# Sabine Lautenschläger: Towards a more cyber secure financial system - the role of central banks

Statement by Ms Sabine Lautenschläger, Member of the Executive Board of the European Central Bank, at the G7 2019 conference on "Cybersecurity: Coordinating efforts to protect the financial sector in the global economy", Paris, 10 May 2019.

* * *

As we all know, cyber threats to the financial sector are continuously evolving and becoming ever more sophisticated. The attackers – whether they be 16-year old script kiddies, hacktivist groups or even nation states – are dynamic and agile. They have different reasons for targeting the financial sector, but they each have the potential to cause disruption. Besides stealing money and data, they can undermine confidence in the entire financial system.

So what can we, as public authorities, do? As the central banker on this panel, I will, of course, focus on what central banks can do. I will first outline some key trends in the financial sector, which make it vulnerable to cyber threats. I will then share some of the insights gained from the ECB's key initiatives on cyber risk.

## Trends in the financial sector

We see a number of trends in the financial sector related to cyber risk:

- First, the close interconnection and complexity of the financial system creates vulnerabilities which can be exploited by cyber attackers.
- Second, attackers seem to be gaining an ever deeper understanding of how the financial system operates. This enables them to swiftly detect and exploit weaknesses more efficiently and should be a concern for us all.
- Third, both banks and financial market infrastructures are struggling to find staff with the skills and experience needed to fend off cyber-attacks. Indeed, the skills gap extends well beyond the financial sector. All relevant stakeholders need to urgently work on strategies to make sure that our workforce has the right skills for our future economies, and that our society is able to reap the benefits of innovation.
- Finally, true innovation is always disruptive. Fintech might disrupt financial markets in positive ways. But it also comes with risks: fiercer competition could lead some market players to embrace and adopt new technologies, services or methods before fully grasping the related risks – cyber-risks in this case.

Let me point to some information and knowledge we have gathered at the ECB in our banking supervisory function as well as in our oversight function for financial market infrastructures.

We do see room for improvement at banks and financial market infrastructures with regard to cyber governance, for example. Financial market infrastructures, or FMIs for short, too often lack board-approved cyber resilience strategies. And if there is a strategy, it is often not operationalised. And if it is operationalised, it is often not monitored, and its effectiveness is not challenged.

FMIs and banks work diligently on technical security measures in order to detect threats and protect their systems. Some of them, though, neglect people and processes. There is a dangerous lack of awareness and training. Successful cyber-attacks often start with a phishing email to an unsuspecting employee.

Having mentioned the complexity of the financial system as a vulnerability, I need to add the complexity of IT-systems as well. Banks, in particular, should aim to simplify their IT landscape.

Simpler IT landscapes have a smaller attack surface. And the easier these systems are to understand and maintain, the better they can be protected. And, last but not least, we see that a significant number of FMIs still lack dedicated cyber incident response plans.

These are just a few of the worrying trends and vulnerabilities that we see. So there is clearly much work to be done.

**How is the ECB addressing cyber threats? An oversight and supervision perspective**

So, what part can the ECB play?

Let's first look at our role in overseeing FMIs. In March 2017 the Governing Council approved the Eurosystem cyber resilience strategy for FMIs. This strategy is intended to operationalise the CPMI-IOSCO[1] Guidance on cyber resilience for FMIs. The strategy rests on three pillars: FMI resilience, sector resilience, and strategic industry-regulator dialogue.

Regarding the resilience of FMIs, we started in 2017 by conducting a survey of 76 FMIs across the European Union, to assess their cyber resilience. The results of this survey have enabled overseers to enter into productive dialogues with FMIs on their ability to address cyber-threats.

Furthermore, while the principles contained in the CPMI-IOSCO Guidance are important, they are also quite high level. Smaller institutions in particular need to be informed about best practices in a more concrete and detailed manner. So, to facilitate the proportionate implementation of the guidance, the ECB published the Cyber Resilience Oversight Expectations, or CROE for short, in December 2018. A tool for FMIs and overseers alike, the CROE sets out three levels of increasingly demanding expectations, tailored to the size of the FMI.

To complement the CROE, the ECB has also developed another tool: the European threat intelligence based ethical red team testing framework (TIBER-EU). By means of "ethical hacking", red teaming helps to assess a financial institution's ability to withstand a cyber-attack. TIBER-EU serves to guide authorities and financial institutions in conducting threat-intelligence based red teaming, and to avoid duplication through the emergence of similar pan-European tests.

But testing the resilience of individual FMIs or banks may not be sufficient. The financial system is highly interconnected and any cyber-attack could thus trigger contagion. This is why the ECB hosted a market-wide crisis communication exercise, UNITAS, in June 2018. UNITAS facilitated a discussion among pan-European financial infrastructures on a scenario in which a cyber-attack resulted in a loss of data integrity and a knock-on effect on other financial infrastructures. The exercise revealed that there were weaknesses at the European level, which are now being followed-up on by the Euro Cyber Resilience Board for pan-European Financial Infrastructures, or ECRB for short.

This brings me to the third pillar of our strategy, which seeks to foster strategic engagement between regulators and industry. The ECRB was established in 2018 with the aim of facilitating trust and collaboration among FMIs and authorities and encouraging joint initiatives.

Moving on to banking supervision, the ECB Banking Supervision has addressed IT and cyber risk from various angles.

First, we have been conducting thematic reviews since 2015 on the topic in the banks that we directly supervise. These gave us a more detailed understanding of the scope of the problem.

Moreover, the latest horizontal analysis of IT risk conducted in 2018 has revealed deficiencies in IT security risk management at several banks. For instance, banks' general risk management frameworks sometimes fail to specifically include IT risk. A significant number of banks have

critical processes that depend on systems which are close to, or have already reached, their end of life. This, in turn, makes them more vulnerable to cyber threats. We also see a failure to rapidly address critical findings in the area of IT security.

In addition, IT outsourcing is increasing, and many supervised institutions outsource their IT to a single provider. A classic case of putting all their eggs in one basket, this creates a concentration risk that should not go unnoticed. There are cases where these concentration risks cannot be avoided, but this should then go hand in hand with tougher requirements for cyber resilience. Further, the ECB insists that banks should employ enough sufficiently skilled staff to monitor and oversee their outsourced activities.

In 2017, the ECB also set up a cyber incident reporting process. The information on incidents reported by banks is used by the ECB to identify and monitor trends, and to facilitate a fast reaction of the ECB in the event of a major cyber incident affecting one or more significant institutions at the same time.

The number of reported cyber incidents has been rather low, the most frequent type being Distributed Denial of Service attacks (DDoS). Other reported incidents were related to unauthorised access, accidental data leakage and phishing attacks. In many cases, there was a delay between the onset of the attack and its detection. Finally, we see that attackers gained access to banks' systems by exploiting both technological vulnerabilities, such as missing IT security measures, and human ones, such as insufficient staff awareness.

Although the number of reported cyber incidents has been rather low, I would not dare to conclude cyber threat levels are low, or even decreasing. I rather think that it is a matter of time until we experience a major attack.

ECB Banking Supervision will continue to monitor IT and cyber risks facing banks; we will continue to push for and request banks' resilience to and preparedness for cyber threats. And we will of course continue to engage and cooperate with a number of other institutions and agencies.

## Conclusion

Ladies and gentlemen,

As you may guess from my brief remarks today, we have a great deal of work ahead of us. Sharing information, knowledge and expertise among public institutions and with the industry will be essential. In this respect, events like today's have a valuable role to play. I look forward to our discussion.

---

[1] Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions.