CERT Finanziario Italiano

Setting up a Financial Sector's CERT: the Italian experience

Conference Hall - MIB Trieste School of Management
Friday 26 May, 2017

Pierfrancesco Gaggi

Co-President of the Italian CERTFin

Head of International Relations ABI

Why a Financial CERT?
The framework scenario

CERTFin

REGULATORY FRAMEWORK EVOLUTION

Increasing attention of regulator and Institutions to the **cybersecurity**

National strategy of cybersecurity
- Enhancement of public private partnership and international cooperation
- Strengthening the protection of the critical infrastructures

Circular 285 Bank of Italy
- IT risk analysis
- IT and data security management
- Incidents reporting

Guidelines on the security of internet payments
- Risk Assessment, tools and monitoring
- Strong customer authentication
- Customers' Education and awareness

PSD2
- Strong customer authentication
- Security in the communication with TPP
- Security and operative incidents management and reporting

European Directive NIS
- National cybersecurity strategies and plans and CSIRTs development
- Operational information sharing through CSIRTs network
- Incidents management and reporting

CPMI/IOSCO Cyber guidance
- Governance, identification, protection, detection, response and recovery of cyber threats.
- Overarching components: testing, situational awareness, learning and evolving

SPREAD OF COOPERATIVE SECTOR INITIATIVES IN OTHER COUNTRIES

Some specific samples for the financial sector, confirming the high attention to this topic…

FinansCERT

Electronic Crime Task Force

Cyber Defence Alliance, FS-ISAC

Definition of an industry CERT

Why a Financial CERT?
Objectives

The Italian Financial CERT:

- responds to the needs of **increasing** the banking sector ability to **manage cyber risks** and of **coordination in case of attacks**
- is an opportunity for a **centralized coordination** of both the countermeasures and the prevention activities in order to set up a cybersecurity strategy even more effective

TO INCREASE CYBER KNOWLEDGE AND AWARENESS

- To **analyse contents** and **impacts** of any **new regulation** dealing with Information Security
- To define and conduct **awareness campaigns**
- To set up and attend **exercises** on **cyber risks** and **attacks**

TO FURTHER DEVELOP AND ENFORCE INFORMATION SHARING

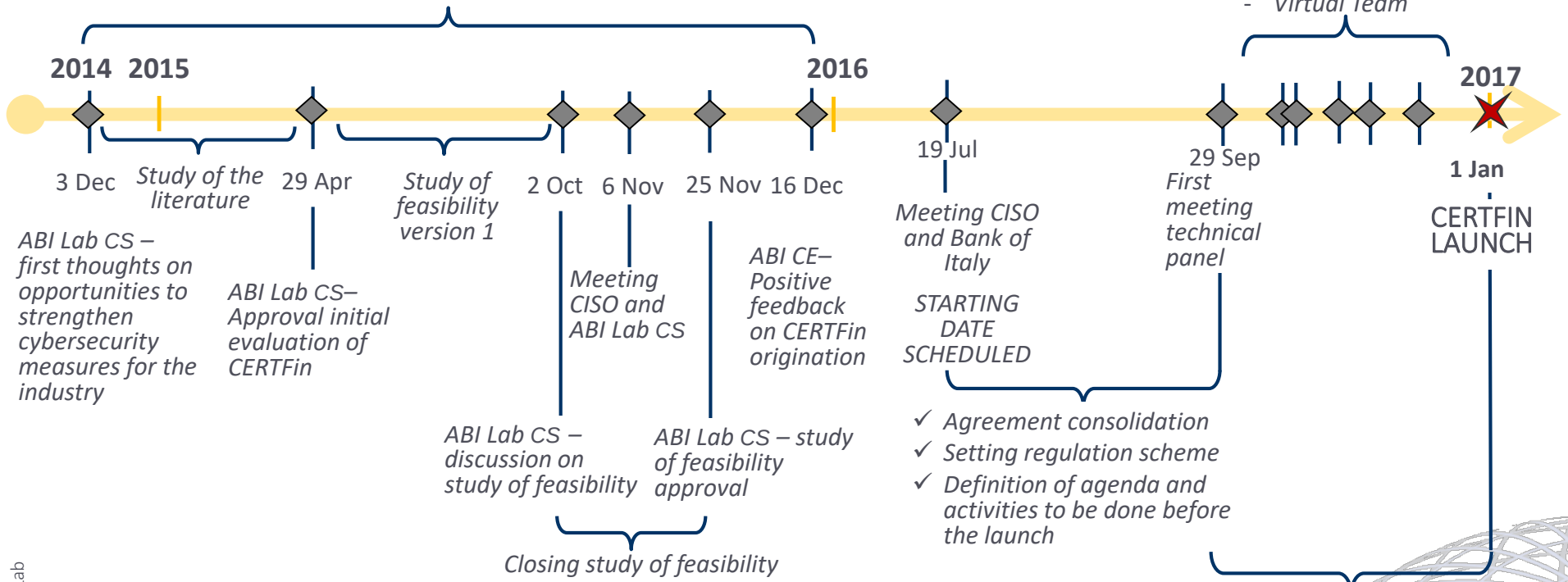
- To **increase** the **infosharing** activities on computer threats/ vulnerabilities/ incidents
- To carry out **advanced analysis** and intelligence on cyber threats
- To study the **amplitude** and the **evolution** of the **phenomena**

TO COORDINATE IT SECURITY EMERGENCIES AND INCIDENTS

- To carry out **central coordination activities** in case of **incident**
- To **support operationally** the **cybersecurity** structures **of each banking entity**
- To share **lessons learned**, in order to prevent **further incidents** in other **banks**

A walkthrough from the idea to the launch

- ✓ *Meetings and consultations with DIS, ABI Lab, and Bank of Italy*
- ✓ *Call one-to-one ABI Lab – banks*
- ✓ *Meetings one-to-one Bank of Italy– banks*
- ✓ *Session ABI Lab – Bank of Italy on the feasibility study*



- ✓ *Agreement consolidation*
- ✓ *Setting regulation scheme*
- ✓ *Definition of agenda and activities to be done before the launch*

- ✓ *Agreement subscription*
- ✓ *Release first version of the Regulation*
- ✓ *Definition of the constituency*
- ✓ *Detailed definition of the work program*
- ✓ *Analysis and activation of basic ICT infrastructure*
- ✓ *Detailed definition of the budget*
- ✓ *First formulation of the services*

CS: Steering Council ABI Lab
CE: Executive Committee

CERTFin activation – Italian Financial CERT

The 1° of January 2017 the CERTFin has been activated

What is the CERTFin?	The CERTFin – Italian Financial CERT is a **public-private cooperative initiative** targeted to enhance both the ability of banking and financial operators to manage cyber risks and the cyber resilience in the Italian financial system.
Who can participate?	The **participation** to the CERTFin is **open**, on a voluntary base, for every operator of the national banking and financial sector, as: payment service providers, banking and financial intermediaries, insurance companies, market infrastructures operators, services centres and providers of services technologically relevant for the sector.

CERTFin – Italian Financial CERT
The mission

- To facilitate the **timely exchange of information** within the sector about potential cyber-threats

- To **act as a liaison** between the financial sector and institutions concerning protection against cyber-attacks and IT security

- To **facilitate responses** to large-scale cyber-incidents

- To **support the cyber-crisis solution** process

- To **cooperate** with similar Italian and international institutions and with other public and private cyber-security agents

- To **raise awareness** and promote a culture of security

CERTFin – Italian Financial CERT
The value

The activation of the **CERTFin** can **bring advantages for all actors** involved in cybersecurity field:

GOVERNMENT

CERTFin responds to the governmental need of a **structured and operational collaboration** between **public bodies** and the **banking sector** on cybersecurity matter, as underlined by the **NIS** Directive, by the **DPCM** on Cybersecurity, and in line with the feedbacks coming by the **G7**

ABI AND BANK OF ITALY

CERTFin supports **dialogue** and operational coordination with Bank of Italy in the **management** of **cybersecurity emergencies**, **incidents** and **issues**, in line with national and European regulations for the sector (Circular 285, PSD2), and enhances the role of **ABI** at both national and European level on **cybersecurity strategy**, that is fundamental for the **Digital Transformation** of banks

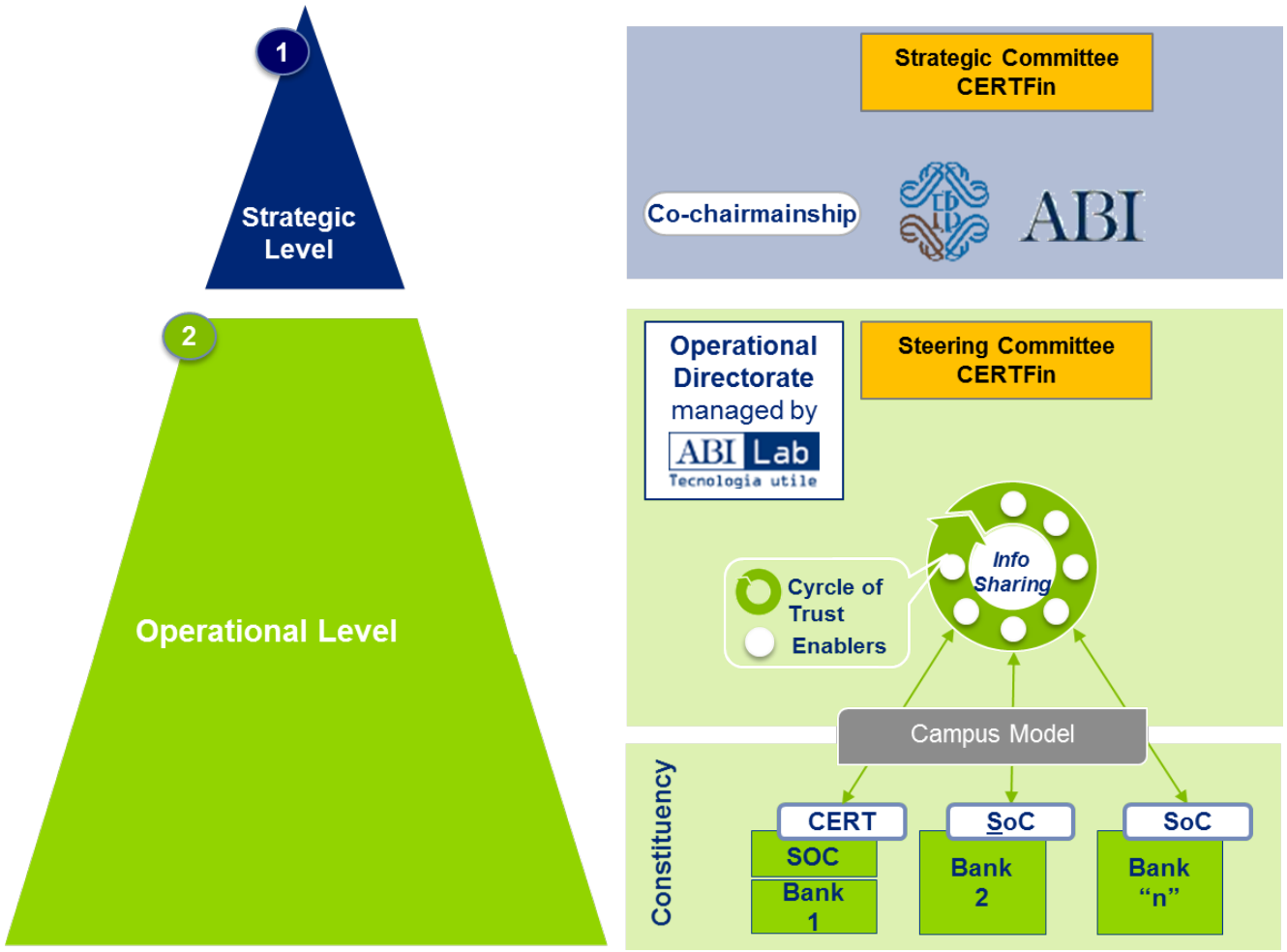
INSTITUTIONAL STAKEHOLDERS AND COMPETENCE CENTRES

CERTFin can become a privileged **point of contact** for the industry in the **dialogue** with **National CERT**, with the **Law Enforcement Agencies** and with **leading research networks** and **experts**, for all cyber issues of common interest

BANKING AND FINANCIAL OPERATORS

CERTFin can **disseminate** competences and initiatives on cybersecurity management, by enabling shared procedures of dialogue and exchange, supporting the industry to the **regulatory compliance**

Organisational and governance structure of the CERTFin



Strategic Committee: it sets the CERT's governance policies and industry development guidelines in response to trends in fraudulent phenomena and cyber-attacks

Steering Committee: it determines and directs operational management of the service offered to participating banks and provides the Strategic Committee with an overview of the current situation, its impact on the industry and effective responses at the operational level and for individual banks

Operational Directorate: it is responsible for CERTFin's operating activities, record-keeping for committees and managing participants

Virtual Team: group of members that actively contribute with own resources to the CERTFin functioning, under the coordination of the Operational Directorate

THE AGREEMENT SIGNED BY BANK OF ITALY, ABI AND ABI LAB DEFINES THE METHODS OF COORDINATION IN THE CERTFIN GOVERNANCE

CERTFin – Italian Financial CERT
Overview

OPERATIONAL TOPICS

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)

CYBER KNOWLEDGE AND SECURITY AWARENESS

CYBER EMERGENCY AND INCIDENT MANAGEMENT

About us:

The **Financial CERT** it is quoted in the report "*Relazione sulla politica dell'informazione per la sicurezza - 2016*" published by DIS and available at the following link:
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/02/relazione-2016.pdf

Subscriptions:

35 subjects joined to the CERTFin
9 participants in the **Virtual Team**

www.certfin.it

Operational Collaborations

NATIONAL OPERATIONAL COLLABORATIONS

Polizia Postale e delle Comunicazioni → Platform

National CERT → Information Sharing

Possible participation to initiatives and partnership already consolidated

INTERNATIONAL OPERATIONAL COLLABORATIONS

Cybersecurity Working Group (EBF)	Banking Associations, banks and EC3
FI-ISAC – Financial Institutions Information Sharing and Analysis Centre (ENISA)	Banks, Law Enforcement Agencies. Banking Associations, CERT, ENISA and EC3
PSSG – Payment Security Support Group (EPC) *CFPF – Card Fraud Prevention Forum (EPC)*	Banking Associations, banks and EC3
European Cybercrime Center (Europol)	Police forces in collaboration with banks on topics of common interest
FS-ISAC – Financial Services Information Sharing and Analysis Center	International banking and financial operators

DEVELOPMENT: *Ongoing the dialogue with other CERTS (NO, DK, RU) to establish new collaborations*

RESEARCH PROJECTS (ONGOING)

IT platform and partnership model between banks and European polices for the information sharing on frauds and cyber attacks

Ongoing the participation to other calls funding other projects focused on the cybersecurity

CERTFin activities report – Jan-Apr 2017
Cyber Knowledge and Security Awareness – Obs. CyKSA

INSIGHTS

- Debate and update on all **IT Security regulations** with impacts on the industry, even during the public consultation phase (RTS EBA on SCA and CSC, CP EBA on Incidents Reporting, etc.)
- **Participation in national and pan-European working groups** to support the industry with the analysis and the understanding of the regulations (EPC-PSSG, EPC-CFPF, EBF Cybersecurity WG, FI-ISAC, Mission in USA International Visitor Leadership Program)
- **Coordination of activities** to comply to the Customer Security Program and dialogue with SWIFT members
- Insights on **GDPR** security focused to support the activities of the ABI Lab Observatory Information Governance

RESEARCH AND ANALYSIS

- Planning together with the banks and execution of the **survey on internet and mobile banking frauds 2017** → Results published at Banks & Security 2017 (23-24 May 2017)
- Leading the activities of the **EU OF2CEN project** - **focus WP2**

MEETINGS/CALLS Observatory CyKSA

- **2 meetings** (03/03, 20/04)
- **3 conference calls** (12/01, 03/02, 24/02)

PLANNING

- Next **appointments** and **events** on the Observatory agenda

CERTFin activities report – Jan-Apr 2017
Information Sharing – FinISAC

OPERATIONAL HIGHLIGHTS

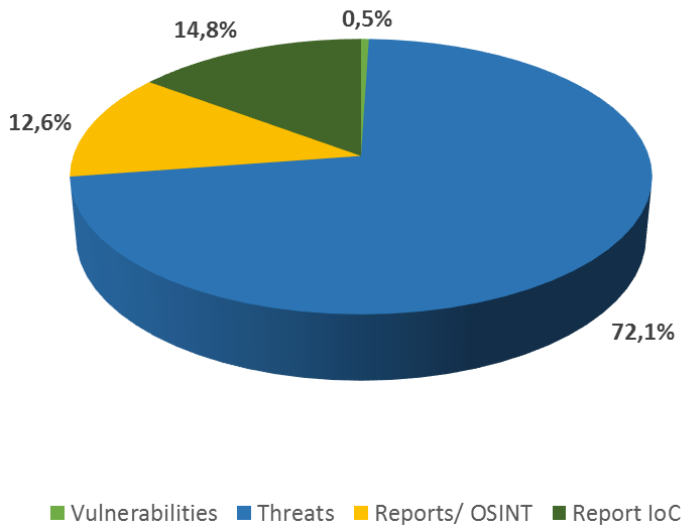
More than **200** cyber events analysed and shared

More than **70 warnings** sent to single FI on potencial comprimises

More than **42** insights and continuous monitoring of specific vulnerabilities

More than **18600** recipients of communications and warnings

TYPES OF CYBER EVENTS



RELATIONS WITH CONSTITUENCY AND STAKEHOLDERS

12 Virtual Team sessions
2 Infosharing sessions open to the CERTFin members
3 Planning meetings (SAL, MISP, Architectures)

Debate and Sharing of the main events with CNAIPIC, Telco Provider and National CERT

Main remarks

- The **CERTFin** is responding to the need for greater **collaboration** and **coordination** among banking and financial operators, as demonstrated by the **large participation** in the initiative already involving **35 subjects**

- The initiative is leading to the **strengthening** of a series of **operational relationships** between **banks** and **relevant stakeholders**, enabling them to **catch events** and **situations** more **effectively** and **timely** than in the past

- CERTFin is a **complex** and **challenging initiative** asking for a further **developments** among which: the evolution of the **ICT infrastructure** supporting the services provided, the definition of **training excercises** and **awareness programs** and the **automation** of the **Information Sharing activity**