SMARCO

SMARt COmmunities Skills Development in Europe

Cybersecurity

Short Term Course – Unit 1

Cefriel

POLITECNICO DI MILANO

Co-funded by the European Union

smarco

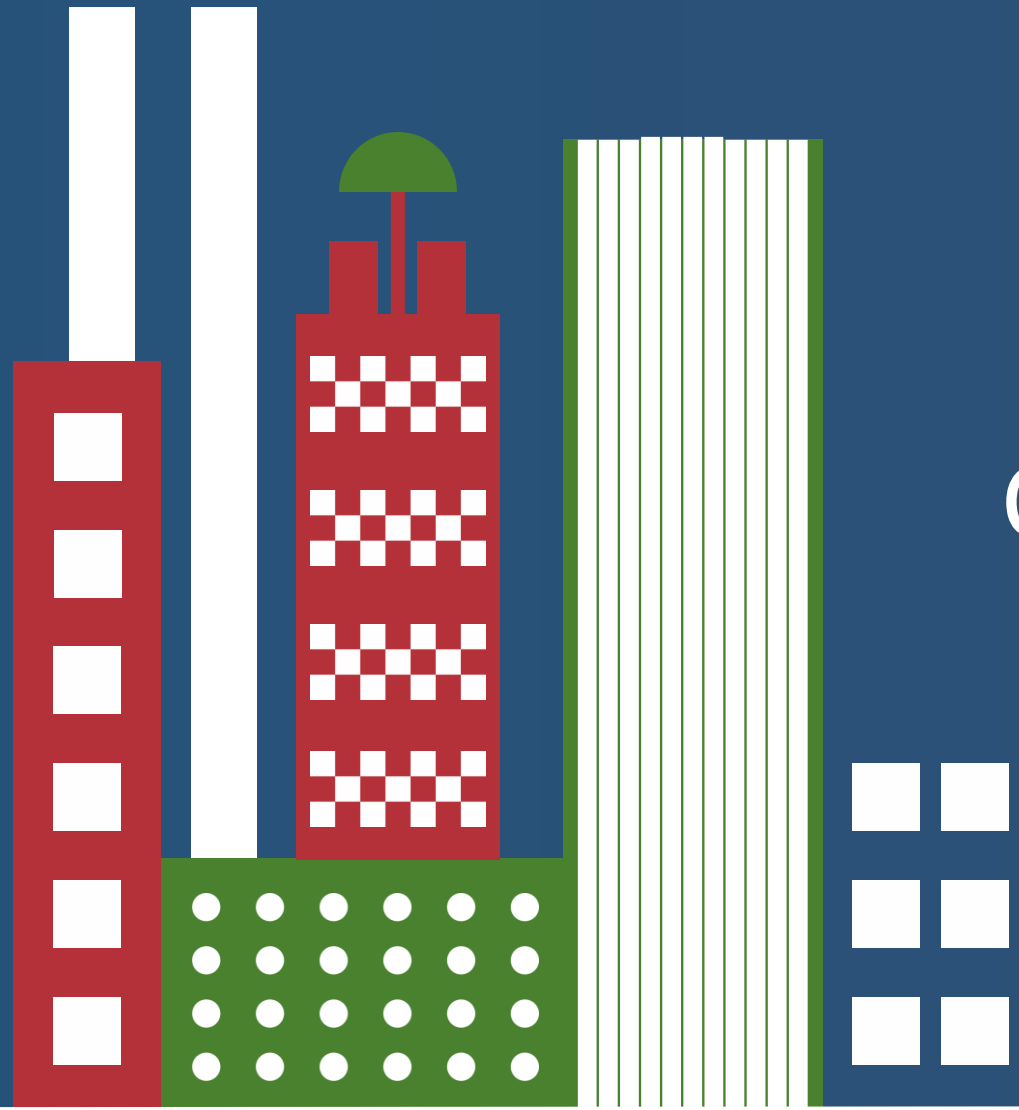
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Aim of the course

This course aims to strengthen the **resilience of smart communities** by promoting a culture of digital responsibility and awareness. Participants learn how everyday actions and informed behaviors contribute to collective cyber hygiene, making the community safer against evolving threats. Special attention is given to understanding and resisting social engineering, empowering individuals to recognize manipulation and protect both personal and shared digital environments.

Co-funded by the European Union

smarco



Unit 1

Cyber Risk Assessment In Smart Communities – an introduction

Co-funded by the European Union

smarco

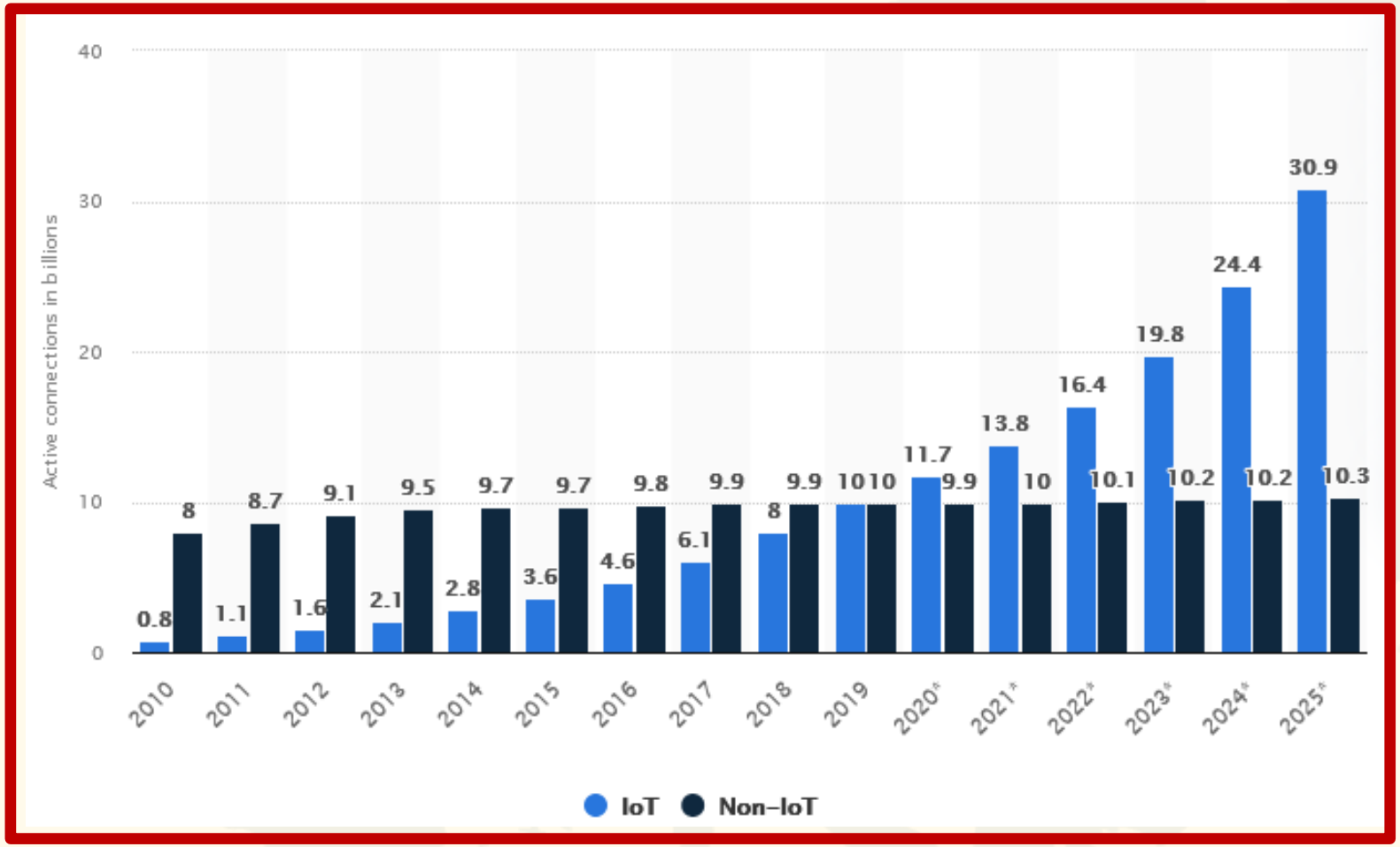
AGENDA

- Cybersecurity relevance for Smart Communities
- What is a Cyber Risk
- The 3 kinds of Cyber Risks
- Cyber Risk complexity

Co-funded by the European Union

smarco

Internet of Things



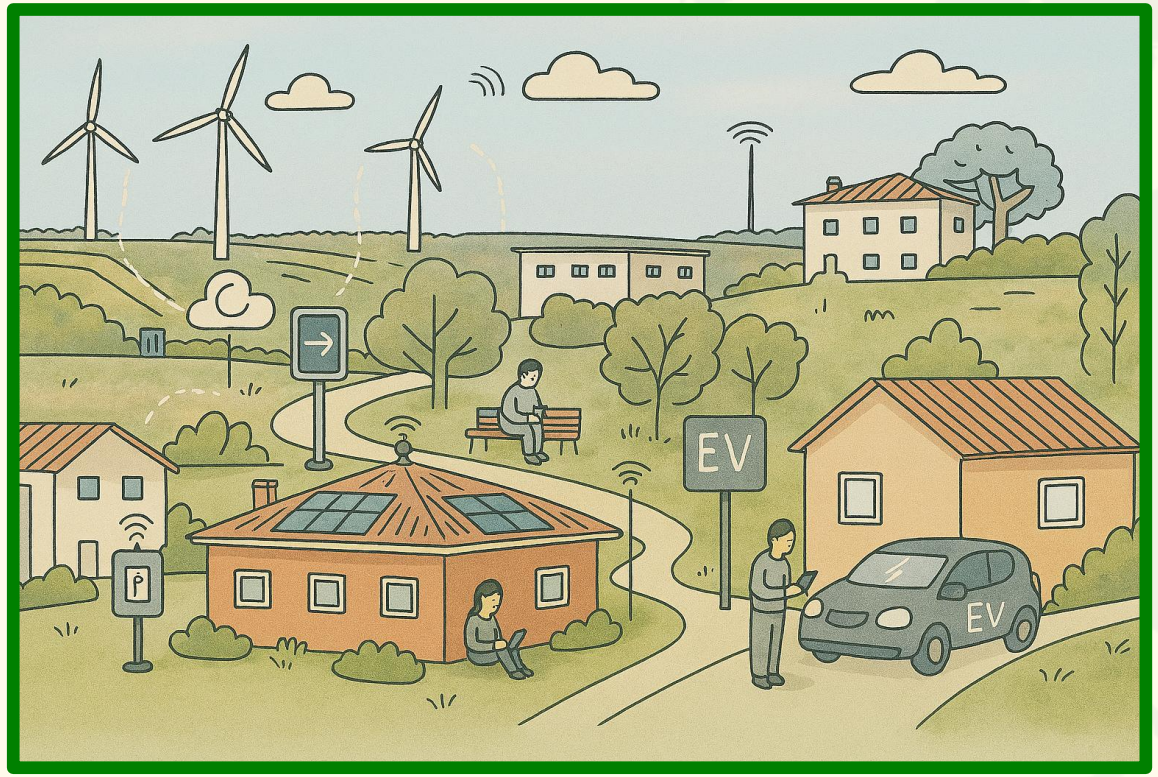
Active Connections in billions

Co-funded by the European Union

smarco

Internet of Things

According to other calculations, in 2025 we have more than 40 billions IoT, 5 for each person alive.



Problem: each IoT is a potential entrance for an attack to a broader IT system.

Impacted sectors:
- Communication
- Emergency
- Energy
- Financial services
- Government
- Public health
- Transportation
- Water

Co-funded by the European Union

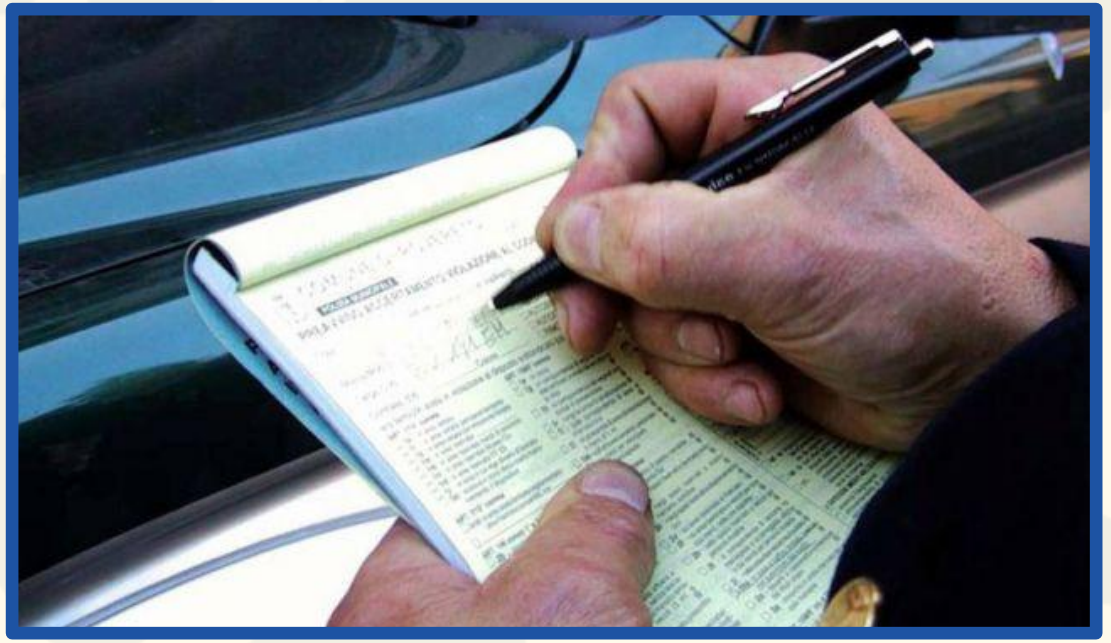
smarco

Cybersecurity in public services - examples

In April 2025, the Municipal Police of Rome was compromised and the officer were forced to go back to pens and paper to emit fines.

The issue was related to the the cloud service, which had been externalised.

This aspect points out to the potential weakness of the supply chain.



Co-funded by the European Union

smarco

Definition of Cyber Risk

- **Definition by the Institute of Risk Management**
  "Cyber risk" means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.

  The definition contains two types of assets:
  - Reputation of an organization, Intangible Asset
  - Failure of its information technology systems, Tangible Asset

  Source: https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

Co-funded by the European Union

smarco

Definition of Cyber Risk

- **Definition in NIST** SP 800-30 Rev. 1, "Guide for conducting Risk assessments", Sep, 2012
  A measure of the extent to which an entity is **threatened** by a **potential** circumstance or event, and typically a function of: **(i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence**

$$\text{Risk} = \text{Likelihood} \cdot \text{Impact}$$

$$\text{Risk} = \text{Attack Probability} \cdot \text{Consequence}$$

Co-funded by the European Union

smarco

The Generic Formula

Risk = Likelihood of an impact * Impact

Likelihood of an impact= Likelihood of an attack * Vulnerability to an attack

Risk = Likelihood of an attack * Vulnerability to the attack * Impact

Co-funded by the European Union

smarco

The Generic Formula

Another adoption of a management approach to risk analysis is an approach that defines risk as a function of:

Risk = Threat Probability * Vulnerability * Impact

The last definition allows you to isolate the threat probability and focus on controllable elements to reduce the risk:
Vulnerability
Impact

Co-funded by the European Union

smarco

RISK = Likelihood of attack * Vulnerability Score * IMPACT

Who would attack the organization?	How the company could be attacked?	Which are the weaknesses of the Company?	Most Vulnerable Assets

• **Threat Agent Identification**
  • Motivations
  • Skills required
  • Trends
  • OPSEC
	• **Identify possible attack Strategies**	• Measure the weak points of company surface through self assessment (**cyber maturity questionnaire**)	• **Likelihood**
			• **Vulnerabilities**

Co-funded by the European Union

smarco

General Risk Model and macro sources of data

RISK **= Likelihood of attack * Vulnerability Score * *IMPACT***

ATT&CK framework and interface with CAPEC and threat intelligence tools (e.g. Threat Agent Library, KEV)

- Inherent risk
- Company-specific risk & risk appetite

CVSS 4.0
EPSS
VISS
SBOM

This activity is specific to each business sector and application. It needs a business analysis methodology. The project should suggest best practices (e.g., CJA or STRIDE/DREAD) for the DevSecOps process or a maturity model (e.g., derived from OWASP 5D or similar DevSecOps CMMs). This information will be in D2.2.

Co-funded by the European Union

smarco

So what is cyber risk?

Cyber Risk is composed of three different kinds of risks:

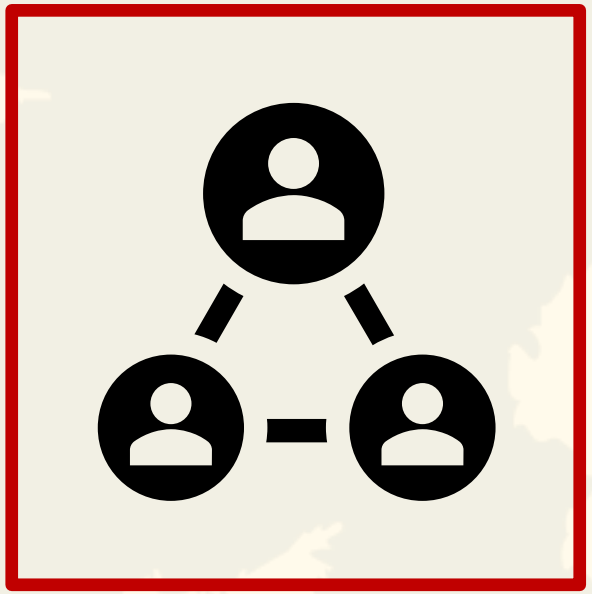
- Human risk
- IT risk
- OT risk

Co-funded by the European Union

smarco

Human Cyber Risk

Human Cyber Risk refers to vulnerabilities arising from human behavior, decisions, and actions that compromise an organization's security. It includes both intentional malicious actions and unintentional errors caused by employees, suppliers, or third parties interacting with technology.



Co-funded by the European Union

smarco

Human Cyber Risk

Human Cyber Risk is central to cybersecurity because attackers often exploit human emotions like curiosity, urgency, or fear to bypass technical defenses. Effective human risk management involves training and monitoring behaviors to reduce susceptibility to phishing attacks, credential theft, and insider threats.

Examples:

- Clicking on phishing emails leading to malware installation
- Weak password practices compromising sensitive systems
- Accidental sharing of confidential data through unsecured channels

Co-funded by the European Union

smarco

IT Cyber Risk

IT risk refers to the potential adverse impacts on an organization due to threats exploiting vulnerabilities in information technology systems, such as servers, workstations, personal laptops, and mobile devices. It is assessed based on the likelihood of occurrence and severity of consequences.

Examples:

- Ransomware attacks encrypting organizational data
- Server outages disrupting business operations
- Exploitation of software vulnerabilities leading to data theft

Co-funded by the European Union

smarco

OT Cyber Risk

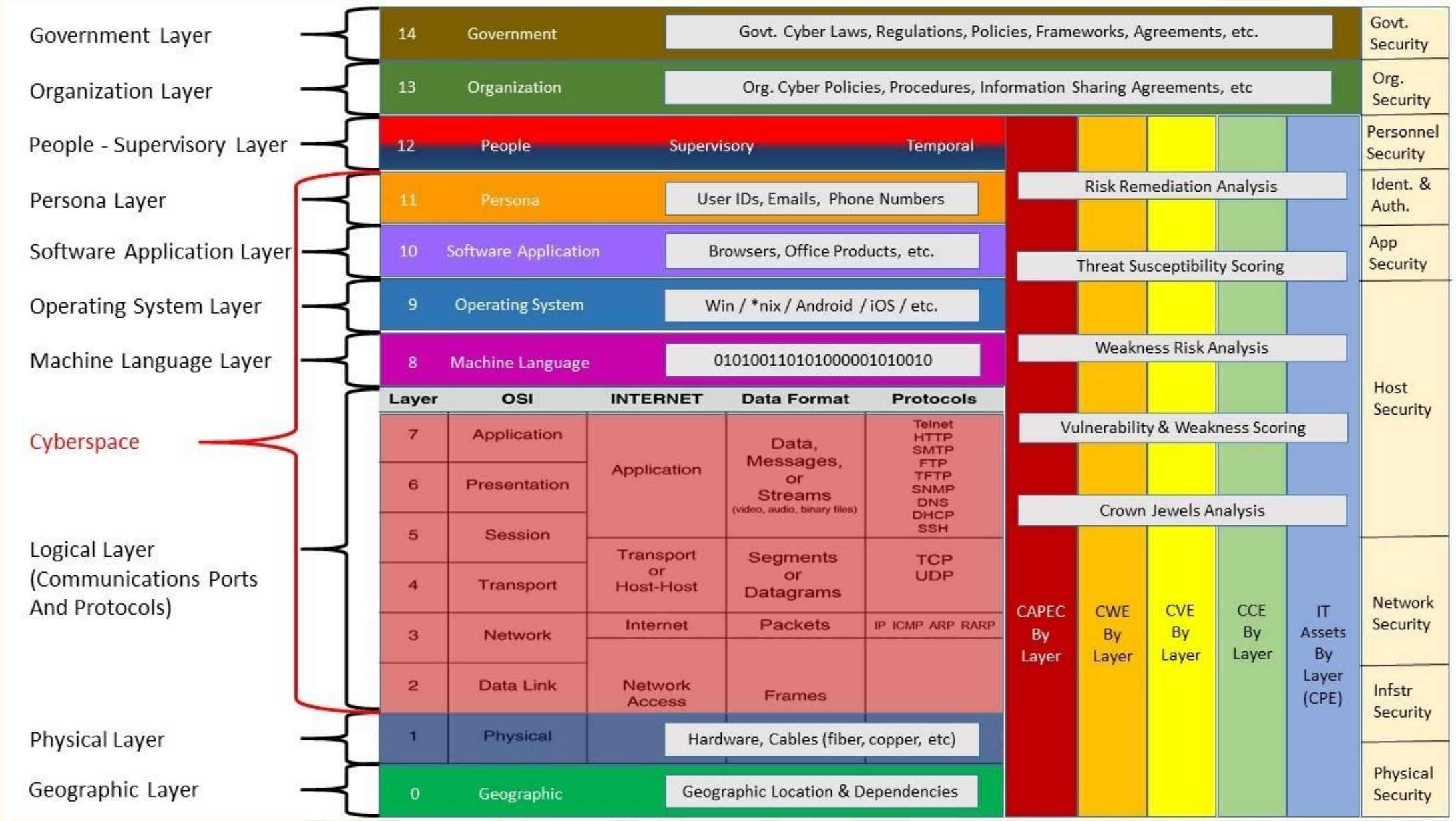
Operational Technology (OT) risk refers to vulnerabilities in systems managing industrial processes and critical infrastructure. These risks arise from increased connectivity and reliance on OT devices for essential operations.

Examples:

- Cyberattacks disrupting power grid operations.
- Manipulation of industrial control systems causing production delays.
- Exploitation of unpatched vulnerabilities in connected OT devices.

Co-funded by the European Union

smarco



Co-funded by the European Union

smarco

Why it’s so difficult to estimate cyber risks

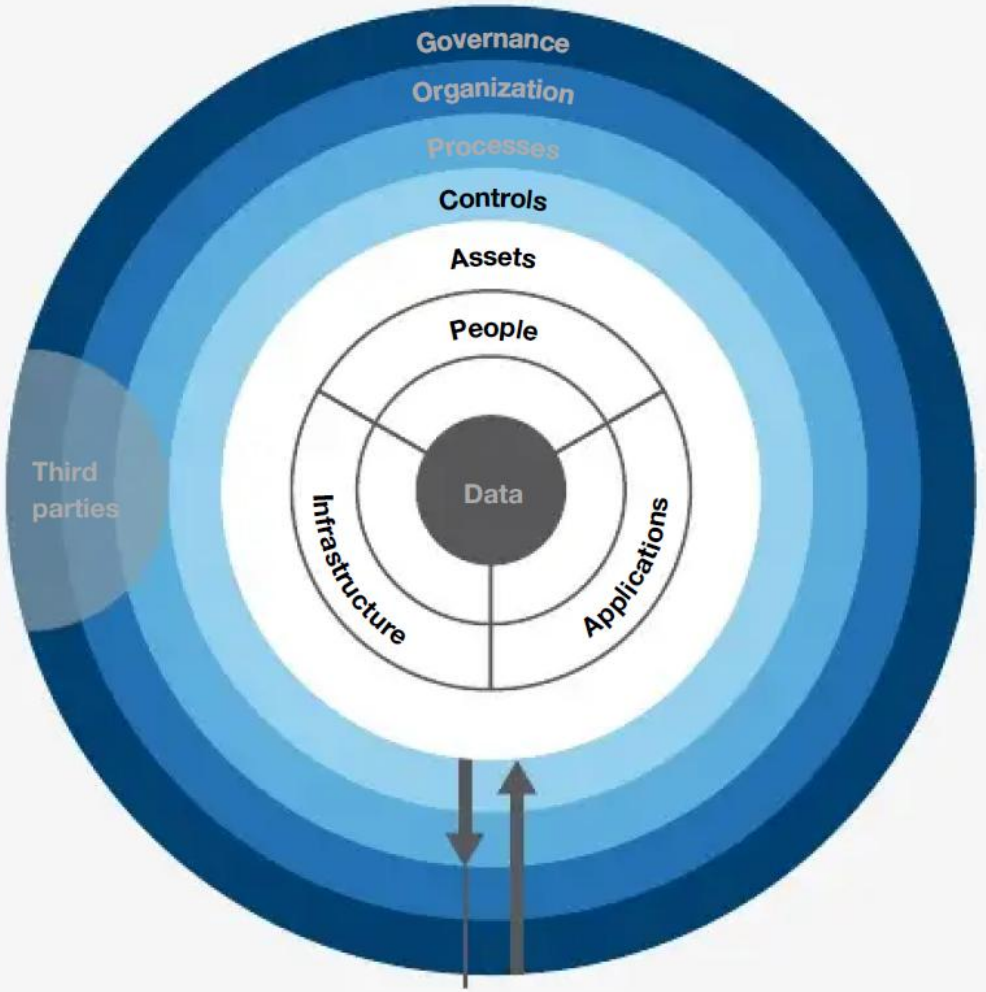
- The attacks come from nowhere and go into nowhere, only the victims are known
- The source of risk is constantly changing, at an unsustainable pace for modelling
- The Data Curse: There Is not Enough data to build any stable model
- Organisations and the impact of cyber risks are profoundly different
- The digital transformation agenda of various businesses is constantly evolving
- Tangible and intangible assets
- Cybercrime evolves through internal and external forces very rapidly

Co-funded by the European Union

smarco

Exhibit 1 **The holistic approach to managing cyber risk proceeds from a top-management overview of the enterprise and its multilayered risk landscape.**

Holistic cyber risk–management approach



Assets. Clearly defined critical assets

Controls. Differentiated controls to balance security with agility

Processes. State-of-the-art cybersecurity processes focused on effective responses

Organization. Right skills, efficient decision making, and effective enterprise-wide cooperation

Governance. Investments in operational resilience prioritized based on deep transparency into cyber risks

Third parties. Coverage of the whole value chain, including third-party services

Co-funded by the European Union

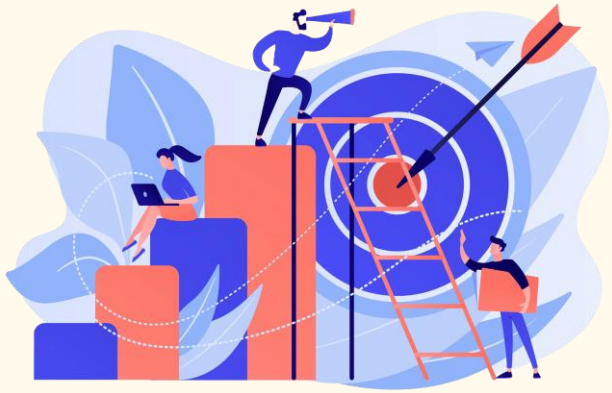
smarco

Unit Completed – What's Next?

To consolidate your learning and reflect on the key concepts covered, please take a moment to complete this quiz.

Your feedback and results will help you track your progress and support continuous improvement of the training experience.

Click the link to begin the quiz!



Co-funded by the European Union

smarco

SMARCO

SMARt COmmunities Skills Development in Europe

www.smarco.eu

info@smarco.eu

We are social! Follow us on:

@smarcoproject

@smarcoproject

@smarcoproject

Co-funded by the European Union

smarco

Cefriel
POLITECNICO DI MILANO

Project 101186291 — SMARCO