INTESA SANPAOLO

Cyber Security Strategy: Stakeholders Networking

Enhancing Cyber Resilience

Bruxelles, 24 January 2019

INDICE

A global perspective

Cyber Security and Digital Strategy

The Banking sector is facing a paradox: Financial Institutions need to reshape their business models investing heavily on innovative technologies and new skills, whilst coping with a structural contraction of revenues due to several contingency forces, such as the unprecedented interest rates reduction, the increasing competitive pressure, and the non performing loans challenge. Bearing this landscape in mind, the financial institutions have to create ***new digital business models*** *and to cope with cybersecurity issue.*

Digital Transformation:
Digital Banking in a EU Digital Single Market and beyond it, creates a paradigm shift on traditional Business Models

Regulation & Harmonisation:
To face the continuously evolving Regulatory Requirements, it is of utmost importance to foster the dialogue among institutions and private stakeholders

Cybersecurity Holistic Vision:
Borderless and interconnected economy leverages new opportunities arising from innovative technologies, whilst introduces cyber risks also related to processes, culture and awareness

Collaboration, Coordination, Communication:
To enhance the cyber-resilience cooperation and info-sharing are the cornerstones at sectorial and cross sectorial level, these are identified as pillars also within the EU Cyber Security Strategy

Six areas to enhance ISP cyber resilience

Collaboration among Financial Institutions

Among all the issues related to Cyber security ISP has identified the following areas of collaboration among Financial Institutions, to be tackled as priorities through the Stakeholders Network:

Infosharing	Enhancing information sharing among Financial Institutions and Member States is a prerequisite to foster cyber security at EU level. These could be adopted both within the specific Financial sector and across industries.
Incident Reporting	The EU framework for Incident reporting foresees the involvement of multiple authorities, applying different procedures and templates, creating possible overlaps and redundancy in reported information. Likely, a single incident might entail to fulfill multiple reporting requirements. It is clear the need for harmonisation and coordination among actors.
Crisis Management Procedures	There is a need for common procedures of cyber crisis management. The definition of such procedures might be done leveraging the progresses achieved in info sharing & incident reporting, and conducting simulation and war gaming exercises.
Secure Supply Chain Management	Supply chain is often the weakest cyber security link and in an integrated and interconnected eco-system this is an unbearable risk. Evaluating every single entity along the supply chain, in order to enhance the overall resilience, is of utmost importance.
Cyber Risk Measuring	The evolution of the measurement models and methodologies for Cyber risk assessment, represents the cornerstone to have an efficient management of Cyber Security within the institution, dynamic in intercepting emerging threat, and risk-based in identifying countermeasures.
Education & Training	Human factor is critical in Cyber Security, thus, to increase the resilience of the entire system, it is necessary to raise awareness and knowledge around cyber-risk. Training and awareness programs for customers and employees should be considered as very relevant.

Improving Cyber resilience

Collaboration among Financial Institutions

Intesa Sanpaolo believes that Cyber Security is a ***collective intangible asset*** and considers that ***improving Cyber Resilience is a common goal***, that ***requires a collaborative peer-to-peer approach*** and a joint effort to assess and address the underlying ***multidisciplinary challenge*** the financial institutions have to cope with. To achieve this common goal, ISP has launched a ***Stakeholders Networking*** initiative with the EU institutions a group of peers.

Improving Cyber resilience is a must
It is a regulatory requirement
It is a business survival need
It is a business growth enabling factor
It is often coming as a top down approach
It is often foreseeing a (multi) Hub and spoke approach

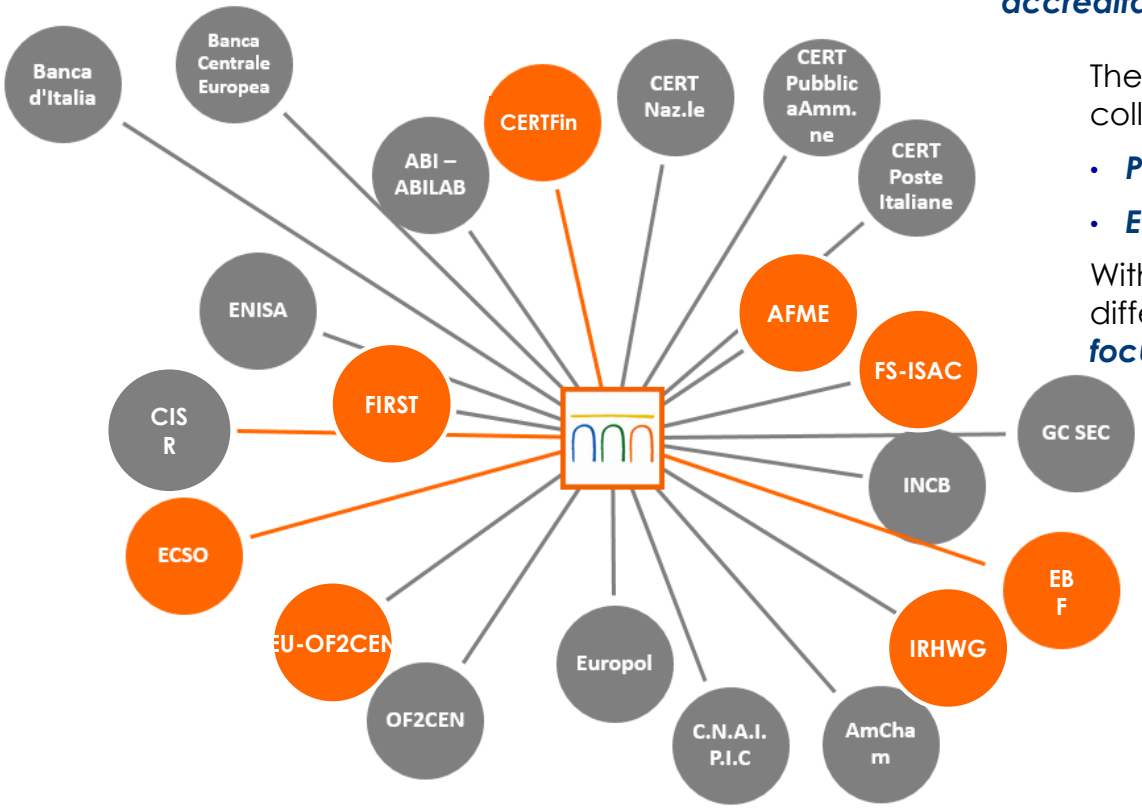
Intesa Sanpaolo ***is willing to combine a top down approach***, arising from regulations and market trends, ***with a collaborative one*** putting forward the ***practitioners experience and their holistic views*** to share best practices and innovative ways to address the Cyber Risk.

While there is no need to create another institutional body, ***there is room for collaboration in harmonising tools and procedures and in getting ready for swift reaction to cyber attacks***

Collaboration among Financial Institutions

Ongoing cooperation in ISP Network

During the last years, several international collaboration activities have been set-up to foster and enhance Intesa Sanpaolo Group cyber security strategy aiming to: A) ***extend the leadership role*** within the Financial sector in the European Cybersecurity domain; B) ***become trustworthy partner*** for Institutions and peers; C) leverage the process of ***accreditation with international financial sector***.



The strategy has been declined in specific collaboration with selected ***partners*** for:

- ***Potential to influence***
- ***Effectiveness in execution of the objectives***

With the partners, have been developed different activities referable to ***three different focus area*** with the aim to:

1. ***Address cybersecurity strategy at European level;***
2. ***Implement solutions of common interest with peers;***
3. ***Support an effective spending of European funds***

See following page for details

Intesa Sanpaolo's Strategy

Focus areas and Common Application Project

Main partner

1 ***Address cybersecurity strategy at European level***

Support – through Institutional meetings, events organisation and partecipation, position paper drafting, proposition of amendments (direct or through trade associations) to the normative drafts of the European Commission – ***Definition of EU strategies*** *consistent with the real needs of Financial Institutions both in terms of cyber risk and the provision of critical services for the community.*

- ***ECSO***
- ***EBF***
- ***AFME***
- ***CEPS***

2 ***Implement solutions of common interest with peers***

Enable - through relationships with peers, vendors and institutional actors - the development of specific projects (eg ***Common Application Tool*** *– for* ***Mandatory Incident Reporting*** *and* ***Voluntary Info sharing)*** *able to offer a practical solution to the needs of Financial Institutions. Participate proactively in dedicated working groups such as the Incident Reporting Harmonization Working Group (****IRHWG****),*

- ***ECSO***
- ***EBF***
- ***AFME***
- ***ENISA***
- ***BBVA***
- ***JP MORGAN***
- ***RABOBANK***

3 ***Support an effective spending of European funds***

Also through the European CyberSecurity Organisation (ECSO), advising the European Commission on the funding priorities within the European Horizon 2020 program. ISP with the involvement in managerial and operational roles in the ***public / private partnership*** *created in collaboration with the private sector (the c-PPP) and by* taking part to the funding opportunities of the European Commission *with EU peers*

- ***ECSO***

ISP Cyber Security Initiatives

Stakeholders Networking: Institutional initiatives

Intesa Sanpaolo strategic approach is to **collaborate with external entities both at local and international level**, and is actively involved in the following initiatives:

1 CERTFin

The **Italian CERT for the Financial sector**, driven by the Italian Banking Association (ABI) and Bank of Italy, has the aim of setting up a coordination and information sharing group for the financial sector on Cyber Security issues, with the objective to enhance cyber resilience in the financial sector.

2 Italian Cyber Security Framework

The Italian Cyber Security Framework aims to provide **public and private organizations with a voluntary and homogeneous approach**. The framework purpose is to address cyber security, reduce Cyber Risk, increase the exchange of information cross-industries and foster cyber-resilience.

3 EBF

EBF works mainly on the regulatory side by analyzing the incoming regulations and by representing the European banking sector position. EBF recognizes that **cyber security is a key priority** and ranks it **high in its regulatory agenda**.

4 ECSO

ECSO works with the EC to foster cyber resilience and security. The cPPP between ECSO and EC defines the **investment priorities** and **ensures that funds allocated** are contributing to the achievement of a Cyber Secure EU Digital Single Market.

5 AFME

AFME is the voice of all Europe's ***wholesale financial markets***, providing expertise across a broad range of regulatory and capital markets issues.

6 Glocal ventures

Major Financial Service providers having a worldwide presence in order to manage cyber threats and to be fully compliant with requirements arising from the involvement in different national and international FMIs, need to adopt **borderless ICT & Cyber Security Governance Models** based on international standards and frameworks (i.e. NIST) **sharing information** with other critical infrastructure and law enforcement agencies.

ISP Cyber Security Initiatives

A Glocal Approach

Intesa Sanpaolo Group is a major ***European*** Financial Service provider active in Banking and Insurance Sectors. With its worldwide presence, the Intesa Sanpaolo Group, has adopted a ***Glocal approach***, thinking Global and acting Local, witnessed by its international attitude and active participation:

Incident Reporting Harmonisation WG for a Common Application

IRHWG

ISP Group is leading a private sector initiative, involving major banks at EU level, to be at the forefront of the IRH challenge. The purpose is to **define a common data-set to standardize Incident Reporting** and **Crisis Management procedures and to design/implement a Common Application** for bi-directional flows between Financial Institutions and Supervisory Authorities. As part of the Consortium CyberSec4Europe that was granted EU funds by the European Commission, ISP will be part of a **Pilot Project aiming at the development of a tool** addressing the common need to respond to incident reporting mandatory requirements.

Information Sharing

Carnagie endowment

This initiative is focused on the discussions among **the G20 regarding cybersecurity and financial stability**. Over the past two and a half years, the Carnegie Endowment for International Peace has been working on this issue including engaging several of the G20 members and other countries as well as experts in private industry.

Information Sharing

FS-ISAC

FS-ISAC Critical Infrastructure Notification System (CINS) is a service that allows to notify all the members about important information in the event of an urgent or crisis situation. The aim of the service is to **speed security alerts to multiple recipients** around the globe near-simultaneously while providing for user authentication and delivery confirmation.

Best practices

FSB – Cyber Lexicon

ISP Group is involved to develop a cyber lexicon for supporting the work of the FSB, standard-setting bodies, authorities and private sector participants, e.g. financial institutions and international standards organisations, to **address cyber security and cyber resilience in the financial sector**.

Best practices

FIRST

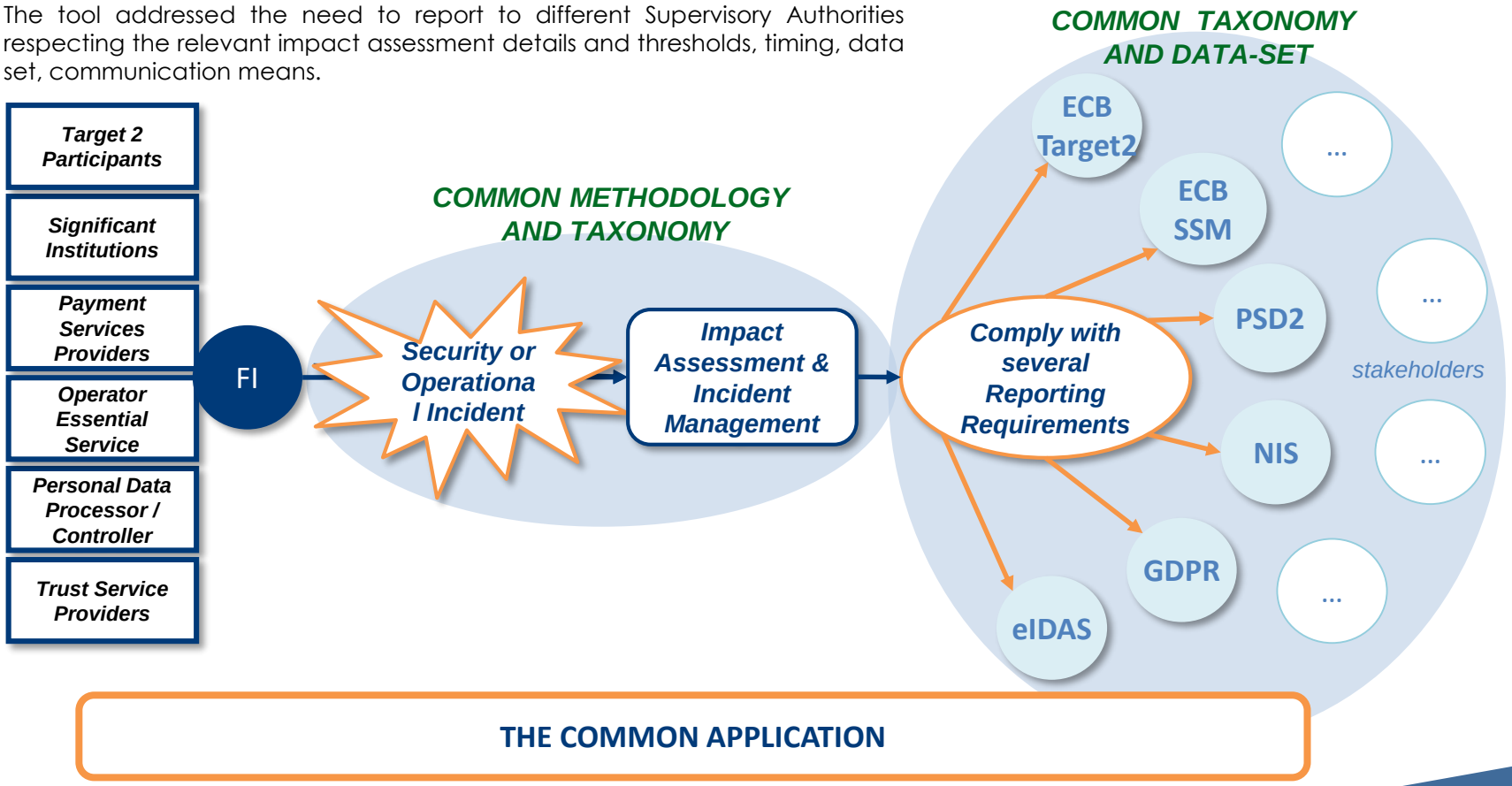
ISP-CERT becomes a ***FIRST full member*** entering in a trusted network of security practitioners and incident response teams which allows a quicker and closer collaboration with other organisations through trusted communication channels.

The Common Application

A project tackling the need for enhanced cooperation

The Project proposal to develop a Common Application to address the need of Mandatory Incident Reporting was granted funds by the European Commission in response to the European Call for Proposal SU-ICT03. BBVA,ATOS and ISP, as part of the CyberSec4Europe Consortium will benefit of Horizon2020 funding to for the development of the tool.

The tool addressed the need to report to different Supervisory Authorities respecting the relevant impact assessment details and thresholds, timing, data set, communication means.



Achievements of the Stakeholders Networking

Goals reached

Proactively collaborating in many initiatives, the ***Intesa Sanpaolo Group*** has provided a significant contribution to different Working Groups, improving ISP **positioning among major EU players**. As of today the following goals have been achieved:

Goals

- Recognised **leading role** on Cybersecurity topics at European Level, not only by private institutions, but also by EU Bodies, Agencies and Authorities
- Creation of a selected **Network of Trusted Partners** whilst becoming a recognized trustworthy partner for peers across jurisdictions and across industries.
- Identify and design with other Stakeholders, cybersecurity related solutions, addressing common needs, starting with Mandatory **Incident Reporting Fragmentation** and **Information Sharing.**