SPEECH

One step ahead: protecting the cyber resilience of financial infrastructures

Introductory remarks by Piero Cipollone, Member of the Executive Board of the ECB, at the ninth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Frankfurt am Main, 17 January 2024

Cyber risks have become one of the main issues for global security. The associated annual cost is estimated to exceed $200 billion globally.[1] And cyber threats have been identified as a systemic risk to the stability of the European financial system.[2] But cyberattacks tend to be underreported.[3]

Against the backdrop of an evolving cyber threat landscape where the risks continue to grow, the Euro Cyber Resilience Board (ECRB) offers a unique forum that brings together pan-European financial infrastructures, their critical service providers, central bank overseers and other key European authorities for strategic discussions on cyber risks. It enables the sharing of sensitive information in a trusted environment, contributing to the resilience of the European financial system.

Just last week a social media account of the US Securities and Exchange Commission was compromised and an unauthorised post was published.[4] As you are no doubt aware, this led to a temporary increase in the price of crypto-assets, especially bitcoin. While it was not a particularly large-scale or complex cyberattack, this example shows that cyberattacks can be used to manipulate market narratives and prices for financial gain. In a world where news and social media can have large real-time impacts on financial markets, the damage can be significant.

In this context, having a forum like the ECRB is very beneficial. It enables its members to combine their cybersecurity efforts for their own benefit and that of the wider financial ecosystem.

By observing the latest trends in cyber threats and what is driving them, we can better anticipate future threats. This is why we have the ECRB's Cyber Information and Intelligence Sharing Initiative (CIISI-EU).

And by sharing best practices and measuring ourselves against common standards, we can better protect the security and integrity of the financial system. Collectively, we are better equipped to deepen our understanding of cyber threats, defend ourselves against them and minimise their possible impact.

In my remarks today, I will briefly discuss the current cyber threat landscape, the potential impacts of new technologies and our approach to assessing and closing gaps in cyber resilience.

The current cyber threat landscape

The ECRB has long cautioned that cyber risks are coming ever closer to the core of the financial system. We have seen sporadic major cyberattacks on financial institutions or their service providers,

resulting in disruption to both the financial system and the real economy. And cyber threats overall have become more aggressive. For instance, we are seeing an increasing number of cyberattacks that attempt to disrupt services or attain unauthorised access to data and services, including ransomware attacks.Geopolitical conflicts are also leading to a further rise in cyberattacks. These developments underline the need for continuous investment in cyber resilience.

Let me highlight two major threat areas.

First, ransomware attacks, such as the recent attack on the Industrial and Commercial Bank of China that disrupted trades in the US treasury market.[5] This demonstrated the need for international cooperation against ransomware attacks, which are a global threat. Such cooperation is necessary to make the business model of criminals unattractive, by making attacks more risky and less profitable.

This is the objective of the International Counter Ransomware Initiative[6], which brings countries together to fight against ransom payments. Given the role of crypto assets as the payment method requested by ransomware attackers, countering ransomware will also require developing effective crypto-asset seizure regimes. Empirical evidence indeed shows strong correlation between cyber risk exposure, investor attention to crypto and the price of bitcoin.[7] This creates a doom loop between cyber risk and crypto valuations. Higher cyber risks raise crypto demand expectations, pushing crypto prices up. In turn, higher crypto prices boost the incentives and resources for ransomware attacks.

Second, financial entities need to put robust risk management practices in place to account for their increasing use of outsourcing and their high dependence on third-party service providers. Such practices are set out, for instance, in the guidance on managing supply chain risk recently provided by the Financial Stability Board.[8]

Over the past year the ECRB has placed particular emphasis on this topic, calling on financial entities to perform due diligence prior to contracting a service provider, to identify and manage all their critical service providers, and to monitor interconnections along the supply chain. Turning to authorities, central bank overseers require financial market infrastructures to identify, assess and manage interdependencies stemming from third-party service providers and oversee critical service providers. The new EU regulation on digital operational resilience – DORA – contains requirements for critical ICT third-party service providers and for the creation of a pan-European forum to oversee these providers.[9]

We are also dependent on utility providers, like energy companies, telecommunications firms or water suppliers. While they are not considered third-party providers as such, we all have a clear interest in the smooth operation of critical infrastructures. We can support their cyber resilience by sharing tools they may find useful. For instance, the TIBER-EU framework simulates cyberattacks, under real-life conditions and in a controlled manner. Some utility providers have made use of the framework already.

The impact of new technologies on the cyber threat landscape

New technologies provide opportunities to support and improve our cyber resilience, but they can also pose challenges for cyber security.

For instance, artificial intelligence (AI) can be used for sophisticated cyberattacks, with malicious actors leveraging its potential for social engineering, reconnaissance and exploitation. Attackers may even be able to reverse-engineer AI models, circumventing their guardrails and utilising them with malicious intent to conduct successful operations. Malicious AI tools have already been designed to assist users in carrying out criminal cyber activity. We can expect these types of malicious tooling to become more advanced as attackers become more sophisticated in their use of AI and the technology evolves further. At the same time, AI can help increase cyber resilience and counter cyberattacks, including AI-generated attacks. For example, AI can support threat intelligence in collecting and analysing data. AI can also help prevent and detect cyberattacks by identifying anomalies in user, system and network behaviours in real time.

The development of quantum computing is another example. Quantum technology holds the promise of vastly expanding computational power and opening up new ways of communicating. While predictions about the availability and impact of quantum technology vary, the effect it may have on cybersecurity deserves special attention and awareness. For instance, it may be able to break the cryptography algorithms currently used for communication and data protection. Discussing post-quantum cryptography environments within the ECRB will help us understand the opportunities and risks.

Identifying potential weaknesses to more effectively mitigate cyber risks

The Eurosystem regularly conducts cyber resilience surveys of financial market infrastructures, in which many ECRB institutions participate. This enables the cyber resilience of each entity to be assessed and helps gain an overview of progress and the remaining vulnerabilities across the sector. The findings at the individual level are discussed and followed up by the entity and its respective central bank overseer. One common outcome that can be derived from the survey is the correlation between good governance and strong cyber resilience of an entity. A good understanding of cyber risks at board level translates into better-informed decision-making and leads to the allocation of the resources needed.

The survey also revealed a correlation between high cyber resilience and red-teaming exercises like those provided by TIBER-EU. Such exercises shed light on the entity's cyber resilience, allowing it to mitigate any identified gaps in its defences in a very tailored manner. The ECB, together with the TIBER community of authorities, is engaged in a high number of tests and facilitates an active exchange to further develop testing tools and promote their use by all stakeholders.

Besides cyber resilience surveys and red-teaming exercises, stress tests and cyber resilience exercises play a crucial role in identifying and closing potential gaps and weaknesses. In 2024 the ECB will stress test 109 directly supervised banks on their cyberattack response and recovery capabilities, based on a scenario of a successful cyberattack that disrupts their daily operations.[10] Similar cyber resilience exercises for financial market infrastructures have been run in the past by the Eurosystem and further exercises are being prepared. These efforts reinforce each other.

A key element of cyber resilience is the reporting and disclosure of cyber incidents by infrastructures and entities in the financial sector as well as other critical sectors. Considerations about the impact on

reputation and customers' or investors' trust may naturally be at play but should not influence incident reporting requirements according to the relevant oversight and regulatory frameworks.[11] Indeed, any underreporting of incidents may worsen the impact and undermine the containment of a cyberattack. In this context, it is also important to have precise plans for disclosing incidents to relevant stakeholders in the ecosystem and for communicating to the public. In addition, trusted groups, like CIISI-EU for ECRB members, help entities analyse and learn from cyber threats and incidents and prepare better plans to avoid contagion. This is a formula that may also be used in other critical sectors.

Conclusion

Let me conclude.

Financial market infrastructures are networks that mitigate risks but can also become a source of systemic risk if they malfunction. The increasing threat of cyberattacks and the damage and disruptions they can cause emphasise this clearly.

Our financial system is only as strong as its weakest link. In other words, cybersecurity is our common good and it leaves no room for compromise: we need to remain one step ahead of attackers. To achieve this, we need to take a system-wide approach and continuously work together.

The ECRB is a major part of this effort, offering a space for trustful sharing of information, practices and techniques that increase our common and individual cyber resilience. At the same time, central banks and authorities work together at international level in close collaboration with the industry, as cyber risk is not a local or regional phenomenon, but a global threat.[12]

As the new chair of the ECRB, I look forward to working on these challenges and improving our common cyber resilience. The information we will share with each other today and the further progress we will make will help strengthen the cyber resilience of Europe's financial sector.

1.

Jamilov, R., Rey, H. and Tahoun, A. (2023), "The Anatomy of Cyber Risk", *NBER Working Paper Series*, No 28906, National Bureau of Economic Research; Dreyer, P., Jones, T.M., Klima, K., Oberholtzer, J., Strong, A., Welburn, J.W. and Winkelman, Z. (2008),"Estimating the Global Cost of Cyber Risk: Methodology and Examples", *Research Reports*, RAND Corporation.

2.

European Systemic Risk Board (2020), *Systemic cyber risk*, February.

3.

Amir, E., Levi, S. and Livne, T. (2018), "Do firms underreport information on cyber-attacks? Evidence from capital markets", *Review of Accounting Studies*, Vol. 23, pp. 1177-1206 .

4.

Financial Times (2024), "Bitcoin swings sharply after false claim that SEC approved ETFs", 10 January.

5.

Financial Times (2023), "Ransomware attack on ICBC disrupts trades in US Treasury market", 10 November.

6.

The White House (2023), "International Counter Ransomware Initiative 2023 Joint Statement", 1 November.

7.

Jamilov, R., Rey, H. and Tahoun, A., op. cit.

8.

Financial Stability Board (2023), *Enhancing Third-Party Risk Management and Oversight – a toolkit for financial institutions and financial authorities*, 4 December.

9.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

10.

ECB (2024), "ECB to stress test banks' ability to recover from cyberattack", press release, 3 January.

11.

National Cyber Security Centre (2023), "Why more transparency around cyber attacks is a good thing for everyone", *NCSC blog*, May; Daniel, M. (2023), "Reporting Cyberattacks Will Soon Be Mandatory. Is Your Company Ready?", *Harvard Business Review*, 19 April.

12.

For international cyber resilience standards and initiatives, see the ECB's website.