BANCO DE ESPAÑA
Eurosistema

25.05.2023

Keynote speech

IIF Cybersecurity Roundtable

Ciudad Financiera Santander/Boadilla del Monte (Madrid)

Mercedes Olano
D.G. Supervision

Good afternoon, and thank you very much for inviting me to be here. It is a pleasure to join such an impressive group of experts to speak of cybersecurity. Let me clarify that I am not an expert myself, but I can assure you that this topic is one of the top priorities in our supervisory activities for both, SIs and LSIs.

Everyone agrees that nowadays banks' digital transformation is key to underpinning their profitability, efficiency and new business activities. Moreover, it is the only way to ensure that banks remain competitive in the new environment, and can offer their customers personalized services in an agile, efficient and innovative way.

While the financial sector has always been keen to adopt new technological solutions, the current speed of digital transformation at financial institutions is unprecedented. Changes in customer expectations, greater competition within the sector and also with new actors offering financial services, and the pace of technological development have significantly accelerated this transformation. But it comes at the price of huge investment and the increase of risks associated with the large-scale use of technological solutions.

- Clearly, increasing digitalization also entails greater ICT[1] and cyber risks. Not only due to the rise of malicious attacks against financial institutions and their customers, but also due to the huge complexity of institutions' ICT systems that makes it challenging to maintain an adequate control environment. This situation increases the likelihood of operational mistakes. The coexistence of llegacy applications and innovative technologies is sometimes difficult. Even more if this situation results from significant transformation processes as well as from the various mergers and acquisitions that have taken place in the Spanish financial sector. A direct consequence of this complexity is that banks need to introduce changes in their technology on a daily basis, whether these are security patches, infrastructure upgrades or new applications and tools, and this high level of continuous modification is an additional factor of instability. Indeed, some of the most severe disruptions we have seen in the last five years were not caused by successful attackers but by small changes that went wrong.

- Another risk factor results from the institutions' increasing reliance on specialized third parties, very often involving a multi-level supply chain, that makes operational risk management an even more challenging affair. In order to carry out their digital transformation processes, and have access to the technological innovations that can best contribute to their business, financial institutions complement their capacities by procuring external services. Just to give you some numbers, between 2016 and 2021 we received and reviewed 159 notifications of potentially critical or important ICT outsourcing contracts from our LSIs. But this seems to be the tip of the iceberg. A further analysis revealed that, in the same period, our LSIs had indeed engaged in more than 800 potentially critical or important outsourcing arrangements, even if they had not been notified. As you can see, the use of external third parties is massive and it has an increasing trend.

[1] Information and Communication Technology

> Moreover, some of these providers have become systemic and the incidents affecting them, including unintentional ones, may have an impact on the sector as a whole. Some of the big names will immediately come to your mind, but we should not forget that there are less well-known niche providers and other third-party dependencies not duly identified, arising from successive sub-contracting along the outsourcing chain, that may also pose risk. For this reason, the cyber security of third parties has become a growing concern for authorities and institutions.

Having highlighted the relevance of cybersecurity, today I would like to go even beyond it and refer to the broader concept of "resilience". The Basel Committee[2] has defined "operational resilience" as the ability of a bank to deliver critical operations through disruption. And the Financial Stability Board[3] defines "cyber resilience" as the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. This last definition encompasses both the cyber security component, which is more preventive, and the business continuity component, which focuses on response and recovery when incidents occur. And let me emphasize that when we speak of cyber resilience we need to have a holistic approach which does not focus exclusively on managing technology, but grants the same importance to persons and processes within the organisations.

Allow me to go even a bit further: given the strong dependence of the financial sector on technology, its appeal to attackers with different motivations, the high degree of interconnectedness among its members and its high sensitivity to participants' loss of confidence, cyber incidents have the potential to not only impact individual institutions, but also amplify their impact to an extent that could jeopardise financial stability. For this reason, improving the financial sector's cyber resilience is key for preserving financial stability and this is why it has become a priority for financial authorities worldwide. Definitely, as we have said, for Banco de España and for the SSM it is a top priority.

This global concern on cyber resilience has led to the emergence of numerous fora for debate in the industry and among authorities, and to a significant regulatory and legislative effort. At European level, we can mention the EBA guidelines on ICT and security risk, and the EBA guidelines on outsourcing.

And, of course, we need to mention the new Digital Operational Resilience Act, the well-known DORA, whose declared goal is "to mitigate the risks of digital transformation in the EU financial sector by establishing a common framework for enhancing digital operational resilience". This piece of legislation contains provisions for institutions on technology risk management, incident management and reporting, digital resilience testing, third-party risk management and information sharing.

Apart from that and with the objective of addressing the increasing dependency of the financial sector on third party services, DORA establishes a novel framework for the direct

[2] BCBS Principles on Operational Resilience, 2021

[3] FSB Cyber Lexicon, 2018

oversight of those technology service providers that become critical for the EU financial sector as a whole. This new provision entails additional complexity for all the participants involved because:

- It is a completely new set-up with complex governance arrangements, in which it is crucial to ensure that all stakeholders participate effectively and efficiently.

- And, in addition, to be able to oversee highly sophisticated technology providers, authorities will have to build the necessary capacity also in terms of skills.

Once in place, the oversight framework will have benefits not only for financial institutions, but also for the affected service providers, by creating a single framework to replace the current fragmented regulatory and supervisory regimes. At the same time, it will allow competent authorities to monitor those providers on which the sector is highly dependent.

Finally, to achieve its goals, DORA requires an unprecedented level of coordination and cooperation amongst authorities. Recognizing that cyber threats are cross-border and cross-sector, DORA establishes several mechanisms through which authorities will have to exchange information and work together, not only within the financial sector, but also with the cybersecurity authorities in the NIS[4] ecosystem. DORA offers a unique opportunity to build cyber threat intelligence in the EU financial sector, a very powerful tool to enhance its resilience.

Beyond the regulatory sphere, initiatives regarding the supervision of these risks have also grown significantly in recent years. Most authorities have allocated specialised resources both for ongoing monitoring and on-site inspections of institutions, and for horizontal activities on the sector as a whole.

I am proud to say that at Banco de España we started performing on-site inspections on ICT risk as far as in 2007, and we continue doing them nowadays, both as part of the SSM supervision as well as in our role of national competent authority for the supervision of LSIs.

Obviously, ICT risk is also a significant piece of our off-site supervision. We were very actively involved in the development of the SSM methodology for assessing this risk in the SREP process, first for SIs and later for LSIs, and we have applied it from the very beginning. Nowadays, it is simply not possible to supervise a bank without a sound understanding of how they manage their technology and its associated risks. It impacts their business model, their governance, their overall strategy and risk management framework and so on. Almost in every supervisory dialogue the words “resilience”, and “technology” come to scene.

But further to on-site missions and off-site supervision, we also perform a good number of activities targeted at enhancing the cyber resilience of Spanish banks. Let me highlight a few:

[4] Network and information systems. See Directive (EU) 2016/1148.

- In 2016, well before the EBA Guidelines on outsourcing (that date from 2019), we established clear requirements for institutions to manage the risks associated with their outsourcing arrangements. Since then, we have engaged in many fruitful conversations with banks and third parties. On one hand, this dialogue has helped banks to understand our supervisory expectations and significantly enhance their procedures to assess and manage third party risks. On the other hand, service providers have come to a better understanding of the specificities of financial institutions and have tailored the contracts they offer to meet these needs.

- I am sure that you are all aware that the significant institutions under the SSM remit have to notify significant cyber incidents. In May 2021 Banco de España established a similar obligation for the LSIs, explicitly covering malicious and non-malicious incidents. Our goal is not having blind spots and being able to swiftly react if needed, and for this reason our procedure allows for 24x7 notification. We strongly believe that in case of really severe incidents financial authorities have a role to play and time is a crucial factor to ensure an adequate coordination between all stakeholders.
-
- In 2022 we rolled out TIBER-ES, the local adoption of the TIBER-EU cyber security testing framework, open to any financial institution operating in Spain. Banco de España is the lead authority, in close cooperation with the other two financial authorities (CNMV and DGSFP). This is an excellent tool for institutions to test their cyber resilience, and for now it is on a voluntary basis. I am glad to say that there are tests going on.

These activities show that our own role as authorities has gradually changed in parallel with the increasing importance of technology and the goal of enhancing cyber resilience. More and more, we are not only supervisors but a key player in the management and coordination of potential cyber incident-related crises. For this reason, authorities are also stepping up our cooperation, not only within the financial sector but also with intelligence agencies and cyber incident response centres like, in our case, INCIBE. We also have frequent contact and collaboration with the industry associations.

Let me finalize my intervention saying that cyber resilience is not an option but a necessity. And it is the responsibility of all the participants in the financial sector, institutions, third-parties and authorities, to contribute to it.

Many thanks for having me here and I wish you a good afternoon.