MFSA

Cyber risk – Relevance to Financial Stability

Digitisation has become a major trend in the financial sector in recent years. In this regard, COVID-19 has acted as a catalyst, accelerating the adoption of digital tools and products to respond to the new pandemic environment which forced financial entities to shift their interaction with customers through online channels. However, the rapid trend of financial innovation has heightened their exposure to cyber risk, becoming a key concern for regulators around the world. Indeed, the incidence of cyber-attacks increased in both frequency and severity, rising by +45% in 2022 compared to 2021. In this context, the current geopolitical tensions play a role in increasing the risk of potential targeted cyber-attacks.

The impact of malicious cyber incidents can result in financial losses due to operational disruptions, data theft, ransomware payments or unauthorised transactions. Cyber-attacks can also cause reputational damage to financial entities and can result in legal consequences. In addition, a failure to adequately price cyber risk could lead to potentially large losses for insurers involved in cyber underwriting.

Increased reliance on third party service providers and shared digital infrastructures has heightened the complexity and interconnectedness of financial firms. In turn, this, has strengthened the linkages between the financial and non-financial sectors, creating the conditions for cyber-attacks to potentially become systemic.

On January 2023, Regulation (EU) 2022/2554 on digital operational resilience (the 'DORA Regulation) came into force and will be fully applicable by January 2025. The DORA Regulation aims to strengthen the financial sector's digital operational resilience by introducing requirements on ICT risk management, incident management, classification and reporting, testing, ICT third-party risk and voluntary information sharing arrangements. Updated information on the DORA Regulation can be found here. More generally, stakeholders can also refer to the Supervisory ICT Risk and Cybersecurity Function's webpage for more information on the Authority's work with respect to cyber and ICT risks.

For further information:

- ECB Financial Stability Review, section 3.3, May 2023
- Advancing macroprudential tools for cyber resilience (europa.eu), February 2023
- ECB Banking Supervision: SSM Supervisory Priorities for 2023-2025
- REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector