G7 ICT AND INDUSTRIES MULTISTAKEHOLDER CONFERENCE

SECURING THE CYBERSPACE FOR BUSINESS

POSTE ITALIANE S.p.A.

Turin, 25/9/2017

Chief of ICT Security Department

Rocco Mammoliti

POSTE ITALIANE
FACTS AND FIGURES

Coordinating about
141.246 employees
on average in the 2016 fiscal year

12.845 post offices
across the national territory

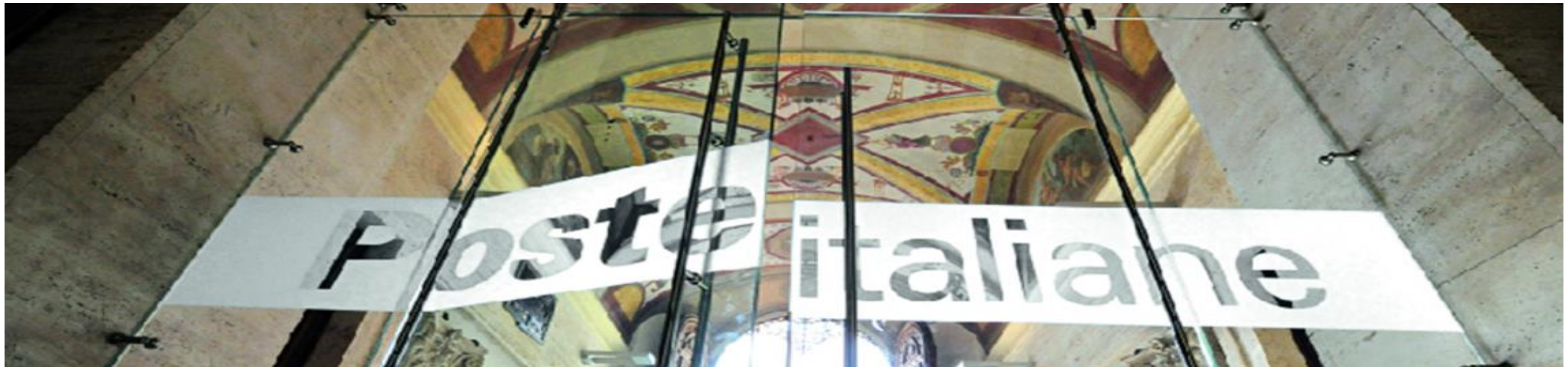
Total revenues
€ 18 Billion
for the 2016 fiscal year
+2,0%
respect to 2015 fiscal year

Financial services revenues
€ 5.294 Million

Savings and insurance revenues
€ 23.772 Million

Logistics and postal services revenues
€ 3.822 Million
in the 2016 fiscal year

Serving over
33 Million customers
in the 2016 fiscal year



12,7 Million customers registered on Poste Italiane online services

7.249 ATMs

250.000 daily access to poste.it

2.400 simultaneous access per day
on home banking website

1,4 Million SPID **registered users**

900.000 monthly accesses to SPID Service Provider

400.000 security events daily processed

Since 2014,
+16 projects
in the infosec domains
funded at National
and European level

Poste Italiane
made operative its own
CERT since 2013

DIGITAL ECOSYSTEM AND CYBERSECURITY

- Economic development heavily depends on ICT
- Protecting the cyberspace means protecting the business and the customers
- Cybersecurity is **mandatory** due to cyber attacks’ **impact on the business**
- The complexity of **interconnections** and **interdependency** means that weaknesses have a global cascading impact
- Cybersecurity becomes a responsibility **shared by all stakeholders and actors in the cyberspace**
- A **safe and trusted ecosystem** is a crucial condition for customers' trust and for the business development in the digital era.

DIGITAL ECOSYSTEM AND CUSTOMERS

Protecting the **business** requires protecting the **customer**

PROTECTING CUSTOMER DATA AND PRIVACY

PROVIDING SECURE PRODUCTS, SERVICES AND INFRASTRUCTURES

JOINING FORCES AGAINST CRIMINAL ORGANIZATION

Improvement and alignment of all **cybersecurity actors** in terms of **commitment** and **response** capability against the continuously **evolving cyber threats**

FOCUS ON MOBILE SECURITY

Mobile Apps are ubiquitous: e-health, finance, e-government, logistics, smart homes, automotive

(e.g. mobile banking apps becoming a preferred access channel to home banking operations)

PROTECTING CUSTOMER DATA AND PRIVACY

- Gathering sensitive data becomes easier
- Protection from stealing sensitive **financial and enterprise data**, personal **customers' data**, and data related to **defense and national security**.

PROVIDING SECURE PRODUCTS, SERVICES AND INFRASTRUCTURES

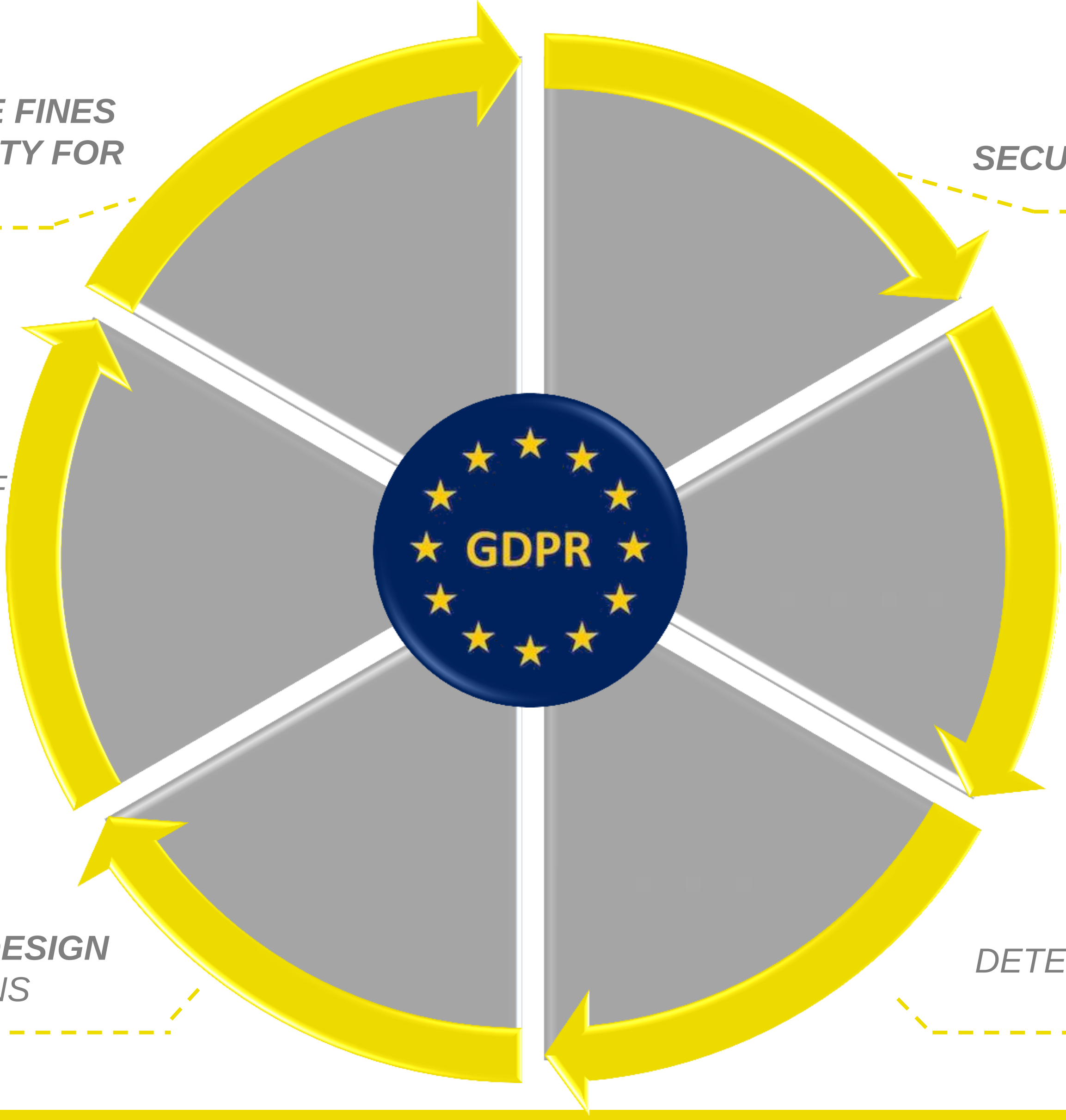
- **Mobile cybersecurity** necessary to protect both the customer and the company
- Mobile security: state-of-the-art **technical measures** + **risk management** of mobile apps (e.g. security-by-design, security monitoring, static and dynamic analysis of app, etc.)

JOINING FORCES AGAINST CRIMINAL ORGANIZATION

- Security perimeter beyond organization's boundary (app store, mobile operating system, app services)
- Same security threats for different player and sectors
- Need for **coordinated cyber threat intelligence and response**

FOCUS ON GENERAL DATA PROTECTION REGULATION – GDPR

EU REGULATION NO. 2016/679 (UE)



ART. 5

PRINCIPLES OF
SECURITY & ACCOUNTABILITY

ART. 32

APPROPRIATE
TECHNICAL & ORGANISATIONAL MEASURES

ARTT. 33 – 34

DATA BREACHES
DETECTION & NOTIFICATION PROCEDURES

ARTT. 25, 42 – 43

PRINCIPLE OF
DATA PROTECTION BY DESIGN
AND CERTIFICATIONS

ART. 35

DATA PROTECTION IMPACT ASSESSMENT
TO BE CARRIED OUT IN CASE OF HIGH RISKS FOR NATURAL PERSONS

ARTT. 82 – 83

HUGE ***ADMINISTRATIVE FINES*** *AND EXTENDED* ***LIABILITY FOR DAMAGES***

FOCUS ON GENERAL DATA PROTECTION REGULATION – GDPR

- **Implement appropriate security measures**, taking into account:
  - the state of the art
  - the costs of implementation
  - the nature, scope, context and purposes of processing
  - the likelihood and severity of risks for people rights and freedoms
- Data controllers/processors shall:
  - **detect** data breaches
  - promptly **notify** the breach details to the competent national data protection **authority**
  - If risk for rights and freedoms is high, data controllers shall **communicate** the breach to the involved **data subjects**

ONE SIZE DOES NOT FIT ALL

DETECTION AND NOTIFICATION AS KEY ASPECTS

GDPR requires a process for regularly *testing*, *assessing* and *evaluating* the effectiveness of such technical and organisational measures

LACK OF SECURITY often brings to LIABILITY AND HUGE FINES

FOCUS ON CYBER INSURANCE

MANAGING RESIDUAL CYBER RISK

Estimated cost of cyber attacks for businesses

$450 Billion a year globally

in 2016

Beyond businesses' efforts to defend their systems and customers, there is a need to transfer the

RESIDUAL CYBER RISK

CYBER INSURANCE

becomes a concrete and effective opportunity for businesses

The demand for cyber insurance increases in line with growth of cyber threats

In a **case analysis** realized by LLOYD'S, the losses from a cloud service disruption scenario were estimated to range from $4.6 billion for a large event to $53 billion for an extreme event, whereas in a mass software vulnerability scenario, the losses were estimated to range from $9.7 billion for a large event to $28.7 billion for an extreme event

The challenge is to develop

NOVEL MODELS FOR CYBER RISK ASSESSMENT

Today, cyber insurance market is estimated to worth between

$3 billion and $3.5 billion globally

and is projected to grow up to

$7.5 billion globally by 2020

The **understanding of cyber risks** makes it possible to **define insurance** classes, premiums and compensations

CYBERSECURITY AS AN OPPORTUNITY

Key aspect from business point of view:

cybersecurity sustainability

Public Private Partnerships (PPPs) to **create value** and to **limit costs** of cybersecurity:

- **Research institutions** contribute with innovation and state of the art methods
- **Law enforcement** contribute with response capabilities that companies simply cannot achieve
- **Companies** are the providers and the access owner of digital infrastructures and technological know-how

Global digital market of cybersecurity as a business opportunity:

- **Fast interaction** of small and large enterprises
- **SME and start-ups** adapt to the continuously changing threats and bring innovative security solutions to the market
- **Large companies** with complex security infrastructures can bring to the market part of their security infrastructure as-a-service

CYBERSECURITY AS A SHARED RESPONSIBILITY

Ubiquity of digital and mobile services: the need of **cybersecurity as a shared a responsibility** for a trusted digital ecosystem and supporting the business

User data gathering and profiling lead to success, but **privacy protection** is required

Cyber insurance: new business opportunity but **novel risk management models are needed**

Sustainability: join forces within PPPs and create new cybersecurity markets

Posteitaliane

poste.it