SPEECH

Cyber risks and the integrity of digital finance

Introductory remarks by Fabio Panetta, Member of the Executive Board of the ECB, at the sixth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)

Frankfurt am Main, 30 September 2021

The pandemic is fundamentally changing how we work, how we conduct business, and even how we live and interact with one another. It is influencing how we pay for goods and services, accelerating the trend towards cashless and contactless payments.[1]

Throughout the pandemic, financial market infrastructures and their related ecosystem have supported the economy's resilience and adapted to new needs. They have accompanied the digital transformation. This process will continue after the pandemic.

Central banks are playing an active role in this change. The ECB is promoting and offering instant payments, investigating the possibility of launching a digital euro, and supporting the G20's work on making cross-border payments faster, cheaper, more transparent and more inclusive while maintaining their safety and security.

But digitalisation also brings with it risks to the payment system, to monetary sovereignty and to the financial system as a whole. In response to these developments, the ECB is adapting its oversight framework.[2] And the European Commission, in turn, has launched regulatory initiatives on crypto-assets and digital operational resilience.[3]

But there will be no integrity of digital finance and payments without protection against cyber risk. Today I will discuss how cyber risks are evolving and the key role of the Euro Cyber Resilience Board (ECRB) in addressing them.

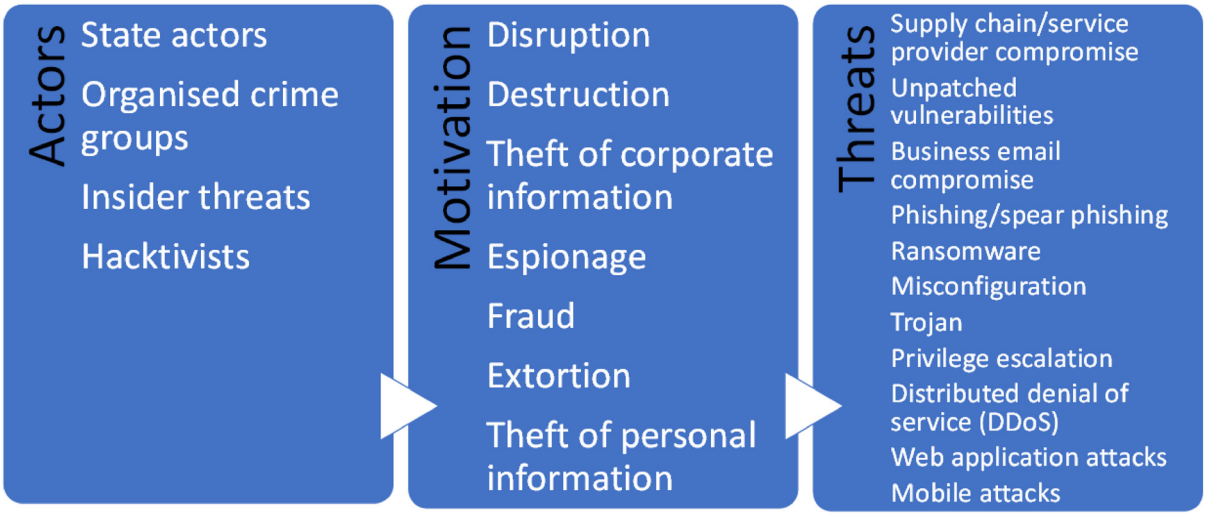
A more complex cyber threat landscape

The increasing use of digital services and the widespread reliance on technology, together with the growing use and interconnectedness of third-party products and services, are increasing financial market infrastructures' vulnerability to cyberattacks. Financial experts single out cyberattacks as the number one risk for the global financial system.

The cyber threat landscape is complex (Figure 1) and steadily evolving. For instance, attackers took advantage of the pandemic to lure victims with coronavirus-themed phishing emails and to exploit weaknesses associated with remote working.

Figure 1

Cyber threat landscape for financial market infrastructures in Europe



Note: Threats (right-hand column) are ordered by degree of assessed severity (most severe threats at the top).

Cyber criminals have also been innovative in finding lucrative ways of stealing money from their targets. Ransomware attacks are usually combined with requests for ransom payments in the form of crypto-assets. Attackers are increasingly exploiting vulnerabilities in the supply chain and third-party providers with a view to compromising or stealing data, disrupting services or demanding ransom payments.

Cyberattacks are becoming more sophisticated and more frequent, and their potential impact has been constantly growing. Supply chain threats to IT service providers and vendors are a source of particular concern. Attackers target these service providers and IT vendors to reach other institutions which use their services or software. Supply chain attacks are often used to compromise a large number of institutions and then demand a ransom from them.

If the institutions affected only detect or learn about such attacks with a delay, the consequences can be immense. We therefore need to monitor all the software and hardware in our IT environments – no matter how small – and not focus solely on our most critical third-party providers. And we need to exchange critical information and tackle this threat.

The contribution of the Euro Cyber Resilience Board

We need to remain vigilant to the evolving threat landscape and continuously maintain the highest level of resilience. This focus cannot be compromised: although the monetary cost of improving cyber resilience may seem high, the costs of successful attacks – in terms of both financial damage and reputational impact – are far higher.

We need to further intensify our efforts. The ECRB provides a unique forum for public-private dialogue and common initiatives. This is first and foremost in the interest of ECRB members, but also in the broader interest of the European financial sector, households and businesses. As I have emphasised before, the resilience of the sector relies on the resilience of all of its components. We must help each other in identifying weak links so that we can strengthen the financial system as a whole.

In our last meeting, I spoke about the success and timeliness of the Cyber Intelligence and Information Sharing Initiative (CIISI-EU). I am pleased that it is fully operational, which has allowed us to make

significant progress in terms of sharing information during the pandemic.

CIISI-EU has become a powerful tool for sharing threat intelligence, information and best practices. It acts as an early warning system for threats and ongoing cyberattacks within the community, raising awareness of the cyber risk landscape. We should strive to build on this pooling of information.

I am also glad that the CIISI-EU model has been adopted in Ireland, where it will be used to share cyber information between the Central Bank of Ireland and critical domestic financial entities. We may see other countries adopt the model in a similar way in the future. Looking ahead, I see value in identifying other CIISI-like initiatives and forming partnerships to share threat and intelligence information.

Conclusion

Despite the progress towards addressing cyber risk, we need to remain proactive in tackling cyber threats. We will need to remain fully committed to protecting cyber resilience in view of the increasing threat level.

The ECRB is a critical forum to achieve this goal. It allows us to share information, address common cyber threats and risks, strengthen crisis management and coordination, and support recovery capabilities. It will evolve as we identify new work priorities. But its foundation will remain the same: trust and collaboration against a common threat.

1. ECB (2020), "Study on the payment attitudes of consumers in the euro area (SPACE)", December.
2. The new Eurosystem oversight framework for payment instruments, schemes and arrangements (PISA framework) is expected to be issued in 2021. In the light of technological developments in the payments ecosystem, with new services, products and new players, the Eurosystem is establishing a holistic, harmonised, up-to-date and future-proof framework based on the international oversight standards. See ECB (2021), "Eurosystem Oversight Report 2020", April.
3. In September 2020 the European Commission proposed a Regulation for Markets in Crypto-Assets (MiCA) and a Regulation on Digital Operational Resilience in the Financial Sector (DORA). The ECB published its legal opinion on MiCA on 19 February 2021 and its legal opinion on DORA on 4 June 2021.

CONTACT
European Central Bank

Directorate General Communications

Sonnemannstrasse 20

60314 Frankfurt am Main, Germany

+49 69 1344 7455

media@ecb.europa.eu

Media contacts