Sabine Lautenschläger: Cyber resilience - a banking supervisor's view

Statement by Ms Sabine Lautenschläger, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the Single Supervisory Mechanism, at the High-Level Meeting on Cyber Resilience, Frankfurt am Main, 19 June 2017.

* * *

This week I learnt that the first computer virus dates back to 1971. It spread via the ARPANET, which was a precursor of today's internet. The ARPANET connected about two dozen universities and government hosts in the United States. The virus had been written for experimental purposes and was not malicious. It just displayed a simple message on infected computers: "I'm the creeper: catch me if you can".

Things are a bit more complex today, and the outcome of cyber incidents much worse: they can disrupt business, cost a lot of money and destroy reputations. And indeed, the potential for damage is great, as so much relies on IT and so much happens online – the financial sector is a case in point. As you all know, banks have always been attractive targets for criminals.

Although the damage has been limited so far, we banking supervisors take cyber risk very seriously. And we insist on banks doing the same.

Cyber risk has been a priority for ECB Banking Supervision from day one. In 2015, we established a working group that had three goals. First, to get an overview of how supervisors deal with such risks both at national and international level. Second, to get an overview of how prepared banks are for cyber risk. And third, to propose to the Supervisory Board a strategic direction and a dedicated work plan on cyber risk.

We have learnt a lot over the past two years. And we have used it to address this risk from several different angles.

For us, one of the first steps was to establish a cyber incident reporting framework. We conducted a successful pilot phase in 2016. And now we will implement a long-term solution for all those banks that we directly supervise. As from this summer, they will be required to report all significant cyber incidents. This will help us to assess more objectively how many incidents there are and how cyber threats evolve. It will also help us to identify vulnerabilities and common pitfalls.

In addition to our ongoing supervision we also perform thematic reviews on cyber security and IT outsourcing. These reviews help us to assess the risks facing each bank as well as the risks that might affect the entire sector. And they also help to raise awareness of cyber risk at Board level.

The insights that we obtained in 2015 and 2016 were applied in three ways. First, they informed a dedicated section in our methodology for on-site inspections. Second, they were used to create new analytical tools for our off-site supervisors. And third, they were used to produce a cyber risk profile of each bank.

So we are working to obtain a comprehensive picture of what is happening out there. But how to deal with cyber risk?

Well, the World Health Organization says that the best way of stopping diseases from spreading is basic hygiene: washing your hands. And the same is true for IT. Basic IT "hygiene" can take banks a long way. Have the latest updates been installed? Are passwords strong enough? Have backups been made and their restoration tested? Such simple things are so important, but often

neglected.

So we are taking a close look at our banks to see whether they are following the relevant standards and best practices. And there are plenty of these; I cannot stress this enough. We also work with the European Banking Authority, the EBA, on how to supervise cyber risk in an effective and harmonised manner across Europe.

As for the euro area, we plan to issue our supervisory expectations on how banks approach IT risks in general. And what we expect clearly goes beyond basic IT hygiene. This will be an important step for two reasons. First, it will help to forge a common understanding of IT risks between supervisors and banks. And second, it will help to ensure a harmonised treatment. To increase awareness and to communicate our expectations, we will organise seminars and discussions with banks.

And we also look beyond the euro area, of course. We cooperate with supervisors worldwide to align priorities and exchange best practices.

To sum up, we take cyber risk very seriously, and we approach it from various angles. My advice to banks is to do the same. It is vital to be alert and ready to react.

Thank you for your attention.