Robert Ophèle: Cyber security in the financial sector

Opening speech by Mr Robert Ophèle, Deputy Governor of the Bank of France, at the Conference "Cyber security in the financial sector", Paris, 17 June 2014.

* * *

Emmanuelle Assouan, Frédéric Hervo, Claudine Hurman, Caroline Keribin, Clément Martin and Axel Petitprez have also contributed to the preparation of this speech.

Ladies and gentlemen, I am very happy to introduce this conference about cyber-security in the financial sector. This issue could be considered in the first place as very technical, the type of issue that has to be addressed only within a limited forum of experts. This would be an error and on the contrary, it is key that public authorities, including central banks, dedicate sufficient attention to cyber-security, given its system-wide implications notably for the functioning of the financial system.

Over the past decade, the financial sector has changed considerably with the emergence of the Internet and the use of new information technologies. The market has been able to innovate and improve the quality, the performance and the efficiency of services such as online banking, mobile payments, and settlement platforms. Public authorities have indeed encouraged dematerialization in the financial sector to foster economic growth and also to reduce the operational risks inherent in previously non-automated processes. For example, the new European regulation on *Central Securities Depositories* requires using dematerialized securities and promotes automated and straight-through processes in securities settlement systems.

In this sense, ***technological evolutions have allowed to address some of the operational risks inherent to financial activities***, especially to curb operating errors in processes (representing a significant source of losses relative to operational risks). From this point of view, cyber-activities are a source of economic growth and progress, being essential for the financial sector.

However, despite the fact that internet development and electronic transactions growth allowed a better control of operational risks due to diminishing human or operating errors factors, it also triggered ***the emergence of new risks***. The rapid expansion of networks and technologies, the opening of IT systems to external exchanges, the growing amount of electronic transactions have caused the emergence of a new type of crime called "Cybercrime".

The financial sector is indeed an attractive target for cybercriminals: an American study[1] led by Symantec shows that the finance and insurance sector is among the principal sectors affected by cyber-attacks, just behind Public Administration. This of course has not remained unnoticed by supervisory authorities which have taken already a number of steps to help the industry address the issue but in so doing face a number of difficult issues.

I. Indeed guidance from supervisory authorities, like the Guidance on operational risk issued by the Basel Committee, published in 2011[2], point out that prevention and proper management of this risk is a financial stability issue to the extent that operational failures can be a source of systemic risk.

---

1 Internet Security Threat Report 2014 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

2 "Principles for the sound management of operational risk", BCBS 2011.

This systemic risk derives first from the dramatic development of interdependencies across financial intermediaries due to increased automation in financial activities, including in clearing and payment activities, which are a major vector of interconnection.

The systemic risk also derives from the possible loss of confidence from the general public in electronic payments that would be triggered by a failure to protect ***the integrity and reliability of data processed by these payment systems***.

However, ***responses to cyber threats can conflict with other established priorities***. This is particularly true for financial market infrastructures. For instance, the principle 17 of the CPSS-IOSCO on operational risk clearly states the business continuity requirements for financial market infrastructures. Business continuity plans should aim for the timely recovery of operations, resuming operations within two hours after disruption, and settlement should be ensured before the end of the day in extreme conditions. However, meeting this requirement is raising specific challenges in case of a cyber-attack or in case data is found to be corrupted, when the highest priority might no longer be a swift resumption of operations, but to first recover the quality and integrity of data in order to avoid any risk of contagion.

This is also true for the access that could be granted to third parties for accessing online a payment account in order to assist in the initiation of payments. Such an access could foster competition and innovation in the payment industry but would obviously multiply the risks of cyber-attacks.

In addition, there is a need to strike the right balance between the requirement to adequately prevent and address the cyber threats and the need for financial players to implement solutions that are economically viable. For instance, implementing a dual contingency software may be an efficient answer to some cyber attacks but does not go without costs.

Finally, ***cyber-security is also a global issue***: for a more effective response, it is necessary to establish cooperation at an international level and across sectors, well beyond the financial sector. In that perspective, initiatives from the Financial Stability Oversight Council (FSOC) in the US to improve cooperation between sectors, particularly those dependent on the financial sector, such as the utilities or telecommunications sectors, or the establishment of *European Network and Information Security Agency* are much welcomed.

II. Against that background, understanding the threats, organizing protection and prevention as well as the coordination of the private and public actions are pre-requisites for effectively fighting cybercrime. The aim of today's seminar is to reflect collectively on this and to share experience.

The first important step is to understand why the financial sector is a popular target of hacker attacks. That's one of the objectives of the first panel of distinguished speakers. They will attempt to answer such questions as: What are the factors making the financial sector a privileged target for cybercrime? How to identify and quantify cyber-attacks? What impacts of cyber-criminality on financial stability?

There is one question we must pay particular attention to: the virtual currencies. Recent operations against financial criminality have evidenced that new payment methods using the internet, and linking the virtual sphere with the real sphere, are a privileged way for cyber criminals to launder money. Virtual currencies have indeed recently drawn attention from authorities and from central banks in particular. Designed as alternatives to official currencies but with no guarantee of reimbursement, they cannot be classified as currencies because they lack legal tender and therefore do not infringe the central banks' monopoly in the issuance of money. However, although they currently do not pose a significant threat to financial stability, they do pose serious questions in terms of money laundering and can be perceived as vehicles for speculative investments. Virtual currencies therefore bring challenges to authorities when it comes to regulating them. Our speakers on the virtual currencies topic could address such questions as: should the use of virtual currencies be prohibited to protect us from cybercrime and the expansion of money laundering or

terrorism? Or is it better to set out the legal, regulatory and ethical issues of the virtual currencies?

A round table dealing with financial sector solutions to curb new cybercriminals' strategies will follow. To what extent do current guidance and principles deal with the threat of cybercrime? Can cybercrime be effectively deterred or only defended against? Have financial institutions taken structural and technological efficient steps to improve their cyber defense? Is cyber-crime insurance effective and how is it pricing the risk? What type of public communication to we need to fight those new threats? We expect such important questions to be addressed in this context.

Besides, overseers and supervisors should ensure that at an individual level, risk management is efficient. A normative framework has been established set up by European institutions to fight cybercrime and ensure the robustness of the financial markets (in particular through the adoption by the European Parliament of the Network Information Security directive); a BIS committee, the CPSS, is currently reflecting on cybersecurity for market infrastructures. Two prominent speakers will share their views on whether the existing regulatory framework provides sufficient guarantee against cybercrime.

Lastly, as a central bank it is of utmost importance to make sure that the marketplace is resilient when facing cyber-threats. The purpose of the last roundtable should be to assess to what extent financial centers resilience should evolve under the influence of cybercrime threats: do increasing cross border interdependencies between financial centers (use of common market infrastructures, existence of international financial actors and cross border providers) call for an international approach? Should a multi-sectorial approach also be worth reflecting on as reliance on common service providers (such as telecoms) create a large community of interest when cyber-security is at stake? This (I hope so) should largely echo Banque de France's priorities, which are to nurture a cooperative and coordinated approach for the Paris financial center robustness and to verify through collective stress testing that individual continuity plans are coherent all together and well adapted to ever evolving threats

Finally, to conclude – and I will stop there –, I would like to draw your attention on 2 points:

First, Banque de France considers indeed as a priority that actions should be coordinated internationally, as global interdependencies are growing.

Second, solutions should emerge from the industry itself and regulation should only be used only in case of market failure. Best practices to enhance cyber-security should be identified and adopted by the various actors. Central banks could be of some help in this process; as an example, Banque de France has for many years recommended the implementation of strong authentication to protect online payments. This efficiently defeats numerous attacks.

I thank you for your attention and wish you fruitful and vivid discussions on all of these aspects, hoping this conference will provide you with a comprehensive overview of the stakes of cyber security and responses to cyber threats. I now give the floor to Dr. Steve Purser.