Speech

Adapting to the fast-moving cyber threat landscape: no room for complacency

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

Frankfurt am Main, 1 June 2022

For the past four years we have been working together on the Euro Cyber Resilience Board (ECRB). With representatives from pan-European financial market infrastructures and their critical service providers, central banks and other authorities, this Board is a unique and powerful forum for openly exchanging our views on cyber resilience and cyber intelligence.

Over the past few years we have built trust among ECRB members, working closely with one another to improve cyber resilience across the European financial sector. The success of our intelligence sharing arrangement – the Cyber Information and Intelligence Sharing Initiative (CIISI-EU) – and the numerous projects we are developing together reflects this trust.

Rather than forming a closed group catering only for direct members, the ECRB aims to promote the efficiency and safety of the entire European financial sector. Each ECRB member serves as an ambassador to the financial community, conveying the Board's proposals for improving cyber resilience. We are transparent about the initiatives we take, with the aim of ensuring they can be applied by other financial stakeholders or sectors, including those outside Europe. The publication of our CIISI documentation is one example of our openness.

Today I will discuss the cyber threat landscape we face and the ECRB's response to it.

The evolving cyber threat landscape

The cyber threat landscape is evolving rapidly and becoming increasingly complex.

According to some estimates, cyber risk tripled between 2013 and 2020. The financial sector is now one of the most exposed. And research suggests that cyber threats are a source of systemic risk for firms and markets, with cyber risks being increasingly priced in by the stock market.[1]

The ECRB community reflects awareness of the need to work together to confront the evolving cyber threats we all face. By cooperating, we can learn and adapt more quickly.

The use of digital services and the reliance on technology are making financial market infrastructures more efficient but leaving them more vulnerable to cyberattacks.[2] We must therefore continuously improve our cyber resilience and make it an integral part of any new project. In turn, this calls for a sustained effort to identify and understand market dynamics.

For example, crypto assets are increasingly being used to conduct ransomware attacks. Crypto actors themselves are also exposed to cyber risks. Often unregulated and having grown quickly, they are an attractive target. And because crypto-assets are increasingly linked to the traditional financial system[3], such attacks could ultimately have an impact on financial stability in the absence of adequate regulation and protection.

Exogenous factors also have an impact on the cyber threat landscape in ways that are difficult to predict.

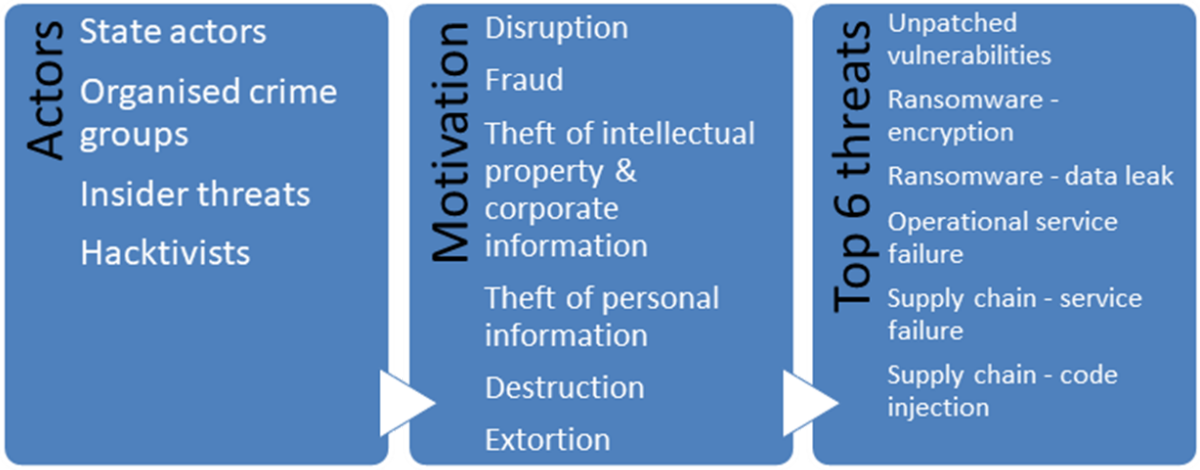
The Russian invasion of Ukraine is a prime example of this, with many cyber threat actors targeting critical infrastructures. Other cyber threat actors have used the invasion to trick individuals and companies by carrying out phishing or other social engineering attacks.

As a result, our CIISI-EU analysis reveals many different threats, motivations and actors (Chart 1). Cyber threat actors attempt to exploit information systems for a variety of reasons ranging from appropriating funds, causing disruption, demanding a ransom or stealing sensitive information.

Phishing, vishing, social engineering and the human factor in general are still the main channels used by cyber attackers to obtain access to our systems. The supply chain cyber threat to IT service providers and vendors[4] observed in 2021 remains an ever-present concern in our interconnected and interdependent infrastructures and calls for the highest levels of due diligence.

Chart 1

Cyber threat landscape for financial market infrastructures in Europe



Note: Threats (right-hand column) are arranged in descending order of estimated severity.

The ECRB response

We established the ECRB four years ago as part of the Eurosystem's comprehensive cyber resilience strategy in the area of market infrastructure. The initiatives launched by the ECRB have enhanced cyber resilience across the community.

But we cannot afford to be complacent. So far, no cyberattack has seriously breached the defences of Europe's financial infrastructures. However, that does not mean that we can take anything for granted in the future. Cyber criminals will undoubtedly continue to ramp up their efforts, and so should we. The cyber activity we are witnessing is clearly visible and felt everyday by the CIISI-EU community.

At our last meeting we agreed on an ambitious work programme. Today we will discuss the progress made on crisis communication, third-party risk, information sharing and training, to name but a few topics.

In particular, training is highly relevant, as cyber attackers continue to target the human factor to gain access to our systems. Basic cyber hygiene is still the foundation required for a proper cyber posture. While we have seen considerable progress over the years, a number of entities are still struggling with this. Training to enhance cyber resilience must therefore remain high on our collective agenda.

Conclusion

Let me conclude.

The ECRB is supporting the cyber resilience of pan-European financial market infrastructures. Collectively and individually, ECRB members can raise awareness of our initiatives and help others benefit from them.

As recent developments on the geopolitical front or in crypto asset markets show, we need to continuously adapt and strengthen our defences. That is why we need to share intelligence and experience to be able to detect attacks earlier, respond to them better and recover from them faster. And that is why we must work together to protect our institutions. The ability to ensure the continuity of our critical functions in the event of an attack is vital.

I now look forward to an open and rewarding meeting.

1.

Jamilov, R., Rey, H. and Tahoun, A. (2021), "The Anatomy of Cyber Risk", *Working Paper 28906,* National Bureau of Economic Research.

2.

Panetta, F. (2021), "Cyber risks and the integrity of digital finance", introductory remarks at the sixth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB), Frankfurt am Main, 30 September.

3.

Panetta, F. (2022), "For a few cryptos more: the Wild West of crypto finance", speech at Columbia University, New York, 25 April.

4.

Attackers target these service providers and IT vendors to reach other institutions that use their services or software. See Panetta, F. (2021), op cit.