



INTESA SANPAOLO
GROUP SERVICES

Cyber Physical Security

Un approccio necessario

Claudio Ferioli

Responsabile Sviluppo Sicurezza Fisica

Milano, 26 maggio 2016

La Cyber Physical Security

- Cosa
- Perché
- Dove
- Come

La Cyber Physical Security

- **Cosa è la Cyber Physical Security**
- Perché
- Dove
- Come

2010: game changer



Stuxnet

oggi: verso un *new normal* ?



DRAFT
Framework for Cyber-Physical Systems

Release 0.8

September 2015

Cyber Physical Systems Public Working Group

Una possibile **definizione**



Cyber-physical systems represent the “melting point” between the physical and cyber worlds.

Every time software is used to manage a physical process or physical phenomena are bridged with each other via software, a cyber-physical interface is available.

The integration of the physical, engineered systems with software environments enforces users to bridge existing silos...

ENISA Threat Landscape 2015

Una possibile definizione: un **approccio**



Cyber-physical systems represent the “melting point” between the physical and cyber worlds.

Every time software is used to manage a physical process or physical phenomena are bridged with each other via software, a cyber-physical interface is available.

The integration of the physical, engineered systems with software environments enforces users to bridge existing silos...

ENISA Threat Landscape 2015

Una possibile definizione: un **approccio integrato**



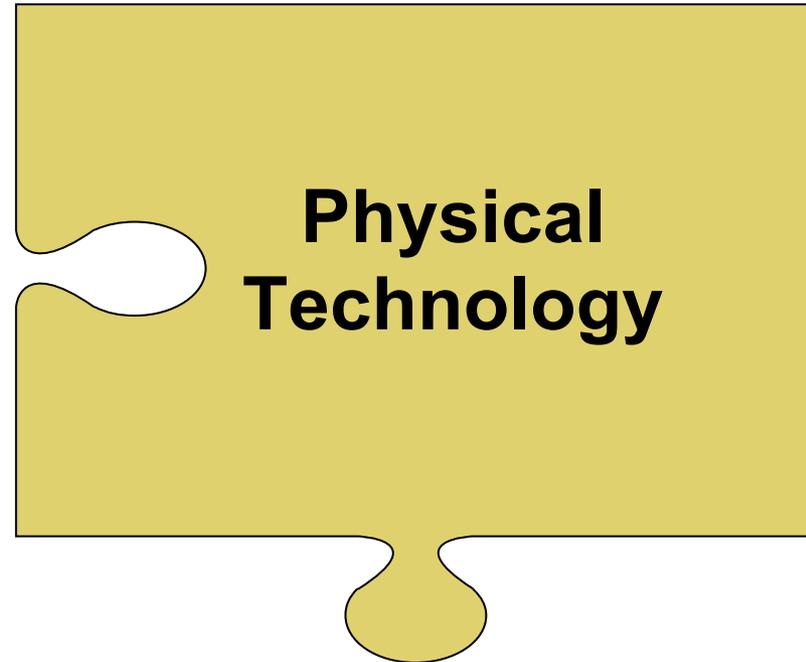
Cyber-physical systems represent the “melting point” between the physical and cyber worlds.

***Every time software is used to manage a physical process or physical phenomena are bridged with each other via software,** a cyber-physical interface is available.*

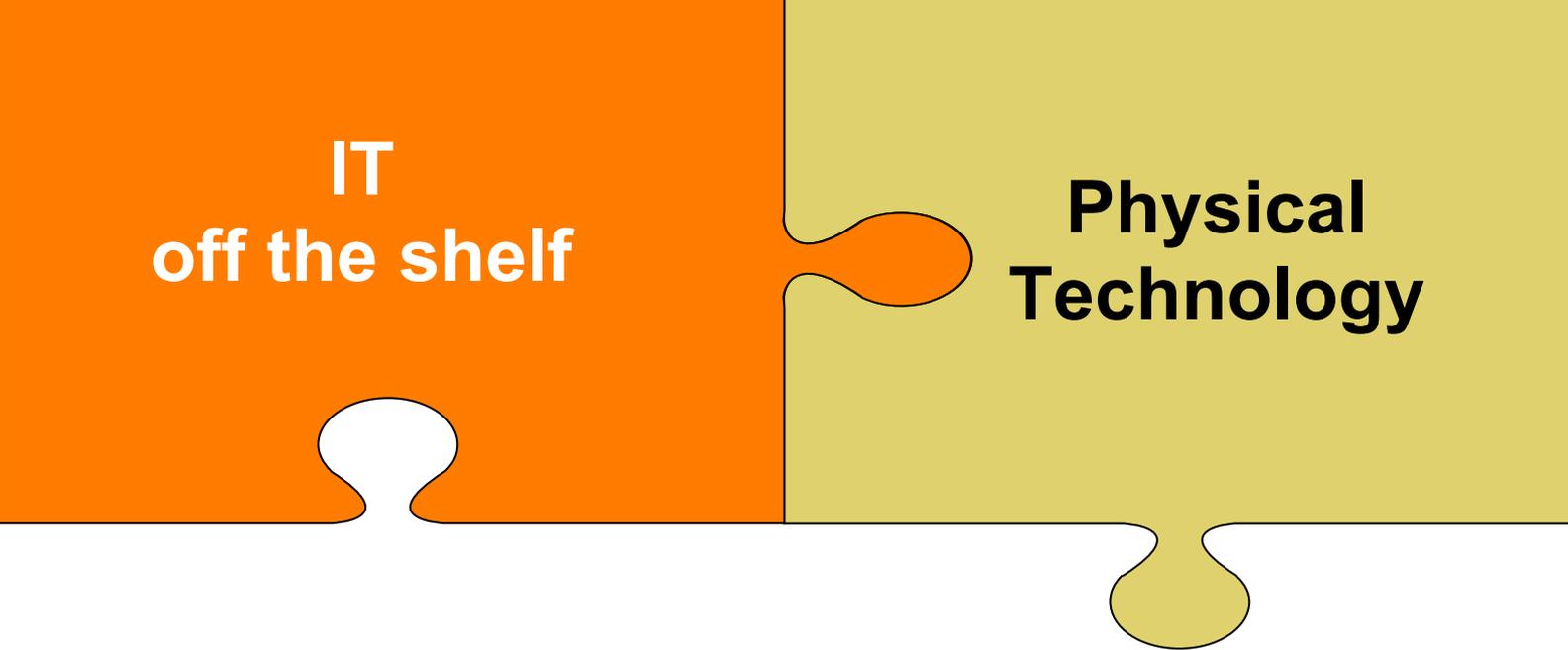
*The integration of the physical, engineered systems with software environments **enforces users to bridge existing silos...***

ENISA Threat Landscape 2015

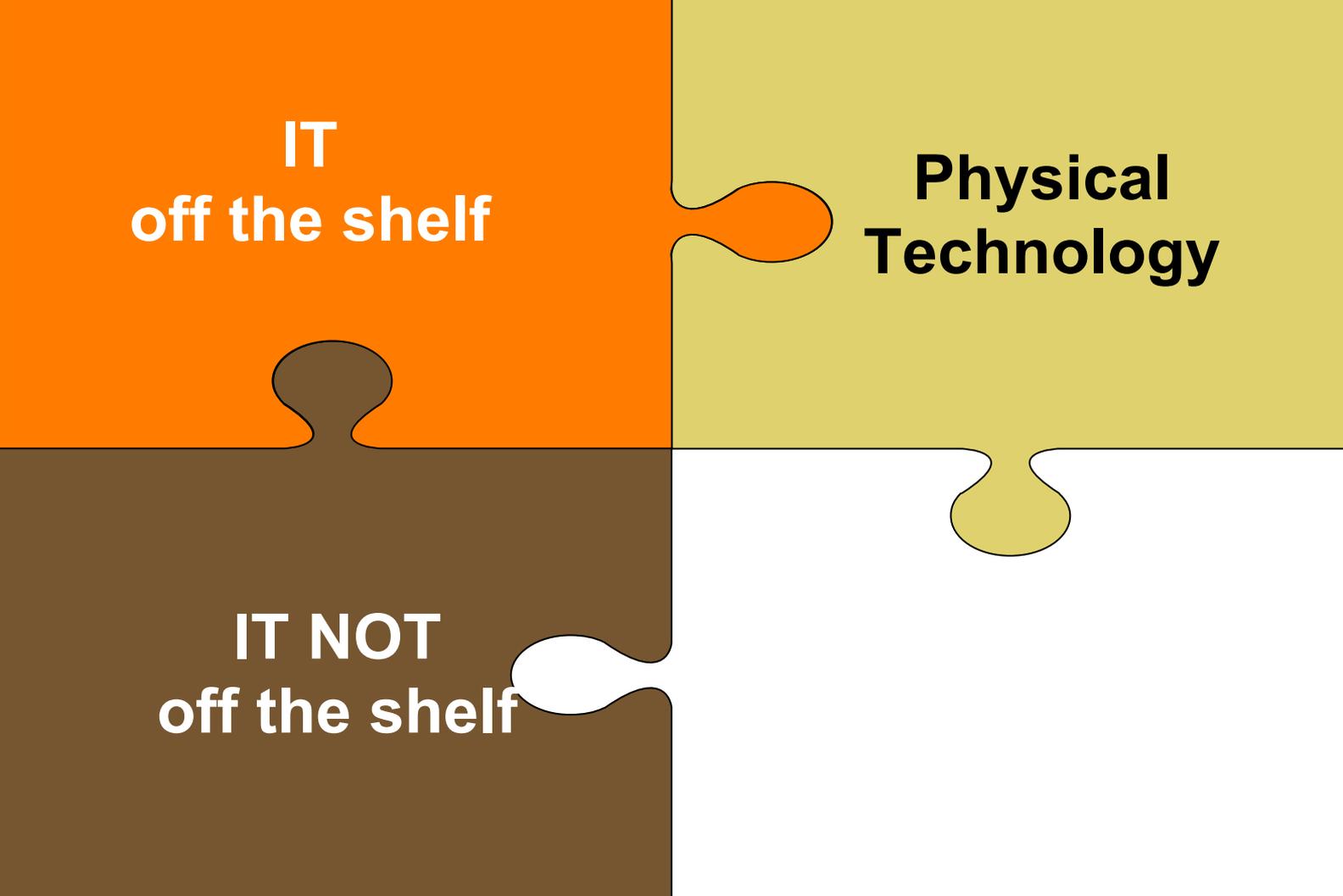
Una possibile definizione: un **approccio integrato**



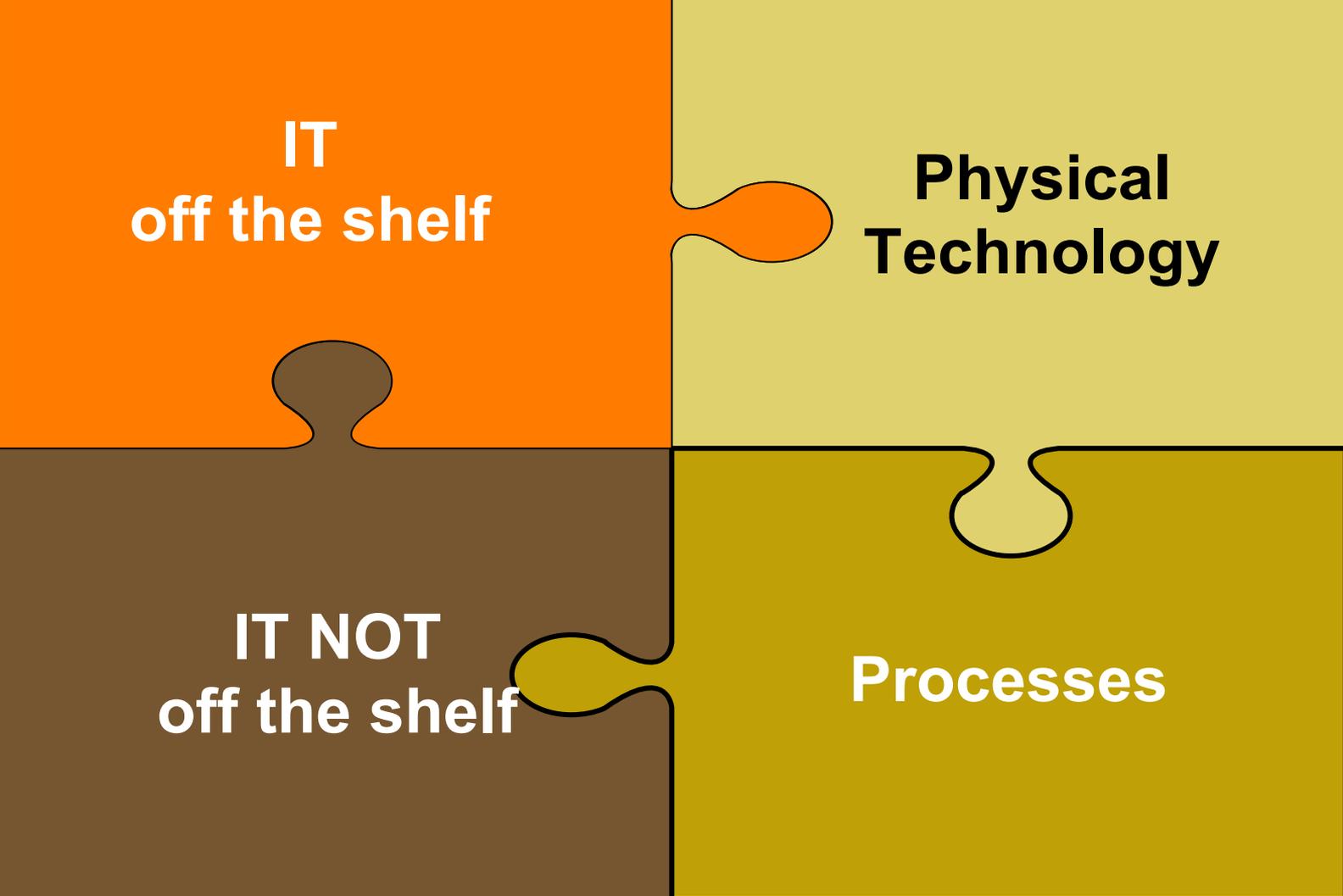
Una possibile definizione: un **approccio integrato**



Una possibile definizione: un **approccio integrato**



Una possibile definizione: un **approccio integrato**



La Cyber Physical Security

- Cosa è la Cyber Physical Security
- **Perché è necessario un approccio Cyber Physical Security**
- Dove
- Come

Una minaccia attuale ed emergente



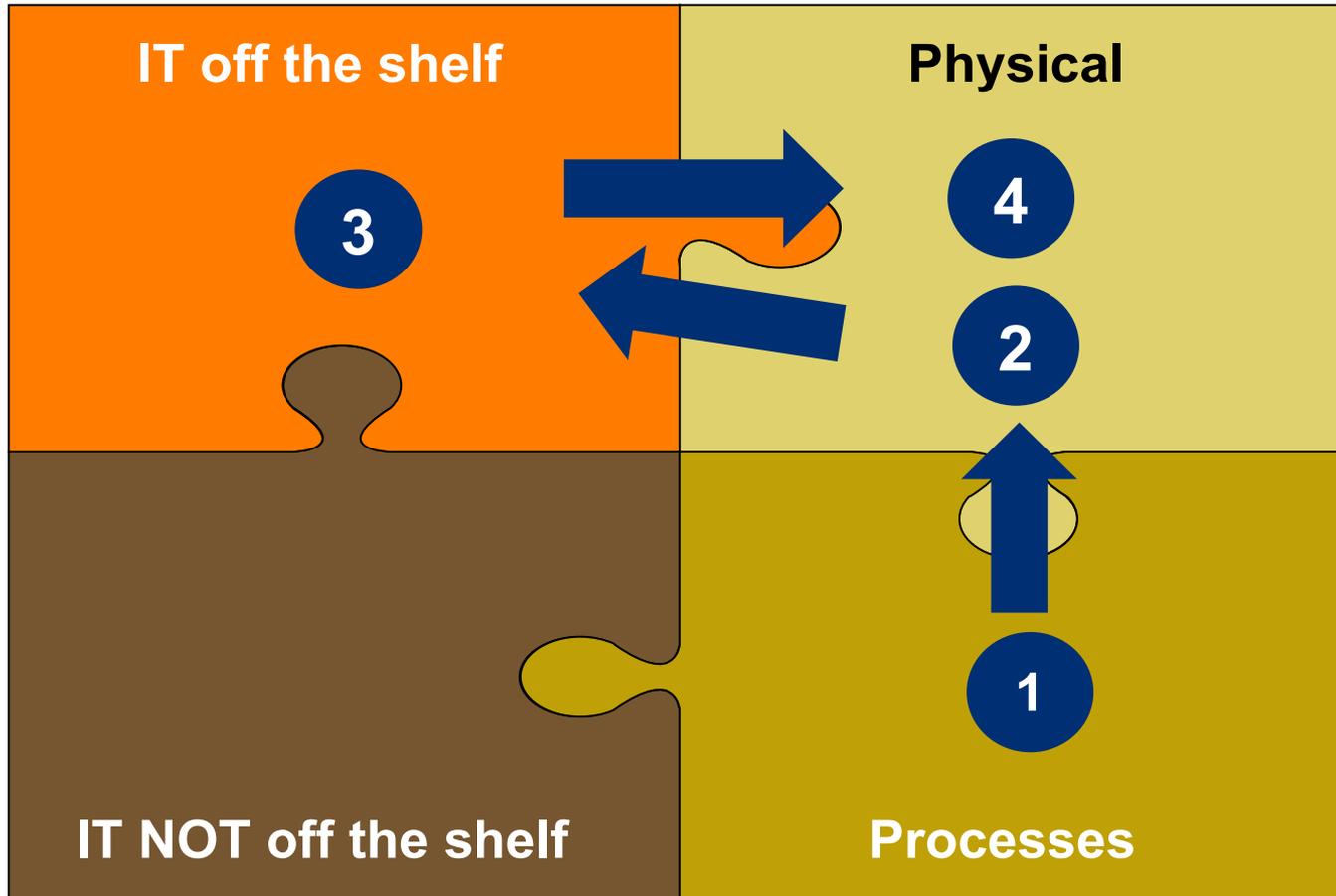
Nell'analisi 2015 viene considerata:

- una delle 16 **cyber threats** più rilevanti
- uno dei **3 attack vectors** principali
- una delle **tecnologie emergenti** più a rischio

Una minaccia attuale:

jackpotting

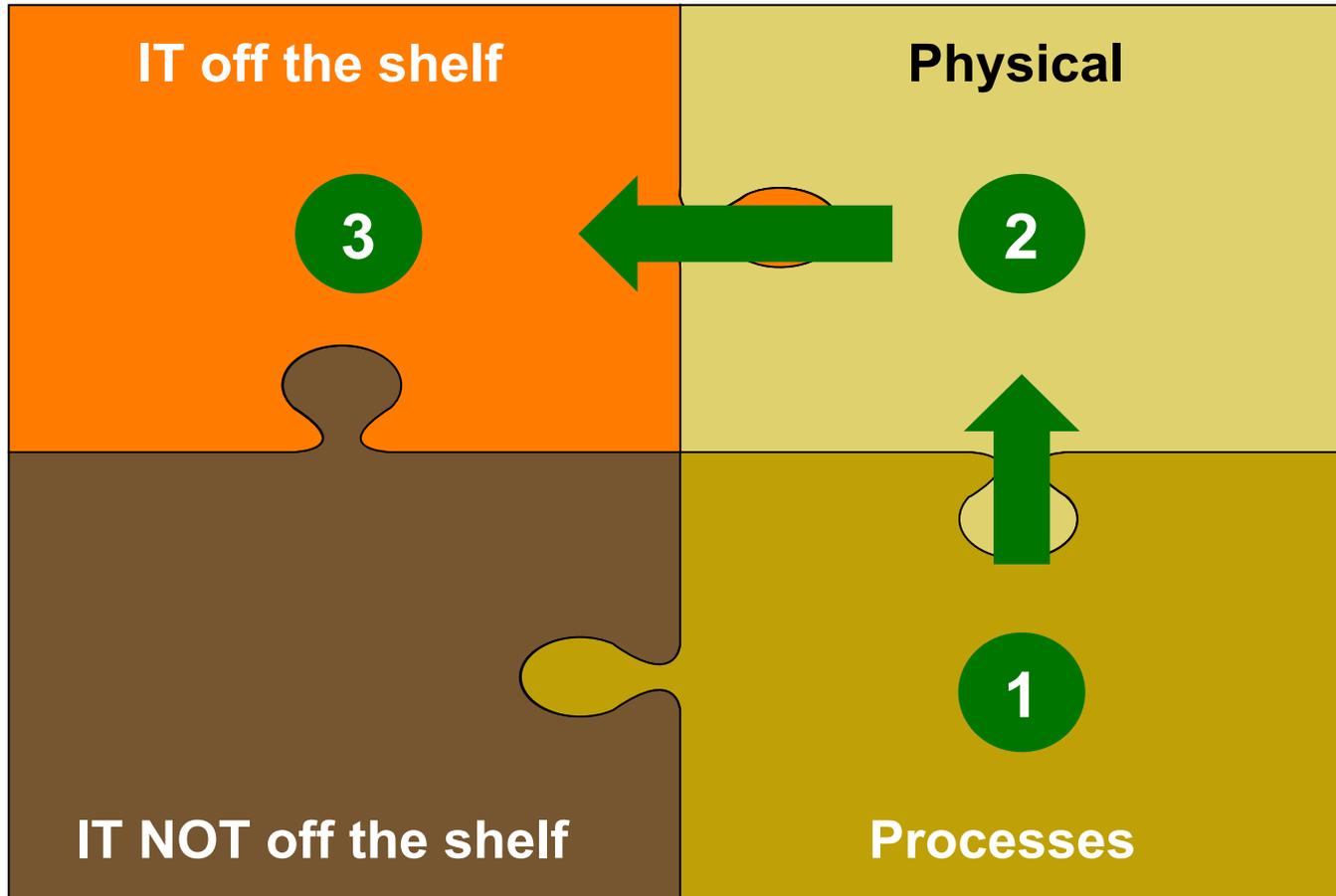
Target: cash nell'ATM



Una minaccia attuale:

keylogging

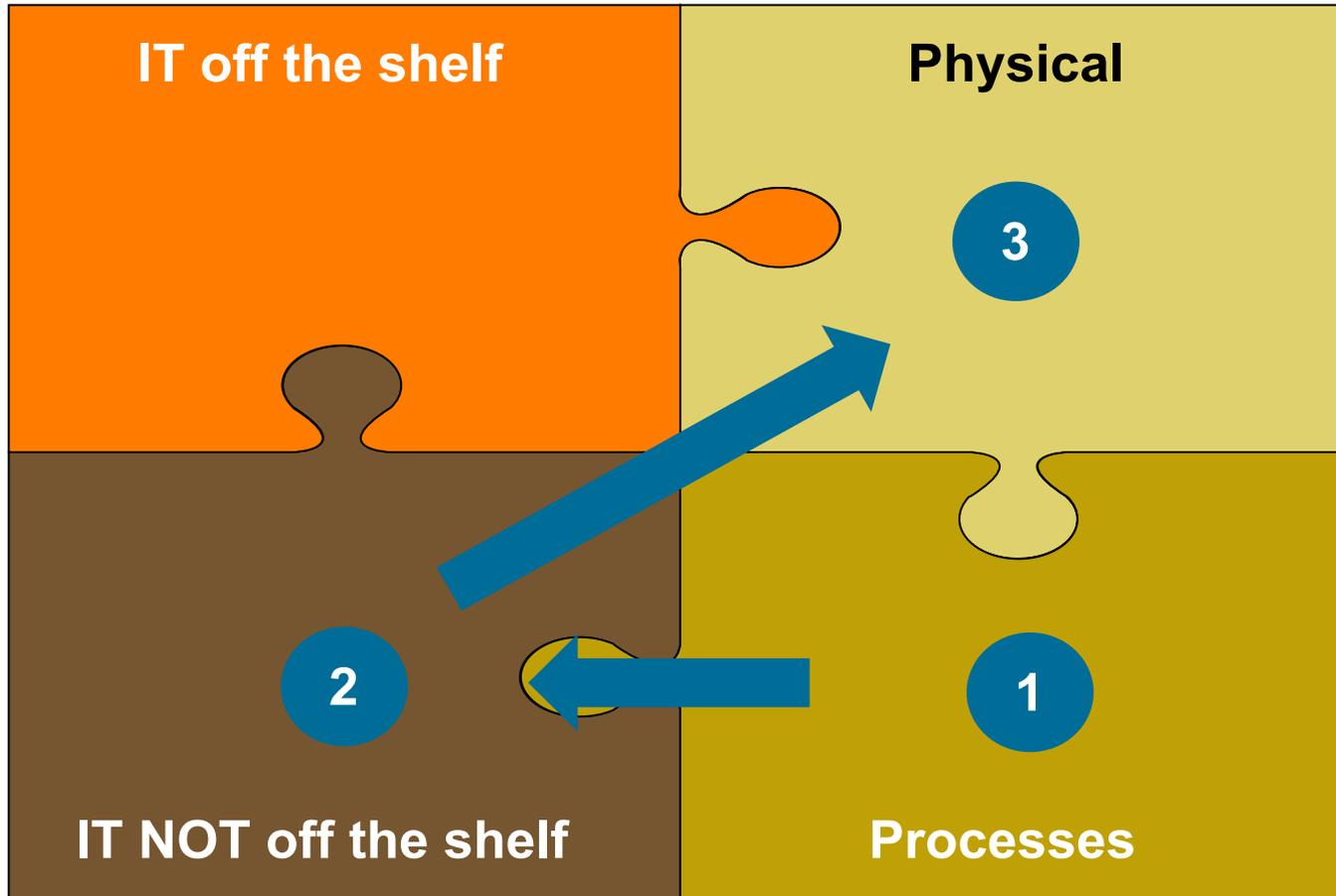
Target: dati / accesso applicazioni



Una minaccia attuale:

alarm neutralization

Target: caveau



La Cyber Physical Security

- Cosa è la Cyber Physical Security
- Perché è necessario un approccio Cyber Physical Security
- **Dove sono le difficoltà**
- Come

Brecce nell'integrazione delle componenti

**Ciclo di
vita**

**IT
off the shelf**

Breve

**IT NOT
off the shelf**

**Molto
Lungo**

Physical

**Molto
Lungo**

Processes

Lungo

Brecce nell'integrazione delle componenti

	<i>Ciclo di vita</i>	<i>Standardizzazione</i>
IT off the shelf	Breve	Alta
IT NOT off the shelf	Molto Lungo	Molto Bassa
Physical	Molto Lungo	Molto Bassa
Processes	Lungo	Bassa

Brecce nell'integrazione delle componenti

	<i>Ciclo di vita</i>	<i>Standardizzazione</i>	<i>Tempi reazione</i>
IT off the shelf	Breve	Alta	Brevi
IT NOT off the shelf	Molto Lungo	Molto Bassa	Lunghi
Physical	Molto Lungo	Molto Bassa	Lunghi
Processes	Lungo	Bassa	Molto Lunghi

Brecce nell'integrazione delle componenti

	<i>Ciclo di vita</i>	<i>Standardizzazione</i>	<i>Tempi reazione</i>	Competenze
IT off the shelf	Breve	Alta	Brevi	IT security
IT NOT off the shelf	Molto Lungo	Molto Bassa	Lunghi	Operational Security
Physical	Molto Lungo	Molto Bassa	Lunghi	Physical Security
Processes	Lungo	Bassa	Molto Lunghi	Organizational Security

Brecce nell'integrazione delle componenti

	<i>Ciclo di vita</i>	<i>Standardizzazione</i>	<i>Tempi reazione</i>	<i>Competenze</i>
IT off the shelf	Breve	Alta	Brevi	IT security
IT NOT off the shelf	Molto Lungo	Molto Bassa	Lunghi	Operational Security
Physical	Molto Lungo	Molto Bassa	Lunghi	Physical Security
Processes	Lungo	Bassa	Molto Lunghi	Organizational Security

La Cyber Physical Security

- Cosa è la Cyber Physical Security
- Perché è necessario un approccio Cyber Physical Security
- Dove sono le difficoltà
- **Come affrontare la CPS: spunti per una possibile agenda**

Spunti per una possibile agenda – 1. informare

**Inserimento nei *radar*
della sicurezza**

**Informazione al
personale delle funzioni
di sicurezza**

**Sensibilizzazione nel
settore**

Banca **ABI**

Spunti per una possibile agenda – 2. comprendere



Creare un metodo sul campo

Analisi degli incidenti

Assessment assets principali

Sharing best practices nella community della sicurezza

Repository incidenti di settore

Spunti per una possibile agenda – 3. intervenire



Policy

Piano mitigazione

Inserimento nel *business as usual* (training, analisi dei rischi, ...)

Stimolo del mercato

Standard

claudio.ferioli@intesasanpaolo.com