WGCR round table

14 September 2018

Remarks by François Villeroy de Galhau,

Governor of the Banque de France

Key notes

Press contact: Mark Deen (mark.deen@banque-france.fr).

Ladies and Gentlemen,

Cher Benoît, Cher Jean-Paul,

Welcome to Paris,

The guidance released by CPMI-IOSCO two years ago was one of the precursors in the field of cyber risks. Since then, the level of cyber-threats has obviously increased. According to different public reports, the number of cyber-attacks (700 million in 2017) has increased by over 100% in two years.

This is why cyber security will be one of the priorities of the G7's French Presidency next year. I would like to share with you three considerations and put forward three concrete measures so that these principles do not remain at the conceptual level but actually lead to tangible actions.

**

I. Three considerations, or three S's: Silos / Security of Systems / Speed

1) The first is of a general nature. Considering that "security is a block", we need to explore how **to break the *silo* within the financial sector**, which does not take account of the multiplicity of its stakeholders: the CPMI-IOSCO principles rightly emphasise the need to take into account interconnections, meaning the link between FMIs, between FMIs and their service providers and suppliers. Nowadays, we should also take into account, alongside regulated and supervised participants, the existence of **Fintechs**, as well as "**big techs**". They are indeed service providers, usually unregulated, vulnerable to cyber risks and, in some cases creators of the most powerful new technologies, which could significantly contribute to spreading risks (application programming interfaces (API), artificial intelligence software, cloud computing structures, etc.). The lack of substitutability of some of these services increases the vulnerability of the financial sector.

2) The second consideration regards **the embedding of *security in systems* from the earliest stages of conceptualisation**. The CPMI-IOSCO guidance refers to this principle as "resilience by design". It makes perfect sense, since it is the most efficient way to ensure the security of IT systems. This principle is however no doubt difficult to implement in the case of urgent and costly IT projects. This is why it requires a more proactive approach from executives and closer attention from regulators and supervisors. The same principle has already been emphasised in the European General Data Protection Regulation which entered into force some months ago. It gives us one more reason to enforce this principle.

3) The third consideration regards ***speed***: **the capacities to resume critical activities within two hours after a cyber-attack**, the two-hour Recovery Time Objective mentioned by Benoît. In this regard, in today's environment it would be both unrealistic and unwise to resume activities without ensuring first that IT data have not been corrupted or that recovery of the activity affected does not trigger a higher risk exposure on its own, and for the whole financial ecosystem.

II. Three short-term concrete measures

Now, I would like to share three initiatives that the Banque de France is striving to encourage:

1) Promoting a homogeneous approach to conducting penetration tests among various players in the financial sector. From this perspective**,** the TIBER-EU framework that the ECB provided earlier this year is a tool that would be helpful to implement in order to test the resilience of the financial system and especially the capacity of cross-border companies. In this respect, TIBER-EU will have to be rolled out at the national level, especially for testing market infrastructures, while taking into account specific local aspects and respecting core requirements in terms of responsibilities, risk management and the conduct of the tests. Through "coordinated frameworks" it will therefore be possible to achieve the much-needed harmonisation of practices and a mutual recognition of tests across the European Union.

2) Carrying out simulation exercises in the particular context of extreme but plausible cyber-attack scenarios, possibly including cross-border exercises. Against the backdrop of the rising number of cyber-attacks in the financial sector, there is a need to supplement on-site and off-site supervision, beyond merely conducting response exercises at domestic level, and possibly even across many countries at the same time.

The G-7 has given priority to the enhancement of cross-border coordination in the event of a significant cyber incident: the Banque de France chairs the sub-group in charge of preparing and performing this exercise in 2019. Such an initiative could usefully be extended to include similar simulation exercises at the domestic level, and even across many countries at the same time. This would help to meet the following objectives:

(i) assess the degree of **preparation** of all stakeholders, namely financial institutions as well as public authorities;

(ii) be sure of their capacity to implement common and consistent measures in order to **restart operations** after a cyber-attack;

(iii) test dedicated crisis **communication tools**.

3) Monitoring the degree of cyber security and the progress of cyber resilience programmes. Irrespective of the nature of our organisation (a central bank, a commercial bank, an insurance company, a FMI), we have to not only deal with a large number of cyber security issues, but also to coordinate a large number of stakeholders (boards, senior executives, Chief Information Officers, Chief Risk officers, Chief Information Security Officers, etc.,).

Therefore it is of utmost importance, but at the same time difficult to obtain an **overview** of cyber security. All levels of management (technical, operational and executive) need to have appropriate information to monitor cyber resilience and cyber risks. Above all, monitoring cyber security at the **executive level** ("tone at the top") may prove to be challenging. Of course, there is a broad range of different metrics and it is necessary to select a limited number of them. For instance, if I had to mention three of them, I would choose:

(i) overseeing the **development of awareness and training** within the organisation;

(ii) monitoring **patch management** in order to make sure that identified flaws are corrected in due time;

(iii) and, last but not least, capturing the **effectiveness of the identification and authentication processes**.

In a nutshell, key indicators help to improve the governance of the IT security system.

**

To conclude, I believe that it is necessary to better structure the **international governance** of cyber security in the financial sector: it is clear that the different regulatory and supervisory authorities are aware of "cyber risks". This is becoming apparent through the numerous initiatives at various levels (domestic, European, and international). While this is welcome, it is both delicate but necessary to strengthen international cooperation in order to ensure that there are neither loopholes nor overlaps and that there is convergence towards proposals and solutions that can easily be shared with others.