Sabine Lautenschläger: Cyber resilience – objectives and tools

In 1903, the Italian inventor Marconi demonstrated his new invention, a wireless telegraph, to a large audience. It didn't go too well for him, though. The machine itself did work in the sense that it transmitted a message. However, it was not the message the audience – or Marconi – had expected. The word "rats" was being sent again and again. The system had been hacked. The culprit in this case was Nevil Maskelyne, a magician. Allegedly, he had been hired by a British wired-telegraph company which was worried that Marconi's invention might ruin its business.

Technology has advanced a lot since 1903. And it has created a deeply interconnected world. The financial system is a case in point. No financial institution can survive, let alone thrive, on its own. No bank can do without the complex web of financial market infrastructures that underpins its day-to-day business. No bank, therefore, must underestimate the associated risks. In particular, no bank must underestimate the IT risks, which include cyber risks. In the worst case, a single hack could compromise the entire system. So cyber resilience is a goal we all share. And anyone who sees it as just another competitive advantage is mistaken; the whole chain is only as strong as its weakest link. And in that sense, many actors in the financial system are parts of the same chain.

ECB Banking Supervision takes cyber resilience very seriously. Naturally, we focus on banks and on the euro area. In doing so, we take into account that banks are not just connected among themselves but also with other market participants and infrastructures. This means that our supervision of IT risks also covers the end-points of payment systems and market infrastructures in the banks directly supervised by us. In short, we aim to ensure the availability, confidentiality and integrity of banks' data and systems.

What have we done so far and what are our plans for the future?

- So far, we have conducted thematic reviews on cyber risk and outsourcing. One result is stating the obvious: there is some concentration in terms of companies to which banks outsource IT functions. Apart from concrete bank-specific findings, the reviews have helped us to get a better idea of the risks. And they have made banks more aware of them.
- We have conducted a stocktake on how IT risks are supervised outside the euro area. This helped us to identify best practices; and it will help us to define our own supervisory expectations. Work is ongoing as part of our contribution to the work programme of the European Banking Authority, the EBA.
- We have conducted quite a few on-site inspections into IT and cyber risks, using state-of-the-art methods. Looking ahead, our aim would be to have such inspections every three or four years for large banks.
- We have set up a reporting framework for cyber incidents. Since

mid-2017, banks have been required to report significant cyber incidents. This will help us to quickly react in a crisis and make us aware of common vulnerabilities.

Drawing on guidelines from the EBA, we have developed comprehensive IT risk self-assessments for the banks we supervise, including an extensive section on IT and cyber security. The results of these assessments will feed into our Supervisory Review and Evaluation Process, in which we will also challenge the information provided by banks. We will do so as a result of our insights from on-site inspections and from reports of cyber incidents. The information collected will then serve as a basis for a thematic review of IT risks. This review will give us a better idea of the overall IT risk landscape in the banking industry. It will allow us to identify blind spots early on and define areas which we need to investigate further; this will eventually feed into our plans for 2019. In addition, the review will also help us to compare banks. Partially anonymised feedback could then be shared with them.

Ladies and gentlemen, there is one thing we need to keep in mind. Right from the start, hacks gained a lot of attention, while preventing them did not. In finance, as in many other fields, it is mostly just mundane work that helps to keep things safe. I wonder whether cyber risk is as unique as we are inclined to believe. I have no doubt that we need to take it seriously and that we need to work towards making banks more resilient. In doing so, we should also welcome new ways of tackling cyber risk, of course. But this I would like to do within the existing framework of banks' risk management. Cyber risk needs to be part of general risk management procedures, of general crisis management, and general business continuity planning. After all, it is an operational risk. And our experience in dealing with operational risks can help us to cope with cyber risk as well.

We must keep in mind that cyber risk does not invariably arise from the technology itself but also from how we use it. It is people who are behind the hacking. And often, it is people who leave doors unlocked and gates wide open for cyber criminals to sneak in. People play a big role when it comes to cyber resilience. Thus, it makes sense to draw on the principles we have established for risk management and governance, and on the experience we have gained in these areas.

Ladies and gentlemen, I am aware that this kind of work is unlikely to capture the public's attention in the same way as Mr Maskelyne did in 1903. But it needs to be done. While cybercrime may have an aura of mystery and power, cyber resilience is quite the opposite: it calls for vigilance and diligence, day in, day out.

Thank you.