Benoît Cœuré: Cyber resilience for financial market infrastructures

Speech by Mr Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the workshop on the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, Frankfurt am Main, 13 January 2016.

* * *

Ladies and Gentlemen,

Let me start by expressing my appreciation to the European System of Central Banks' Payment and Settlement Systems Committee for taking the initiative to organise this workshop on cyber resilience and to the representatives of other authorities and the financial market infrastructures (FMI) community for coming here today to discuss with us this very important topic in the international agenda.

Financial stability usually conjures up questions about capital and liquidity and the network of financial exposures and interdependencies that make up the financial sector. But the sector is an operational network too. On a daily basis it delivers financial intermediation between market participants and end users, whether the transmission of salaries and other payments from one bank account to another or the settlement of market transactions through a web of settlement banks, clearing houses, settlement systems and custodians. As overseers of FMIs, we need to ensure that each of the nodes in this network is operationally resilient and in a position to provide the services that are important to the system as a whole.

We also need to ensure that where disruptions do occur, firms can continue to operate or recover quickly, minimising any adverse impact on the functioning of the system as a whole.

FMIs play a critical role in promoting the stability of the financial system, and the world in which they operate is evolving and changing rapidly. Computing and digitalisation are becoming increasingly pervasive and enhancing nearly all aspects of personal life and business, creating more opportunity for innovation, but also more and more threats. Industry leaders and authorities alike consider cyber risks as a top priority.

And so, what about cyber risk? Well cyber presents new challenges. It is not a game against nature. Unlike other causes of operational disruption like fires and floods, we know there are agents out there – criminals, terrorist organisations – that have the will, if not necessarily the means, to attack and exploit the system. Motivations vary. More often than not they are economic – to defraud banks or their customers or to extract information. But we have seen cases where the motivation is to damage the system, either to destroy data or cause non-availability of systems or both. The capabilities of these actors, and thus the nature of the threat, are rapidly evolving – barriers to entry are low in cyber space and attacks are readily scalable. Low level attacks are now not isolated events but continuous. Unlike physical attacks that are localised, these attacks are international and know no boundaries.

Add to this, ***the cyberattack surface is rapidly growing***:

- in 2015, there were 3 billion digital users, and by 2019, this will increase to 4 billion;
- in 2015, there were 3.3 billion smartphone connections, which will increase to 5.9 billion in 2020;
- in 2015, there were 16.3 billion IP-connected devices, which will increase to 24.4 billion by 2019;
- and it is estimated that network traffic will more than double from 2015 to 2019.

The routes for exploitation and potential disruption are therefore clearly increasing.

Furthermore, the ***threat to FMIs is increasing***. FMIs represent critical infrastructure to the financial system. In a recent survey on critical infrastructures, more than 70% thought

cybersecurity threats to their organization are increasing; and 48% found it likely that a cyberattack will take down their critical infrastructure.

Cyber defence as a result has become not a matter of designing a hard perimeter that can repel attacks but detecting where networks have been penetrated and responding effectively where this occurs. As it changes and multiplies, cyber is elusive, hard to define and to measure.

It is clear that the risk is on the rise and a growing cause of concern to industry and authorities alike. It is within this context that the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) joined their efforts in developing the ***Guidance on cyber resilience for financial market infrastructures*** which you will discuss today.[1]

From the outset, this guidance is aimed towards financial market infrastructures, overseers, supervisors and authorities, making it clear that our response to cyber risk must be a collective and united effort, based on a partnership model. This is why on the side of CPMI and IOSCO we seek the views of the industry through a public consultation, and hence this workshop is an important opportunity to bring us all together for some shared reflections during the consultation period.

The CPMI-IOSCO Guidance is the first set of internationally agreed principles in the field of financial markets and institutions to support consistent and effective oversight and supervision in the area of cyber resilience. It is a real achievement and it is setting the standard for other committees. It will be important that going forward, other authorities, committees and market sectors approach cyber standards and guidance in a harmonised manner, to ensure that there is no duplication and inconsistency, and to ensure that there is cross-fertilisation and evolved collective learning.

Within this context, events like the one today is vital, and we must ensure that all the relevant stakeholders remain involved and work together, as cyber threat recognises no border and stakeholder. It is a risk to us all, and only through such events will we increase the common understanding and approach, and begin to address the risks.

In this regard I would like to emphasise to the FMI community that it is important that you ***support the CPMI-IOSCO work and respond to the public consultation*** with your comments, observations and ideas regarding the Guidance within the February deadline. We want your views, as from the outset, I have stated that this is a collective journey, one of partnership.

Thank you for your time, and let us work together in 2016 to enhance cyber resilience at EU level and beyond.

---

[1] See: CPMI-IOSCO consultative paper "Guidance on cyber resilience for financial market infrastructures", November 2015, https://www.bis.org/press/p151124.htm. See also CPMI, "Cyber resilience in financial market infrastructures", November 2014; and IOSCO, "Cyber-crime, securities markets and systemic risk", Staff Working Paper, July 2013.