Joint press release

23 April 2024

G7 Cyber Expert Group Conducts Cross-Border Coordination Exercise in the Financial Sector

The G7 Cyber Expert Group completed a cross-border coordination exercise on 17 April 2024. G7 authorities routinely exercise to ensure they can effectively coordinate and communicate their response in the event of a widespread cyber incident affecting the financial system.

The primary objective of the exercise was to strengthen the ability of G7 financial authorities in effectively communicating and coordinating their respective responses to facilitate crisis management in the event of a significant cross-border cyber incident affecting the financial sector. The exercise built on previous simulations and workshops, which focused on cyber incident response, recovery management, and crisis communication.

To optimize coordination among G7 financial authorities, the exercise assumed a large-scale cyber attack on financial market infrastructures and entities in all G7 jurisdictions. The exercise brought together 23 financial authorities, including ministries of finance, central banks, bank supervisors, and market authorities, as well as private industry participants.

By conducting such exercises, the G7 Cyber Expert Group aims to bolster the financial sector’s resilience and minimise disruptions across all G7 jurisdictions. This exercise allows the G7 financial authorities to continue to integrate the multiple lines of effort necessary to respond effectively to an incident.

In an ever-changing and interconnected world, cross-border coordination, incident response preparedness, and information exchanges remain G7 priorities. The G7 Cyber Expert Group continuously collaborates on cybersecurity and stands ready to respond to cyber threats posed to the financial system.

About the G7 Cyber Expert Group

The G7 Cyber Expert Group coordinates cybersecurity policy and strategy across the G7 jurisdictions. The G7 Cyber Expert Group seeks to improve the cyber resiliency of the financial sector through preparedness, a consensus of the threat landscape, and a shared approach to mitigating risk and to this end has published various sets of Fundamental Elements, e.g. G7 Fundamental Elements of Ransomware Resilience for the Financial Sector and G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector. More information about the G7 Cyber Expert Group and publications can be found here.