

Poste Italiane CERT: Strategy, Mission, and Services

40° TF-CSIRT Meeting

London, 27h September 2013





Poste Italiane is one of the main Italian organization with 144,000 employees, 13 Mln of online customers and a widespread presence in Italy with 12,000 post offices. It provides financial, logistics, postal, insurance, digital communication, mobile and TLC services.

Finance and Insurance

- 5.8 Mln banking account
- 18 Mln payment cards
- 10 Mln prepaid card

Logistics and Postal

- 12,000 postal offices
- Ecommerce services
- 38,000 vehicles

Digital communication

- Web channel – more than 70 Mln page/month viewed
- Certified email

Mobile and TLC

- >3 Mln SIM cards
- 23,500 postman with mobile terminal for mobile services

With 144,000 employees, Poste Italiane is the largest Italian company and State owned enterprise

Poste Italiane's customers are citizens, Public administrations and private enterprises

Poste Italiane provides traditional and new services through internet and mobile channels

Poste provides e-finance, e-government, e-commerce, e-post digital communication services

POSTE ITALIANE NEEDS

- **Protecting customers** is a top priority in Poste Italiane business strategy
- Providing **secure and continuous services** is essential to guarantee customer satisfaction
- More and more sophisticated cyber attacks working on a global scale call for a deeper **cooperation at international level**



The evolution of the Cyber Security scenario calls to define a strategic approach

World increasingly interconnected

The technology pushes toward never ending interconnections

- People, machines, things
- Big data

The Society has never been so open and connected

- PA and Institutions
- Companies & People

New threats scenarios

- New criminal actors (governments, enterprises, cyber-criminals, ...)
- Globalization of attacks vs. local defense
- Industrialized attack processes (ex. hackers “for rent”)
- Advanced threats attacks (mobile devices, cloud, WiFi, big data, IoT)

Increase target to be protected

- Public sector
- Private sector
- Citizens
- Critical civil and military infrastructures

New strategic challenges

Legislation evolution

EU CYBER SECURITY STRATEGY

The proposed NIS directive (February 7, 2013) would require all Member States to:

- **Achieving cyber resilience**
- Drastically **reduce cybercrime**
- **Developing cyberdefence policy** and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the **industrial** and **technological resources** for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

ITALIAN GOVERNMENT

A decree of the President of the Council of Ministers (January 24, 2013) sets forth the new government architecture that is entrusted with the task of facing potential cyber security threats in Italy

Italy has a new cyber security governance, pursuant a more precise accountability among governmental bodies and also opening to non public actors

Italy has to develop a national cyber security plan: the Prime Minister is in charge of adopting the plan.

Operators who manage critical infrastructure at national and European levels:

- **send communication** of each and every **security or integrity breach**
- use the **best practices** as well as **cybersecurity measures**;
- **supply information** to security information bodies
- grant access to the database for the purposes of cybersecurity
- assist in **managing the cybernetic crisis**.



New strategic challenges

The **Cyber Security** must be a **strategic priority** at Country level, under a European / international common framework:

- **Governance** and well established role system
- Real time **monitoring** and **sharing** critical incident response through **information** to key stakeholders
- Increase **people awareness** (culture, competences, behaviors)
- Promote advanced Cyber Security capabilities through stimulating **innovation industrial clusters** on prevention, even through PPP

POSTE ITALIANE CYBER SECURITY STRATEGY

Has focused on **cyber security as a strategic leverage** to provide secure services and protect customers, on-line services and transaction, acquiring an acknowledged **leadership at national level**

GOALS

TO PROTECT company's network and infrastructures, while **preserving customers privacy**, on line services and **service usability**

TO STRENGTHEN **collaboration between public and private** stakeholders to contrast cyber crime

TO INCREASE cyber security capabilities through **research, education and awareness**

TO INTEGRATE and coordinate **prevention, analysis and response** capabilities **through a unique interface**

POSTE ITALIANE NEW OPPORTUNITIES

As one of the **most advanced player in the cyber security** field, Poste is in a great position **to deliver cyber security services to the market**

SERVICES

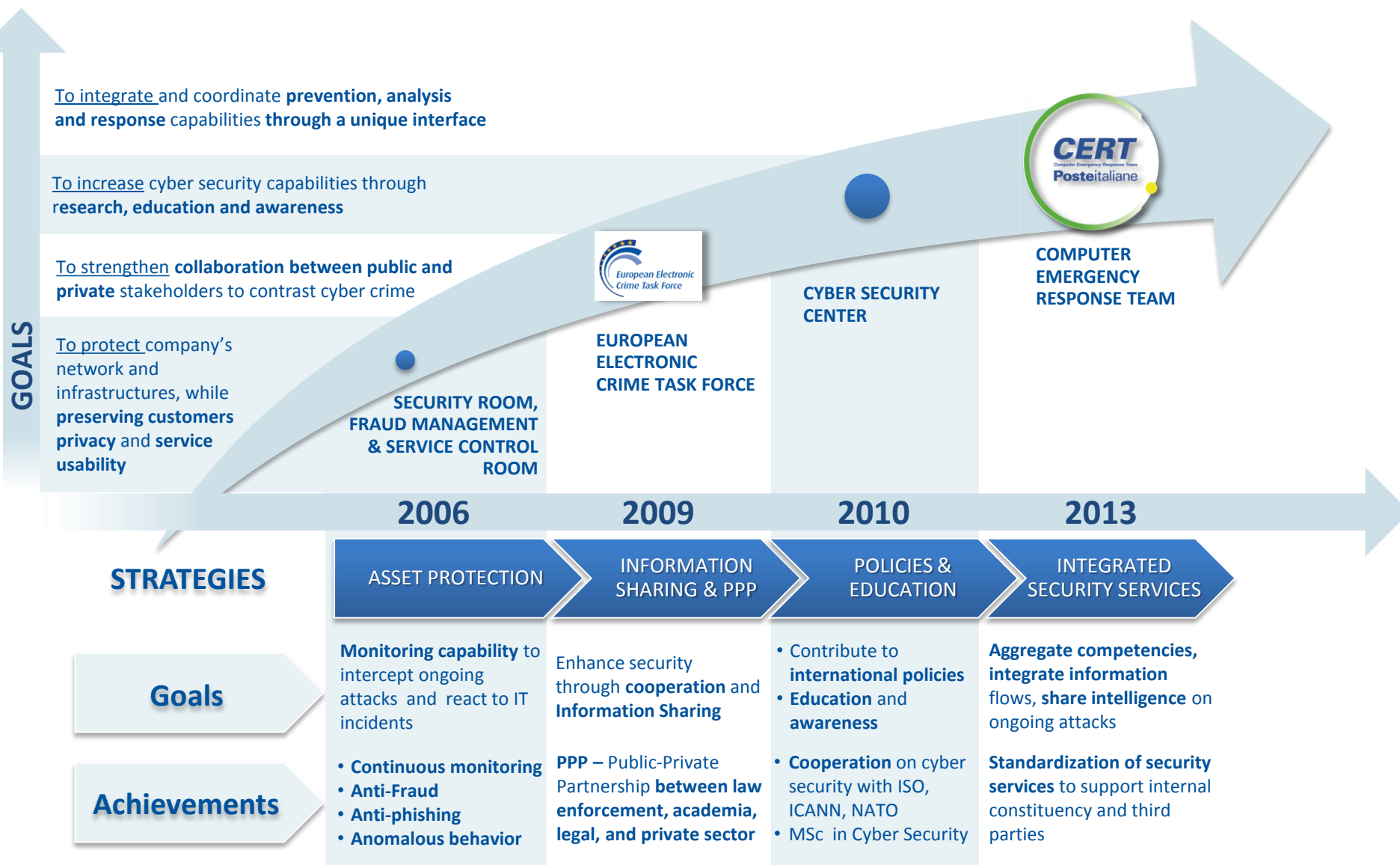
Prevention and protection services, specifically addressed to **SMEs**

National / local cyber security services might be **delegated** from PA bodies to market operators

Educational formats, deliverable through physical or virtual channels

Existing or **new offering** (ex. **Cloud**) integrated with **high level security standards**





Computer Emergency Response Team

Organization whose aim is to analyse the security of system and networks in order to provide response services to incidents, share early warning bulletins on vulnerabilities and threats and offers support for improving network and system security

Mission

“to provide a unique point of coordination of all the activities related to prevention and handling of cyber threats impacting the information assets of Poste Italiane, by an integrated management of all the relevant flows coming from each of the already active operation centers, and to represent, at the same time, a unique interface towards the outer world with reference to all the operative information exchange activities”



Constituency

*“refers to the **Poste Italiane Group**, the relevant **online services and its Customers**, including the **holding and the affiliates**: Poste Italiane SpA, Postecom, PosteMobile, Postel, PosteShop, PosteTutela. This initial constituency is planned to grow, in order to include all of the other entities belonging to the Group.”*



The 1st Computer Emergency Response Team (CERT) was created by Carnegie Mellon in 1988 at DARPA's direction in response to the Morris Worm



European Agency on Network and Information Security, whose mission is to support the creation of CERTs in Europe and to foster networking



Trusted Introducer is the European CERT network, a service infrastructure whose mission is to provide support for all security and incident response teams.



FIRST is the recognized global leader in incident response teams worldwide coordination and is the reference global network for CERT cooperation



Security Monitoring

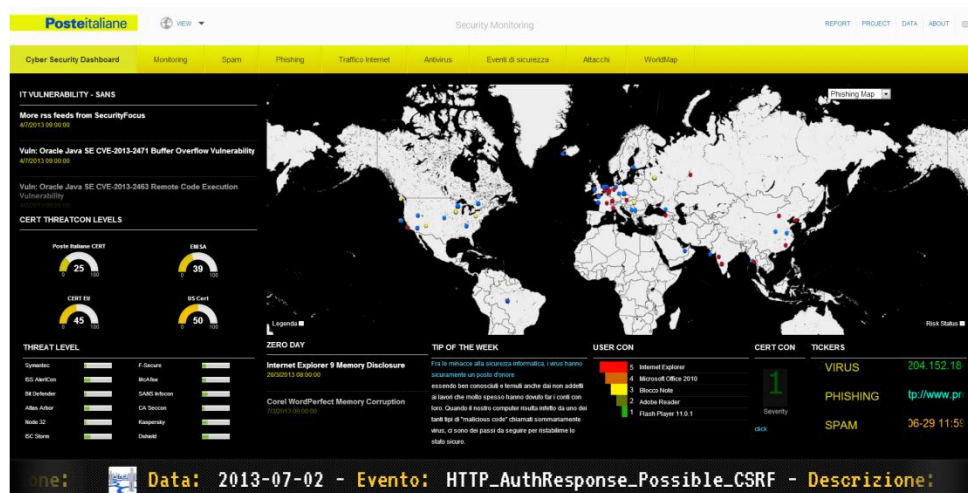
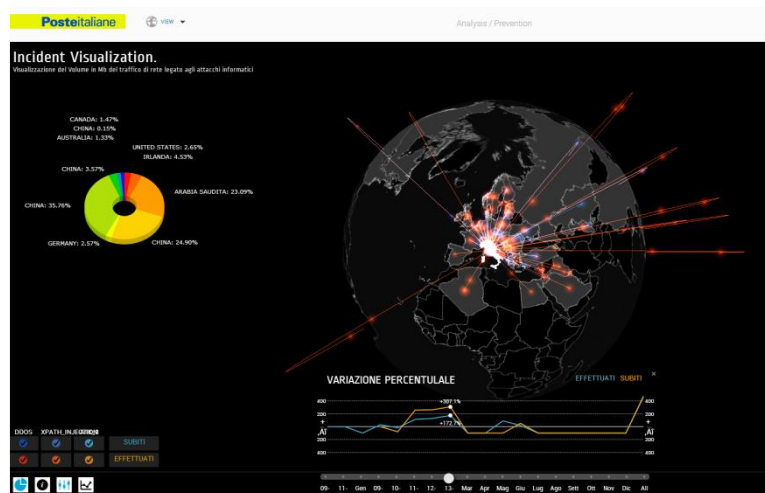
Real-time continuous monitoring of security status of systems and vulnerabilities in the wild, with the aim of detecting new potential attacks or security criticalities and give the start to effective response activities

Analysis & Prevention

Analysis and correlation of collected evidences and alerts coming from the monitoring activities, with the aim of preventing security incidents that may occur on IT systems and services, assessing their potential impact on business

Modeling & Simulation

Definition of mathematical models and algorithms to evaluate **potential IT impacts of cyber security threats**, by simulating their spread over the company's network and delivering worst-case scenario analyses



CERT
Computer Emergency Response Team
Posteitaliane



The Early Warning service aims at providing alerts to the PI CERT constituency

Main Goal

Early Warning aims at **identifying, analyzing** and **promptly reporting** emerging vulnerabilities and threats that may impact CERT constituency, also providing countermeasures for their mitigation

Information Gathering



Information collection:

Vulnerability information are collected from various sources, such as:

- Vendor vulnerability product information
- Websites
- Public and closed mailing lists

Analysis



Analysis of information collected:

- Trustworthy of the source is evaluated and further and deeper analysis are performed
- Information are filtered and classified basing on the criticality of the vulnerability reported

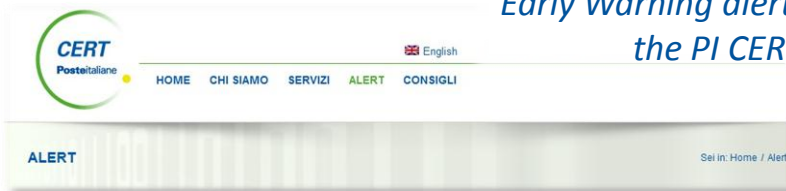
Vulnerability Alert



Distribution of information:

- Bulletins templates are filled with the Information processed
- Vulnerability alerts s are distributed to the constituents

Early Warning alerts will be available on the PI CERT web portal



Posteitaliane

It is structured in three main services:

1

Threat Intelligence

Threat analysis, including implications and actionable advices, about an existing or emerging techniques by means of direct involvement of internal and external security research centers.

- Threat Analysis Report
- Technology Watch Report
- Flash Report

Deliverables



2

Incident Investigation

Investigation of security incidents with an impact on networks under monitoring, through correlation of information from public and private sources, aimed at threat identification, quick response and mitigation.

- Incident Report Sharing
- Flash Report



3

Communication Center

Collection, analysis and dissemination of IT security related topics within all constituency and the relevant world communities of peers.

- Early Warning Bulletins
- Actionable Intelligence IS
- Knowledge Base
- EECTF Newsletter
- Trusted Networking Hub





- **OPERATIONAL CONSOLIDATION**

As a newborn organization supporting a large Group we have been investing to consolidate our internal processes and to formalize interactions within our constituency, in order to also properly design the relevant services and the underlying infrastructure

- **GLOBAL COOPERATION**

We have joined several international communities to foster information sharing of operational data and co-operate on incidents involving Italian critical information infrastructures

We are ready and willing to **cooperate with TF-CSIRT community**, sharing information, providing capabilities and developing joint analyses

- **INTERNATIONAL ACKNOWLEDGEMENT**

We have a roadmap to become **FIRST affiliate** and **accredited TI Members** by the end of 2013

- **CONTINUOUS IMPROVEMENT OF COMPETENCIES AND SKILLS**

TERENA training sessions and other international events



THANKS A LOT FOR YOUR ATTENTION



ANY FURTHER INQUIRY CAN BE SUBMITTED TO

cert@posteitaliane.it

