Cybersecurity risks and the TIBER-ES framework

MONTSERRAT MARTÍNEZ PARERA, VICE-CHAIR OF THE CNMV
2 February 2022

Good morning, all.

It is a pleasure for me to participate in this event and to do so after the presentation of the Deputy Governor of the Bank of Spain and the speech given by the Director-General of Insurance and Pension Funds.

Today's objective is to emphasise the importance of cybersecurity, to highlight the value of the TIBER-ES testing framework and to encourage companies to value the use of this framework for advanced cybersecurity testing.

I share the messages that my colleagues have already said: it is key that we devote efforts and resources to promote proper technology risk management in financial institutions and securities markets.

And that means that we have to act preventively to prevent attacks, which are bound to happen, from affecting the proper functioning of the institutions, and that in the event of a serious incident we know how to respond.

Cybersecurity

If we look at the figures, all available sources and data point to a steady increase in cyberattacks in Spain, and in the world, and in particular in recent years, and this trend seems to be continuing. In 2020, for example, the number of very high-risk cyber incidents doubled compared to 2019[1]. We are, therefore, registering record figures, with more cyberattacks, and more dangerous than ever, and often originating in organised cybercrime, which has financial institutions as one of its targets.

There is no doubt that technological innovation in the field of financial services is a key factor in driving economic and social progress: it increases the supply of products and services, which benefits investors and businesses, and enhances the efficiency and competitiveness of the sector.

But it is also true that every transformation brings with it new risks to which we must pay attention. In this case, there are also three factors that make this transformation particularly relevant.

[1] Cyber Threats and Trends, 2021, National Cryptologic Centre

Firstly, because of the high intensity of technological change, especially in the wake of the pandemic, which has given an impetus to the adoption of digital technology. The pace of digital innovation has accelerated exponentially and with it the emergence of new risks.

Secondly, changes in the financial services business model and the emergence of new players. Technological developments are increasing competition in the sector and fragmenting the traditional value chain. This means that companies are increasingly reliant on external providers as they make greater use of technology services, whether FinTech or BigTech. And these companies are often outside the financial sphere, which opens the door to new risks and new interdependencies.

And finally, and related to the above, by the development of the so-called platform economy, which takes advantage of network economies to grow rapidly in size and favours the connection between a multitude of providers and users.

This leads us to a context of growing interdependence, in which we must necessarily work in a close and coordinated manner, fostering cooperation and collaboration between all parties involved (supervisors and companies). Hence the importance of initiatives such as the one we are presenting today, jointly between supervisors and under the impetus of the Bank of Spain.

TIBER-ES and the CNMV

The TIBER-ES testing framework allows us, precisely, to have an advanced test that will allow us to be more prepared for cyberattacks and also to do so under a European umbrella, the European TIBER-EU framework, which gives us additional guarantees on the quality of the tests and allows us to recognise each other among countries that also adopt it.

At the CNMV, as supervisor of the securities markets, we support and actively participate in this initiative.

It is important to us that institutions have adequate technology risk management, and we are devoting increasing resources to encourage institutions to do so[2]. Indeed, as announced in our activity plan, this year we have completed the review of market infrastructures' compliance with the IOSCO-CPMI guidelines on cybersecurity.

In addition, it is worth recalling the forthcoming approval of the regulation on cybersecurity at European level, the Regulation known as DORA (Digital Operational Resilience Act), which will establish requirements for the entire financial system.

However, as you know, our sector is very large and varied, and is made up of entities with multiple characteristics. It should be borne in mind that the approach to technological risk may differ between institutions, depending also on the critical functions they perform and, of course, on their maturity in this area. It is therefore necessary to adopt a principle of proportionality, so that the requirements are adjusted to the risks and characteristics of each financial institution.

---

[2] CNMV - Financial innovation

The TIBER-ES framework offers advanced cybersecurity tests that require high capabilities and resources and, as such, it is a particularly suitable framework for those entities that perform critical functions, such as, for example, the different market infrastructures integrated in the BME Group, whose activity is key to the stability and proper functioning of the Spanish markets.

Conclusions

Finally, I would like to highlight once again the collaboration and cooperation between supervisors in the production of these TIBER-ES guidelines. And thank you to the entities that are following this session for your interest in participating. Cybersecurity management is no longer a requirement, rather it is now a matter of survival. And on this road ahead, collaboration and cooperation between all parties is undoubtedly a strength that will help us move in the right direction.
I hope you enjoy the technical sessions that follow my presentation.