EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB views on the regulation of cyber security

Keynote speech by Marc Bayle de Jessé, Director General Market Infrastructure and Payments, ECB, at the Central Bank Payments Conference, Copenhagen, 21 November 2017

Ladies and gentlemen,

The Nordic countries are among the European leaders in innovation, regularly topping the European innovation scoreboard and other comparable rankings. And it is fitting that we meet here today in Copenhagen to discuss cyber resilience, which is a prerequisite for allowing innovation to flourish in a safe and systemically sound environment.

Indeed, as we see on a daily basis, cyberspace opens up boundless opportunities to innovate and excel across multiple spheres of endeavour. And the financial sector is no exception, with new products and players redefining the financial landscape as we know it. But, as with all things in life, there are two sides to every coin. The potential threats to cyber security, as several speakers already touched on this morning, are equally immense. And no one – no financial institution, market infrastructure or institution – is immune. For the ECB, cyber threats can potentially impact the financial ecosystem, including central banks themselves, and this in turn, has implications for financial stability and the Eurosystem's reputation.

In addition, the European financial ecosystem rests on a highly interconnected and interdependent operational network. It involves a complex web of interactions between a range of actors, including financial market infrastructures (FMIs), banks and critical service providers. The ECB acts as an overseer or supervisor for such entities, so ensuring they are at a high level of cyber resilience is critical for us. But the issue is not limited to the market only; central banks sit at the heart of the financial ecosystem, given our multiple roles. For example, the ECB's core functions include monetary policy, financial stability, market operations, supervision, oversight, banknotes, analysis of statistics of individual institutions, and operating critical payment and market infrastructure, such as TARGET2 and T2S.

Given the complexity of the ecosystem and the role of central banks, our biggest focus must be to ensure that we can protect the confidentiality, integrity and availability of the systems and data held. The cornerstone of the ECB's work, both as central bank and supervisor, is trust. And, at a very basic, technical level, this trust depends on the integrity of information. Indeed, the risk from cyber threats applies not only to the availability of systems, but also to the confidentiality and integrity of the data they contain. Of course, without IT systems available, the ecosystem would be seriously affected. But ensuring the confidentiality and integrity of information is equally critical, as wrong or manipulated data may lead to incorrect analysis and decisions by central banks and market participants.

On the whole, if the European System of Central Banks or the ecosystem were compromised, this could not only cause disruption but potentially undermine confidence in the financial system, majorly impact the Eurosystem's reputation and affect financial stability.

It is not surprising therefore that public authorities have recognised that the interconnectedness of the global financial system requires a strategically aligned approach to cybersecurity at the international level. Indeed, the regulatory landscape has evolved over the years, and we are finding more interventions from standard-setting bodies and institutions – e.g. the Directive on the security of network and information systems, or NIS Directive, the General Data Protection Regulation, the Revised Payment Service Directive (PSD2), the guidance from the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO), the G7 fundamental elements of cyber security, etc.

All these are essential inputs which serve as a basis to strengthen the regulatory landscape in the EU and beyond. But we must not forget that cyber risk is dynamic and ever-evolving. When we speak to the market, we are constantly told that – due to the dynamic nature of this risk – imposing too many regulatory requirements can actually be counter-productive. With this in mind, we need now to

move towards working with our systems to ensure they have a high level of cyber resilience and that they have embedded the core requirements from the different regulations, standards and guidance from the different institutional bodies. Simultaneously, we must develop effective solutions and establish structures that facilitate a collaborative approach to this issue. So in essence, we must balance regulation with the appropriate tools to implement the right cyber resilience measures at institutional and sector level.

With this is in mind, the ECB's Governing Council recently approved the Eurosystem's cyber resilience strategy for FMIs in March 2017, which is intended to support implementation of the CPMI-IOSCO guidance. The strategy aims to develop a range of tools which can be used by the regulators and markets, to facilitate effective cyber resilience and marry regulation with actual structures, solutions and processes to implement the right actions. It is centred on three main pillars, similar to the approach taken in some of the G7 countries: 1) we work with our financial firms and FMIs to ensure they build their defences and enhance their level of cyber maturity; 2) we are strengthening the resilience of the sector, through cross-regulatory collaboration, information sharing, improved threat intelligence, close collaboration with European law enforcement agencies, market-wide exercises based on cyberattack scenarios, and a deeper understanding of third parties and the supply chain; and 3) we are establishing strategic dialogue between the industry and regulators to catalyse joint initiatives and develop effective solutions.

Under Pillar 1, the Eurosystem is implementing a harmonised approach to assessing payment systems in use in the euro area against the guidance. In addition, it is developing a range of tools that can be used by FMI operators to enhance their cyber resilience maturity.

One of these tools was a cyber survey, which we sent out to all payment systems in the Eurosystem. This proved to be an invaluable endeavour, as we learnt a lot about our systems. We know that cyber resilience is not just about technology. It encompasses governance, company culture and business processes. But our survey results showed that there are weaknesses in cyber governance amongst the European payment systems. Notably, payment systems are overly focused on technological security measures related to protection and detection and are neglecting people and processes. Against this backdrop, emphasis needs to be on governance and on avoiding an overly narrow focus on technological security – important as this is – while forgetting the human element. Likewise, we noted that there is more work to be done on raising awareness via training within each FMI; more needs to be done on getting assurance of third party service providers and the wider supply chain, which are risks themselves; and a lot of work is required on developing dedicated cyber incident and recovery plans.

One further assessment tool that we are developing is a European Red Team Testing Framework – a concept derived from the military practice of targeting "friendly" installations to test their security. It is an exercise which mimics the tactics, techniques and procedures of real attackers, based on bespoke threat intelligence, and seeks to target the people, processes and technologies of an FMI or firm, in order to test its protection, detection and response capabilities without prior warning. It is regarded as one of the most comprehensive ways to test cyber resilience.

The testing framework, inspired by similar initiatives in the UK, Netherlands, Hong Kong and Singapore, aims to ensure standardisation and mutual recognition of cyber testing across the EU, thereby avoiding FMIs being subject to tests in or by every Member State. Indeed, a key element of effective cyber resilience is to encourage multi-jurisdictional, group testing that is recognised by different authorities. In addition, the framework sets out standards for penetration testers and threat intelligence providers to catalyse accreditation at the EU level and help the market access the best and most reliable testers for their critical infrastructures.

Under Pillar 2, we look at sector resilience. As we have already touched on, cyber resilience in an FMI depends not only on its own readiness, but also on that of its participants, service providers and interconnected FMIs. There is a broad range of entry points through which an FMI could be attacked, e.g. via participants, service providers, vendors and vendor products, and linked FMIs. The FMI itself could even become a channel for propagating cyberattacks, e.g. by inadvertently distributing malware to other FMIs. From a cyber perspective, a small-value/volume participant or a vendor providing non-critical services may be as risky as a major participant or a critical service provider.

In order to strengthen the sector's cyber resilience, it is important to understand the operational interdependencies through sector mapping, foster cross-border and cross-authority collaboration, establish effective information-sharing and implement market-wide business continuity exercises. This is why the Eurosystem's overseers are currently developing an analytical framework and methodology for sector mapping. The aim is to produce a number of sector/network maps that will be used to understand key risk areas, improve crisis communication procedures, enhance information-sharing and debate other policy issues.

Furthermore, cross-border, cross-authority collaboration needs to be enhanced to avoid different levels of cyber resilience maturity within the financial sector and to ensure that authorities have a similar approach and focus. And, along the same lines, it is vital to foster cooperation on cyber resilience among authorities at both the European and the national level, particularly because different authorities have their own separate mandates for the various types of FMI and financial institution. For instance, with the transposition of the NIS Directive into national law, Member States should not assign to themselves oversight or supervision responsibilities on

pan-European FMIs which have a national component. European oversight/supervision structures are already in place and this will only create fragmentation.

Linked to this, another key component of sector-wide resilience is the efficient sharing of information on threats among market participants, between market participants and regulators, and among regulators. The availability of reliable data is essential to support the coordination and development of relevant policies. Our banking supervision, for example, has established a cyber incident reporting database. But, over and above this, there needs to be a strategy for overcoming the current fragmentation in the European information-sharing landscape, as well as a mind-shift to move beyond incident reporting towards also sharing ex ante operational, tactical and strategic threat intelligence.

Indeed, there is currently a clear focus on protecting against cyberattacks. However, the cornerstone of effective resilience is to acknowledge that an attack is imminent, and all infrastructures must be in a position not only to withstand such attacks, but also to respond in an appropriate way and recover in a safe and efficient manner. This is why, to further enhance the readiness of FMIs, market-wide exercises and cyber simulations are key.

Finally, under Pillar 3 on strategic regulator-industry engagement, the EU recognises the importance of establishing a forum which brings together market actors, competent authorities and cybersecurity service providers. A number of Member States are leading the way, having established formal public-private partnerships or industry associations for cybersecurity. However, there is no pan-European equivalent at present.

The sector mapping I mentioned before will not only identify the critical nodes in the EU financial system, but also help to pinpoint those market participants and regulators that should be involved in a pan-European regulator-industry forum. Such a pan-European forum should ensure Board-level participation and focus on strategic discussions rather than overly technical details, as well as aim to raise awareness and catalyse joint initiatives for developing effective solutions for the market, sharing best practices and fostering trust and collaboration. Indeed, tackling cyber risk is not for regulators or the market in isolation; it is an endeavour they must undertake together. In light of this, we are in the process of establishing the Euro Cyber Resilience Board.

Finally, it is equally important to emphasise the need for the different internal functions of central banks to collaborate and work together. As I have stated above, central banks have multiple roles and responsibilities, and for effective cyber resilience, it is critical that there is greater alignment internally and we leverage off each other's skills. I have spoken about collaboration amongst regulators and with the market, but within the Eurosystem, we are developing structures and mechanisms to improve our own internal set-up, to enhance how oversight, supervision, operators and information systems work with each other, while respecting each other's institutional responsibility.

And this, as I now conclude, takes us back to the two core elements for effective cyber resilience which we mentioned at the start: trust and collaboration. Trust as a cornerstone of a soundly functioning financial system, and collaboration as a means of ensuring this. We have seen that cyber resilience is a collective and multilateral endeavour, and that this collaboration cannot take place within the set parameters, practices and mind-set of "traditional" risk management. Indeed, cyber threat is continuously evolving, and we must be equally agile and adaptive in our response. This means not only introducing the notion of cyber resilience into our thinking and practices, but also remaining operational with the understanding that attacks and incidents happen on a continuous basis. And it means balancing regulation with the appropriate tools to implement the right cyber resilience measures at institutional and sector level.

Going forward, the only thing that's cast in stone is the certainty of future change. And, to embrace this together, we must not see regulation as an adjunct to cyber security, but as a vital part of it.