# Governing cyber risks for organizations' IT and OT assets

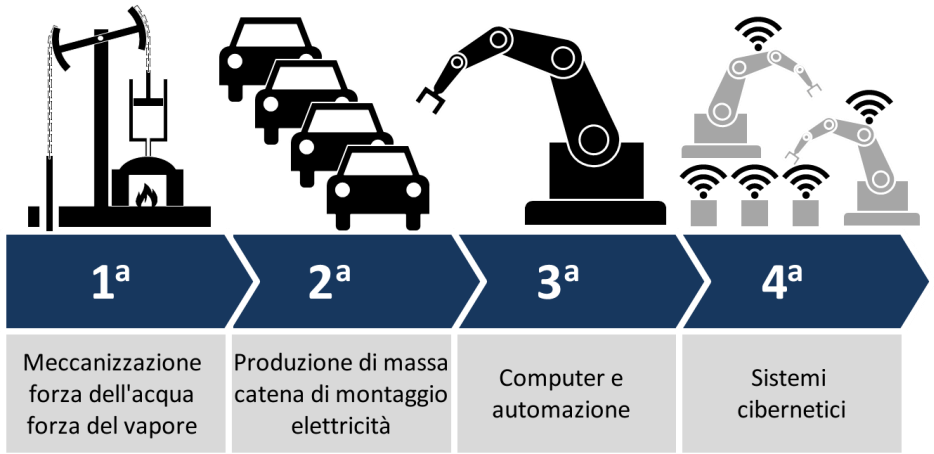
Marco Angelini

Marco.Angelini@eng.it

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

# Industry 4.0

- "The Fourth Industrial Revolution, or **Industry 4.0**, conceptualizes rapid change to technology, industries, and societal patterns and processes in the 21st century due to increasing interconnectivity and smart automation" (Wikipedia)



# CyberSecurity in the age of Industry 4.0

- **Industry 4.0** must face a series of **"cyber risks"** unthinkable until a few years ago
- The OT world was used to talk about **"safety"** meant avoiding **accidents** at work or damage to things
- **Expansion** of the **attack surface** due to the connection of the previously isolated system
- One of the **impacts of COVID-19** is the **reduction of on-site staff;**
- IT and OT are still missing a **holistic approach** that includes:
  - cyber-physical security,
  - an integrated cyber-risk estimation, and

# Emerging Industry 4.0 best practices

- Adopt a risk-based **security mindset** (tying business criticality to defense strategies).
- Keep an accurate **inventory of all OT assets** in real-time.
- Marry the best of IT and OT as an **integrated defense strategy** across all attack surfaces.
- Identify and **fix outdated systems**, unpatched vulnerabilities, and poorly secured files.
- **Real-time vulnerability assessment** and risk-based prioritizations.
- Ensure that **technology suppliers** and connected **equipment manufacturers** commit to **regular security and software patches and audits**.

# PrOTectME Solution

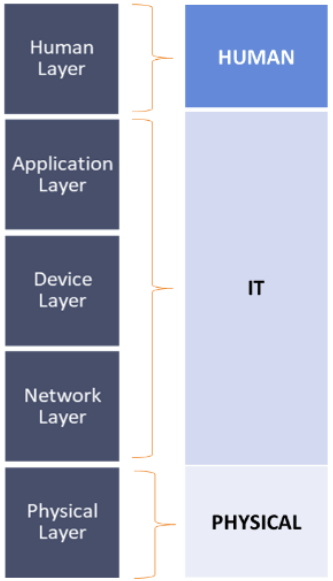
**PrOTectME** aims at addressing most of the needs by offering a methodology and a corresponding toolset to:

- **Model the infrastructure** at different level of detail
- Identify **weaknesses** and **vulnerabilities** that need to be addressed
- Identify the **major direct threats** to the company's tangible and intangible assets through a simple and straightforward procedure
- Determine the **cascading effects** on other company's tangible and intangible assets
- Estimate the **attack-related costs**

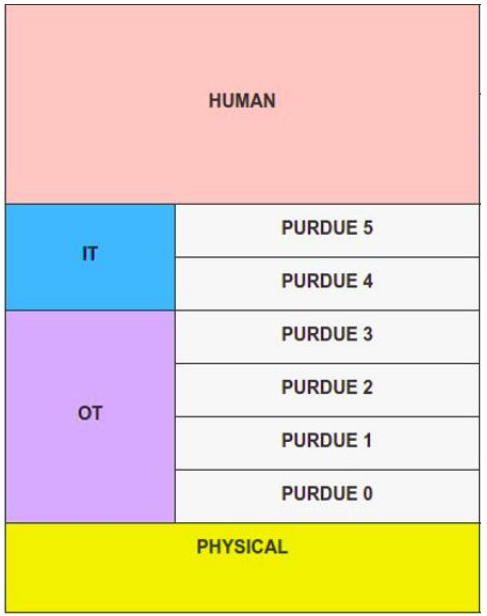
# IT vs OT

Threat Agents

Attack Strategies



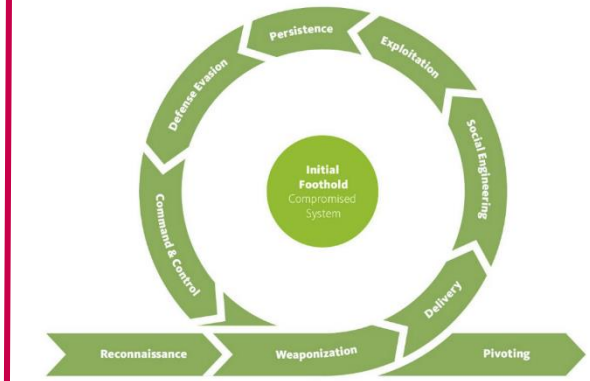

Attack Levels

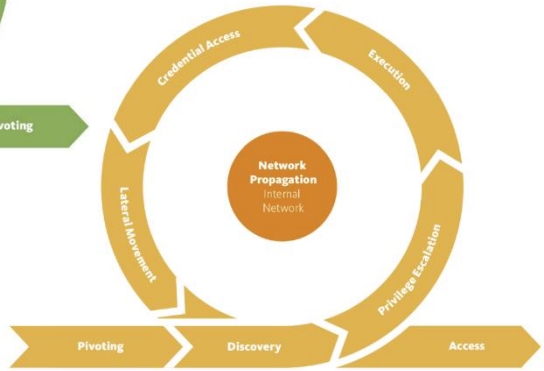


IT zone

OT zone

# IT vs OT



Cyber Kill Chain
+
MITRE ATT&CK
=
**Unified Kill Chain**

# RATING-OT

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

# How to evaluate the risk?

RATING-OT is a decision support tool
whose aim is to profile both privacy and cyber-security **RISKs**
for business services and main assets.

***RISK* = Criticality * *IMPACT***

**Criticality = Attack Likelyhood * Vulnerability Score**

# Cyber Maturity Model

| | |
|---|---|
|  Who would attack the organization? | **Threat Agent Identification**<br>• Motivations<br>• Skills required |
|  How the company could be attacked? | **Identify possible attack Strategies** |
|  Which are the weaknesses of the Company? | Measure the weak points of company surface through self assessment (**cyber maturity questionnaire**) |
|  **Vulnerabilities** | |

# Identified Threat-Agents

Threat Agents

| Threat Agent | Skills | Level of Interest |
|---|---|---|
| **Hacker** | High | 100% |

| Property | Value |
|---|---|
| Description | An Hacker combines the skills od a Data Miner and a Mobster. A Data Miner is a professional data gatherer external to the company (includes cyber methods); while a Mobster is a manager of organized crime organization with significant resources. |
| Motivations | Dominance , Organizational Gain , Personal Financial Gain , Notoriety , Personal Satisfaction |

| | | |
|---|---|---|
| **Competitor/Hireling Hacker** | Medium | 100% |
| **Script Kiddie** | Low | 100% |
| **Unpredictable Person** | Low | 100% |
| **Unaware** | Low | 100% |
| **Governament Hacker** | High | 75% |
| **Hacktivist** | High | 67% |
| **Terrorist** | High | 50% |
| **Insider** | Medium | 25% |

# Impact Analysis

| | |
|---|---|
| Asset Profiling | **Tangible and Intangible Asset identification and relationship** |
| Cascading Effects | **Indirect Consequences** |
| Costs related to the attack | Regulatory Costs, System Maintenance, Restoring Machines… |

**Qualitative and Quantitative Impacts Analisys**

# OVERALL process

ProtectMe Expert and Customer CISO

1) CISO answers RATING-OT questionnaire with the support of a ProtectMe Expert for company profiling


4) RATING-OT refines the company profile based on input received automatically from the ResilBlockly and release a final company cyber posture to the CISO

*ProtectMe Company Premises*

2) ResilBlockly Modeler builds the company/infrastructure model to identify weaknesses and vulnerabilities based on input (documentation, interview, etc.) received from CISO

ResilBlockly OT Customer infrastructure Modelling

Model details for the refinement of the profile


Cascading Effect Analyzer

3) Cascading effect analyzer identifies how a succesful attack propagetes its effect to other assets. This allow to refine the model and the final results

*Customer Company Premises*

# Sviluppi futuri: CyberSEAS project

## 26 organisations, 3 years, 30 tools

**Objective:** protecting Electrical Power and Energy Systems interconnected data and systems against cyber threats with the **highest impact** in terms of:

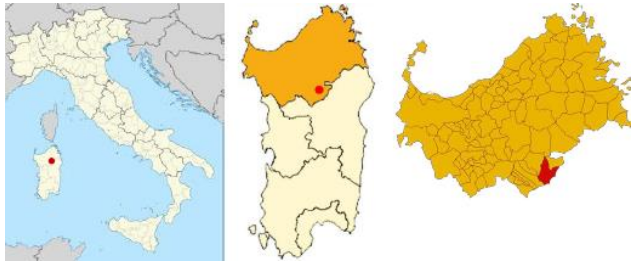
- Business continuity of energy distribution
- Safety
- Substantial damages to infrastructures
- Critical privacy breaches

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101020560

# CyberSEAS: pilota Italiano

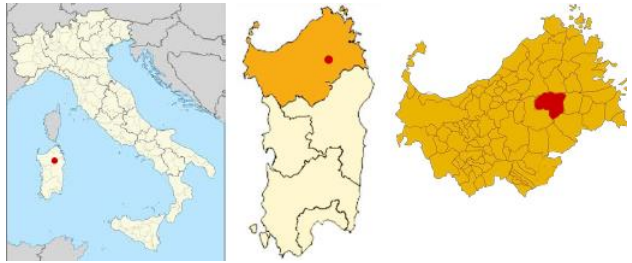
## Municipality of Benetutti

- Located in the central North of Sardinia (IT)
- 1737 inhabitants
- Surface of 98 km2
- 103 photovoltaic plants, 13 owned by the municipality (113 kWp installed), 90 private plants (1,405 kW installed)
- Renewable energy produced: 1.843.000 kWh per year
- Average energy consumption: 3.700.000 kWh per year



## Municipality of Berchidda

- Located in the North East of Sardinia (IT)
- 2668 habitants
- Surface of 200 km2
- 71 photovoltaic plants, 5 owned by the municipality (113 kWp installed), 66 private plants (1,405 kW installed)
- Average energy consumption: 6.164.000 kWh per year



# Mockups

# Threat-Agents Questionnaire

## HACKER

10 Does your company manage relevant data that could be easily resold to competitors or in black markets?

- (•) Yes
- ( ) No

11 Does your company have a well-known brand?

- (•) Yes
- ( ) No

## Competitor Hacker

12 Does your company has industrial secrets or intellectual properties?

- (•) Yes
- ( ) No

13 Is your company a market leader?

- (•) Yes
- ( ) No

## Government Hacker

1 Does your company manage relevant/important data?

- (•) Yes
- ( ) No

2 Does your company have a national or international visibility?

- (•) Yes
- ( ) No

3 Does your company manage critical infrastructure/SCADA?

- (•) Yes
- ( ) No

4 Does your company have offices in countries with political tensions?

- ( ) Yes
- (•) No

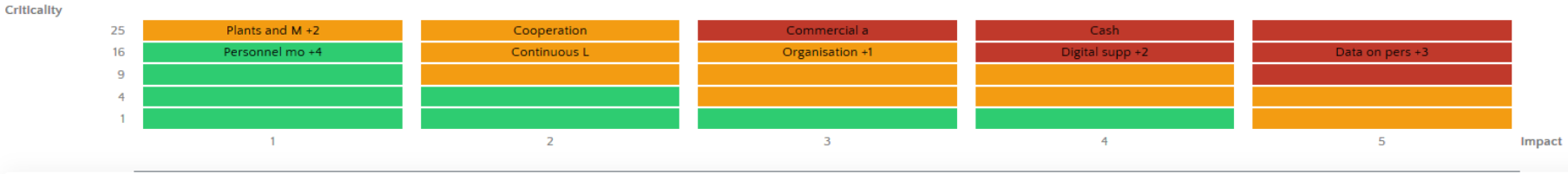
# OT Attack Strategies - Domain Expert Evaluation

Considering an organization, indicate a value for the skills, resources and frequency of each attack strategy.

| Name | Skills | Resources | Frequency |
|---|---|---|---|
| Supply chain attack | Low: 19% Medium: 34% High: 47% | Low: 9% Medium: 41% High: 50% | AS Frequency * Low |
| OT domain OSINT | Low: 17% Medium: 33% High: 50% | Low: 10% Medium: 48% High: 42% | AS Frequency * Medium |
| OT network scanning & enumeration | 0% Low: 25% - Medium: 25% High: 50% | Low: 0% Medium: 50% High: 50% | AS Frequency * High |
| OT device connection scanning/enumeration | Low: 7% Medium: 35% High: 58% | Low: 0% - Medium: 0% High: 100% | AS Frequency * Low |
| Physical OT information gathering | Low: 0% Medium: 100% | Low: 0% Medium: 100% | AS Frequency * Medium |

Items per page: 5 1 – 5 of 25

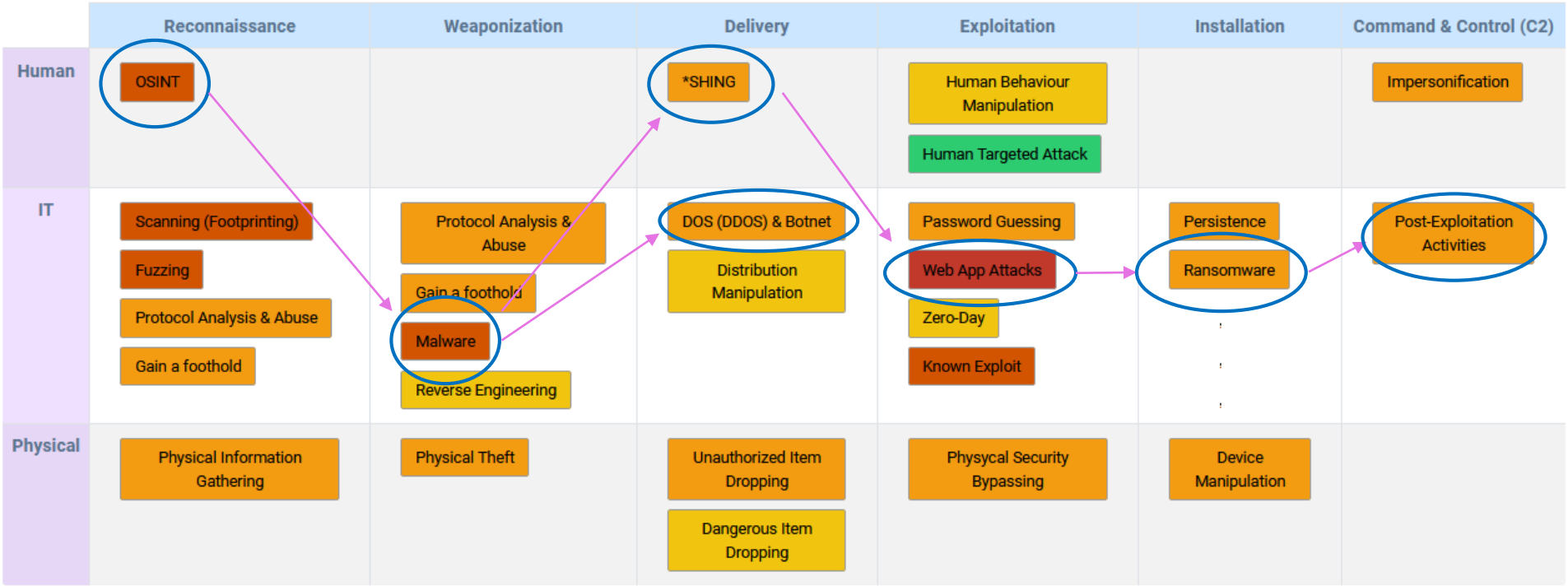
# Risk Analysis




Tangible | Intangible

| Category | Asset | Description | Likelihood | Vulnerability | Critical | Impact | Risk | Mitigations |
|---|---|---|---|---|---|---|---|---|
| Data | Data on personnel | Personal data of organisation staff. | 4.25 | 3.5 | 15 | 5 | 60% | Antivirus , Data Encryption , Awareness , DR , Hardening , Physical Access Control , Surveillance |
| Data | Data on clients and partners | Personal data releted to organisation partners and clients. | 4.25 | 3.5 | 15 | 5 | 60% | Antivirus , Data Encryption , Awareness , DR , Hardening , Physical Access Control , Surveillance |

# Attack Strategies and Cyber Kill Chain



# Grazie per l’attenzione

Marco Angelini, Prince2 Practitioner

Project Manager of Cybersecurity Unit

Marco.Angelini@eng.it

https://www.eng.it/who-we-are/engineering-group/research-innovation

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY