BANCA D'ITALIA
EUROSISTEMA

Challenges for the financial sector in adapting to cyber threats

Remarks by Ignazio Visco
Governor of the Bank of Italy

G7 Conference on 'Cybersecurity: Coordinating efforts to protect the financial sector in the global economy'

Banque de France
Paris, 10 May 2019

Today we are discussing how cyber risk is evolving in the financial sector, and what we should do about it. To set a course of action for the future, I believe we should go back to one fundamental question: why did financial authorities get involved in cyber defence in the first place?

Our overarching goal has always been to preserve a high degree of trust in the financial system. This is by no means limited to cybersecurity – it is our *raison d'être*. That is why we regulate financial risk-taking and why we do not grant disreputable players any licence to banking activities. That is also the reason why we make sure that vital systems such as payment infrastructures are not taken down by hackers.

When it comes to financial risk-taking, we all acknowledge that markets fail to deliver socially optimal results on their own, hence regulation and supervision are needed. The same argument applies to cyberspace. Financial firms have their own reasons to protect themselves. They do not want to lose their credibility and their customers because of a cyberattack. But this is not enough. Cyber vulnerabilities have extensive negative externalities – individual entities such as financial institutions do not have the incentives nor the means to internalise them all. Authorities need to rectify this.

The nature of cyberspace is such that externalities are not contained within national borders, or within any single sector. One important source of cyber risk for supervised entities is their increasing reliance on third-party suppliers who fall outside the jurisdiction of financial authorities.

In the past, attackers have leveraged vulnerabilities in the IT systems of third parties to strike financial institutions. In the *G7 Fundamental Elements For Third Party Cyber Risk Management in the Financial Sector* published last year, we introduced tenets on the appropriate management of third-party risk. We must now accelerate work on implementation. When it comes to third parties who operate in regulated sectors, such

as energy and telecoms, the different authorities must step up their coordination and cooperation efforts.

There are two dimensions to cooperation.

First, within each country there needs to be a cohesive national system of cyber defence that allows different authorities to work together effectively. In this context, governments have a natural role as coordinators.

Attacks are getting more sophisticated. Some involve resourceful actors, such as nation-states and terrorist organisations. The financial sector remains a prime target, and we cannot effectively mitigate the risk by simply mandating supervised entities to follow good practices. Complex attacks can be deployed via obscure tools. Even large financial institutions with excellent (and expensive) defence systems can be lost in the face of cutting-edge threats; they can, of course, work out some of the technical details, but they might miss some of the broader, systemic elements, simply because they ignore relevant information: precedents that affected other sectors; attacker tactics; and effective defences adopted elsewhere. This kind of information is generally available only to intelligence agencies and the military. Cross-sector, nationwide as well as international cooperation is therefore essential.

There needs to be a mechanism within each country that allows appropriate public bodies to coordinate and jointly support, each within its own mandate, the victims of a cyber campaign. In the European Union, the Network and Information Security (NIS) Directive takes this course.

Second, cooperation must extend beyond borders given the nature of many of the attacks and the interconnectedness of the financial system. This will always be a challenge because disclosing vulnerabilities to entities from another jurisdiction might endanger national security. Nonetheless, we need to find feasible solutions to this problem, since this kind of *infosharing* might prove crucial in order to respond to some attacks.

The G7, as a group of like-minded countries, remains the most favourable context for international cooperation – the many achievements of the G7 Cyber Expert Group (CEG) provide a good example of what can be done. The CEG was established in 2015 under the German presidency, and it went on to deliver results during the presidencies of four other countries – Japan, Italy, Canada, and now France. We need to persevere on this route.

One area that is ripe for more cooperation is the establishment of common security standards for hardware and software, which also covers the growing market for financial technology apps. In the European Union, we have a tradition of very strict safety, physical health and environmental protection standards. We require a *Conformité Européenne* certification – the CE mark that you see on labels – for any product in certain commodity sectors that enters our markets. Certification mechanisms are not exclusive to the EU – think of the FDA approval process for pharmaceuticals in the US.

In the EU, a new regulation (currently under approval) will introduce a mechanism of cybersecurity certification for many products, too. This is an important step, but it would

be more effective if G7 countries could converge at least on a subset of requirements. If a service is not safe according to our own laws, it should not be on the market – and there should be a reasonable degree of convergence between laws in like-minded jurisdictions.

I would like to conclude by posing two questions.

First, I would be very interested to hear from my co-panelists as to what their perspective is on the state of cooperation between authorities and the private sector, especially when it comes to vital infrastructure like clearing and settlement systems. Are regulators in this room happy with what we have achieved so far? What do private institutions think should be improved and how?

Second, are we leveraging technology strongly enough? Artificial intelligence (AI) is emerging as a pervasive game changer in our economies. It introduces new possibilities in all sectors, and cybersecurity is no exception. AI facilitates the detection and the exploitation of vulnerabilities – attackers know this, so they are starting to deploy machine learning to analyse and penetrate target systems. Cybersecurity companies use the same AI analytic tools, with the goal of fixing the weak spots. By the same token, authorities could employ AI, let us say, to ascertain whether supervised entities are meeting mandated security standards on a continuous basis.