risk and therefore covered by regulatory standards for operational risk. Furthermore, given the limited access points to FMIs' core systems, it was considered that there was limited risk of them being compromised via the internet. Accordingly, regulatory requirements were focused more on preventing and recovering from operational disruptions such as software or hardware malfunctions. However, as the sophistication of cyber attackers and awareness of cyber risks in the financial sector started to grow – particularly in the years following publication of the PFMI in 2012 – the international regulatory community turned its attention to the identification of cyber risks for FMIs and to developing measures to specifically address these.[1] This work gained greater urgency in 2016 when sophisticated cyber attackers targeting the central bank of Bangladesh managed to steal US$81 million. In the same year, CPMI and IOSCO issued guidance to the PFMI for FMIs to increase their cyber resilience.[2] This guidance was adopted by the Reserve Bank, and all Australian-licensed FMIs have since been assessed against it.

In the case of RITS, the Bank has an interest in cyber resilience both as operator and overseer. The Bank has an ongoing program of work to maintain high levels of cyber resilience, which includes complying with the requirements under the ISO 27001 standard for Information Security Management and the SWIFT Customer Security Controls Framework. In addition, the Bank's operational staff have participated in various working groups promoting industry coordination in managing cyber risks and related contingency measures.

One of the most sophisticated tools to measure cyber resilience of FMIs is red-team testing. Also known as 'ethical hacking', it mimics the tactics, techniques and procedures of real-life cyber adversaries. A red-team framework has been released by the CFR and is being used (in a pilot exercise) to test the resilience of the live production systems of FMIs and financial institutions in a controlled environment and under the scrutiny of supervisors.[3] The CFR is also

[1] See Committee on Payments and Market Infrastructures (2014), 'Cyber Resilience in Financial Market Infrastructures', BIS, November. Available at <https://www.bis.org/cpmi/publ/d122.pdf>.

[2] Committee on Payments and Market Infrastructures, and Board of the International Organization of Securities Commissions (2016), 'Guidance on Cyber Resilience for Financial Market Infrastructures', BIS and IOSCO, June. Available at <https://www.bis.org/cpmi/publ/d146.pdf>.

continuing to enhance the coordination of cyber-related work programs among its agencies and is supporting Australia's Cyber Security Strategy 2020, an Australian Government initiative to further improve cyber security across the economy.[4]

[3] Council of Financial Regulators (2020), 'CORIE Framework Launched to Test Cyber Resilience of Australia's Financial Services Industry', Media Release No 2020-06, 8 December. Available at <https://www.cfr.gov.au/news/2020/mr-20-06.html>.

[4] Australian Government (2020), 'Australia's Cyber Security Strategy 2020'. Available at <https://www.cyber.gov.au/acsc/view-all-content/news/australias-cyber-security-strategy-2020>.