Competitive Methods to protect local Public Administration from Cyber security Threats (COMPACT)

Luigi Romano

71th Meeting of the IFIP 10.4 Working Group on Dependability and Security
Queenstown, New Zealand - January 26-30, 2017

COMPACT in a nutshell

- Innovation Action
- H2020 Call DS-02 – 2016
- Topic: Cyber Security for SMEs, local public administration and Individuals
- Start date: sometime soon
- Duration: 30 months; partners: 14; countries: 7
- Will deliver a comprehensive cyber-security solution for local Public Administrations that will be:
  - tested and validated across 5 pilots
  - involving 5 users
  - from 4 European countries

Consortium

Participant no.	Participant organisation name	Part. short name	Country
1 (Coordinator)	Engineering International Belgium sa	EIB	Belgium
2 (Tech. Coord.)	Consorzio Interuniversitario Nazionale per l'Informatica	CINI	Italy
3	INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS	INOV	Portugal
4	Silensec Limited	SIL	UK
5	Grupo S21sec Gestión, S.A.	S21SEC	Spain
6	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione	ISCOM	Italy
7	Austrian Institute of Technology	AIT	Austria
8	Katholieke Universiteit Leuven	KUL	Belgium
9	KASPERSKY LAB UK LTD	KSP	UK
10	Amadora Municipality	CMA	Portugal
11	Afragola Municipality	CDA	Italy
12	Bologna Municipality	BOL	Italy
13	Donostia-San Sebastián Municipality	DSS	Spain
14	Betrieb für Informationstechnologie Bremerhaven	BIT	Germany

Problem Statement

- The advent of the Internet has opened up new opportunities for Public Administrations (PAs) to improve their efficiency while also providing better services to citizens via an ever larger set of specialized networked applications, e.g. e-government, e-health, and more
- The cybersecurity landscape is thus changing, and Local Public Administrations (LPAs) are rapidly becoming an attractive target for cybercriminals
- The consequences of cyber-attacks to LPAs may be catastrophic - ranging from data losses and theft of intellectual property to control of smartly operated cities – with impacts both on individuals and on organisations

Main Issues

- Lack of standardized data classification
- Lack of effective Non-Disclosure Agreements (NDAs)
- Lack of plans for responding to security breaches and for disaster recovery
- Lack of uniformly enforced security policies
- Lack of adequate policies and practices for data disposal
- Lack of effective access control mechanisms
- Large set of legacy unmaintained and undocumented systems, representing an attack surface of unknown dimension.
- Inappropriate management of security updates (patches), as well as usage of out of date software in computers, mobile devices and central servers
- Limited capacity, and motivation, of LPAs personnel in detecting and reporting cyber-attacks

The Human Factor

- Since a major fraction of attacks succeeds exploiting human error, **cyber-security bottlenecks** can only be removed if security solutions:
  1. can effectively be used
  2. are well received by all the components of the LPAs’ workforce
- This translates into a number of challenges (and corresponding quality requirements), and in particular:
  - Solutions must be intuitively useable by all employees
  - It must be possible to persuade people to use them
  - They must fulfil the subtle needs of user groups with profoundly diverse characteristics
- So far, security solutions have mostly focused on technical software and security considerations
- With the prospective growth and associated quality demands, the **usability** (learnability, efficiency, error tolerance, and memorability), the **context of use** (different work settings, task goals, physical and social environment) and **user experience** factors (such as trust and accountability) need to be considered throughout the development cycle

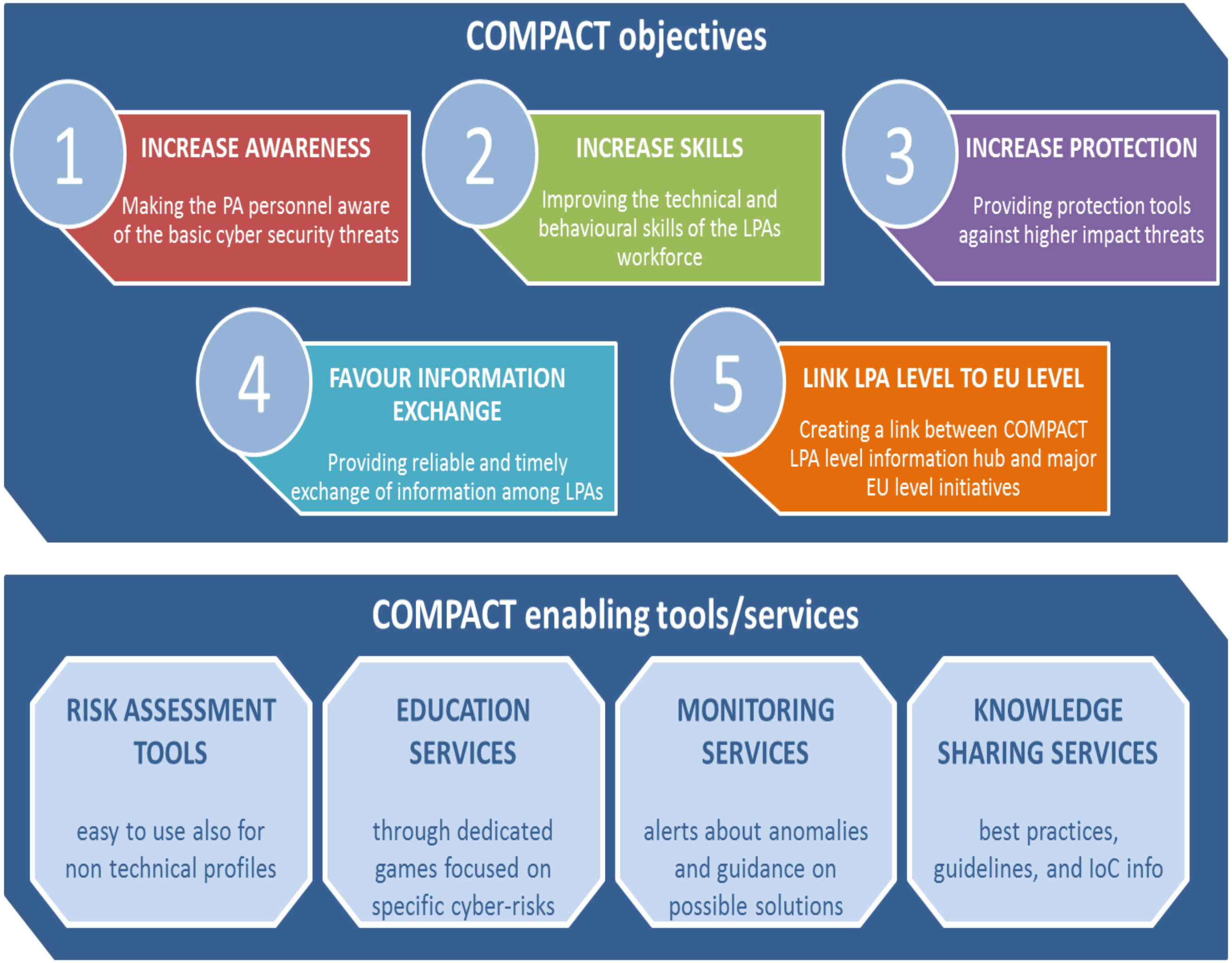
COMPACT objectives

- Make the LPA **personnel aware** of the **basic** - i.e. those with a higher impact on LPAs - cyber security **threats** they are exposed to
- Improve the **skills** – both **technical** and **behavioural** – of PA personnel via training tools that are well received by the (non IT-expert) workforce
- Provide **protection tools** against basic cyber security threats, e.g. phishing, ransomware, Bring Your Own Device (BYOD), jailbreaking the cloud, cross-site scripting, code (particularly SQL) injection, and more
- Create a LPAs level **information hub**, for favouring reliable and timely exchange of information among LPAs on cyber security **guidelines** and **best practices**, as well as on Indicators of Compromise (**IoC**)
- Link COMPACT **LPA level** information hub to major information sharing initiatives at the **EU level**

COMPACT tools/services

- Risk assessment tools
  - Tailored to the LPAs context
  - Will enable LPAs to prioritize countermeasures, for maximum efficiency of resource usage
- Education services
  - Dedicated game-based training
  - Take into account psychological and behavioural factors, to maximize effectiveness while also containing the training time
- Monitoring services
  - Continuously collect and correlate events
  - Timely spot anomalies and suggest recovery actions
- Knowledge Sharing services
  - Best practices and guidelines + connection to related initiatives

Objectives + tools/services



COMPACT objectives

1 **INCREASE AWARENESS**

Making the PA personnel aware of the basic cyber security threats

2 **INCREASE SKILLS**

Improving the technical and behavioural skills of the LPAs workforce

3 **INCREASE PROTECTION**

Providing protection tools against higher impact threats

4 **FAVOUR INFORMATION EXCHANGE**

Providing reliable and timely exchange of information among LPAs

5 **LINK LPA LEVEL TO EU LEVEL**

Creating a link between COMPACT LPA level information hub and major EU level initiatives

COMPACT enabling tools/services

RISK ASSESSMENT TOOLS

easy to use also for non technical profiles

EDUCATION SERVICES

through dedicated games focused on specific cyber-risks

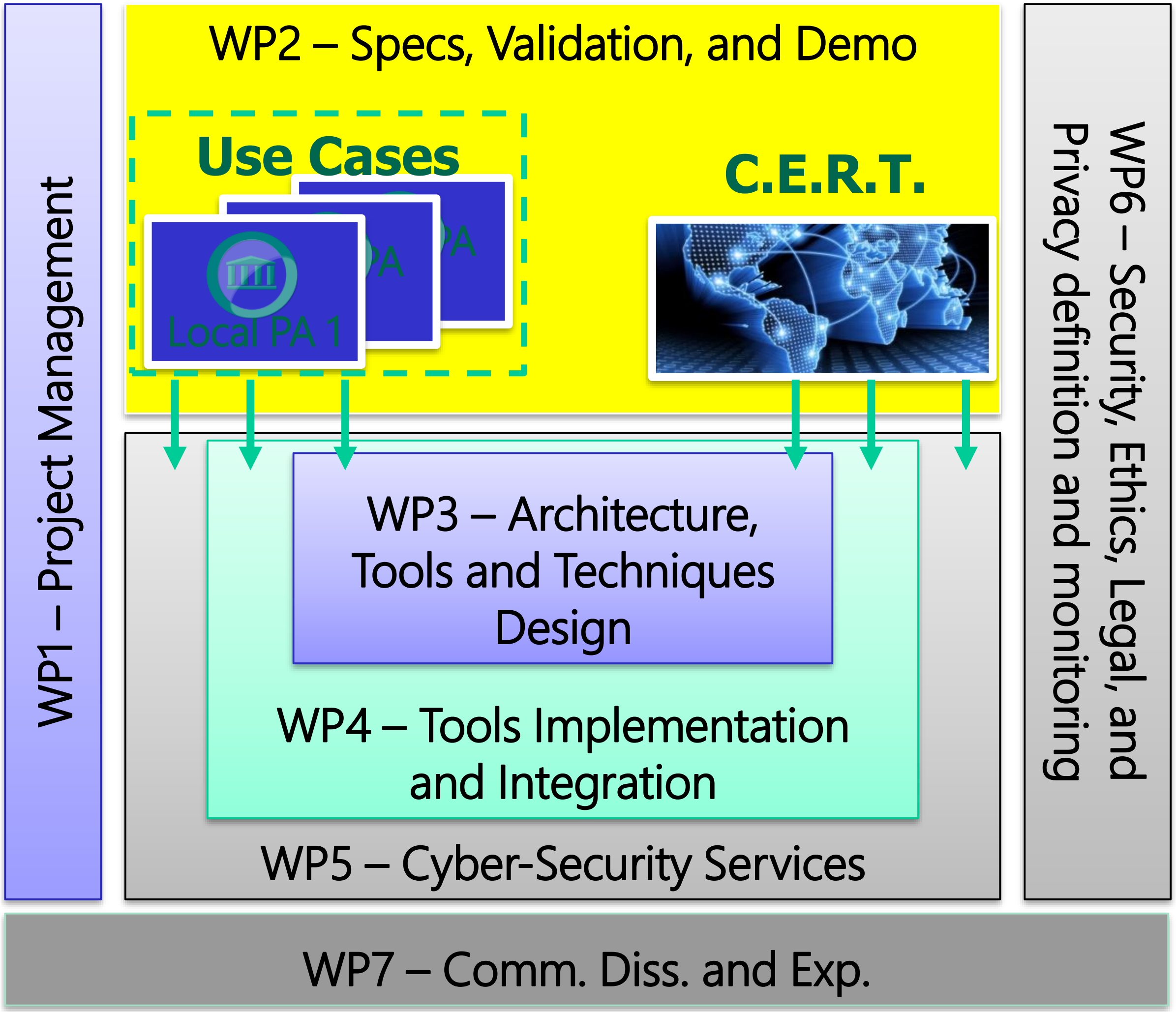
MONITORING SERVICES

alerts about anomalies and guidance on possible solutions

KNOWLEDGE SHARING SERVICES

best practices, guidelines, and IoC info

WP breakdown structure



WP1 – Project Management

WP2 – Specs, Validation, and Demo

Use Cases

Local PA 1

C.E.R.T.

WP3 – Architecture, Tools and Techniques Design

WP4 – Tools Implementation and Integration

WP5 – Cyber-Security Services

WP6 – Security, Ethics, Legal, and Privacy definition and monitoring

WP7 – Comm. Diss. and Exp.

Contact Info

Luigi Romano

e-mail: prof.luigi.romano@gmail.com

Cell: +39-333-3016817
Tel: +39-081-5476700

The **F**ault and **I**ntrusion **T**olerant **NE**tworked **S**ystem**S** (FITNESS)
Research Group
http://www.fitnesslab.eu/