

# Cybersecurity for the financial sector

## Why is cybersecurity an important topic for the ECB as overseer of financial market infrastructures?

As digitalisation and globalisation change the way we do business, the operational network of financial market infrastructures has become increasingly interconnected. As an overseer of a number of systemically important financial market infrastructures operating in the euro area, the ECB needs to ensure that not only the individual systems but the network as a whole is operationally resilient.

Cybercrime is a serious threat not only to individual market actors but also to the overall operational network. Cybercriminals could seek to hack into the network for their own economic gain, or they could be driven by the aim of damaging the financial system, bringing down the operational network and destroying data. This is a serious issue for the ECB as such an act would undermine trust in the financial system and in the single currency.

Cybercrime knows no borders. The agents of cybercrime are adapting and increasing their level of sophistication fast, calling into question our traditional approach to managing operational resilience. We need a paradigm shift in how we manage resilience and security in the financial sector.

## How do public authorities, international committees and international organisations address cybersecurity in the financial sector at global level? What is the ECB's role in this process?

Public authorities have recognised that the interconnectedness of the global financial system requires a strategically aligned approach to cybersecurity at international level. Hence, the G7 countries (i.e. Canada, France, Germany, Great Britain, Italy, Japan and the United States) created a Cyber Expert Group that was tasked with drawing up a list of "fundamental elements

of cybersecurity for the financial sector". The ECB contributed to this work, welcomes adoption of these elements by the G7 finance ministers and central bank governors, and encourages all jurisdictions to work on implementing them.

The elements provide a concise set of best practice principles on cybersecurity for public and private entities in the financial sector. In conjunction with the guidance on cyber resilience for financial market infrastructures recently published by the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO), the G7 elements underline that cyber risk must be met by a collective and united effort by the financial industry and the public authorities, both within and across borders.

**CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures**

**G7 Fundamental elements of cybersecurity for the financial sector**