BANCA D'ITALIA
EUROSISTEMA

DIGITAL TRANSFORMATION OF THE RETAIL PAYMENTS ECOSYSTEM

CYBER SECURITY – THE BALANCE BETWEEN COOPERATION AND REGULATION

KEYNOTE SPEECH BY FABIO PANETTA, DEPUTY GOVERNOR OF BANCA D'ITALIA

At the joint ECB and Banca d'Italia conference
Rome, 1 December 2017

Information and communication technologies play a fundamental role for people, businesses and the public sector. Digital transformation is modifying the economic system and the whole of society at unprecedented speed.

Innovation is having a powerful effect on the financial sector. The value chain is becoming more complex, and the participation of non-financial providers is increasing. The tech giants as well as the new fintech start-ups are expanding the supply of innovative services to a broad and diverse customer base through new business models.

As a result, confidence in the financial sector is no longer based on bilateral trust between customers and service providers but is dependent on the governance of digitalization and especially on the reliability and safety of the products offered.

Emerging risks in the digital ecosystem

The increasing role of digital platforms is creating enormous benefits for users. At the same time it is offering ill-timed advantages for new groups of hostile agents, such as hacktivists, fraudsters and criminal and terrorist organizations. By exploiting the vulnerabilities within cyberspace, these agents may endanger the provision of digital services or disrupt critical infrastructures.

The new risks are exacerbated by the complex network of interconnections that forms the digital ecosystem: the 'Internet of Things' is exploding and the number of interconnected devices is expected to grow at an unprecedented

pace, to more than 200 billion in 2020.[1] The area at risk is expanding enormously. Any weakness in security controls, any vulnerability in technology may offer an entry point for cyber attacks.

In the financial sector, cyber attacks can create disruptions that propagate instantly and globally with effects that are hard to predict. Recent cyber attacks, like the one against the Central Bank of Bangladesh, exemplify the vulnerabilities – of both process and technology – that affect interbank payments and core financial infrastructures, which were once considered less exposed to cyber risks. As the Financial Stability Board has emphasized, certain cyber attacks[2] show that the vulnerability of financial institutions is a systemic issue, although it is unlikely as yet to represent a real threat to global financial stability.

These attacks were a wake-up call for regulators and financial authorities, emphasizing that the safety of cyberspace is not just a prerequisite for the reliability of financial services but also an essential element of financial stability. Cyber risks threaten the core functions of the financial sector, including banking operations, payments and securities settlement. Central banks and, more generally, public authorities may themselves be on the radar screen of cyber attackers; cyber security is no longer a matter for specialists but a policy priority.

The pillars of an effective cyber security strategy

In today's world, central banks, regulators and supervisors face the formidable challenge of ensuring that the technological revolution does not undermine trust and confidence in the financial system. This is no easy task: like acrobats walking a tightrope, the authorities must strike the right balance between potentially diverging forces such as innovation, complexity and the safety of the system.

This entails enhancing and complementing the traditional regulatory and supervisory approaches with the adoption of an effective toolkit tailored to address cyber risks.

[1] From 2 billion in 2006. Source: World Economic Forum, *Mitigating Risks in the Innovation Economy. How Emerging Technologies are Changing the Risk Landscape*, (September 2017).

[2] Such as the Wannacry campaign in 2017 and the Corkow Malware in 2015.

In 2016 the G7 published a set of widely applicable recommendations encapsulating cyber security best practices for public and private financial entities. They were followed last October by the 'fundamental elements for effective assessment of cyber security for the financial sector'.

Having in mind these G7 principles, I would like to focus the rest of my speech on the main pillars on which – from a central bank's view – an effective strategy should be based: regulation, cooperation and risk awareness.

The first pillar: regulation

Regulation is a crucial component of an effective strategy to ensure sustainable innovation and preserve cyber security. A number of European laws have recently introduced requirements and obligations for both private companies and public bodies in order to increase cyber security in critical sectors of the economy.

A general framework is given by the Network and Information Security Directive (NIS-D), which establishes security-related obligations for critical service providers, including credit institutions, stock exchanges and financial infrastructures. To guarantee data protection and the privacy of personal information, the General Data Protection Regulation also imposes strict security requirements for private and public entities, including financial firms.

Specifically focusing on the financial field, the second Payment Services Directive (PSD2) has introduced security requirements throughout the payment cycle: from payer authentication to communication between service providers, security risk management by financial firms and the reporting of major incidents to the authorities. The European Banking Authority (EBA) was delegated to issue secondary regulation.

The Guidance on cyber resilience for financial market infrastructures was published by CPMI-IOSCO in 2016. To ensure its harmonized implementation within the euro area, the Eurosystem has delivered a cyber resilience strategy that national supervisors must adopt to enhance the cyber resilience framework of financial institutions.

However, regulation alone is not sufficient to protect the financial system from cyber risks**.** Indeed, excessive reliance on regulation may even have undesirable side effects owing to the complex interactions between different regulatory levels, such as domestic versus international legislation or

economy-wide versus sector-specific rules. Hence, other forms of intervention are necessary, such as cooperation.

The second pillar: cooperation

Owing to the existence of externalities, individual intermediaries may lack sufficient incentive to contribute to the supply of a common good – cyber security – that would generate benefits for their direct competitors as well. They may be tempted, therefore, to free ride on the action of other companies and to under-invest in security-enhancing projects. In this situation, central banks, as third parties entrusted with preserving financial stability, may act as a catalyst to stimulate cooperation, centralized cyber threat intelligence and information sharing initiatives.[3]

At European level, the recent establishment of the European Cyber Resilience Board (ECRB) under the Eurosystem cyber resilience strategy is a valuable example of virtuous cooperation among public authorities, financial market infrastructures and critical service providers to enhance the cyber resilience of the European financial ecosystem.

Financial authorities may also leverage such cooperative initiatives to promote effective practices and tools for cyber risk assessment, including simulations and tests, which are difficult for individual firms to implement in isolation. This is a new paradigm, in which authorities and regulated entities work closely together, complementing compliance with a collaborative approach. This allows the authorities to gain a deep understanding of the level of cyber resilience achieved and of any additional initiatives required.

The third pillar: promoting risk awareness

The third pillar of action focuses on the human factor, as in cyber security people are still the weakest link. For example, the spread of cyber extortion (ransomware) – which is becoming one of the major threats to digital businesses – can be attributed to several factors. Some are technical,[4] but the

[3] Threat intelligence may support financial institutions in taking the right decisions to prevent cyber attacks, effectively protect their critical assets and respond appropriately in the event of a successful cyber attack. Information sharing about cyber events through trusted channels facilitates a sector-wide response to large-scale cyber incidents (CPMI-IOSCO, *Cyber guidance*, 2016).

[4] We refer to the growth of ransomware-as-a-service, easily and cheaply accessed on the dark-web by cyber criminals, or the availability of crypto-currencies as a ransom payment tool. Today, cyber attacks can easily be organized, even by purchasing as-a-service packages and simple downloads for installation on rogue servers. In 2016, 638 million ransomware attacks were recorded, 167

most significant ones are totally human related: the growing habit of working remotely on personal devices, combined with users' lack of attention to cyber risks, can easily open the door for attacks on corporate critical information assets. Employees, consumers and public officials need to be educated about the risks that can arise from new technologies. The financial authorities are in the best position to promote long-term education initiatives and cyber awareness campaigns.

The role of the authorities: the experience of the Banca d'Italia

For central banks, translating all these principles into concrete action means first of all strengthening internal governance and cyber security capabilities. Let me talk about the Banca d'Italia's experience in this area.

To ensure a comprehensive strategic vision and the alignment of internal and institutional policies, a cyber security steering committee has recently been set up at Board level.

Under this governance, the Banca d'Italia's three-year strategic plan envisages two specific initiatives: one focuses on protecting the Bank's critical assets by reorganizing security functions inside the IT Department; the other focuses on enhancing the cyber resilience of Italy's financial sector by adapting the Eurosystem cyber strategy in line with the Italian National Cyber Security Framework and keeping an open dialogue with the competent national bodies.

On the cooperation front, the Banca d'Italia and the Italian Banking Association have sponsored the establishment of the Italian Financial Cyber Security Unit (called CERTFin), which coordinates information sharing and cyber threat intelligence among the participating financial companies, allowing them to share critical information and enhance the awareness of cyber risk beyond what would be possible within the perimeter of their own organization.

Since January 2017, CERTFin has examined more than 800 cyber events, sharing with its members any lessons drawn and circulating more than 150 warnings on potential compromises to individual financial firms. It cooperates with similar national and international cyber security bodies. Furthermore, CERTFin cooperates closely with government cyber security agencies, contributing to national cyber security.

---

times more than 2015 (source: SonicWall, 2017 annual report - www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/#3d5df45558dc).

Conclusions

Digital innovation and cyber security are two faces of the same coin and so cannot be addressed separately. Hostile agents and criminals have always existed. However, compared with other threats or other types of crime, cyber attacks are rapidly evolving and, given the central role of cyberspace in modern economies, represent a concrete global risk.

In the final communiqué of the G7 meeting held in Bari in 2017 under the Italian Presidency, finance ministers and central bank governors stated that they 'recognise that cyber incidents represent a growing threat for our economies and that appropriate economy-wide policy responses are needed. No point of cyberspace can be absolutely secure as long as cyber threats persist in the surrounding environment'.

Transposing this principle into concrete action is challenging and requires us to recognize that cyberspace is a global public good. Ensuring its security, openness, reliability and interoperability falls under the joint responsibility of governments, public institutions, private industry and researchers. How should we tackle this challenge?

One answer lies in the words of the Roman philosopher Seneca: *Longum iter est per praecepta, breve et efficax per exempla*.[5]

After two thousand years, this sentence is more than ever pertinent in describing an effective approach to innovation. In the field of cyber security, regulatory or supervisory tools may become less effective unless accompanied by other concrete action: as our experience has shown, the authorities may support joint initiatives with the private sector on information sharing and the promotion of best practices, playing a role as trust-builder to foster the broad and open participation of all stakeholders. This approach may help us respond appropriately to digitalization by reconciling innovation, security and competitiveness.

Thank you for your attention.

[5] 'The way is long if one follows precepts, short and effective if one follows examples'.