EUROFI VIEWS MAGAZINE - ZAGREB APRIL 2020

Morten Bech

Head of Secretariat, CPMI, Bank for International Settlements

Avoiding a cyber mess

"Don't put all your eggs in one basket" is good advice for life, and for operational resilience too. The job of concentrating functions and risk in the financial system needs to be handled with care, and maximum resilience. Decades of work on financial market infrastructures have strengthened business continuity arrangements to ensure continuity of services through fires, floods and power outages, and pandemics. The eggs are safe in the basket.

Cyber risk has made keeping our eggs safe a far more complex and challenging task. Now, replicating data for a seamless failover to a backup site could help spread compromised data across all systems. It might not be obvious that any irregularities are even malicious until it is too late to share information. Outsourcing critical services might help better distribute operational risk, but if everyone uses a common service provider, then an issue can quickly become systemic. Cyber scrambled egg is a risk.

The CPMI's strategy to avoid the omelette is to "protect the core and secure the periphery". The core of the financial system comprises the financial market infrastructures that are covered by the CPMI- IOSCO Guidance on cyber resilience for financial market infrastructures, which led the way for standard setters in this field. Yet cyber defence cannot be boiled down to a pass-or-fail test; improving it requires a cooperative approach. A CPMI-IOSCO roundtable that brought together the 22 largest global and regional FMIs and their supervisors identified three key challenges that need a common solution: (i) data integrity, (ii) information-sharing and (iii) third-party service providers.

International industry-led working groups were set up to tackle each of these challenges. This is the first time this type of cooperative approach has been adopted. Each group has a tough challenge. For data integrity, or how to recover if underlying data are corrupted, there are a number of possible avenues to explore, including contingency arrangements, segregated ledgers and frequent reconciliations. For information-sharing, common protocols exist to share financial events, but operational incidents are still segregated by type of FMI, market and jurisdiction. Setting expectations and developing a practical arrangement for alerting on international operational incidents could enable faster and better-informed responses. Third-party services (eg cloud) can benefit from cooperation by users, provide a clearer view of risk management practices at the common service provider and avoid duplicating third-party risk assessments.

So, although the challenges are tough, financial authorities, infrastructure and their members all have an incentive to cooperate and avoid a cyber crisis. Working together now, to strengthen common operational resilience, can ensure we avoid scrambling our cyber eggs. If we fail to do this, we will all end up with egg on our face. ●