ABI Lab
Tecnologia utile

Response to consultation on the document "Guidance on cyber resilience for financial market infrastructures"

23 February 2016

1. Contents

1. Introduction and general comments

With the intention of supporting Financial Market Infrastructures (FMI) in improving their resilience against cyber threats, the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) have prepared the document "Guidance on cyber resilience for financial market infrastructures" for public consultation.

The document is an additional Guidance to the "Principles for FMIs" (PFMI). However, it does not introduce any new requirements or principles, but rather provide further details, particularly in the context of Governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risks (Principle 17) and FMI links (Principle 20).

In particular, the Guidance provides indications on the five primary areas of risk management – governance, identification, protection, response and recovery – and deals with three aspects transversal to them – testing, situational awareness and continuous learning and evolving – with the following objectives:

- define principles and not rules, in order to avoid rapid obsolescence of the recommendations it contains, without imposing any rigidity in implementation of the principles;
- emphasise the importance of robust ICT controls, without entering into detail, to leave operators with flexibility, partly in consideration of the numerous standards present on the market;
- promote greater awareness of company top management and their full involvement in strengthening cyber resilience.

The contents of this Guidance therefore complete implementation of the framework introduced by the PFMI, simultaneously guiding and reinforcing certain specific aspects of cyber resilience.

The ABI Lab Consortium, the Banking Research and Innovation Centre promoted by the Italian Banking Association, therefore appreciates the fact that CPMI-IOSCO has published this document and opened it up for consultation, making it possible to acquire and benefit from the opinions of a wider group of parties concerned. Although the Guidance is addressed at FMI, the principles it contains focus on strengthening cooperation between all the entities and organisations involved in cyber risk management and in protection of market infrastructures.

This document contains the comments prepared by ABI Lab with the support of the banks representatives having expertise on this issue.

General comments are reported below. More detailed comments on the impact of this Guidance in the Italian banking sector are contained in the subsequent paragraph.

Information sharing and situational awareness

The Guidance on cyber resilience is aligned with financial sector regulations and based on the principal standards (e.g. ISO/IEC 27000, ISO/IEC 22301) and acknowledged best practices (ENISA, NIST, etc.).

As we know, all recent regulations, from the new Payment Service Directive (Directive 2366/2015 – "PSD2") to the future European Privacy Regulation, and also national and sector provisions, no longer require simply a contingent reaction to the malicious event, but rather careful management of cyber issues, a wider and more reasoned analysis of the causes of events/attacks, notification of the competent authorities and, hopefully, sharing at sector level. The protection solutions must also be scaled according to the results of detailed risk analysis.

The attention focused in the document on promotion of information sharing among all those involved, with a view to acquiring a wider awareness of cyber events which have occurred and potential future trends in attack mechanisms, is therefore appreciated.

For the threat intelligence activities to be effective, however, it is important to set models, procedures, criteria, languages and channels for exchanging information which are as standardised as possible. In that view, a centralised mechanism for coordinating countermeasures and preventive actions to cyber incident and attacks could guarantee the right level of cooperation between all stakeholders, by enabling a shared intelligence and "trusted" channels for exchanging and transmitting information. That approach could be promoted by setting up a financial CERT, as recently approved in the Italian context by the banking Association.

Involvement of stakeholders who participate in market infrastructures

In view of the increasing interconnections and interdependence in the financial system, the attention focused in the Guidance on aspects of cooperation between all stakeholders participating in the financial market infrastructures (as telecommunications suppliers and providers) and the relative competent Authorities, is greatly appreciated.

This aspect could be further emphasised by promoting *responsible disclosure* actions and providing indications for the various parties involved, differentiated according to their importance in the different business processes and, consequently, in recovery and response actions.
Widening the perimeter of cooperation and exchange of information to include technology firms, whether providers of services to the FMIs or operators on the cybersecurity market, should take place in a manner which guarantees the necessary confidentiality of the information.

2. Assessment of possible adoption of the Guidance in the Italian banking sector

The recent updates (15th Circular Update no. 263, July 2013, and 11th Circular Update no. 285, July 2015) of the Supervisory Provisions of Banca d'Italia focus particular attention on the issue of information systems management, security incidents and business continuity, and they heavily impacted the sector in terms of investments and planning activities, for adaptation of the provisions issued.

It is fundamentally important to understand how the Guidance must be interpreted in light of current local regulations and which analysis and working solutions the banks

would be required to adopt if the Authority intends to incorporate it into Italian law, in view of the compliance efforts recently made on precisely these issues. If it becomes clear that incorporation of the Guidance into the national context is limited solely to critical infrastructures, the integration of the principles into current regulations - which apply to the entire sector - would have less impact.

Several comments are made below on possible integration of the principles contained in the Guidance into the national banking context, with particular reference to:

- Compatibility of the Guidance with the cyber resilience plans and strategies of Italian banks;
- Method of assisting coordination between FMIs, participants and other market operators, including technology firms, in order to increase the individual and collective responses to cyberattacks;
- Possible strategies and plans for improving use and sharing of intelligence on cyber threats;
- Level of commitment of top management and complexities in adoption of the principles contained in the Guidance;
- Estimate of the time needed to achieve the most challenging objectives of the Guidance;
- Support of the national Authority in achieving cyber resilience objectives.

2.1 Compatibility of the Guidance with the cyber resilience plans and strategies of Italian banks

Generally speaking, and partly in response to the demands of European and national supervisory institutions, plans and strategies for dealing with cyber risks already form part of the complex strategies of banks for security risk and business continuity management.

The viewpoint of the document in consultation therefore offers important aspects for further analysis and checking of the consistency of the strategies adopted.

With specific reference to Italy, the Guidance returns to several aspects examined in the recent prudential supervisory provisions of Banca d'Italia, revised in 2015, (Circular no. 285), particularly in relation to risk acceptance, management of the asset inventory, adoption of controls and correct management of incidents. These provisions allow banks to align even further with the cyber resilience strategies discussed in the present document, with respect to which no specific incompatibilities are perceived.

At the same time, the Guidance encourages the various parties involved to further deal with cyber aspects in their internal Information Security policies, with a possible impact on existing policies and procedures (and on the related supporting instruments and tools); moreover, the current document further enhances the number of frameworks and the cyber risk analysis models which are being increasingly introduced nationally and internationally.

2.2 Method of assisting coordination between FMIs, their participants and other market operators, including technology firms, in order to increase the individual and collective responses to cyber attacks

Coordination and sharing of information between FMIs, their participants and market operators are among the principal elements which can assist a correct approach to response strategies and preventive management of malicious cyber events.

In order to improve the joint response of the entire sector to cyberattacks, the possibility of carrying out, or improving if already present, several initiatives and specific activities under the coordination of a central entity could be assessed, including:

- periodic joint round tables to share information among all participants, both public and private, involved in the fight against cybercrime (National CERT, Law Enforcement Agencies, CERT of individual companies, etc.);
- common countermeasures on cybersecurity, also through creation of a financial CERT;
- simulation and a cyber incident/emergency exercise, at sector and inter-sector level;
- shared protocols and models for information exchange, with a view to preventing cybercrime, and appropriate communication frameworks;
- development/ sharing of contingency solutions to cope with possible extended interruptions of ICT services under cyberattack.

ABI Lab also believes it is necessary to guarantee, at individual FMI level, sufficient cybercrime awareness and an efficient internal coordination model, also by identifying company officers who act as the interface in both ordinary management and in management of incidents/emergencies, and in synergy with existing responsibilities defined for business continuity management.

2.3 Possible strategies and plans for improving use and sharing of intelligence on cyber threats

There is an increasing awareness in the sector that the fight against cybercrime has to be systemic and that achieving high security levels must be a joint objective. Use and sharing of intelligence activities are therefore a valuable approach in the fight against cyber threats, but it is equally important to develop, including with the support of category associations and the competent Authorities, a strategy and shared and common procedures for exchanging and transmitting data related to frauds.

Furthermore, in a prevention and early warning system, it is important to develop and maintain a cybersecurity culture and awareness within the individual organisations, which starts in all the structures responsible for managing Information Security and, with various levels of detail, reaches all employees transversally.
In this case, the FMIs could assess whether it is worth:

- channelling information and reports containing the principal results of intelligence activities on cyber threats internally;

- creating internal "communities", formed of Business Continuity, Risk Management and Information Security people, for the exchange of information, to check effectiveness of continuity plans and incident management processes or for coordination in the case of emergencies.

In this case, many Italian banks already have specialised cyber threat intelligence instruments and services, have defined *ad hoc* internal plans to react on cyber threats and share information and vulnerability and threat analysis, in order to identify attacks as soon as possible and continually improve the response to them. In this context, the ABI Lab Consortium has introduced a permanent Observatory, responsible for updates and exchange of information on fraud and computer security issues, to the benefit of the entire banking sector.

In conclusion, alongside the practice runs and tests which the FMIs already carry out internally, it would be a valuable opportunity to promote exercise and simulations of sector cyberattacks involving the various FMIs and other market operators, with the objective of identifying any areas of improvement and prevention, also through performance of subsequent lessons learned and debriefing sessions.

2.4 Level of commitment of company top management to any complexities in adoption of the principles contained in the Guidance

The involvement of company's board and top management in issues of Information Security and the cyber risk proposed by the Guidance is in line with what has already been demanded of Italian banks by the Supervisory Authority. Senior executives are therefore focusing a great deal of attention on these issues, also with a view to digital development of banking, which requires the right balance between customer experience and easy use, on the one hand, and security and prevention of cyberattacks, on the other.

Nevertheless, a possible adoption of the requirements of the Guidance would also require further analysis and review of existing processes; therefore, an obstacle to introducing in the Italian context the principles described in it is the economic impact, as compared with the actual cyber risk, associated with implementation of the adaptation procedures, to which must be added the difficulty of creating a secure communication channel between FMIs.

In conclusion, any adoption of the principles in the national context must be part of a process of integration with existing provisions and therefore of the current management in the bank of logic/IT security issues, without creating a further layer of additional regulations to the existing framework.

2.5 Estimate of the time needed to achieve the most challenging objectives of the Guidance

In the national context, the majority of banks have already planned and/or developed initiatives to increase their own level of cyber resilience. Therefore, many of the principles indicated in the Guidance, which are cornerstones on which to focus cyber resilience strategies, are, in many cases, already included in the intervention policies and plans of the individual organisations.

However, certain indications, such as the detailed checking consistency of the strategies currently adopted with the principles described in the Guidance, may prove to be a challenging objective which cannot be achieved in the short term, but which would require planning and performance over the medium term (2 - 3 years).

In this case, prior (or current) sharing of the specific features and methods for incorporating this Guidance into the national context could support those responsible for prior identification of solutions and the related implementation activities.

2.6 Support of the Authority in achieving cyber resilience objectives

In order to support the sector in achieving the objectives of the Guidance, also with a view to increasing the ability to deal with threats/events, national banking Authority could promote initiatives aimed at strengthening cyber security mechanisms for the entire sector.

With this aim in mind, the importance of creating a centralised mechanism for coordination in response to cyberattacks – as a means to increase the sector's ability to respond to and coordinate cyberattacks and threats and to consolidate an information sharing community for the whole banking sector – together with more detailed examination of cyber issues at the existing central structures for coordination of operating crises. In Italy that approach is going to be defined through improving cybersecurity defence according to a financial CERT model.

In conclusion, in addition to promoting a culture of cyber resilience among top management (although without developing separate regulations), the national Authorities could encourage adopting of sector information sharing logics, including through identification and arrangement of communication methods, protocols and secure channels for shared and joint exchange.