Cefriel

Urgent Up-Skilling

Cybersecurity and ESG

Co-funded by
the European Union

Digital 4 Sustainability

Urgent Up-Skilling

Cefriel
POLITECNICO DI MILANO

CYBERSECURITY AND ESG

CORRELATIONS, IMPACTS AND LEGISLATIONS

A dialogue between laws on cybersecurity and sustainability in the EU

Co-funded by the European Union

Urgent Up-Skilling

This course is provided by:

Cefriel

POLITECNICO DI MILANO

Massimiliano Colombo, Enrico Frumento, Domenico Orlando

January, 2025

Digital 4 Sustainability
Skills for Europe's Twin Transition

Cefriel

Agenda

1. ESG in general and its role within the company life – Massimiliano Colombo
2. Sustainable Cybersecurity – Enrico Frumento
3. Cybersecurity and ESG legal frameworks, touching points – Domenico Orlando
4. Exploring the links between cybersecurity and ESG with practical examples of attacks and consequences – Enrico Frumento
5. Conclusions, Q&A

Co-funded by the European Union

What we'l cover today

How do the three dimensions of ESG relate to cybersecurity?

Which regulations are most relevant for promoting a sustainable approach to cybersecurity?

What impact can cybersecurity have on each of the ESG dimensions?

Meet the speaker

Enrico Frumento

Researcher (Cybercrime intelligence, Offensive security, Social engineering)

Cefriel

Linkedin: www.linkedin.com/in/enricofrumento/

Medium: enrico-frumento.medium.com

The example of EGSS

The **Environmental Goods and Services Sector (EGSS)** is one of the fastest-developing economic areas in the European Union's economy.

This development is caused by implementing **Sustainable Development Goals (SDGs)** in the organization's strategies and by the growing importance of digital technologies.

Green Cybersecurity protects the processes related to energy production and the production of goods and services in EGSS.

Cybercrime trends and challenges

ATTACKS TO IT, OT AND HUMANS

- IT-OT convergence.
- Adoption of Legacy systems.
- Increased attack surface (IoT).
- Lack of awareness.
- Systemic risk due to high impacts.
- Attacks to Humans
- Holistic/integrated risk model: for too long the cyber risk has been considered an IT/ICT only responsibility.

ATTACKS TO SMEs AND MEs

- Target of 60% of attacks.
- 99.8% of all companies in the non-financial sector in the EU.
- 68% have no systematic approach to ensuring cybersecurity.
- Average of 6 months to detect a data breach.
- Limited budget and relative loss of up to 25% of annual revenue strength for end activities.
- Lack of cybersecurity experts.

RESEARCH CHALLENGES

- How can a risk model reduce SMEs' cyber exposure?
- What are the limitations of
  - current cybersecurity risk models?
- How can risk models be adapted from IT to OT?
- "Sustainable cybersecurity"

The case of Colonial Pipeline

- Type of attack: **RANSOMWARE**
- Critical Infrastructure: **Oil Pipeline**
- Country: **USA**
- Impact: **8850 km of unusable pipelines** and 2.5 million barrels/day paralyzed.
- Interruption duration: approx. **7 days**.

Sabotage

Cyber attack forces Colonial Pipeline to close one of the largest US oil pipelines

by Sissi Bellomo

May 9, 2021

Colonial pipeline fuel tanks in Woodbine, Maryland EPA)

The company explained that it blocked the pipeline to contain the attack on its computer network. The FBI is also involved in the investigation

Healthcare

Hollywood hospital's systems held hostage by hackers

Have you read the new issue of our digital (IN)SECURE Magazine? If not, do it now.

The Hollywood Presbyterian Medical Center, an "acute-care facility" located in Los Angeles, has had its computer systems compromised by hackers. The attackers are asking for 9,000 Bitcoin (approximately $3.6 million) in exchange for giving the hospital access to the systems again.

Ransomware Gangs to Stop Attacking Health Orgs During Pandemic

By Lawrence Abrams — March 18, 2020 — 06:36 PM — 6

Some Ransomware operators have stated that they will no longer target health and medical organizations during the Coronavirus (COVID-19) pandemic.

Last night, BleepingComputer reached out to various ransomware operators such as the Maze, DoppelPaymer, Ryuk, Sodinokibi/REvil, PwndLocker, and Ako Ransomware infections to ask if they would continue targeting health and medical organizations during the outbreak.

Patients' medical records are inaccessible, and according to US healthcare-related blog The Medical Quack, some of the hospital departments – namely Radiation and Oncology – have been temporarily shut down as they can't use their computers.

Healthcare

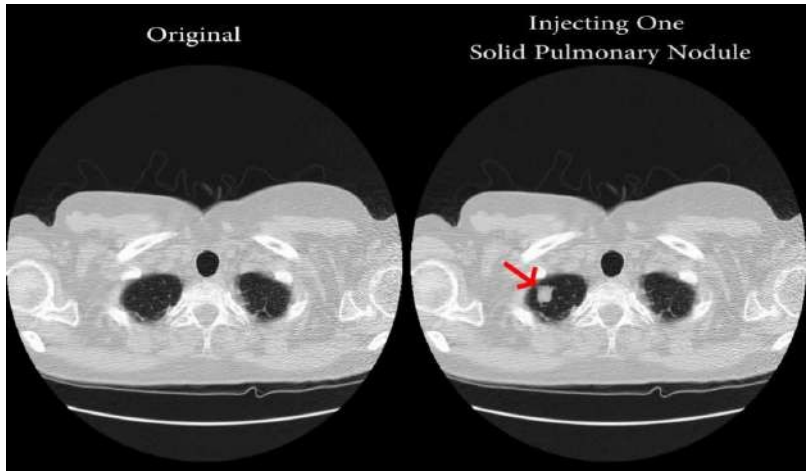
- Change Healthcare was the target of an attack caused by a vulnerability in ConnectWise ScreenConnect (severity score: 10 - CRITICAL). The attack resulted in 6TB of leaked data, which affected 90% of pharmacies in the US (Feb 2024)
- CVE-2024-1708 - path-traversal issue
- CVE-2024-1709 - authentication bypass issue

Healthcare

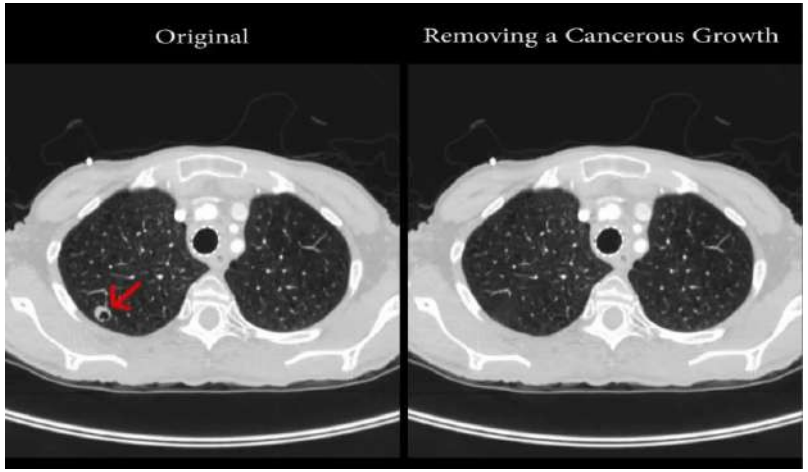
- Change Healthcare, a subsidiary of UnitedHealth, initially reported a data breach in October last year that was considered the worst in the industry.
- The breach, which affected up to 100 million users, has now grown to an alarming 190 million, according to Tech Crunch.
- Cybercriminals reportedly exploited an employee
- system that lacked multi-factor authentication
- Social Security number, driver's license number, passport number, diagnoses, test results, medications, and health insurance information

Healthcare

- The area of cyber-physical threats remains largely unexplored.
- This is especially true when considering the current security measures for cyber-medical devices
- Source: https://www.securityweek.c om/hackers-can-add- remove-cancer-ct-scans- researchers

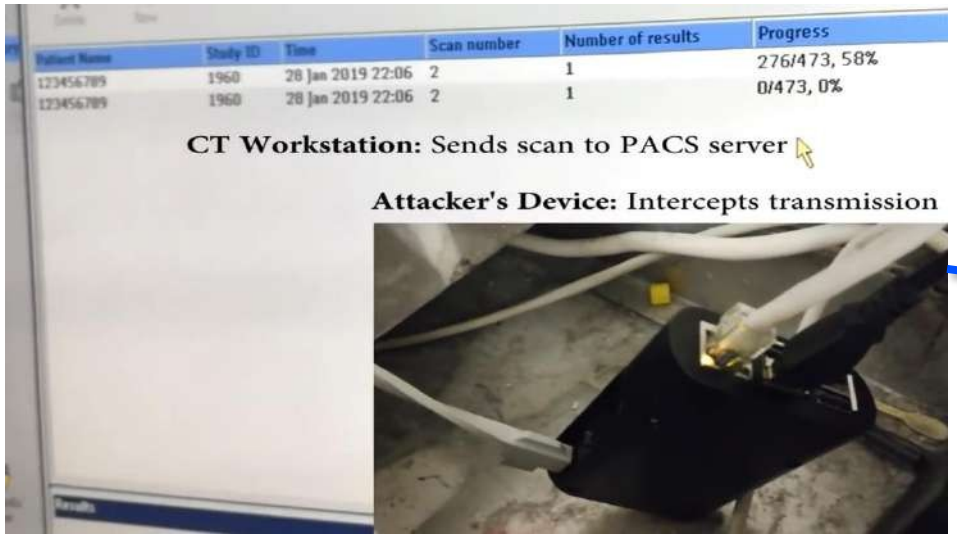


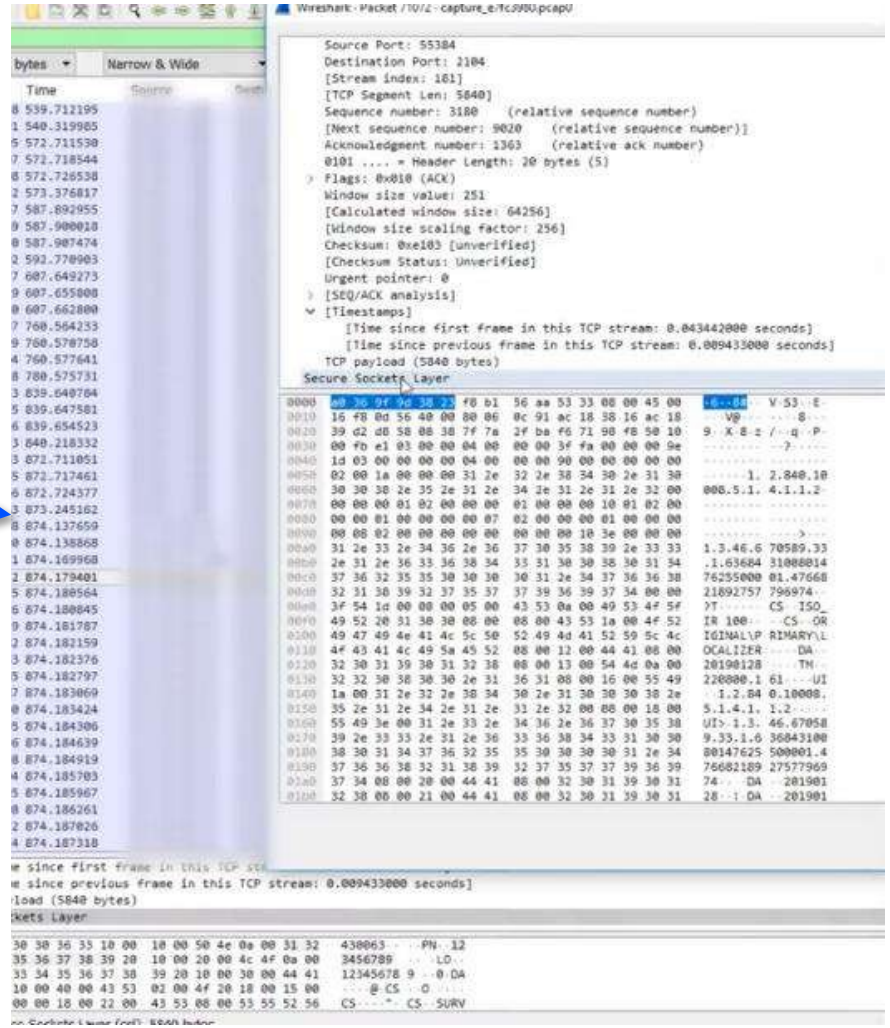
- Un-aware technicians: 99% fail
- Aware technicians: 60% fail



- Un-aware technicians: 94% fail
- Aware technicians: 87% fail

Healthcare





Attackers can intercept scans that are not encrypted through an online bundle that hosts the malware.

The authors noted that although encryption using TLS v1.2 is enabled, the payload is transmitted in plaintext.

In many other instances, network encryption via TLS is not utilized at all.

Healthcare latest changes

- **Regulation** (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (**Cyber Resilience Act)**
- **Directive** (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on **liability for defective products** and repealing Council Directive 85/374/EEC

Healthcare latest changes

- The commission published its action plan to enhance cybersecurity in the healthcare sector. This is the first of several similar measures for other relevant sectors. (15 Januar 2025)


European Commission
EN
Search
Shaping Europe's digital future
Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office
Home News & Views Commission unveils action plan to protect the health sector from cyberattacks
PRESS RELEASE | Publication 15 January 2025

Commission unveils action plan to protect the health sector from cyberattacks

The Commission has presented an EU action plan aimed at bolstering the cybersecurity of hospitals and healthcare providers. This Action Plan was announced in President von der Leyen's political guidelines as a key priority within the first 100 days of the new mandate.

The initiative is an important step in shielding the healthcare sector from cyber threats. By enhancing threat detection, preparedness and response capabilities of hospitals and health providers, it will create a safer and more secure environment for patients and health professionals.

Digitalisation is bringing a revolution to healthcare, enabling better services to the patients through innovations such as electronic health records, telemedicine, and AI-driven diagnostics. However, cyberattacks can delay medical procedures, create gridlocks in emergency rooms, and disrupt vital services which, in severe cases, could have a direct impact on the lives of Europeans. Member States reported 309 significant cybersecurity incidents affecting the healthcare sector in 2023 – more than in any other critical sector.

The action plan proposes, among others, for ENISA, the EU agency for cybersecurity, to establish a pan-European Cybersecurity Support Centre for hospitals and healthcare providers, providing them with tailored guidance, tools, services, and training. The initiative builds on the broader EU framework to strengthen cybersecurity across critical infrastructure and marks the first sector-specific initiative to deploy the full range of EU cybersecurity measures.

Read the full press release

Read further information:

– Action Plan on the cybersecurity of hospitals and healthcare providers
– Questions and answers
– Factsheet

AdobeStock © meeboonstudio

Related topics

Creating a digital society | eHealth | Cybersecurity | mHealth

Healthcare latest changes

- The commission published its action plan to enhance cybersecurity in the healthcare sector. This is the first of several similar measures for other relevant sectors. (15 Januar 2025)

European Commission

EN Search

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home News & Views Commission unveils action plan to protect the health sector from cyberattacks

PRESS RELEASE | Publication 15 January 2025

Commission unveils action plan to protect the health sector from cyberattacks

The Commission has presented an EU action plan aimed at bolstering the cybersecurity of hospitals and healthcare providers. This Action Plan was announced in President von der Leyen's political guidelines as a key priority within the first 100 days of the new mandate.

The initiative is an important step in shielding the healthcare sector from cyber threats. By enhancing threat detection, preparedness and response capabilities of hospitals and health providers, it will create a safer and more secure environment for patients and health professionals.

Digitalisation is bringing a revolution to healthcare, enabling better services to the patients through innovations such as electronic health records, telemedicine, and AI-driven diagnostics. However, cyberattacks can delay medical procedures, create gridlocks in emergency rooms, and disrupt vital services which, in severe cases, could have a direct impact on the lives of Europeans. Member States reported 309 significant cybersecurity incidents affecting the healthcare sector in 2023 – more than in any other critical sector.

The action plan proposes, among others, for ENISA, the EU agency for cybersecurity, to establish a pan-European Cybersecurity Support Centre for hospitals and healthcare providers, providing them with tailored guidance, tools, services, and training. The initiative builds on the broader EU framework to strengthen cybersecurity across critical infrastructure and marks the first sector-specific initiative to deploy the full range of EU cybersecurity measures.

Read the full press release

Read further information:

- Action Plan on the cybersecurity of hospitals and healthcare providers
- Questions and answers
- Factsheet

AdobeStock © meeboonstudio

Related topics

Creating a digital society | eHealth | Cybersecurity | mHealth

Meet the speaker

Massimiliano Colombo

Business Advisor

Cefriel

e-mail: massimiliano.colombo@cefriel.com

Linkedin: www.linkedin.com/in/massimiliano-colombo-mc1977

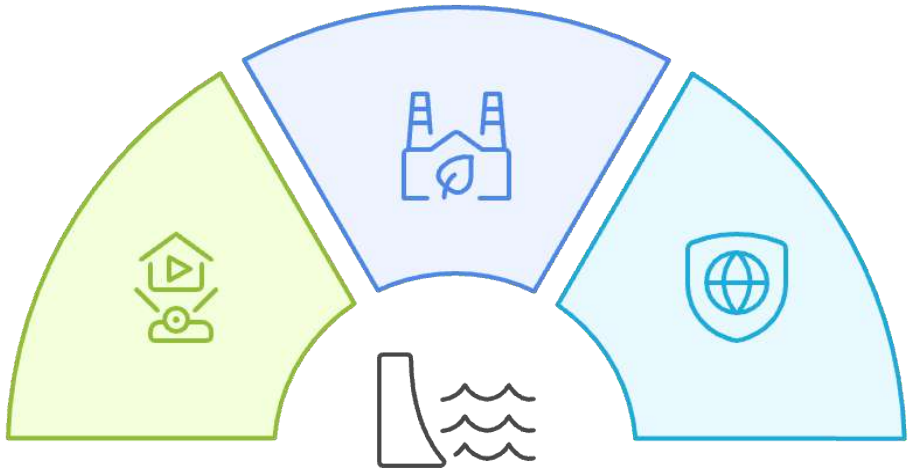
Agenda

Sustainability into a real Company

background and challenges

Sustainability into the holistic Enterprise 5.0

vision



Sustainability & Cybersecurity

quick intro to possible links

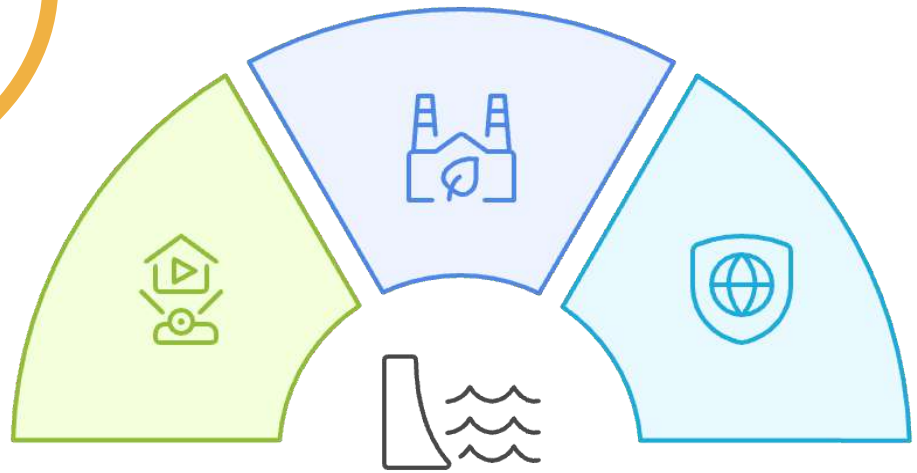
Agenda

Sustainability into the holistic Enterprise 5.0

vision

Sustainability into a real Company

background and challenges



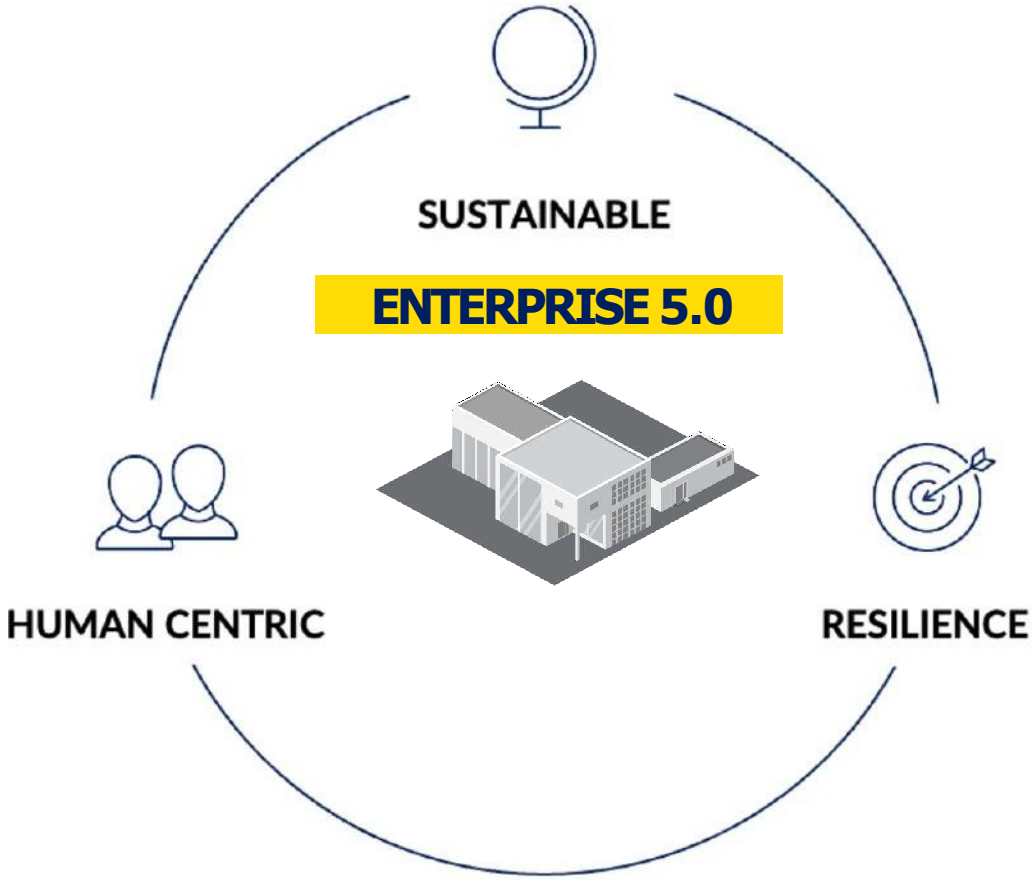
Sustainability & Cybersecurity

quick intro to possible links

The Vision: Enterprise 5.0

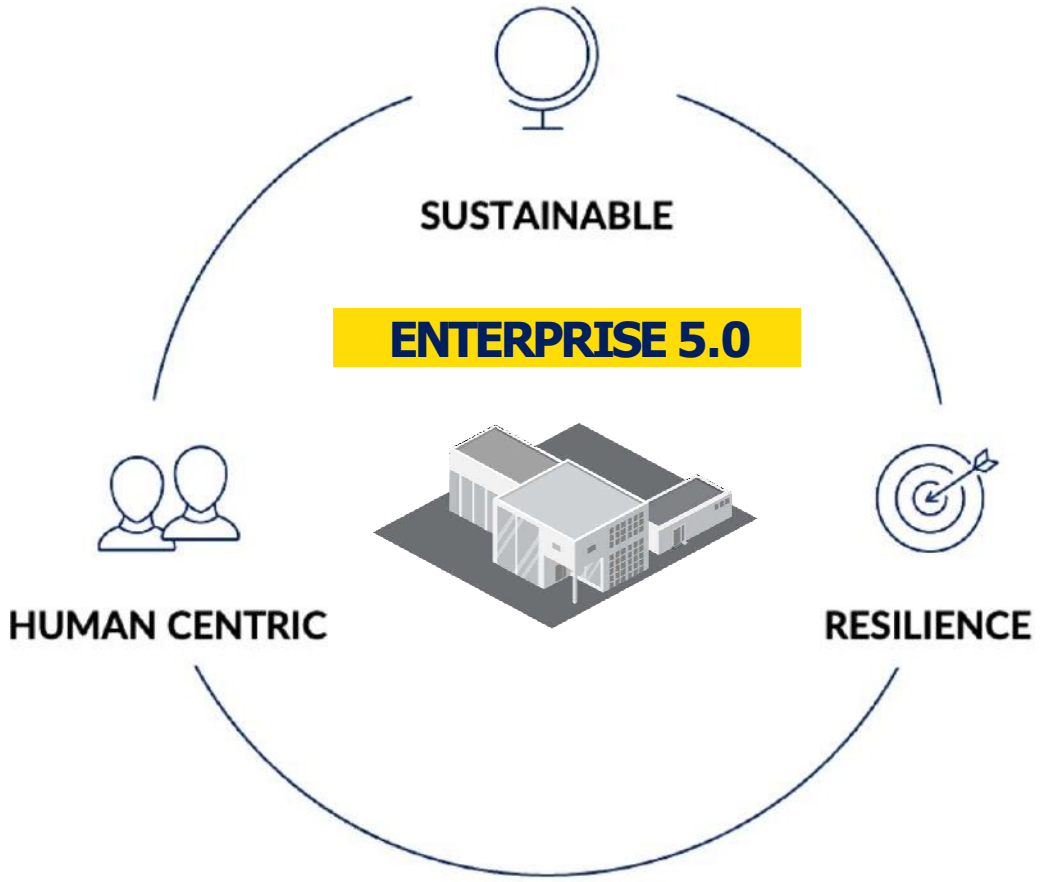
Industry 5.0 (used **here** as synonym of **Enterprise 5.0**) represents the EU Commission's vision evolving beyond Industry 4.0, built on **three** pillars:

- *Human-centric* - places workers at the core of production, blending human skills with advanced technologies
- *Sustainable* - promotes circular economy and zero-impact manufacturing aimed at climate neutrality
- *Resilient*: Strengthens supply chains and production systems to withstand future crisis.



This vision balance technological advancement, environmental sustainability, and worker wellbeing in European industry.

Today's focus: sustainability



Entry point: a definition

Sustainable Development

Sustainable development is described as '*development that meets the needs of the present generation without compromising the ability of future generations to meet their own needs*' (Brundtland Commission, 1987).

This approach focuses on integrating economic growth with social justice and environmental protection, aiming to ensure a prosperous and sustainable future for all.

Entry point: a definition

Sustainable Digital

Digital for Sustainability

The relationship between Digital and Sustainability is at least twofold:

- **Sustainable Digital:** on the one hand, it is important for Digital itself to be more Sustainable (through different techniques and approaches such as, for example: the Green Cloud, for the reduction of consumption and emissions through the use of the Cloud from carbon neutral regions; Green Coding, for software development through sustainable practices and the introduction of ways to control both consumption and related emissions. In general, we can talk about Green Computing).
- Digital for Sustainability: on the other hand, the project initiatives that a company undertakes as part of its sustainability journey can be supported or even enabled by the use of digital technologies.

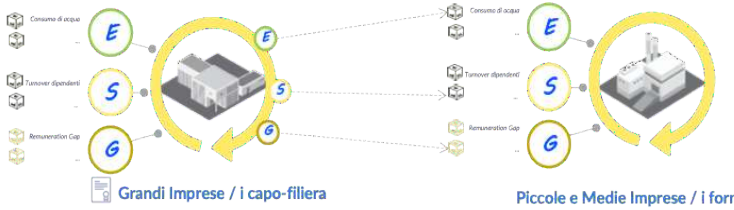
Innovation is the connecting element between Digital and Sustainability: for an Innovation that is both Digital and Sustainable.

Digital for Sustainability: holistic view (Big Picture)

Digital should above all represent the enabling element **to accelerate and make measurable** (i.e., monitorable in a quantitative manner) the sustainability of a company in its E, S and G dimensions, **to the benefit of both the company itself and the ecosystem of stakeholders with which the company interacts.**

In other words, in accordance with this vision, **being sustainable does not only mean reporting in a standard**, final format; rather, **it means being able to act 'during'**, in itinerary, but thanks to monitoring actions also carried out in accordance **with synergetic drivers of both business and sustainability**.

Pay-off: **from** ESG data sharing for **COMPLIANCE**... to 'real-time' ESG data sharing (e.g., with the supply chain and other stakeholders) **to CREATE VALUE**



Digital for Sustainability: holistic view (Big Picture) – for more details

https://www.cefriel.com/whitepaper/innovazione-digitale-per-la-sostenibilita-nella-filiera/

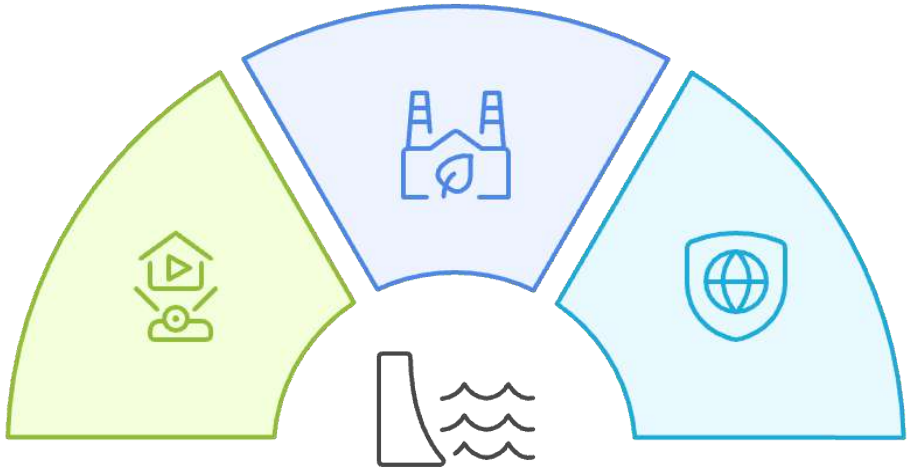
Agenda

Sustainability into a real Company

background and challenges

Sustainability into the holistic Enterprise 5.0

vision



Sustainability & Cybersecurity

quick intro to possible links

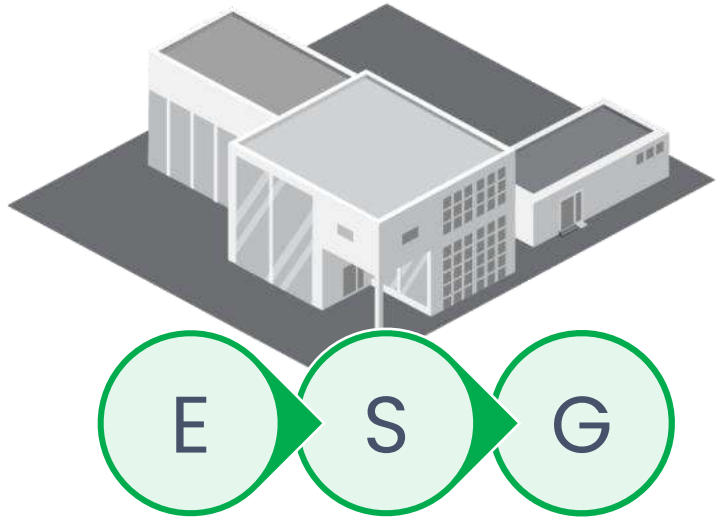
Examples of frameworks for measuring sustainable development: SDG

Simplifying, there are two main 'assessment frameworks' of Sustainable Development pathways, born in very different environments and for very different reasons, but certainly related.

The 17 Sustainable Development Goals (SDGs) – which form the backbone of the 2030 Agenda approved by the United Nations in 2015 - represent high-level goals (subdivided, in turn, into 169 overall targets) born to direct all Member States' initiatives, in order to achieve sustainable prosperity of both the Planet and the People living in it.

Examples of frameworks for measuring sustainable development: ESG criteria

Environmental, social and governance (ESG) criteria are an increasingly popular way for investors to evaluate companies in which they might want to invest. ESG criteria can also help investors avoid companies that might pose a greater financial risk due to their environmental or other practices.



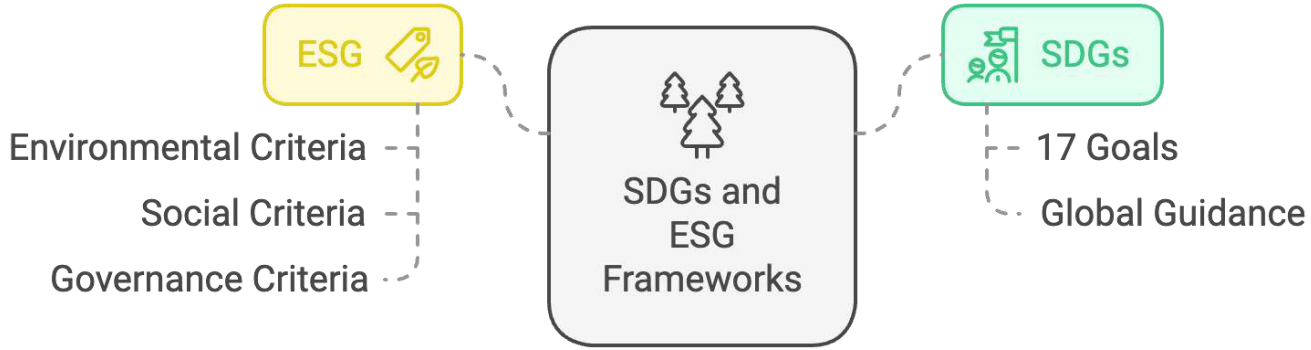
SDG & ESG frameworks: link

SDGs (Sustainable Development Goals) and ESG (Environmental, Social, Governance) **are complementary frameworks:**

- SDGs are 17 UN-defined goals guiding global sustainable development through 2030.
- ESG criteria are used by the financial sector to evaluate corporate sustainability performance.

Simplifying, **ESG metrics measure how organizations concretely contribute to SDG achievement**.

SDGs define "what" to achieve, while ESG measures "how" companies contribute to these goals.



Sustainability: evolution of the legal framework (some milestones

Adopted in 2014, it requires large companies **to disclose non-financial information related to sustainability and social responsibility**.

Published in March 2018, it establishes **a strategy to direct capital flows towards sustainable investments**.

Presented in December 2019, it is a **package of measures** aimed at making Europe the first **climate-neutral continent by 2050**.

Came into effect in July 2021, providing a **classification system for sustainable economic activities**.

Approved in November 2022, **it replaces the NFRD and expands sustainability reporting requirements to more companies**

Approved in July 2024, **it aims to ensure that companies respect human rights and the environment in their operations and supply chains**.

Implementing CSRD directive: EFRAG

The **European Financial Reporting Advisory Group (EFRAG)** is an independent organization established in 2001 with the support of the European Commission.

Its primary role is to **provide technical advice on financial reporting matters to the European Commission**, ensuring that European views are properly considered in the development of international financial reporting standards.

In recent years, EFRAG's mandate has expanded to include sustainability reporting, reflecting the growing importance c ; in

Implementing CSRD directive: EFRAG and ESRS standards

To address the need for standardized sustainability reporting, EFRAG has developed the European Sustainability Reporting Standards (ESRS). These standards are designed to provide a comprehensive framework for companies to

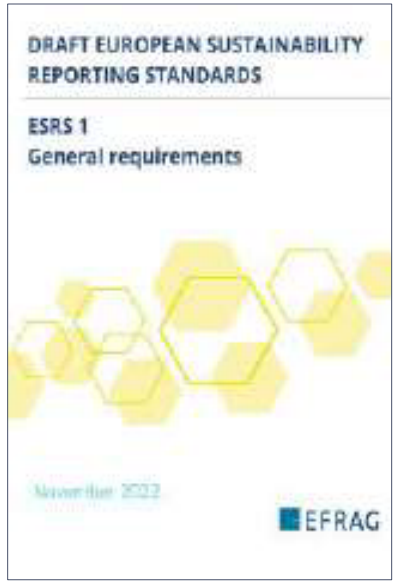
report on a wide range of ESG topics, ensuring relevance, faithfulness, understandability, comparability, verifiability. The ESRS framework comprises several standards, each focusing on specific aspects of sustainability reporting: ESRS 1: General Principles

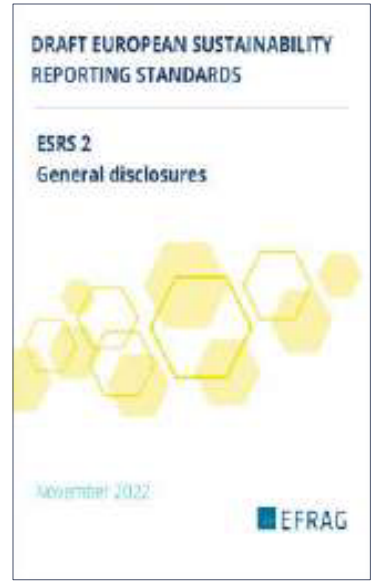
This standard outlines the overarching principles and concepts that companies should apply when preparing sustainability statements, ensuring coherence and alignment with the Corporate Sustainability Reporting Directive (CSRD).

ESRS 2: General, Strategy, Governance, and Materiality Assessment Disclosures This standard requires companies to disclose information about their sustainability governance, strategy, and processes for determining material sustainability topics.

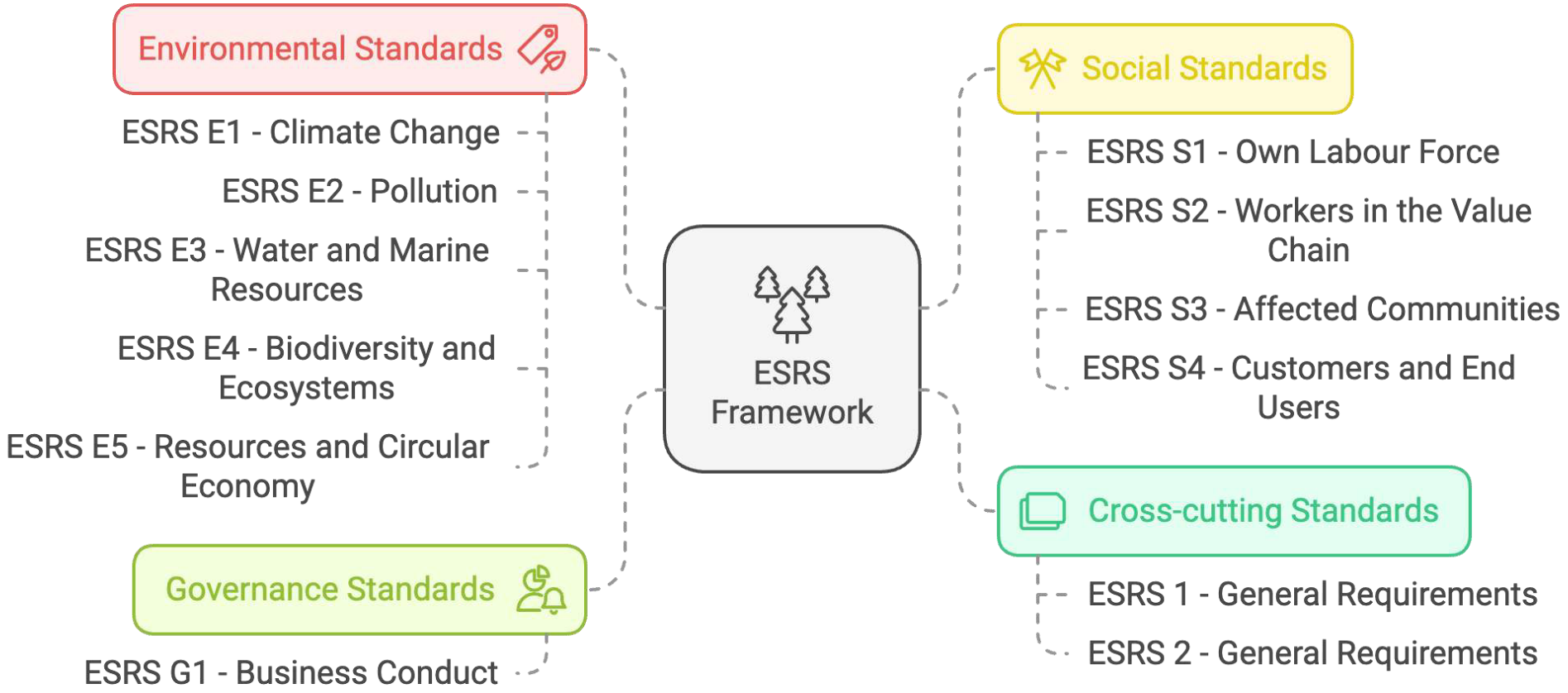
Topical Standards These standards are divided into environmental (E), social (S), and governance (G) topics, each addressing specific areas.

It's important to note that EFRAG is also developing sector-specific standards and guidance for small and medium sized enterprises (SMEs) to ensure proportionality and relevance in sustainability reporting across different types of organizations.





ESRS standards:
overall architecture and sustainability disclosure topics

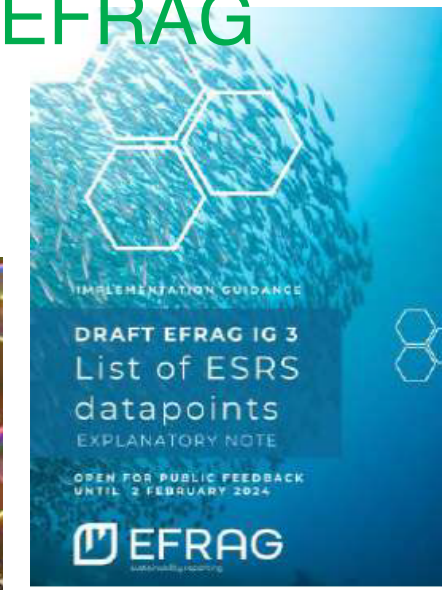


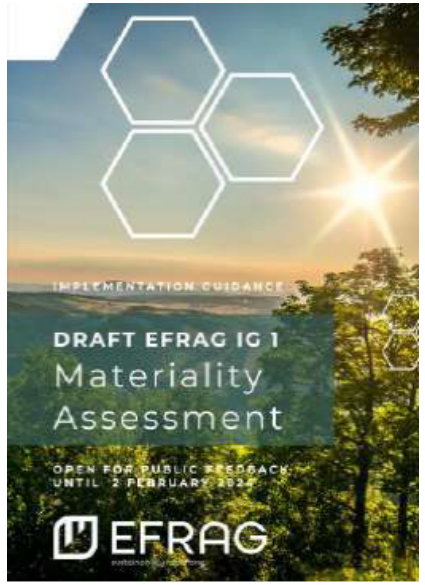
Implementing CSRD directive: a deep dive on ESRS EFRAG implementation guides

To support companies in using these new standards EFRAG has developed Implementation Guidance (IG)

covering:

- **EFRAG IG 1-** Materiality assessment implementation guidance - describes the reporting requirements on materiality assessment, including an illustration of the possible steps in the process to identify the informationto be reported on the impacts, risks and opportunities (IROs) of one's activities on environmental, social and governance issues. It also contains frequently asked questions on assessing dual materiality
- **EFRAG IG 2** - Value chain implementation guidance - describes the requirements for reporting on the value chain during the materiality assessment, providing guidance on identifying who is part of the value chain and who to consider in assessing the impacts, risks and opportunities affecting the company's business
- **EFRAG IG 3** - Detailed ESRS datapoints implementation guidance - presents the full list of requirements contained in each disclosure obligation and related application requirements in Excel format (more than 1000 datapoints, quantitative, narrative, semi-narrative).





The enabler for Sustainability Disclosure: Double Materiality Assessment

The CSRD (Corporate Sustainability Reporting Directive) explicitly requires a double materiality assessment in sustainability reporting, in order to determine the sustainability disclosure information .Double Materiality Assessment is a fundamental concept in sustainability reporting that considers two distinct but interconnected perspectives:

Impact Materiality (inside-out perspective, typically assessed by means of a due diligence):

- Considers how the company impacts the environment, society, and economy
- Evaluates the positive and negative effects of the organization on external stakeholders
- Practical example:
  - The company's CO2 emissions contributing to climate change o Impact on local biodiversity due to extractive activities
  - Working conditions in the supply chain affecting local communities

Financial Materiality (Risks and Opportunities, outside-in perspective, typically assessed by means of a traditional Risk Analysis activity):

- Concerns how sustainability factors influence the company's financial value • Focuses on how ESG issues impact the organization's performance, position, and development
- Practical example:
  - Climate change can damage production facilities of a coastal company
  - Lack of diversity in management can lead to talent loss and reduced innovation
  - Cybersecurity risks can cause direct financial losses

- **Double materiality assessment helps organizations to:**
  - Identify the most relevant ESG issues
  - Define strategic priorities
  - Improve sustainability reporting quality
  - Meet stakeholder expectations
  - Anticipate future risks and opportunities

Balancing External Impact and Internal Value

CSRD and EFRAG ESRS Standards: complexity issues (Mario Draghi's opinion)

The EU's sustainability reporting and due diligence framework is a major source of regulatory burden, magnified by a lack of guidance to facilitate the application of complex rules and to clarify the interaction between various pieces of legislation.

The goal of this framework is to strengthen rules concerning the social and environmental information that companies have to report. This entails a major compliance cost for companies in the EU, ranging from EUR 150,000 for non-listed undertakings to EUR 1 million for listed ones. Moreover, risks of over-compliance (e.g. over-reporting) exist across the value chain.

Reasons for this currently include unclear definitions and requirements, for instance concerning the application of the 'do no significant harm' principle within the EU taxonomy and its alignment with the related assessment for the EU budget; burdensome and potentially overlapping methodologies for emissions accounting between the eco-design for sustainable products regulation, the ETS and the product environmental footprint; and unharmonized timelines for different but related reporting requirements.

Further changes in this framework, including sector-specific reporting standards required by the CSRD, may raise compliance costs.

Sustainability: evolution of the standardization framework (just three milestones)

Published on November 11, 2022, it provides **guidelines for organizations to achieve net zero greenhouse gas emissions** and align their strategies with science-based pathways.

Published on March 16, 2022, serves as a reference framework for organizations to **implement a gender equality management system.**

Published on November 14, 2024, it will serve as a framework for organizations to implement **environmental, social, and governance (ESG) principles effectively**

ESG KPIs: some examples (extracted from ISO IWA 48: 2024)

KPIs for E:

- KPI 1 - Percentage of on-site renewable energy
- KPI 2 - Normalized water consumption
- KPI 3 - GHG (greenhouse gas) emissions Scope 1, 2 and 3
- KPI 4 - Total waste by type
- KPI 5 - Percentage of operational waste not disposed in landfill/incineration
- KPI 6 - Normalized energy consumption
- ...

KPIs for S:

- KPI 1 - Incidents of discrimination, hate and violence
- KPI 2 - Gender pay gap
- KPI 3 - Diversity in senior management
- KPI 4 - Accessibility of products and services
- KPI 5 - Performance evaluations
- KPI 6 -Women in senior management
- ...

KPIs for G:

- KPI 1 - Customer privacy breaches
- KPI 2 - Corruption cases
- KPI 3 - Environmental violations
- KPI 4 - Ethics violations
- KPI 5 - Anti-corruption due diligence
- ...

Source: elaboration from ISO, November 2024, «IWA 48:2024 Framework for implementing environmental, social and governance (ESG) principles», Published Edition 1 https://www.iso.org/standard/89240.html

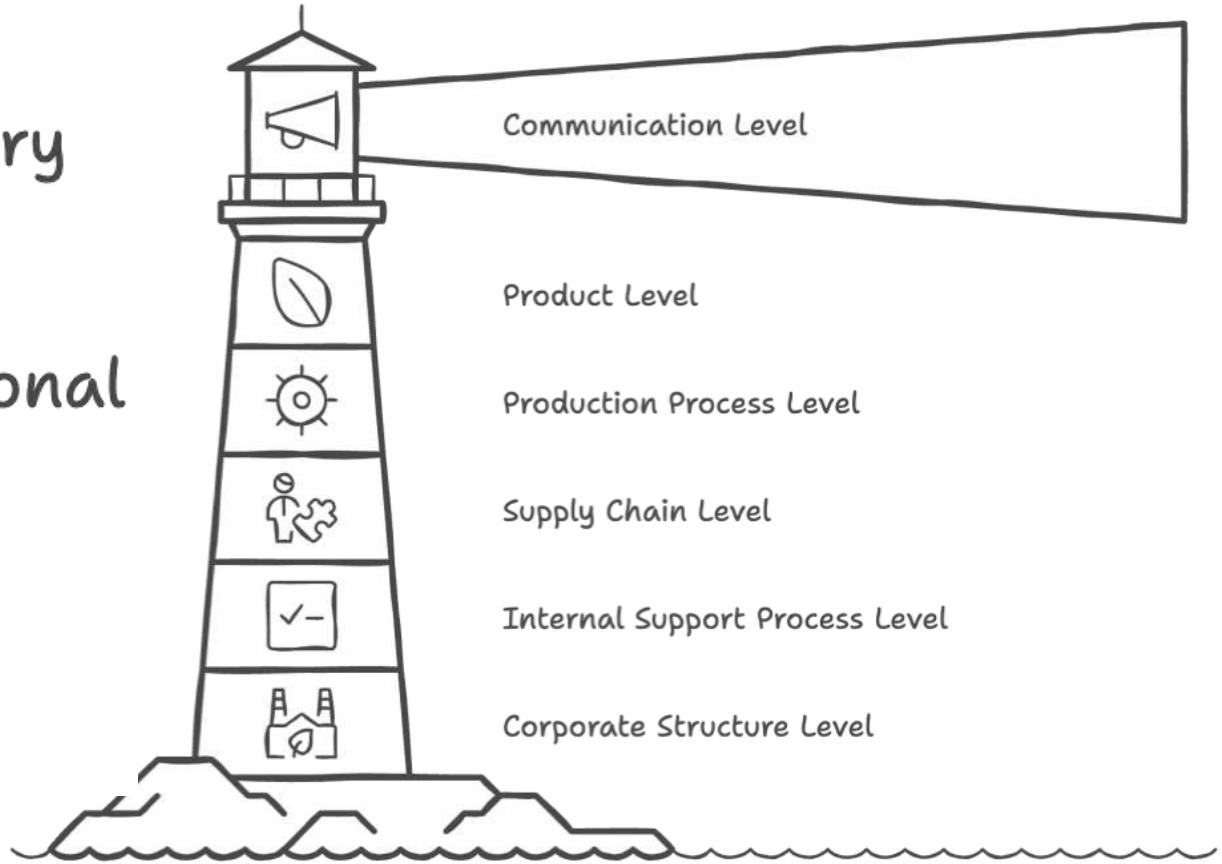
Companies' viewpoint: why are they moving on sustainability?

Companies' viewpoint: on what «playing field» can they move?

Regulatory Reasons

Reputational Reasons

Strategic Reasons

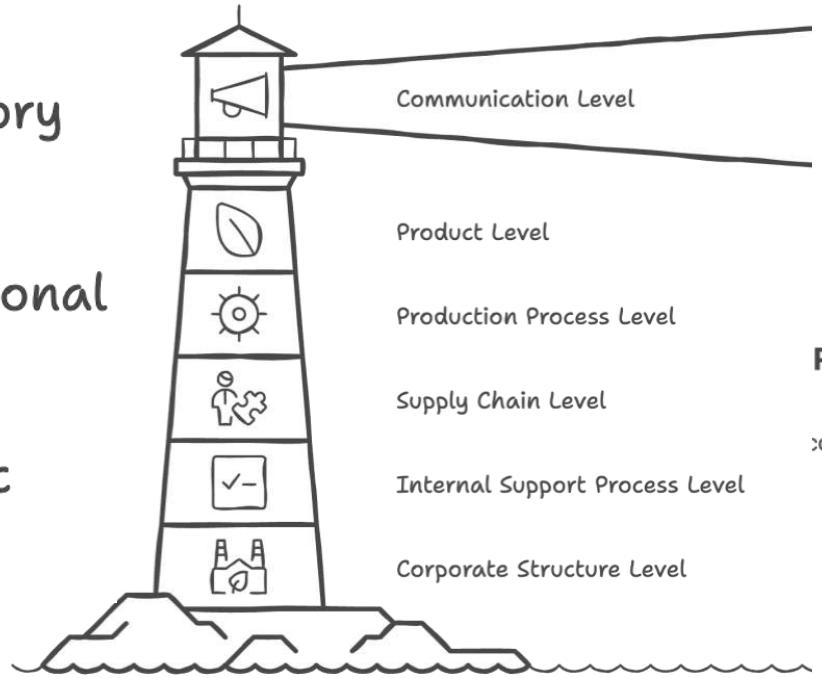


Companies' viewpoint: what are the risks of NOT moving?

Regulatory Reasons

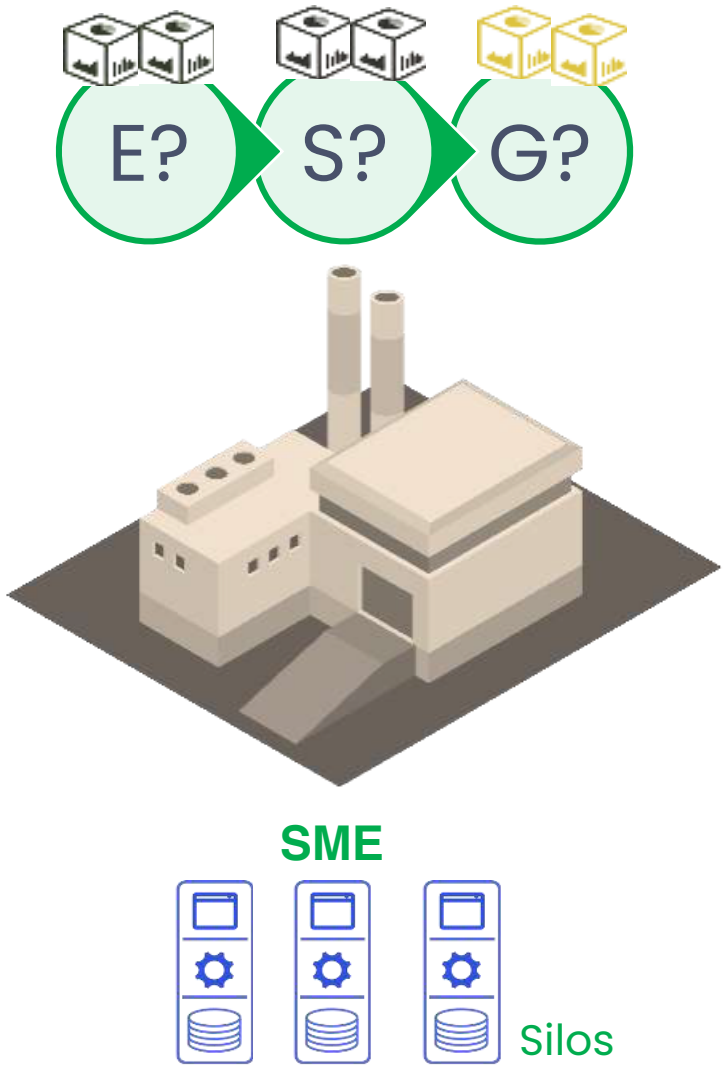
Reputational Reasons

Strategic Reasons

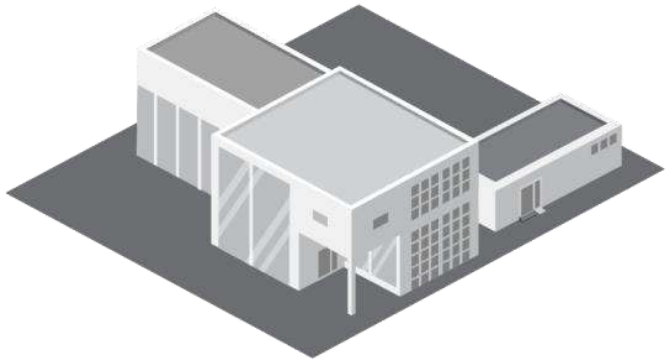


SMEs viewpoint: what are the problems they face when they move?

- Digital competence
- Data Culture (and in particular: culture of data sharing and transparency)
- Lack of ready-made data (there is no 'ready-made' data model for sustainability
- information, and data is typically collected one-off and manually from different systems/ silos)
- Competence on sustainability (which has many facets)
- Need to be accompanied - not only assessed with ESG scoring and / or rating



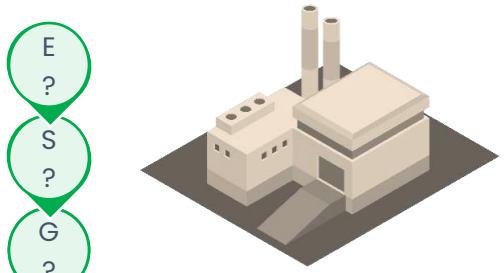
Large Enterprises (and typically Supply Chain leader) viewpoint: what are the problems they face when they move?



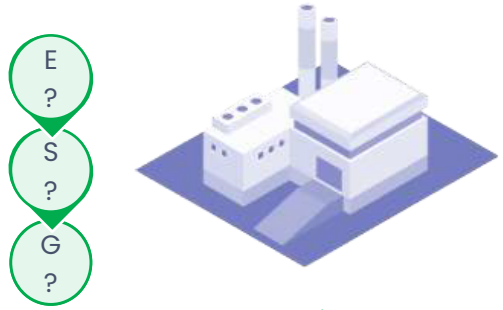
LARGE ENTERPRISE

- The supply chain leader is struggling to assess his sustainability as he does not have an overview of the sustainability of his suppliers
- The supply chain leader is struggling to govern the sustainability path of its suppliers by directing some choices / areas for improvement

Supplier A



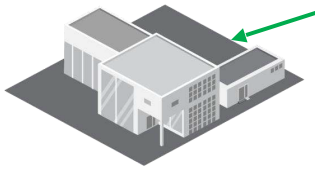
Supplier B

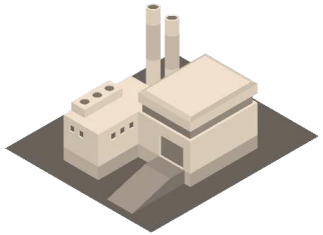


Supplier C

SMEs and Large Enterprises: a deep dive on Knowledge Management issues

Where knowledge in sustainability now resides:





Knowledge (at least partially) structured, contained in databases

E.g. structured data of the number of permanent employees in the company, for each year

E.g. (potentially) number of training courses taken by company staff, for each year

...

UNSTRUCTURED knowledge (contained in documents of various kinds in one or more document repositories, even at a local level, of a single person)

E.g. certifications in the field of environmental sustainability

E.g. the risk assessment procedure

E.g. the description of the company's main products and services

E.g. The business plan

...

Implicit knowledge, in people's heads

E.g. some details of a procedure

E.g. some risk assessment thresholds

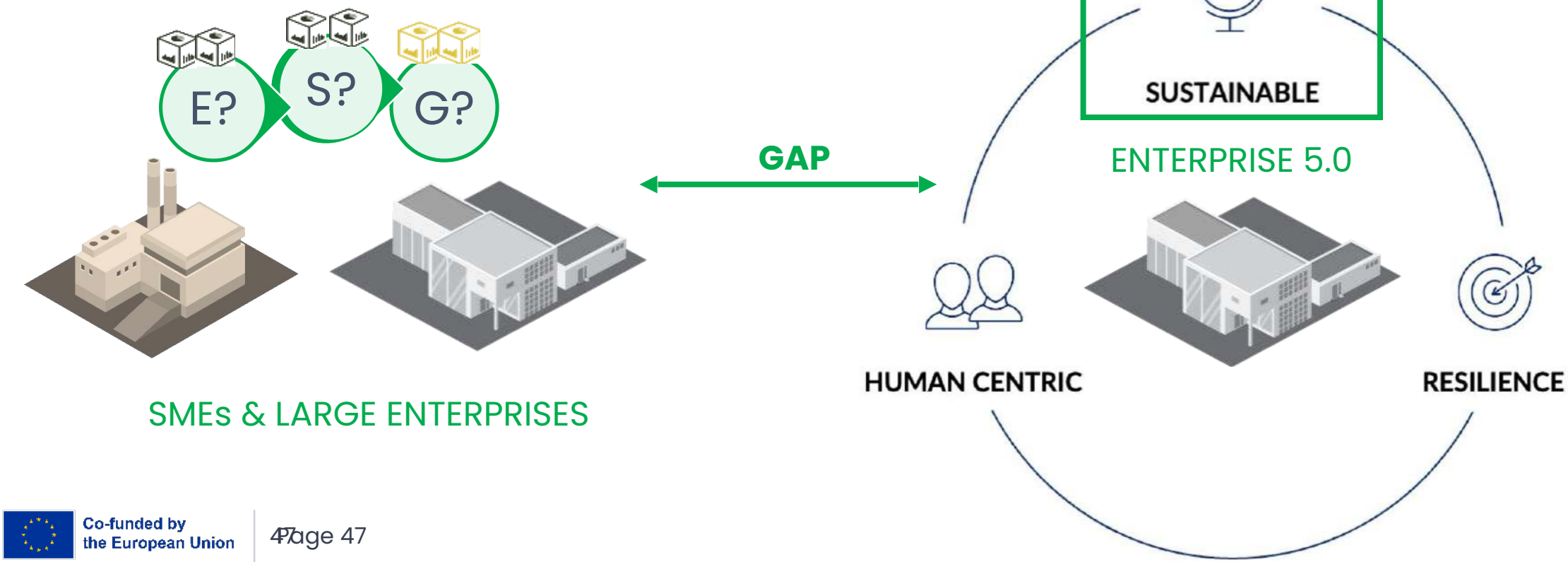
...

Notes:

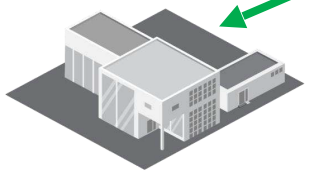
Typically, this knowledge is managed in silos, possibly linked to each other in the case of ad hoc initiatives, created to answer urgent questions (*e.g.: coming from top management*)

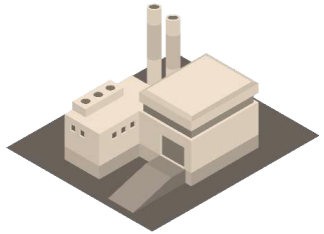
Briefly..

On average, we are still far from realizing the vision



What should be done





Sustainability report

Monitoring of interventions and related impacts

Live Supplier Monitoring

...

Business Development

Operational-Organizational Model for Knowledge Management in the Sustainability Area

Define and incrementally acquire the capabilities to manage all the knowledge that the company has / must create on the subject of sustainability for:

- Be ready to draw up the first sustainability report
- Be able to provide evidence on what is described in the sustainability report and on the methodology used behind the scenes to support what is reported
- Less effort in preparing subsequent sustainability reports
- Monitor your sustainability path in progress to redirect it with a view to the development of the company

Structured knowledge

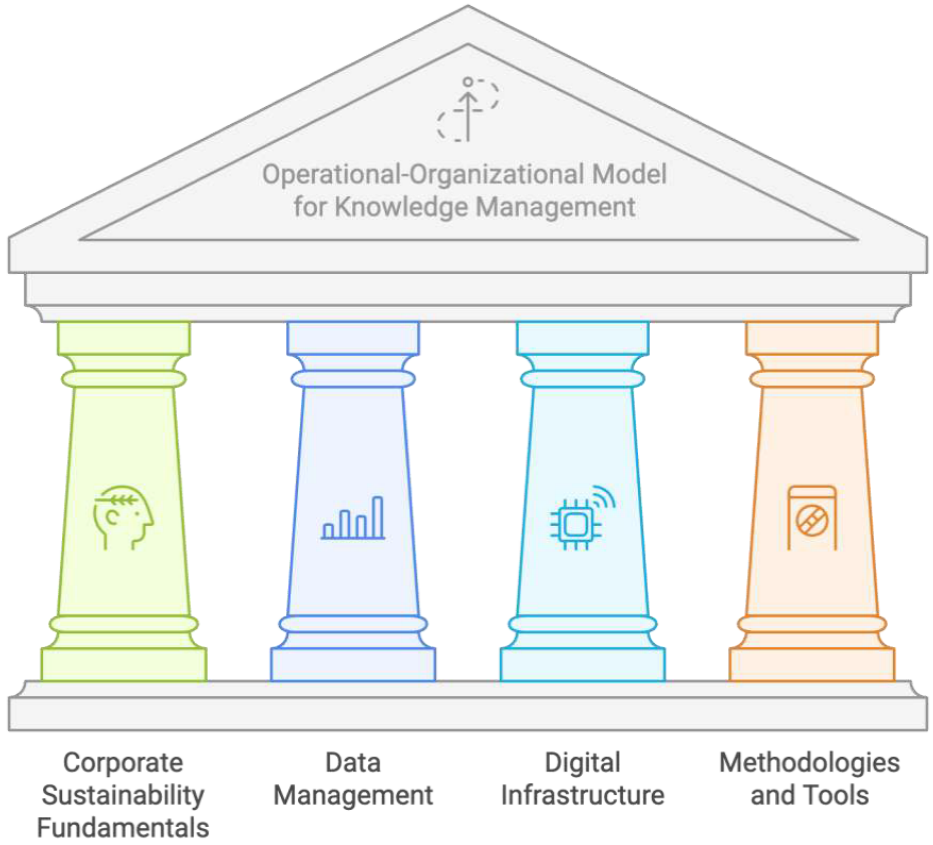
UNSTRUCTURED knowledge

Implicit knowledge, in people's heads

Required Competences (overview)

To build the operational-organisational model for knowledge management in the field of sustainability, it is necessary for companies to equip themselves with competences on:

- the fundamentals of corporate sustainability
- the analysis and management of data for sustainability
- the digital infrastructure for sustainability
- the methodologies and tools for measuring and incrementally monitoring sustainability



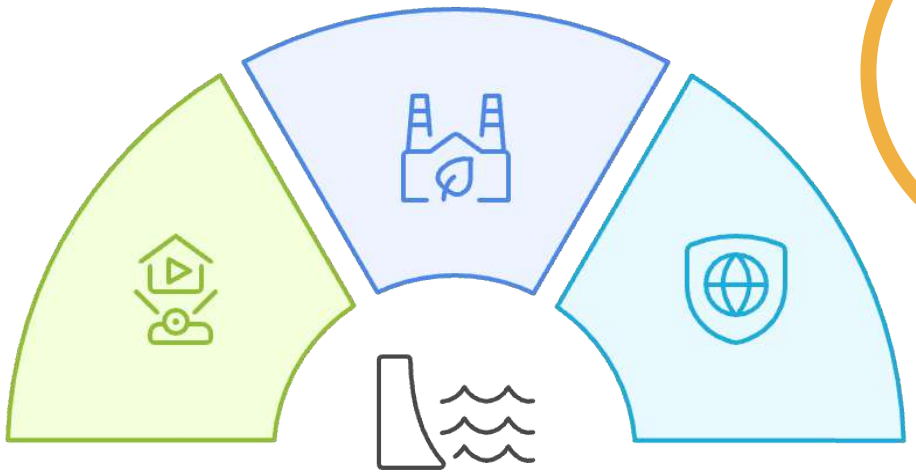
Agenda

Sustainability into a real Company

background and challenges

Sustainability into the holistic Enterprise 5.0

vision



Sustainability & Cybersecurity

quick intro to possible links

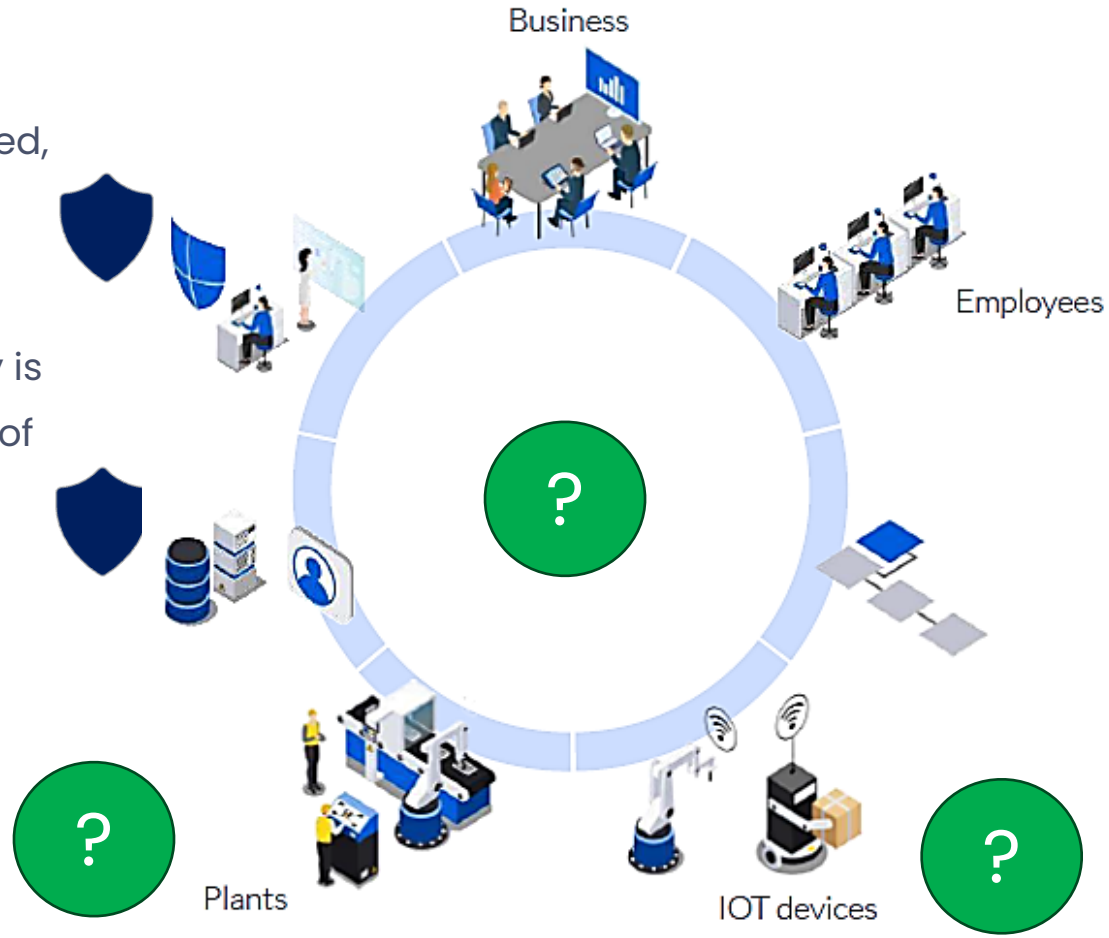
Cybersecurity into a Company: the Holistic Vision (or Utopia ;)?

Risks derived from each threat is minimized

- All assets are protected at the highest level (including the Human Element asset)
- All people know how to manage cyber risks to the best of their ability

Cybersecurity into a Company: the real situation

- Cybersecurity improvement must be approached, like sustainability, using a risk-based approach and in an incremental (prioritized) manner.
- Otherwise (pardon the wordplay), cybersecurity is not … sustainable (we will return to the concept of sustainable cybersecurity in a moment).



Cybersecurity & Sustainability: two areas of strategic importance for companies

- Cybersecurity and sustainability are two of the most significant risks – as highlighted by the World Economic Forum in its latest 2024 report – and enter the top ten global risks
- Source: WEF, 2024, «Global Risks Report 2024», https://www.weforum.org/publications/global-risks-report-2024/digest/

Figure B:

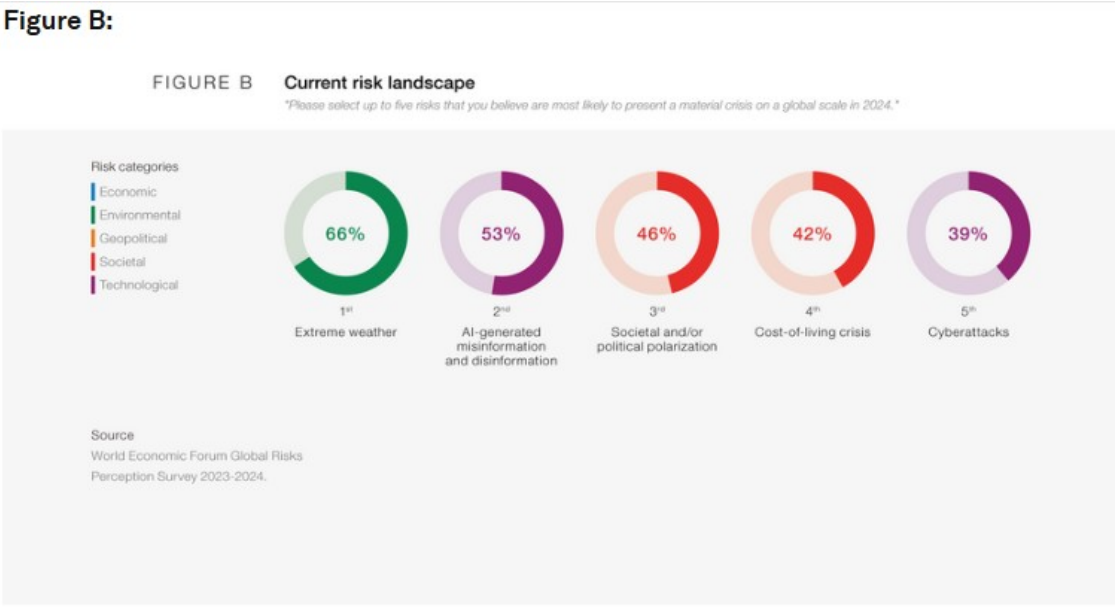
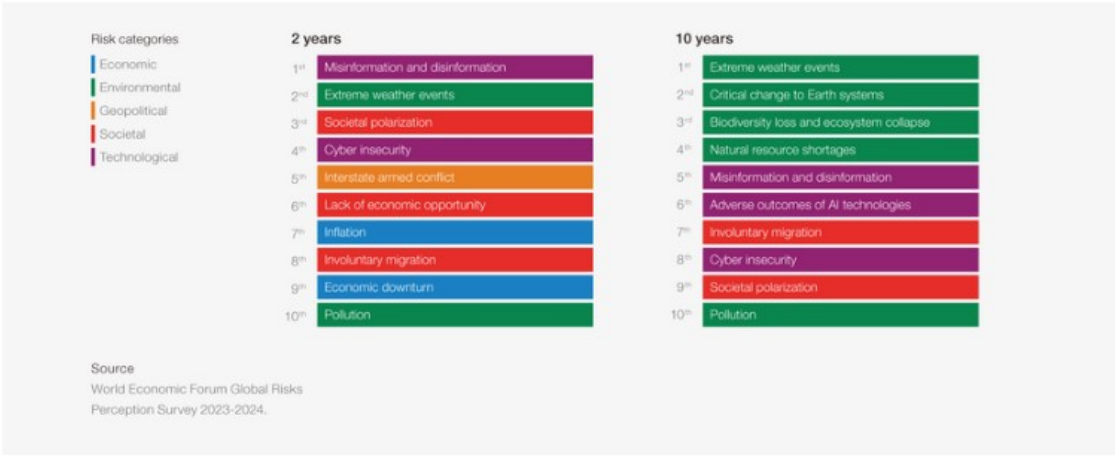


Figure C:



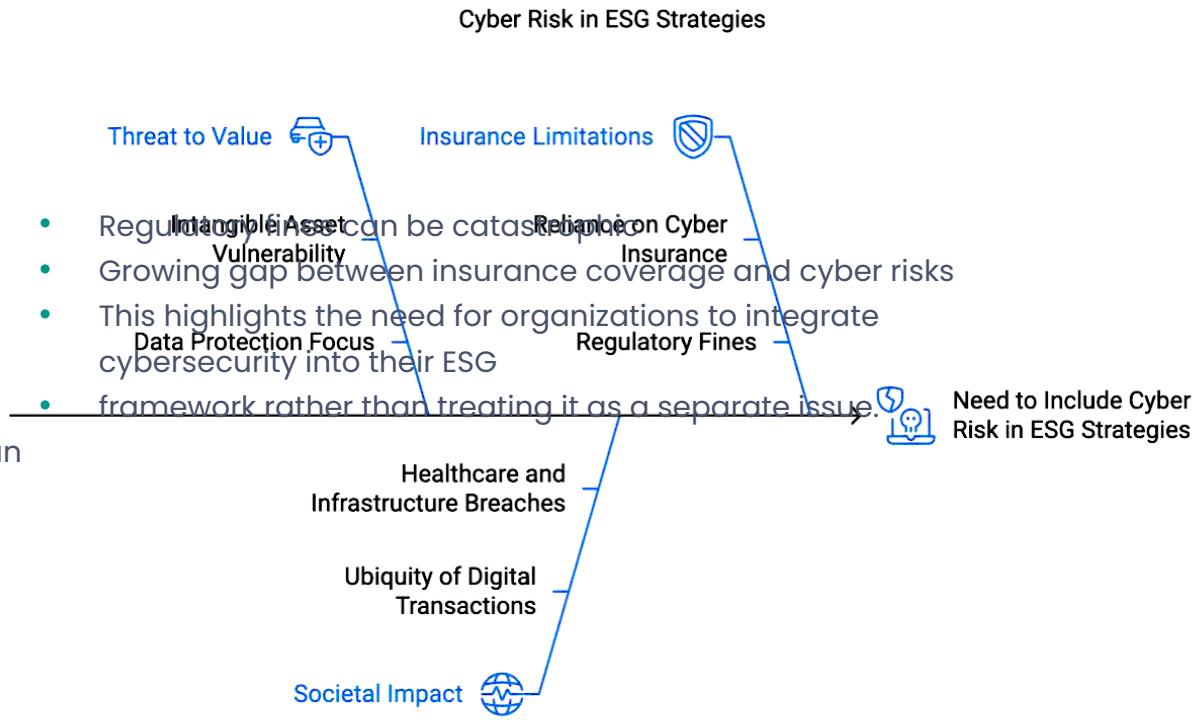
Why Cybersecurity Impacts Sustainability: quick considerations

Key Reasons for Including Cyber Risk in ESG Strategies:

1. Threat to Value
- Intangible assets now represent 90%of organizational value (S&P 500)
- Data is the most critical intangible asset
- Companies must focus on protecting critical assets rather than all systems

2. Societal Impact
- Digital transactions are ubiquitous across sectors
- Identity theft increased 23%in 2021
- Breaches affect healthcare quality and critical infrastructure

3. Insurance Limitations
- Organizations can't rely solely on cyber insurance
- Coverage scope is narrowing
- Regulatory fines can be catastrophic
- Growing gap between insurance coverage and cyber risks
- This highlights the need for organizations to integrate cybersecurity into their ESG framework rather than treating it as a separate issue.



Source: Elaboration of what reported in WEF, 2022, "Cybersecurity is an environmental, social and governance issue. Here's why" https://www.weforum.org/stories/2022/03/three-reasons-whycybersecurity-is-a-critical-component-of-esg/

Why it makes sense to talk about cybersecurity where we talk about sustainability: quick considerations

"**A structured process for communicating cybersecurity** should not be limited to the notification of breaches and incidents but **should also demonstrate the organization's ability to address cyber challenges**.

To date, the primary tool used by companies to update stakeholders on non-financial aspects is the Non-Financial Statement (NFS), which is based on the application of ESG (Environmental, Social, and Governance) frameworks"

Source: Polimi School of Management, 2023, "Comunicare in modo efficace la cybersecurity: ESG e gestione degli incidenti, https://www.osservatori.net/report/cybersecurity-data-protection/comunicaremodo-efficace-cybersecurity-esg-gestione-incidenti/

Cybersecurity & Sustainability Frameworks: Cybersecurity & SDG objectives (quick info)

"Cybersecurity also plays a crucial role in the implementation of the Sustainable Development Goals (SDGs) established by the United Nations, aimed at guiding global policies and addressing key challenges.

Efforts to adopt and implement cybersecurity standards and protocols, monitoring and incident response systems, as well as best practices for cooperation among global organizations, **particularly fulfill the requirements of Goal 9** (industry, innovation, and infrastructure), **Goal 16** (peace, justice, and strong institutions), and **Goal 17** (partnerships for the goals)"

Source: Polimi School of Management, 2023, "Comunicare in modo efficace la cybersecurity: ESG e gestione degli incidenti, https://www.osservatori.net/report/cybersecurity-dataprotection/comunicare-modo-efficace-cybersecurity-esggestione-

Cybersecurity & Sustainability Frameworks: Cybersecurity & the E, S & G dimensions (quick info)

E

Dimension E:

- The consequences of a cyber attack can affect the environment. E.g. Colonial Pipeline attack

S

Dimension S:

- Cyber risk impacts on the provision of essential services. E.g. Healthcare
- People's privacy and digital security. E.g. Facebook - Cambridge Analytics.
- The well-being of people in the workplace. E.g. studies note how people in the Incident Response Team live constantly under stressful conditions; other studies note how a Ramsomware attack can cause a shock to the person/employee who received it.

G

Dimension G:

- Cyber risk can compromise the value of the company (*strong correlation with Risk Management & Compliance topics*)

Source: *rielaboration* of what said in Polimi School of Management, 2023, "Comunicare in modo efficace la cybersecurity: ESG e gestione degli incidenti", https://www.osservatori.net/report/cybersecurity-data-protection/comunicare-modo-efficace-cybersecurity-esg-gestione-incidenti/

Sustainable cybersecurity

- The Jevrons Paradox
- Green Cybersecurity
- Meaning of sustainable cybersecurity: the five dimensions
- Cybersecurity as a process
- The central role of cyber risk estimations
- Correlation between SDGs and trust boundaries
- Towards a holistic (cyber)risk model

Jevrons Paradox

Reference: York, Richard (2006) "Ecological paradoxes: William Stanley Jevons and the Paperless Office", Vol. 13, Human Ecology Review.

In economics, the Jevons paradox (sometimes Jevons effect) **occurs when technological progress increases the efficiency with which a resource is used (reducing the amount necessary for any one use), but the falling cost of use induces increases in demand enough that resource use is increased, rather than reduced.**

Today, there is much discussion about this paradox and the increasing digitalization of many contexts, especially in Industry 4.0 or AI.

Jevrons Paradox & Cybersec

- Cybersecurity and Sustainable Development (SD) are both global challenges.
- Countries within the EU have set objectives that address both SD and cybersecurity, collaborating through various interorganizational networks where these two areas have gained significant attention.
- Growing investments in Renewable Energy Sources (RES) can support the Sustainable Development Goals (SDGs), but they increasingly depend on ICT systems and cybersecurity.
- Conversely, these investments are also tied to the banking sector.
- These intricate relationships have not yet been examined in the existing literature on the EGSS.

Green Cybersecurity

- Technology helps us save energy and resources while simultaneously placing us at the front line in the war against cybercriminals whose power is growing.
- **Green cybersecurity focuses on protecting processes linked to energy production and service delivery within the Environmental Goods and Services Sector (EGSS). It aims to safeguard the digital infrastructure essential for sustainable energy and environmental initiatives.**
- **Problem: how to measure its green level?**

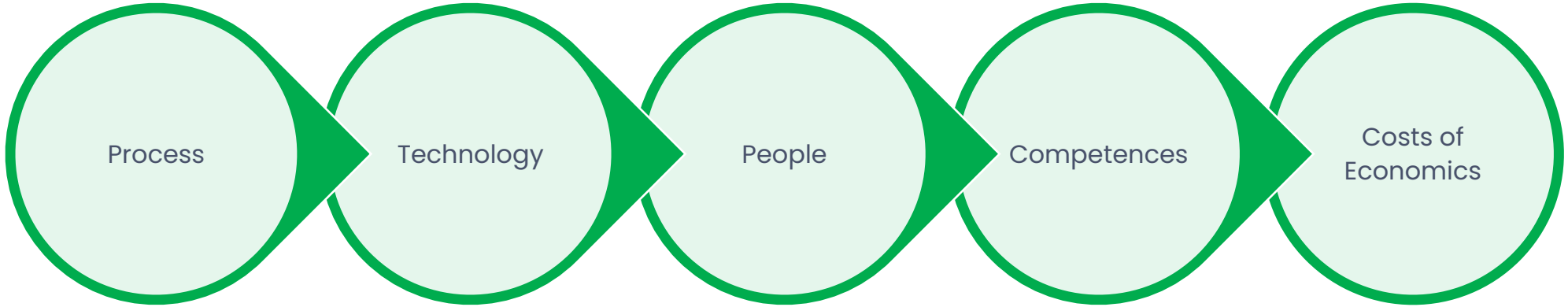
Deny of Sustainability (DoSt)

- Cloud-operated systems are known to be vulnerable to Denial of Sustainability attacks (DoSt), which aim to inflate provisioned infrastructure resources for a service to render its operation unsustainable.
- It may also affect the environmental monitoring of IoT networks

Sustainability of cybersecurity

- New security threats and issues related to emerging technologies need to be understood and managed together with the opportunities that arise from them.
  - Cybercrime is a stakeholder in corporate information systems and one of the most profitable industries.
    - Sustainability of cybersecurity, but not in energy-consuming terms: in technological, economic, process, human and knowledge-related terms.
      - A holistic approach that includes human factors, governance, and technologies is needed to guarantee safety and its longterm sustainability in economic and process terms

Sustainability of cybersecurity



Processes reflect people's needs in relation to policy & technology

Reducing dependence or complexity on people and organizations

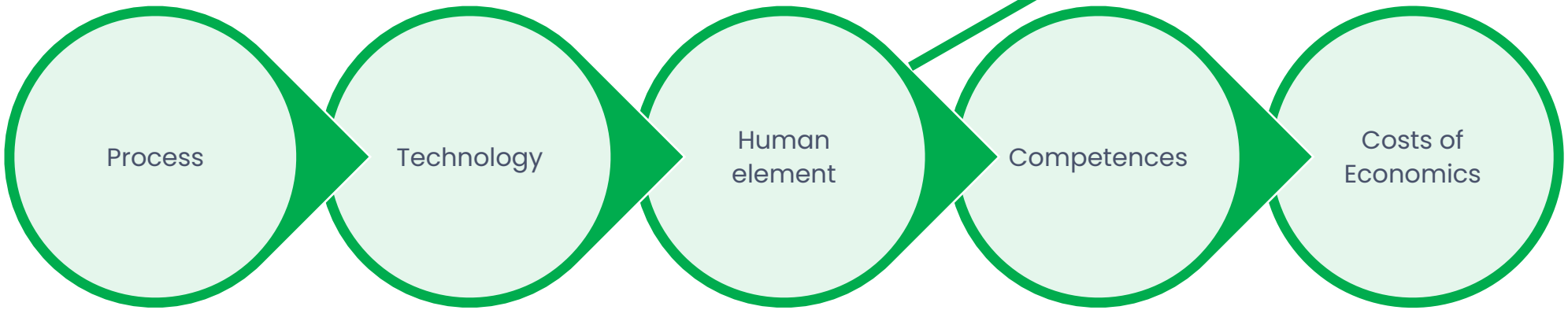
Making responsibilities clear and correctly considering the human element of security

Training is a risk mitigation tool and must be sustainable

Spending the oftenlimited resources to mitigate relevant risks

Total cost of cybersecurity ownership

- Capability Maturity Model
- 'Trusted, customized and comprehensible' cyber risk estimates
- ROSI



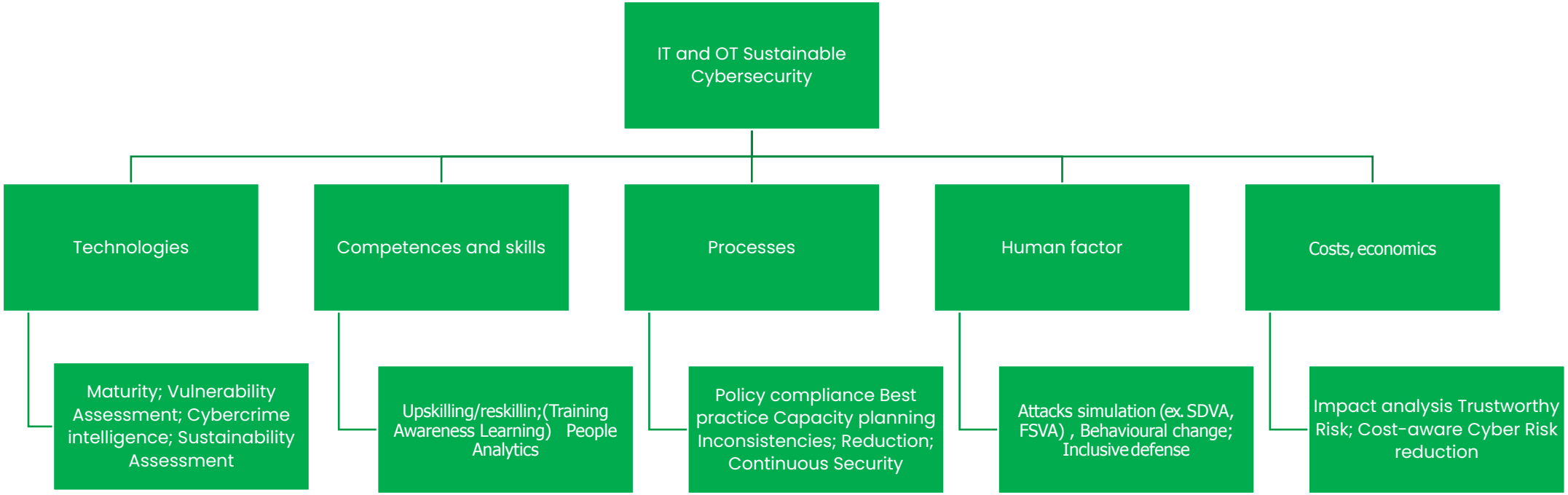
Processes must be closely adapted to the needs of organizations and existingoperations, digital with a purpose

Reducing the dependency and overall complexity of an organization, eliminating data silos, integrating tools, understanding what is involved in adopting them

Clarify responsibilities and roles, train correctly, include the human element in all cybersecurity processes

Training, awareness and learning are different things and must be part of cyber risk mitigation processes

Put limited resources where they are needed and where the risks are greatest, but also improve the trustability and explainability of cyber risk estimates



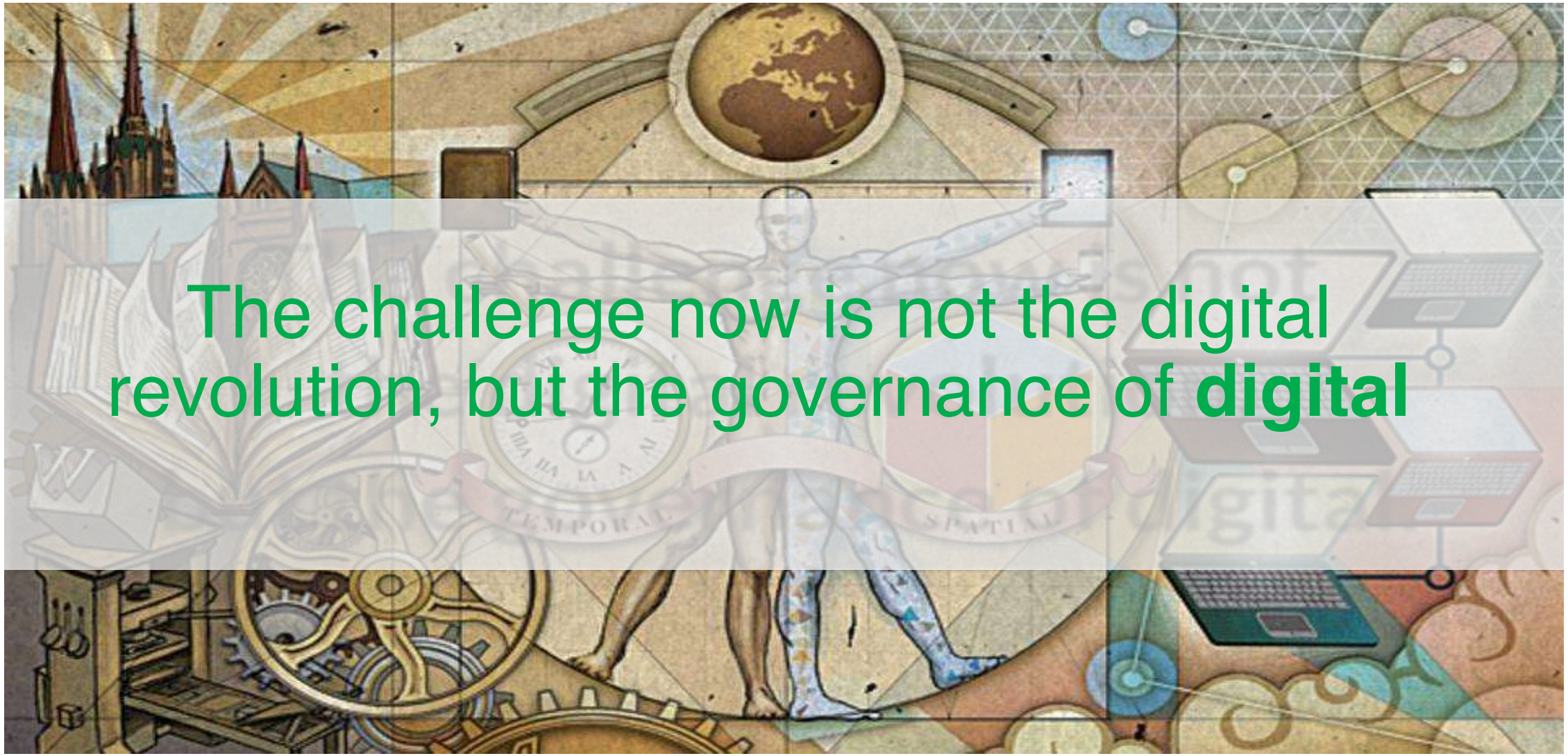
Links with green it

- While the **sustainability of cybersecurity** does not directly pertain to lowering energy usage, embracing more sustainable practices suggests the establishment of greener infrastructures from an energy perspective.
- This is due to the intricate relationship between the energy consumption of an IT infrastructure and the complexity of the processes (both technological and governance-related) that it supports (such as IoT).

The Example of IoT

- Deloitte (2017) reported that "the interconnected nature of Industry 4.0-driven operations and the pace of digital transformation mean that cyberattacks can have far more extensive effects than ever before".
- Statista reports that the number of interconnected end devices grows year by year and is forecast to reach **25.44 bln by 2030**.

- Attacks against TCP/IP stack of IoT nodes: URGENT/11 [1][2], Ripple20, AMNESIA:33, NUMBER:JACK, NAME:WRECK, INFRA:HALT, etc. impacted millions of devices.
- **Remediation efforts are huge, especially in large networks, because most of the time implies physical access to nodes.**



KEY CONCEPT

Cybersecurity is a process, not a product.

The situation in Italy

General situation

- Out of the 55% of organizations that publish an ESG report, 70% incorporate references to cybersecurity

- Dedicated section 25%
- References 44%
- Introduction to the topic 17%
- No references 14%

- Source: Survey CISO 2023; 109 big Italian organisations (Osservatori del politecnico di Milano, Nov 2023)

Evidences

- Difficulty standardizing and measuring cybersecurity through ESG metrics
- Cybersecurity is seen as unrelated to ESG metrics
- Cybersecurity needs to be communicated with ad-hoc reporting

Cyber risk is a business risk and is included in the non-financial statements

Definition of cyber risk

Definition of cyber risk 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**

Risk = Likelihood • Impact

Risk = Attack Probability • Consequence

Evidences

- Difficulty standardizing and measuring cybersecurity through ESG metrics
- Cybersecurity is seen as unrelated to ESG metrics
- Cybersecurity needs to be communicated with ad-hoc reporting

def·i·ni·tion
defəˈniSH(ə)n
noun
a statement of the exact meaning of a word, especially in a dictionary.

Definition of cyber risk

Risk = Likelihood of an impact * Impact

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

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

def·i·ni·tion
defəˈniSH(ə)n
noun
a statement of the exact meaning of a word, especially in a dictionary.

Evidences

- Difficulty standardizing and measuring cybersecurity through ESG metrics
- Cybersecurity is seen as unrelated to ESG metrics
- Cybersecurity needs to be communicated with ad-hoc reporting

Definition of cyber risk

- Risk is generally defined as the product of the consequence and the probability of that consequence occurring.

Risk = Probability of Attack * Consequence

- 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

Why it's so hard to estimate cyber risk

- 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
- Organizations 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

- Reference (ITALIAN): L'importanza di stimare il rischio cyber e le difficoltà nel farne unastima corretta - Cyber Security 360

Why it's so hard to estimate cyber risk

- Kasperson et al. (1992) defined five objectives for risk communicators that apply to different domains (health, environmental risk, etc.).
- Risk management in cybersecurity can have nuances that require you to operate differently than any other risk. For example:

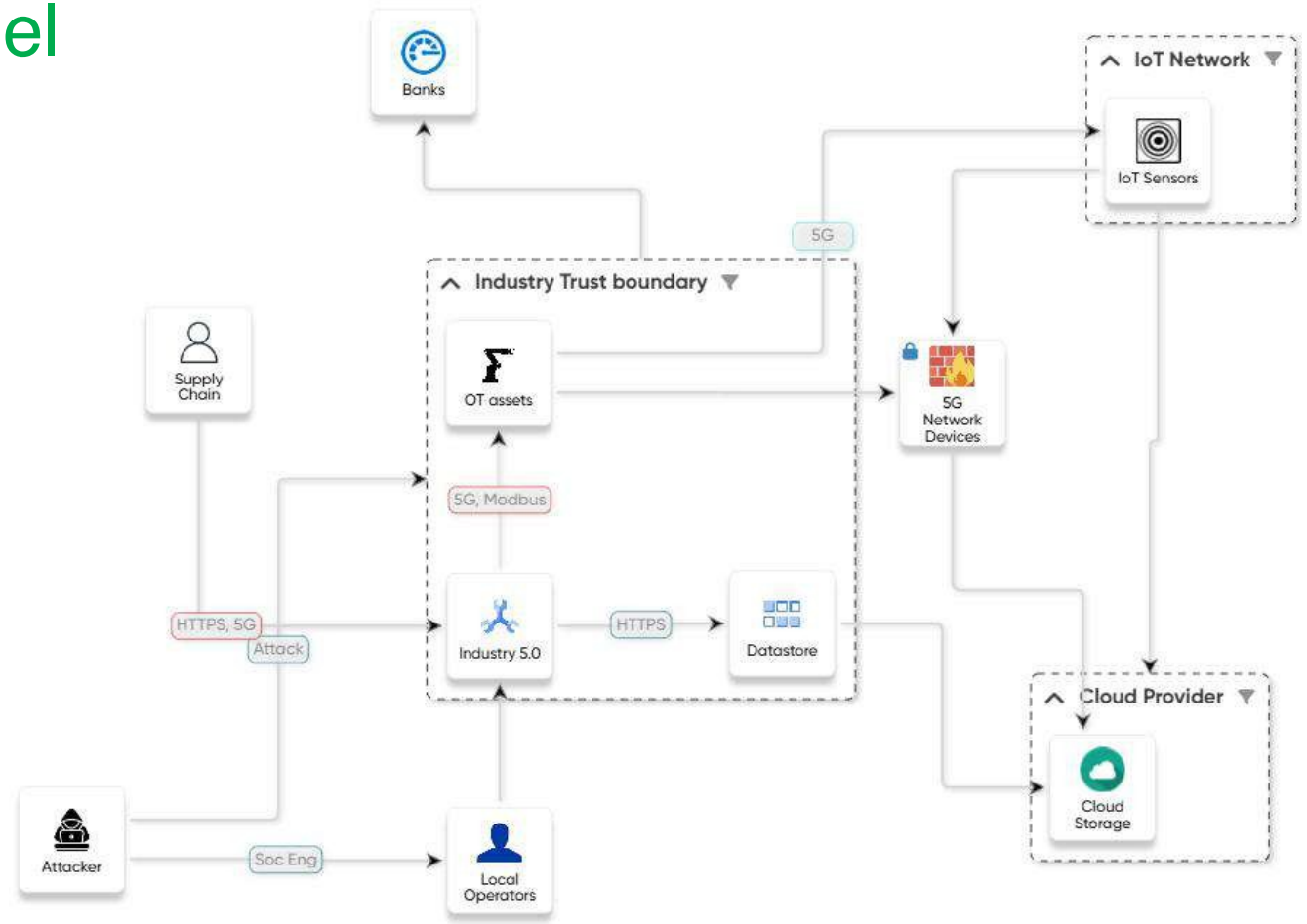
- **Cybersecurity and especially cybercrime is a dynamic field:**
  - **Relative lack of safety knowledge on the part of the public and many technicians;**
  - **Economic impact of hard-to-measure cyber risks;**
  - **Less tangible consequences.**

- Kasperson RE, Golding D, and Tuler S. (1992), "Social distrust as a factor in siting hazardous facilities and communicating risks", Journal of Social Issues, Vol. 48 No. 4, pp. 161–187.

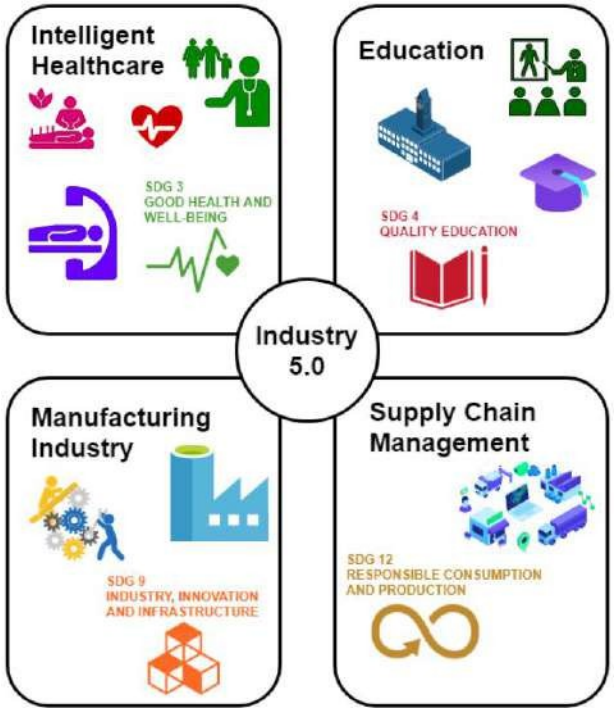
Industry 5.0 threat model

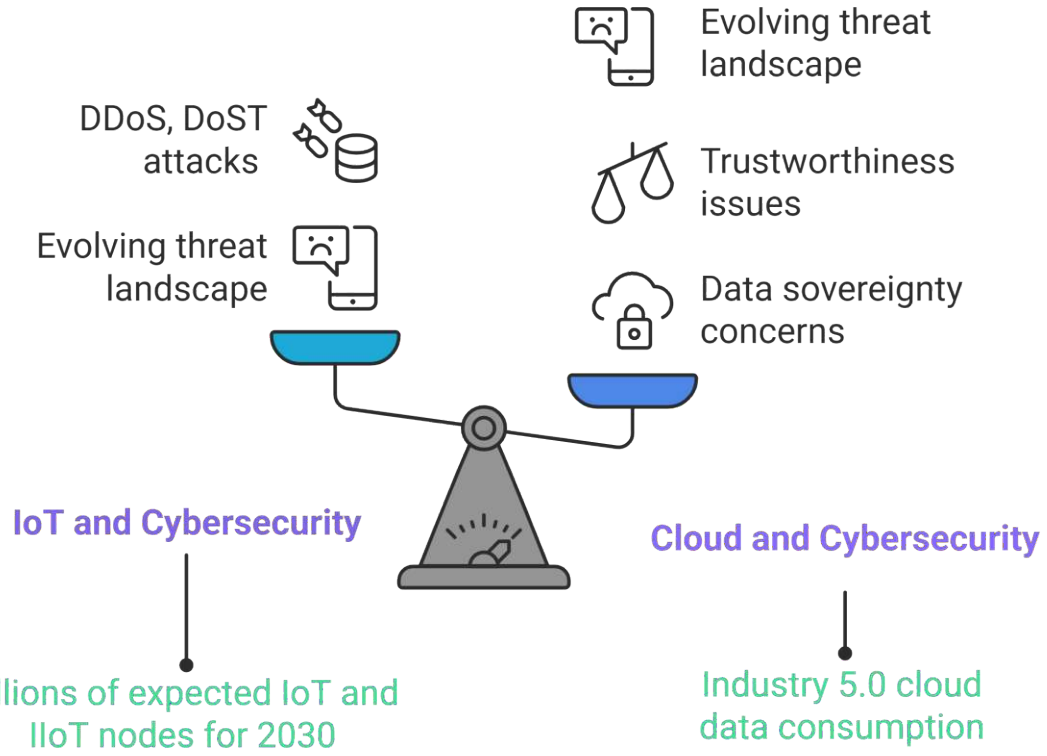
Industry 5.0 threat model

- SDGs focus on data and reality assessment.
- Important trust boundaries need to be established for ESG to be effective; otherwise, it could be exploited (i.e., hack the sense of reality)
- There is no such thing as zero trust in ESG.



Industry 5.0 threat model and SDGS



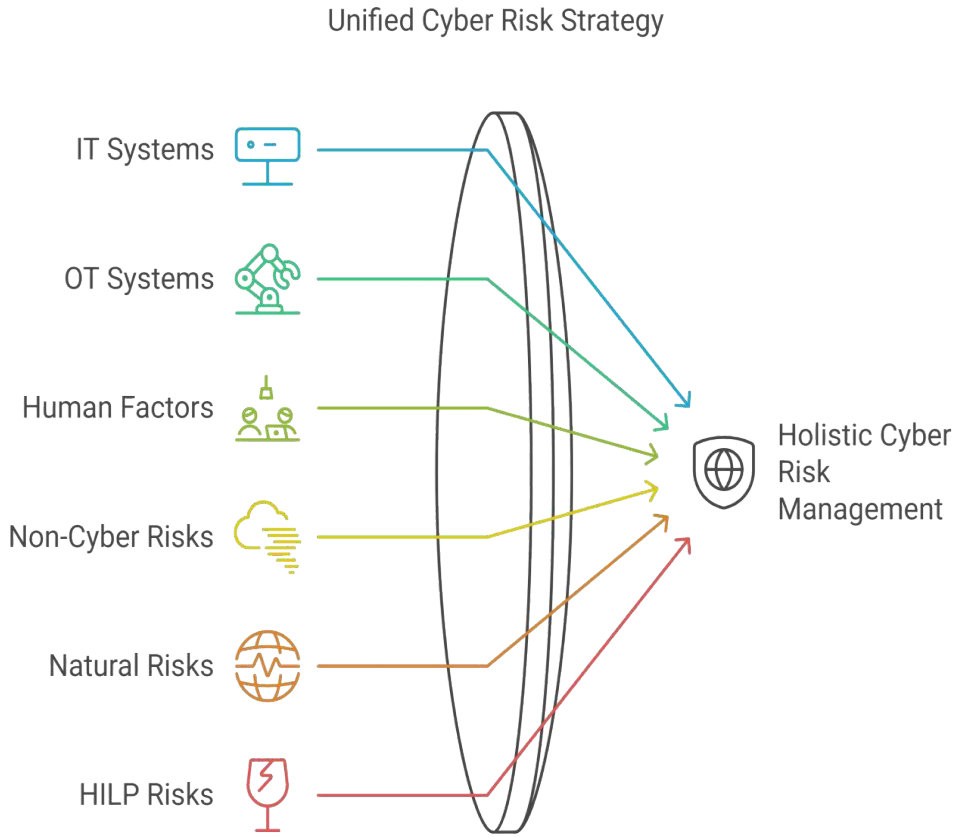


Challenges

Incident Communications

- A structured cybersecurity communication process should not be limited to breach and incident reporting but should represent the organisation's ability to deal with cyber challenges.
- **To date, the main tool used by companies to update stakeholders on non-accounting aspects is the Non- Financial Information Statement (NFIS), which is based on the application of ESG (Environmental, Social and Governance) frameworks.**
- **Gold Teams**
- **Strategic Commination and ESG**

Challenges



- **Holistic/integrated risk model: for too long cyber risk has been considered an IT/ICT only responsibility.**
  - IT
  - OT
  - Human
  - Non-cyber risks
  - Natural risks
  - HILP risks
- **On both tangible and intangible assets**

Meet the speaker

Domenico Orlando

Cybersecurity and Data Protection Law Researcher.

Cefriel

Contents

- Laws focused on cybersecurity that present references and examples of practical relevance to sustainability in its three dimensions (economic, social, and environmental).
    - NIS 2
    - DORA
    - GDPR
- Laws on sustainability that show attention to cybersecurity.
    - CSRD
    - CS3D
- Beyond laws, some case studies incentivized by EU policy (Renewable Energy Communities – RECs)
- Drawing conclusions

Sustainability (ESG) in Cybersecurity and data protection laws

NIS 2

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union.

Cybersecurity refers to the activities necessary to protect **network and information systems**, the **users** of such systems and other **persons** affected by cyber threats.

This law impacts both the 3 dimensions of ESG.

Recital 3: "(...) *Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalization.*".

NIS 2 - Society

- Energy
  - electricity
  - heating and cooling
  - oil
  - gas
  - hydrogen
- Transport
- Drinking water
- Wastewater
- Digital infrastructures (data centers, clouds, networks)
- Space
- PA
- Healthcare
- Postal services and couriers
- Waste management
- Chemical
- Food
- Manufacturing (computer, electronics, motor vehicles, etc.)
- Digital providers (search engines, marketplaces, social networks)
- Research

NIS 2 - Environment

- Energy
  - electricity
  - heating and cooling
  - oil
  - gas
  - hydrogen
- Transport
- Drinking water
- Wastewater
- Digital infrastructures (data centers, clouds, networks)
- Space
- PA
- Healthcare
- Postal services and couriers
- Waste management
- Chemical
- Food
- Manufacturing (computer, electronics, motor vehicles, etc.)
- Digital providers (search engines, marketplaces, social networks)
- Research

NIS 2 -Governance

At **Corporate level**

Governance and sustainability are broad concepts. Some clues:

• Article 20 (1) requires that the **management body** (e.g., executives, board of directors) of essential and important entities approves the risk management measures, oversee their implementation and **can be held liable for infringements.**

• Article 20 (3) requires that the members of the management body follow **training** (cascade effect on the rest of the organization and cybersecurity mindset).

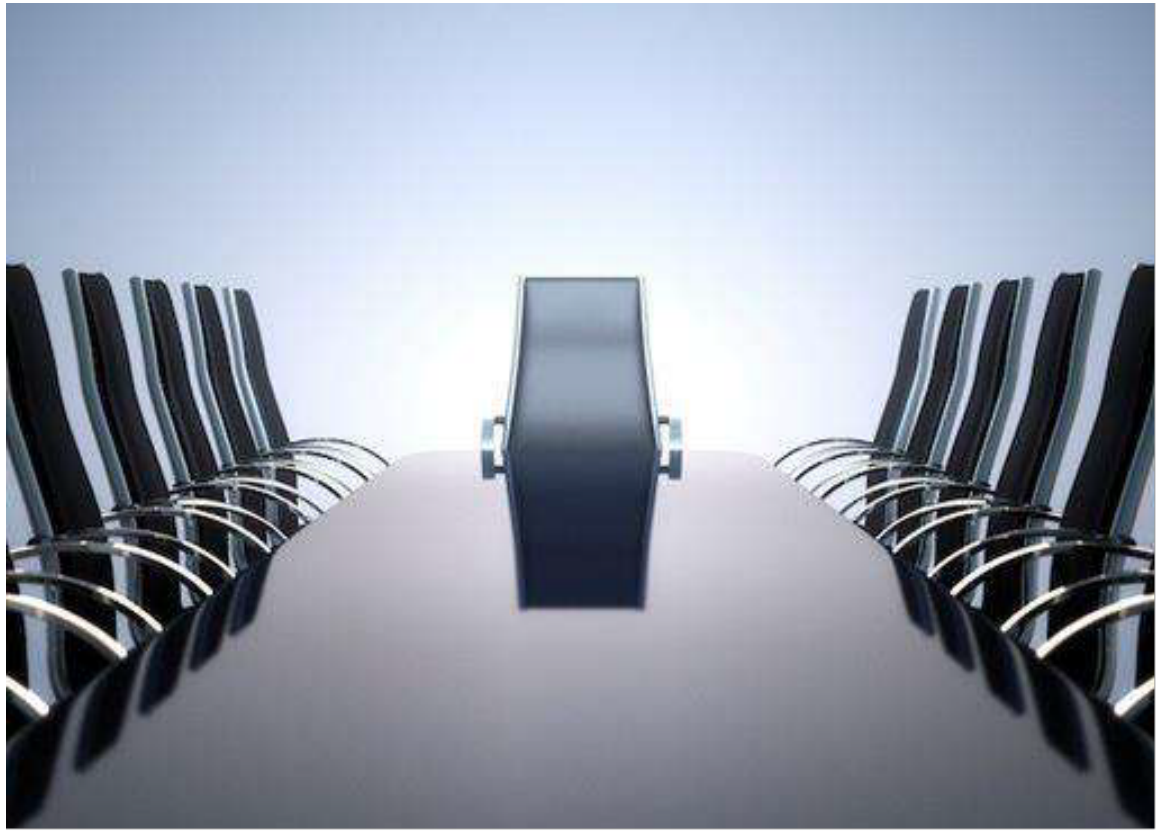
• Article 21 (2), among other things, requires **policies and procedures** on: risk analysis, incident response, business continuity and disaster recovery, supply chain security (see the pager attack), risk management assessment.

NIS 2 -Governance

NIS 2 introduced personal accountability for senior executives.

Article 32 (6) “Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive.”

Articolo 23 D.lgs. 138/2024: “Gli organi amministrativi e gli organi direttivi (…) (c) sono responsabili delle violazioni di cui al presente decreto.”



NIS 2 -Governance

At **State level**

At national level, Member States should set up a **governance framework** clarifying the roles and responsibilities for relevant stakeholders (Article 7).

In this dual level governance, the identified authorities are:

At national level:

• Competent authorities (ACN in Italy) with monitoring, auditing and enforcing powers, Article 8.

• Computer Security Incident Response Teams (CSIRTs) that handle incidents and monitor cyber threats, Article 10.

• Single point of contact (SPOC). It Italy it coincides with ACN. It cooperates with other EU SPOCs and ENISA for information exchange.

At EU level:

• Cooperation Group, is made of MS's representatives, Commission, ENISA, Article 14.

• EU-CyCLONe, European cyber crisis liaison

DORA -Society

Regulation (EU) 2022/2554 on digital operational **resilience** for the financial sector.

Resilience =/= Sustainability

This piece of law is of direct application throughout EU and impacts mainly two dimensions of ESG, namely **society** and **governance**.

Financial institutions are, whether we like it or not, at the backbone of a functioning society.

They include, among the others: credit institutions, payment institutions, crypto-asset providers, insurance, crowdfunding.

DORA -Governance

Article 5 Governance and Organization.

The management body shall

(a) bear the ultimate responsibility for the financial entity's ICT risk

(b) put in place policies for cybersecurity

(c) set clear role and responsibilities

(d) set and approving the cybersecurity strategy

(e) approve and oversee the business continuity plan

(f) approve and review the audits

(g) approve and review the allocated resources for awareness and training too

(h) approve and review the policy on ICT providers

(i) Put in place reporting channels to mgmt. on ICT providers matters

GDPR -Society

The General Data Protection Regulation (EU)2016/679 has the goal to preserve persons' fundamental rights and freedom.

Personal data protection itself is a human right. European Convention of Human Rights (ECHR), Article 8, Right to respect for private and family life Charter of Fundamental Rights of the European Union, Articles 7&8, Respect for private and family life;

Protection of personal data.

Article 37 Environment Protection

A high level of environmental protection and the improvement of the quality of the environment must be integrated into the policies of the Union and ensured in accordance with the principle of sustainable development.

GDPR –Environment & Governance

Sinergy between personal **data minimization**, reduced **power consumption**, and more **efficient data management**.

Data minimization is a principle enshrined in the GDPR, according to which personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

GDPR –Environment & Governance

The other way around, Cybersecurity in Sustainability law

Corporate sustainability reporting directive

Corporate Sustainability Reporting Directive (EU) 2022/2464 (**CSRD**).

It requires corporations (large and medium-sized ones) to **calculate** and **report** their sustainability in ESG.

Article 29(d) requires the undertakings to produce their report in a specific format that would allow for easier access, machine-reading and comparison. The format is called **XHTML** (eXtensible Hypertext Markup Language) and the language established by the EC is called **XBRL** (eXtensible Business Reporting Language).

Non financial reports – a study

Study conducted on 45 Italian organizations that presented their sustainability report + 62 questionnaires (2023 for 2022).

- 25% addressed cybersecurity with its own section
- 43% merely mention cybersecurity
- 32% do not even mention cybersecurity
- 18% declare their intention to include cybersecurity in its next report.

https://www.osservatori.net/

Corporate sustainability due diligence directive

Corporate Sustainability Due Diligence Directive (EU) 2024/1760 (**CS3D**).

It requires undertakings to identify risks for the environment and human rights, prevent and mitigate those risks, remedy, report and communicate.

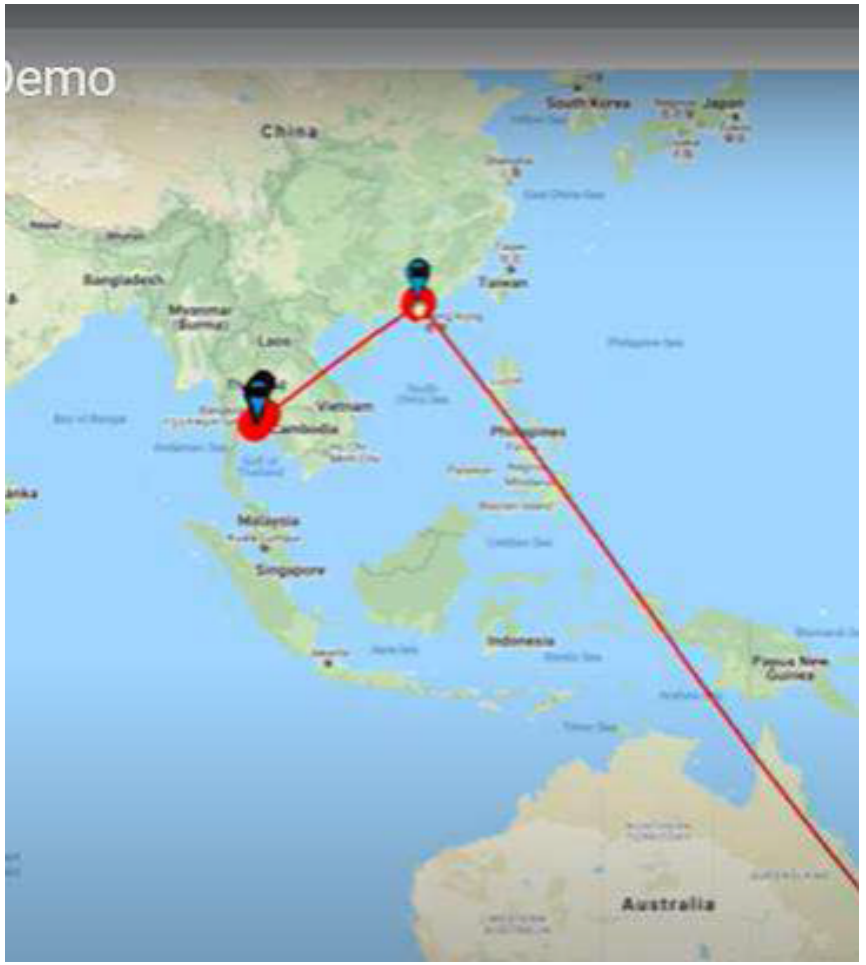
Article 19 (2) CSDS. The law refers to **technologies and tools** that could help obtain sustainability and compliance.

Recital (68) specifies that those technologies and tools should be secure. "*When using digital tools and technologies, companies should take into account and appropriately address possible risks associated therewith, and put in place mechanisms to verify the appropriateness of the information obtained.*"

Waste-tracking devices

Waste-tracking devices use GPS technology to track the path of waste across the globe. In this way the waste producer can verify compliance, report on it and show accountability to stakeholders (authorities and others). The tool can last for years and it is often linked

to a platform showing a map. In a video shared on its website, a waste-tracking tool provider called Earth eye follows a waste container all the way from Australia to China and finally to Thailand. The details allow to identify the company responsible for the ultimate waste disposal.



The smart meter

- IoT such as the smart meters
- This technology enables the smart city and smart grid projects. It is fundamental to have a smart meter for RECs too (Renewable Energy Communities).
- RECs are communities that aim at being energy independent and isolated. They rely on wind or solar power and are made of prosumers (consumers+producers). Solar and wind are intermittent technologies, therefore, it is of paramount importance to monitor consumption and production in a granular way in order to have a reliable supply.

The smart meter

At the same time, the smart meter could be a target for cyberattacks.

It must be secure in its hardware and software.

The smart meter

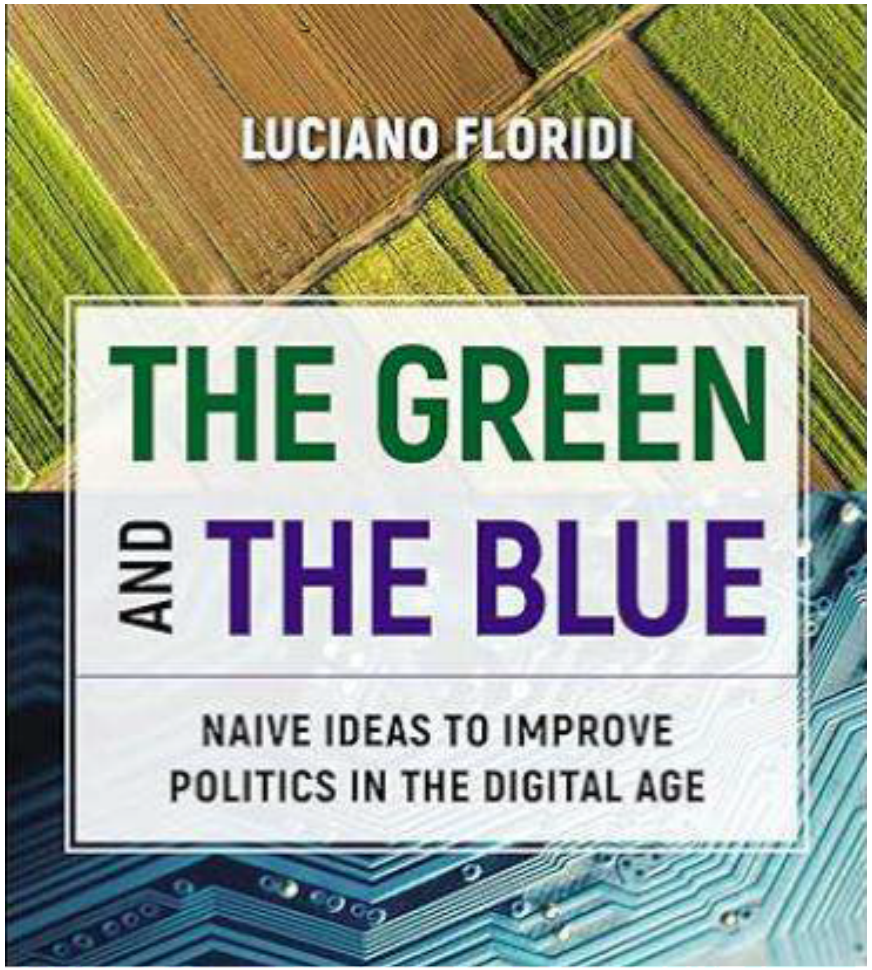
- REC and the Smart Meter are subject to multiple laws at the EU level.
- NIS 2 potentially, in case >50 members (energy producer)
- Cyber Resilience Act (CRA), which applies to IoTs (the smart meter)
- Directive for the Internal Market of Electricity (EU) 2019/944, Article 20, requires cybersecurity and data availability.

Conclusions

Sustainability and Cybersecurity EU laws are quite linked, but not inextricably.

This is probably due to a good coordination of the lawmaker.

This aspect was more evident during the Green Deal, 2019, rather than today.



Meet the speaker

Enrico Frumento

Researcher (Cybercrime intelligence, Offensive security, Social engineering)

Cefriel

Linkedin: www.linkedin.com/in/enricofrumento/

Medium: enrico-frumento.medium.com

Governance

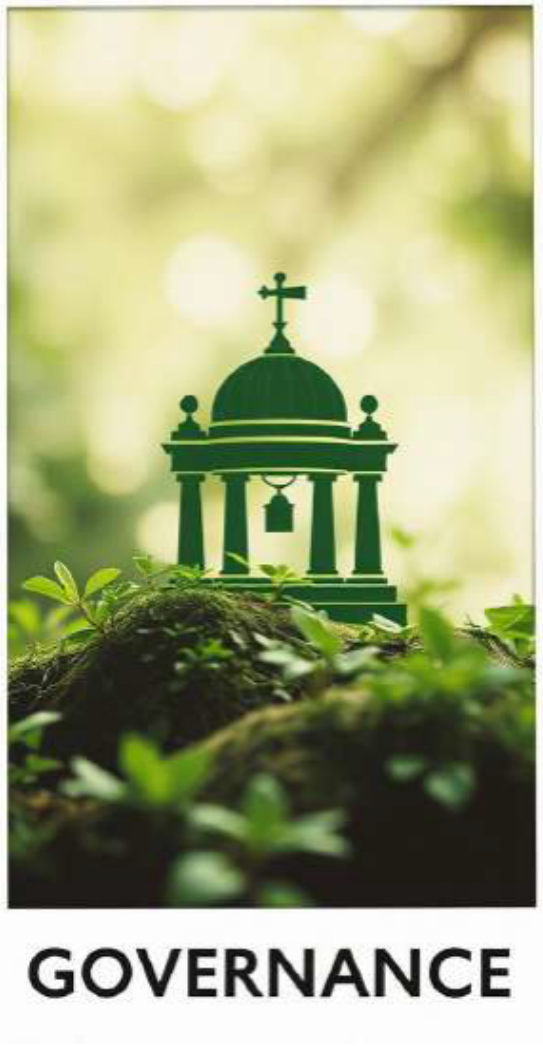
Cyber risk can compromise the value of an enterprise

Environment

Cyber attack consequences could impact the environment

Society

Cyber risk impacts the delivery of essential services and the digital security of people



Governance

Cybersecurity governance challenges

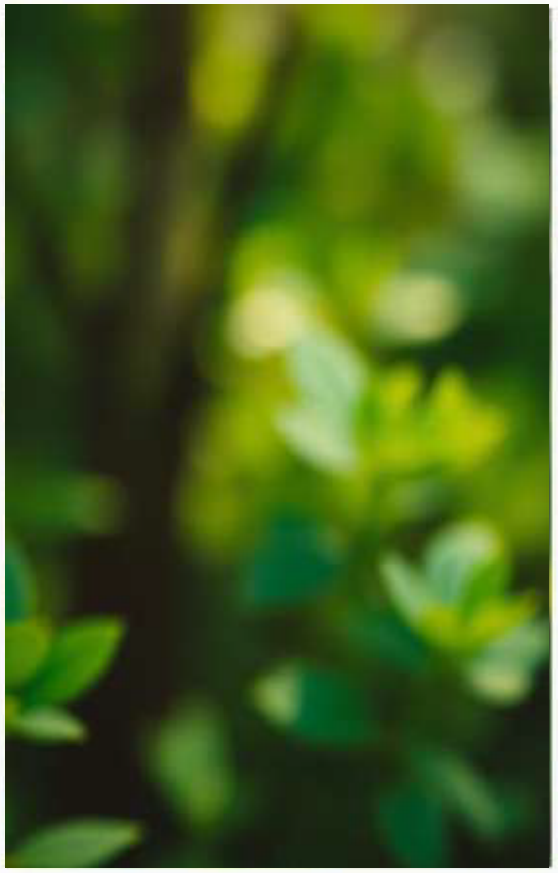
- **Governance is the most evident challenge intersecting ESG and cybersecurity.**
- The existing narrowly focused cybersecurity methodologies fail to holistically incorporate socio-technical considerations
- Needs of a holistic risk evaluation
- Incorporate governance on all the layers of cybersecurity (actually, there are 15!)
- Cybersecurity impacts on the governance of a company
- New legislation impacts e.g., on DevSecOps, insurance, cyber risk evaluation, etc.

Society

Cybersecurity society challenges

Evolution of Healthcare systems, m-health and Hospitals 2.0

- **We are no longer protecting computers; we are protecting society!**
- Mental health and PTSD of cybercrime victims and operators
  - **64%** of cyber security professionals feel that their work negatively impacts their mental health. (State of Mental Health in Cybersecurity, Tines.com, 2022)
  - **47%** of cybersecurity incident responders have experienced burnout but lack the support to avoid it. (VMWare, 2022)
  - **51%** of people within cyber have experienced depression, anger or anxiety due to overwhelm from work. (Vector Report, 2023)



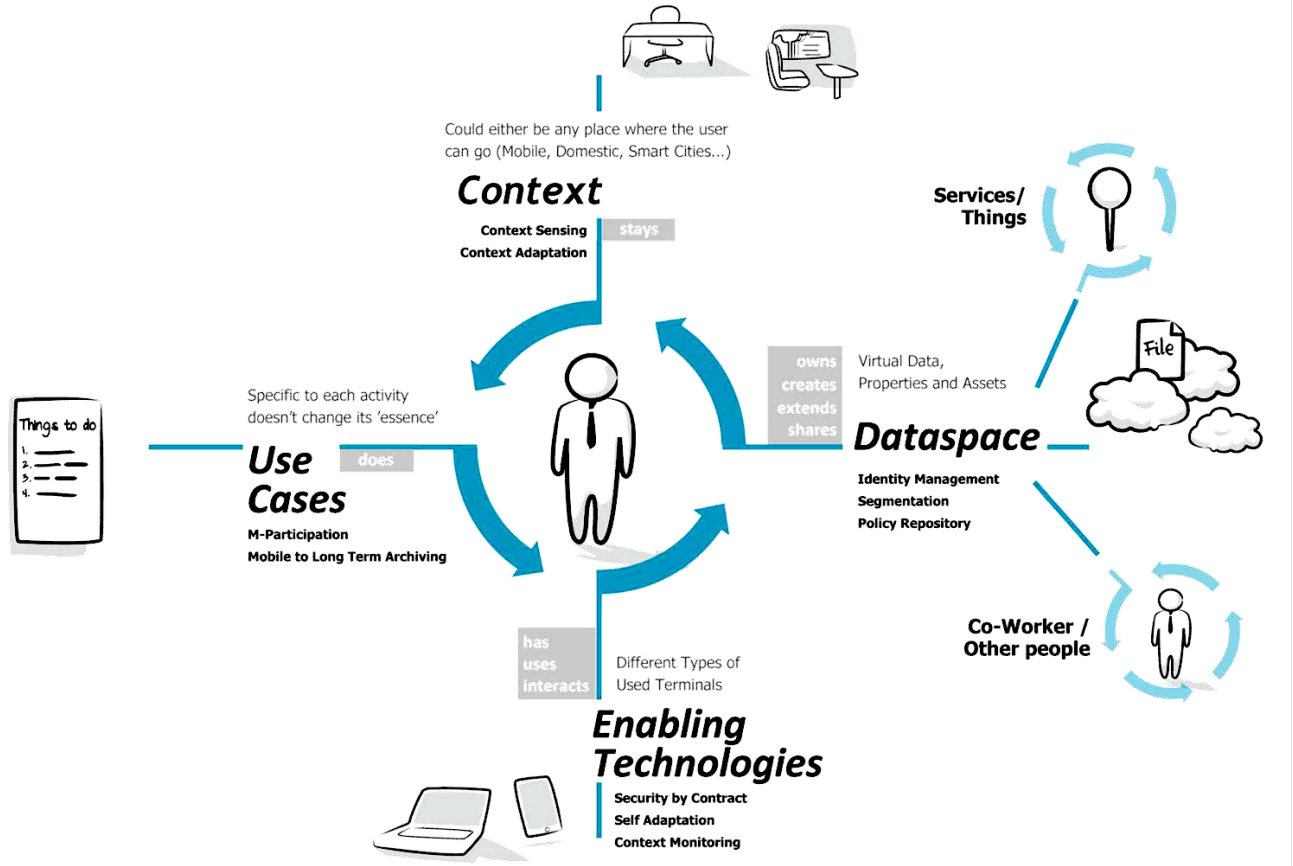
ENVIRONMENT

Environment

In a world of physically capable computers. Automation, autonomy, and physical agency will make computer security a matter of life and death and not just a matter of data [B Schneier]

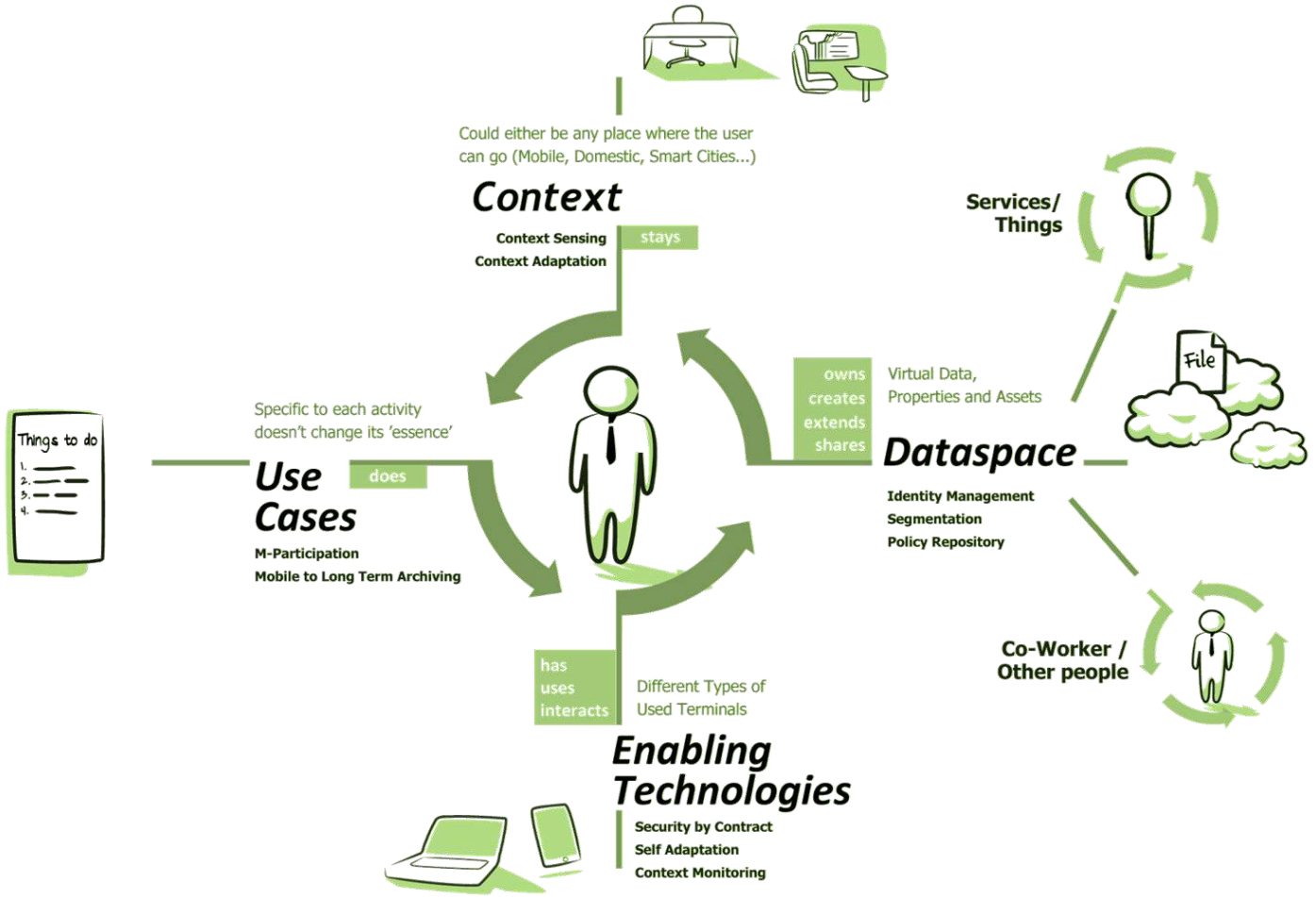
- **Example**: opportunistic attacks in conjunction with epidemics, catastrophic events against healthcare, OT, and chemical implants.
- **Context**: smart cities or harbor

MODERN WORKFORCES and future of ENTERPRISEs



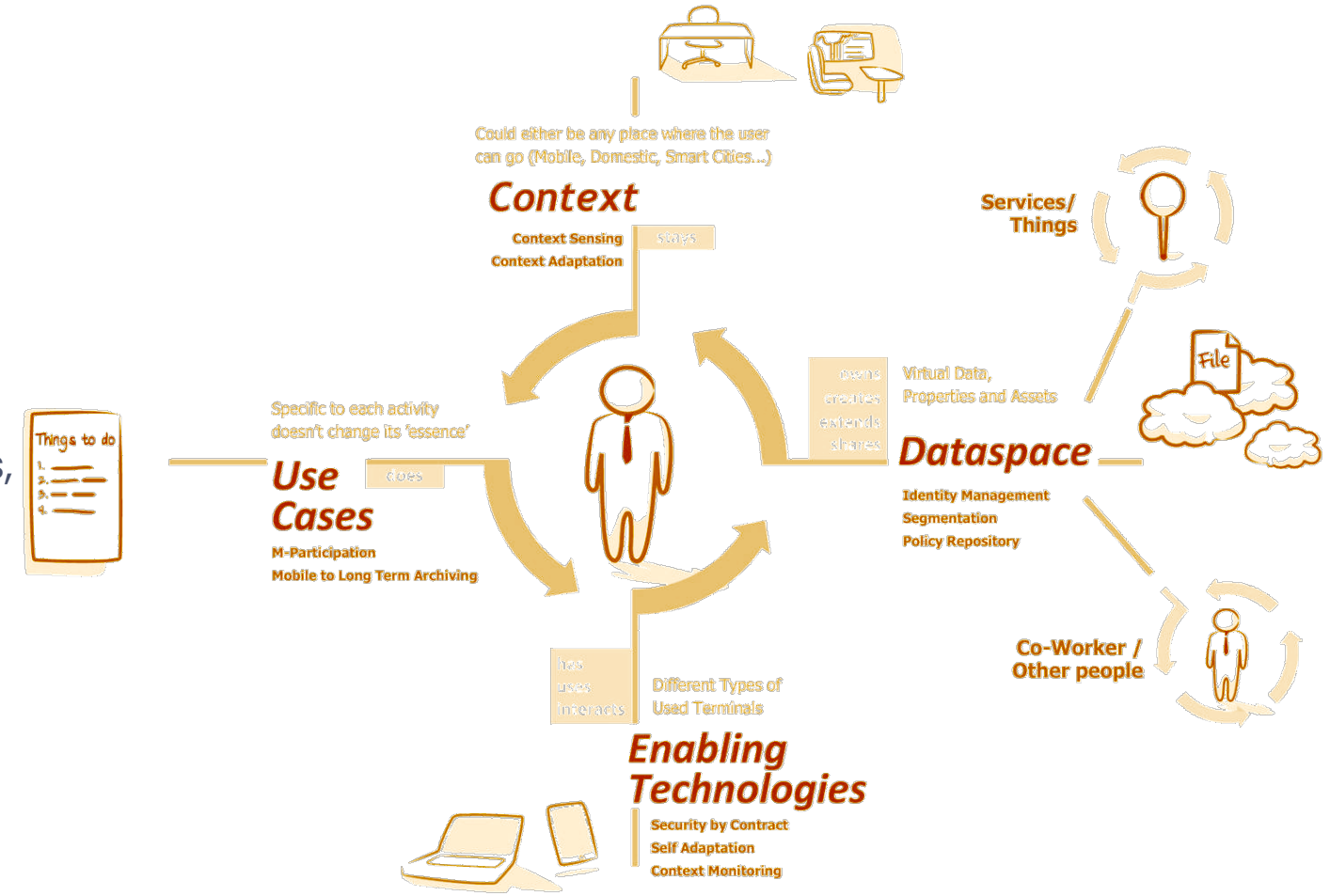
MODERN WORKFORCES and future of ENTERPRISEs

- The entire system operates only in the presence of trust at all levels.
- A reliable system involves having trust in the places where assets are used.
- Cybercrime causes a loss of trust in certain elements, making them untrusted.
- All this is linked to the concept of exploiting trust chains of security.



MODERN WORKFORCES and future of ENTERPRISEs

- Social Engineering, Immersed humans
- BYOD, mobile things, wearable
- Nomadic contextualized threats,
- Insecure asset exchange, data breach, insecure smart objects, insecure cloud, Insecure AIs
- New working and societal habits, and new ways in interacting with entities (e.g., hospitals or PAs)



One last thing

PARTICIPANTS

- Obtain the materials and complete the survey.
- Kindly ensure the survey is finished before you exit the session.

Cefriel

Thank you for your time

Disclaimer

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.

Co-funded by the European Union