Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

COEUS TRAINING PRESENTATIONS

Video lectures support material





INTRODUCTION TO CORPORATE DIGITAL RESPONSIBILITY (CDR) IN SMEs

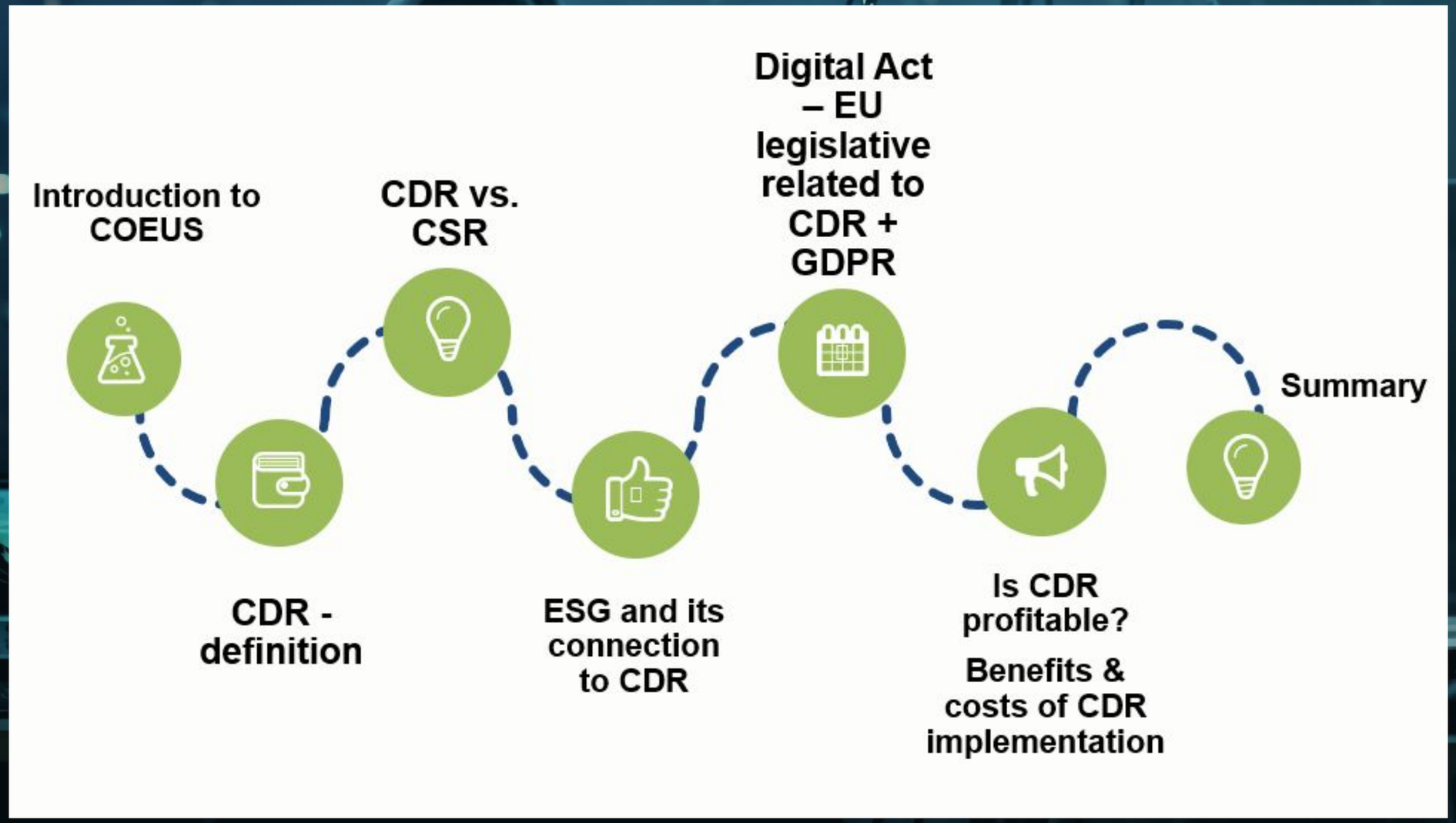
Katerina Fotova Čiković, PhD

Assist. Prof., University North, Croatia

kcikovic@unin.hr

Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

Syllabus – What to expect?



Module 1: Introduction to COEUS

- Interreg Central Europe
- Lead Partner Organization: Digital Innovation Hub Slovenia
- Programme priority specific objective: SO1.2: Strengthening skills for smart specialisation, industrial transition and entrepreneurship in central Europe
- COEUS tackles the challenge not only of ensuring that digitalisation is achieved in Central Europe (CE), but that it is achieved with social, economic, technological and environmental responsibility.
- It does so by supporting Corporate Digital Responsibility (CDR) skills for traditional and innovative SMEs, with a focus on smart specialisation priorities for digitalisation.

Project partner overview

Partner Number	Status	Name of the organisation in English	Partner role in the project	Country (NUTS 0)
1	Active	Digital Innovation Hub Slovenia	LP	Slovenija (SI)
2	Active	Metropolitan City of Turin	PP	Italia (IT)
3	Active	Styrian Business Promotion Agency	PP	Österreich (AT)
4	Active	Innovation Centre of Usti Region (registered association)	PP	Česko (CZ)
5	Active	Chamber of Commerce and Industry of Slovenia	PP	Slovenija (SI)
6	Active	Lubelskie Voivodeship	PP	Polska (PL)
7	Active	University North	PP	Hrvatska (HR)

Project partner overview



Current world challenges

Climate Emergency
One of the largest modern challenges of mankind is undoubtedly the reduction of greenhouse gases and slowing the global warming rate.

Waste of Natural Resources
The earth's surface, its natural resources, and their regeneratio rate, are finite. By 2050 it is estimated that people will consume for three planets



Uncontrolled marine pollution
Marine Litter is one of the most important environmental problems of the seas, coastal areas and inland waters.

Loss of Biodiversity
Biodiversity is the key to healthy ecosystems and human life. According to a UN report (IPBES, 2019), up to a million species of fauna and flora are expected to be threatened with extinction.

SOURCE: https://iasi-inco.com/sustainable-development-our-priority-for-years-now/

On the other hand...

Digital transformation,

Industry 4.0,

cloud computing,

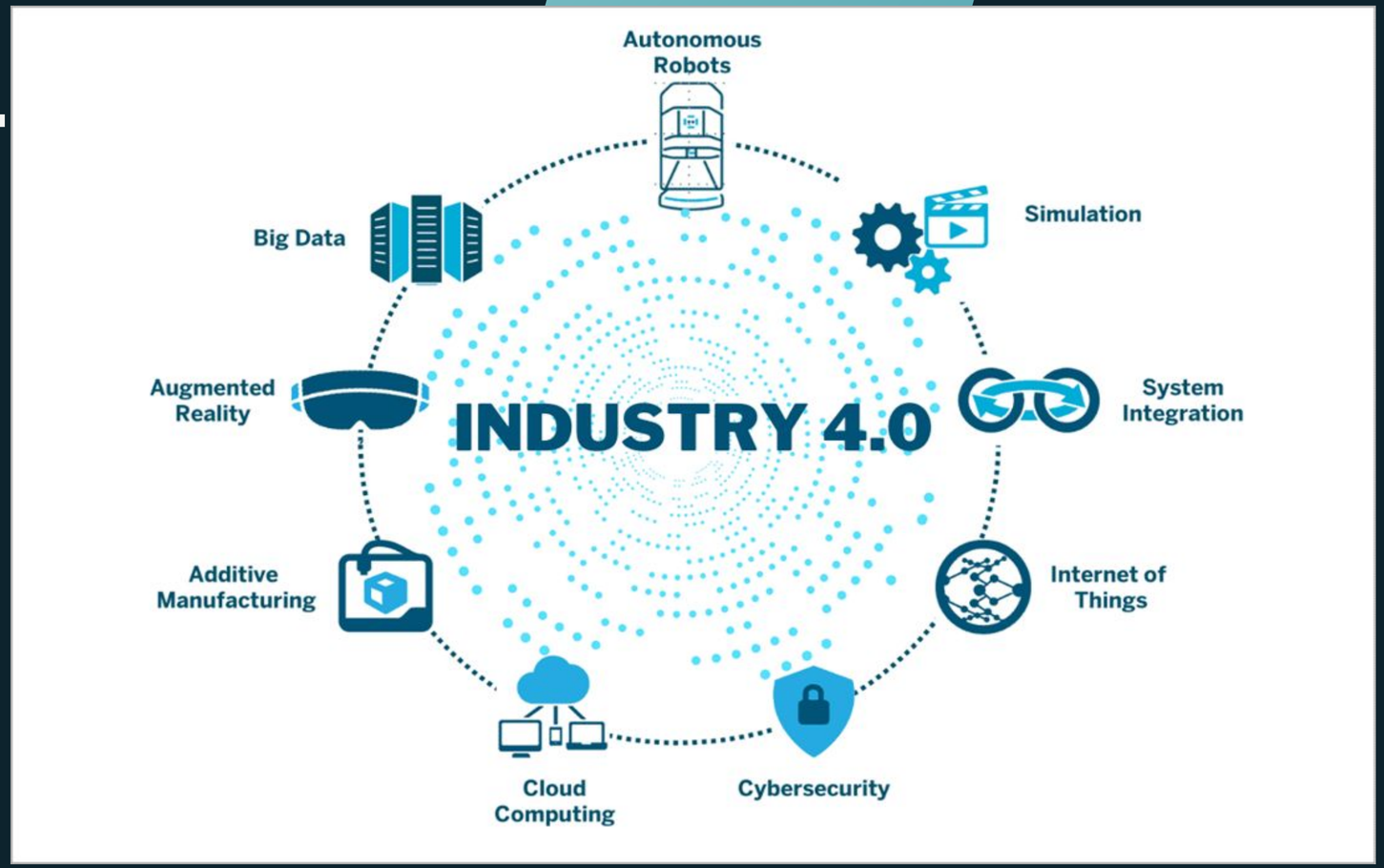
artificial intelligence,

robotics,

Internet of Things (IoT)

Blockchain technology

.....



SOURCE: https://www.calsoft.com/what-is-industry-4-0/

global buzzwords that are being used more and more frequently, not only in politics, business and society, and are becoming increasingly important these days

All these terms are often summarised under the synonym **digitalisation.**

The digital transition is one of the great transformative forces of our time

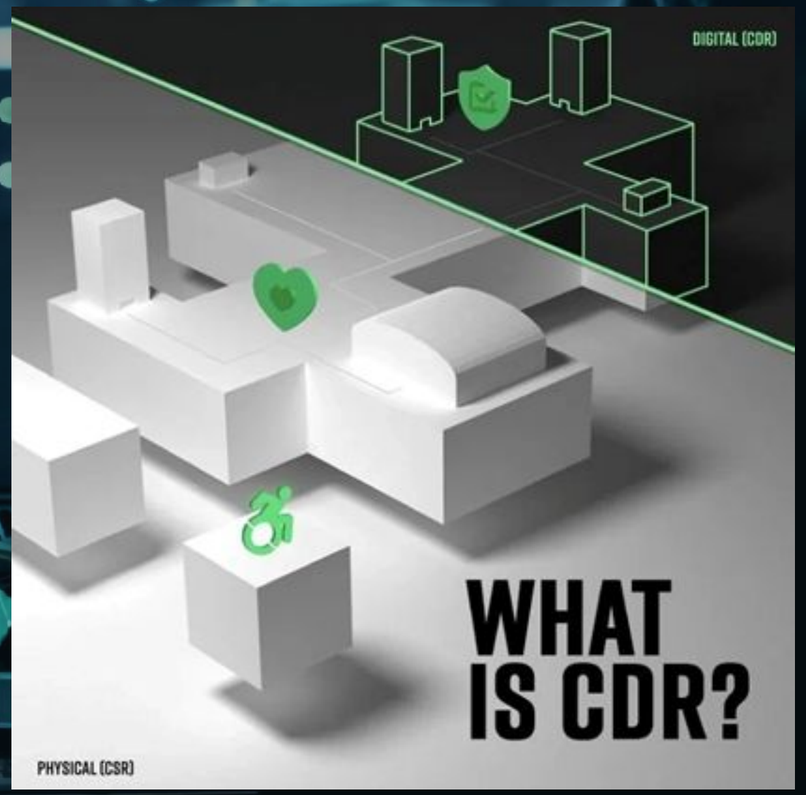
The digital transition brings new hope, but also raises new questions.

What are its environmental and social consequences?

What are the consequences regarding the work organisation and professional relations?

https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2021-corporate-digital-responsibility-2._environmental_and_social_issues.pdf

Module 2: CDR - definition



Corporate Digital Responsibility (CDR) is a set of practices and behaviour that help an organisation to use data and digital technologies in a way that is socially, economically, technologically, and environmentally responsible.

In theory, it sounds obvious.

In practice, it is not so easy to achieve, particularly for SMEs (CDR Europe Interreg)

A digitally responsible company should thus respond to several major challenges - in line with the Sustainable Development Goals:

01 **Regulatory responsibility** for data protection and compliance with the GDPR and sectoral regulations;

02 the **ethical responsibility** of artificial intelligence software;

03 **societal responsibility** in relation to data management, transformation of working patterns, data sharing, inclusion of all;

04 **environmental responsibility** for the use of data in considering the environmental impacts of business activities.

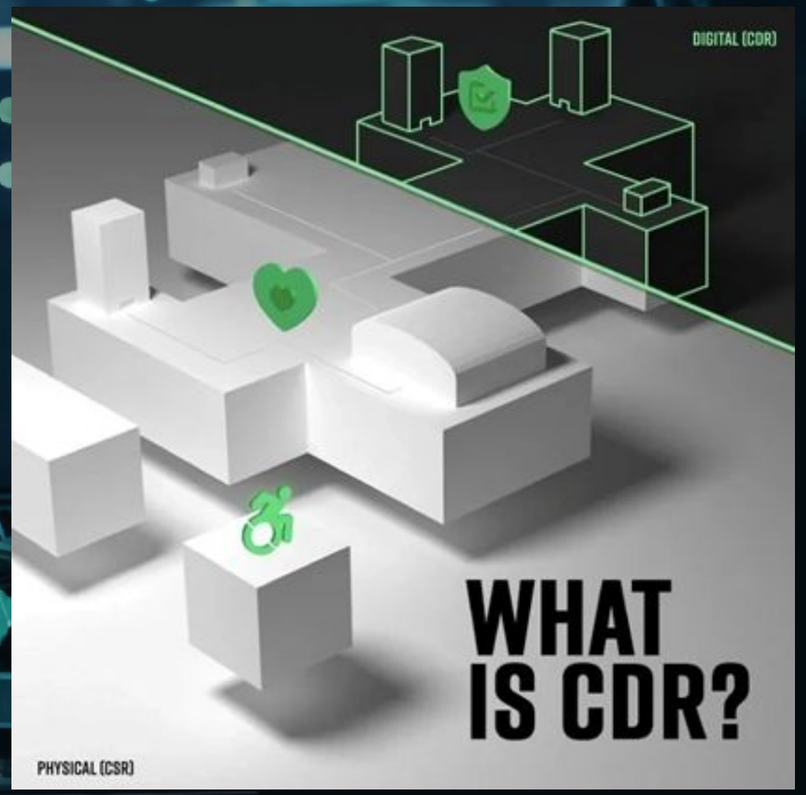
CSR Platform (2020), Corporate Digital Responsibility -1. L'enjeu des données, France Stratégie, July.

Companies nowadays are particularly required to take responsibility for their digital actions and to communicate what place they want to occupy in the digital society.

Under the term Corporate Digital Responsibility, companies worldwide are committing to **greater responsibility for sustainability, data protection and consumer protection**.

SOURCE: https://ihk-kompetenz.plus/wissenswertes/corporate-digital-responsibility-cdr-definition/

Module 3: CDR vs. CSR



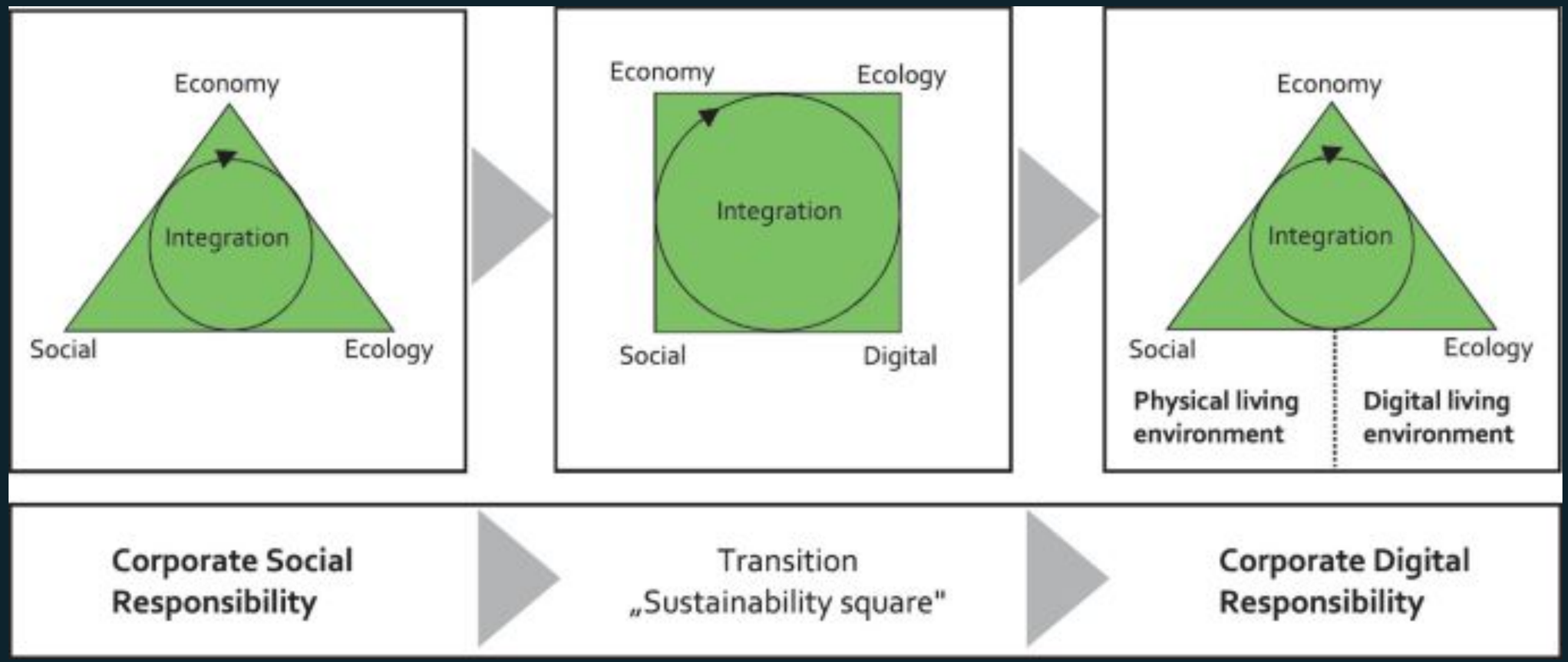
In essence, the main difference between **CDR and CSR** is given by the role that technology plays in the respective concept.

While CSR has a relatively broad goal towards society that affords technology only subordinate importance, CDR revolves around technology and its implications for corporations and society. Besides these main differences between CDR and CSR, there is no clear cut between the two concepts, so that thematic overlaps are possible (Lobschat et al. 2021).

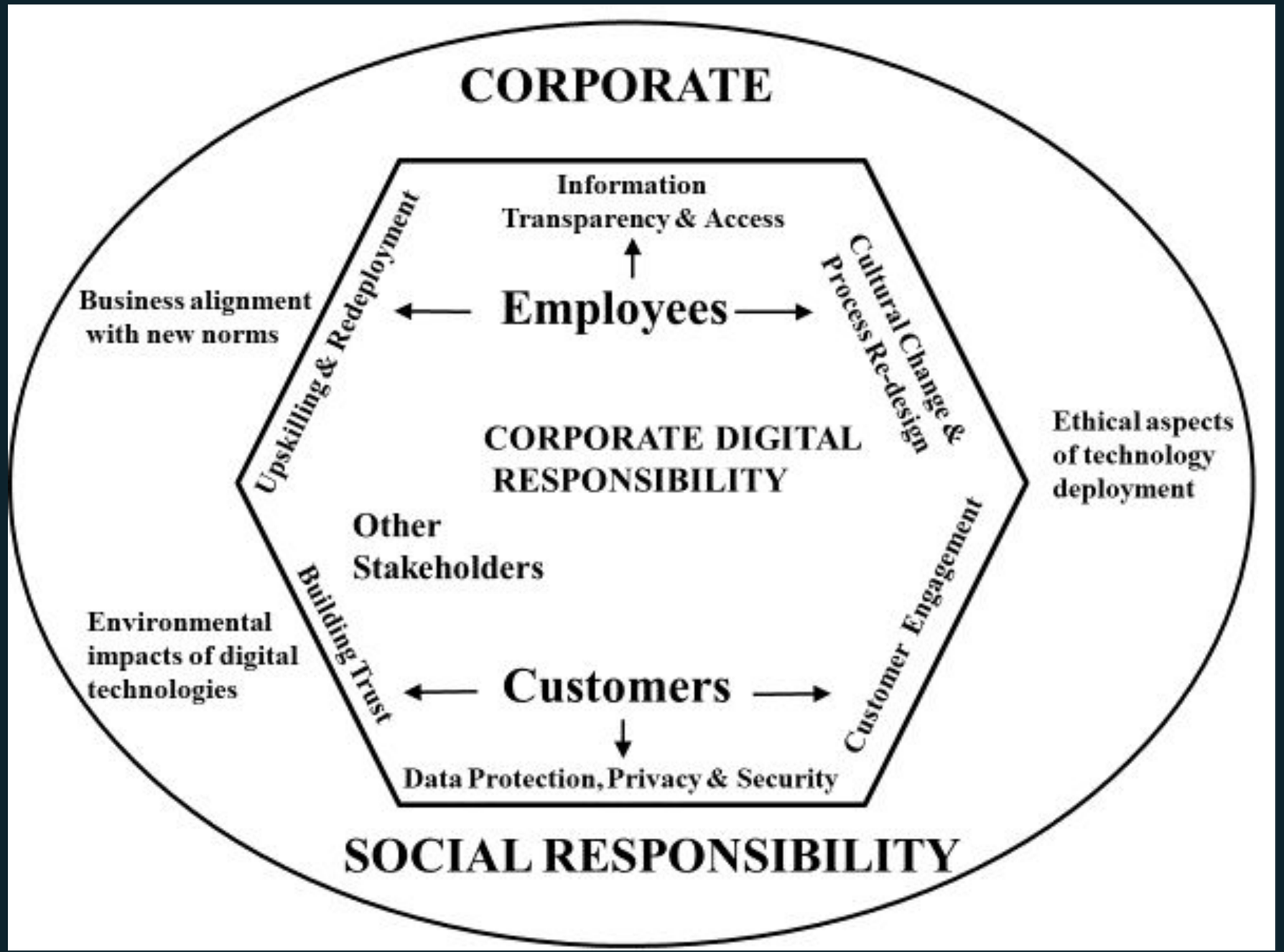
- CDR is increasingly seen as a subset of Corporate Social Responsibility (CSR).

Lobschat L, Mueller B, Eggers F et al (2021) Corporate digital responsibility. J Bus Res 122:875–888

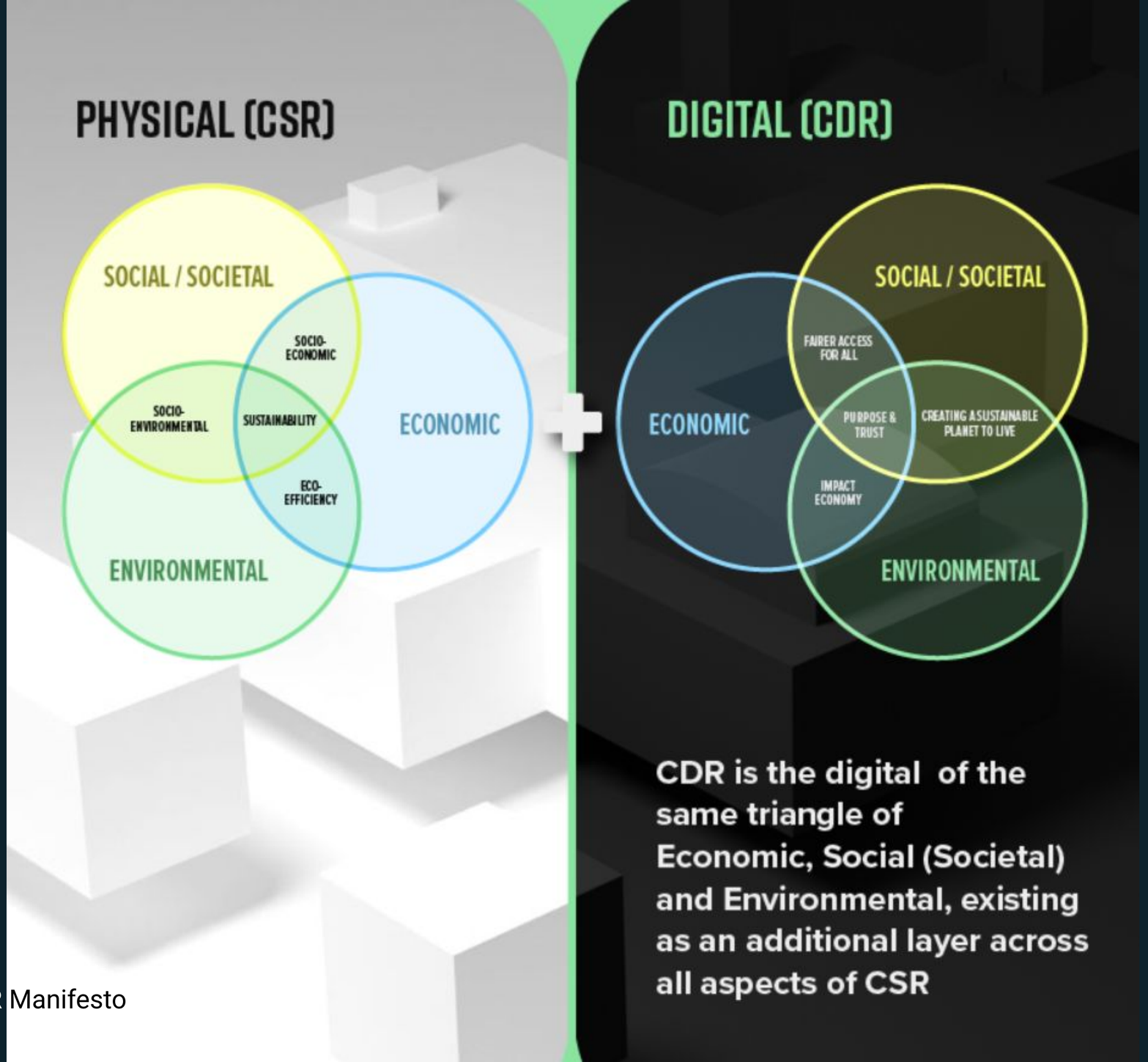
CSR vs. CDR



Pelters, E. (2021). Corporate Digital Responsibility—Understanding and Applying. In: Herberger, T.A., Dötsch, J.J. (eds) Digitalization, Digital Transformation and Sustainability in the Global Economy. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-030-77340-3_6



SOURCE: Wynn, M., & Jones, P. (2023). Corporate responsibility in the digital era. Information, 14(6), 324.



SOURCE: CDR Infographic, CDR Manifesto

Corporate Digital Responsibility Examples

Implementation

The CDR manager is responsible for creating and implementing a CDR policy (a company guideline to promote corporate digital responsibility). Do you want to make digitalization in your company sustainable and responsible?

Data protection

"What happens to my data?" This question is becoming increasingly important for customers. Not only do applicable regulations such as the General Data Protection Regulation require companies to protect data, but trusting data handling is also important for their customer relationships. The most important procedures are the ones covering how you can collect and evaluate data securely.

Artificial intelligence

A relatively new development that has been gaining momentum since the appearance of Chat GPT and Co.: Artificial intelligence (AI). AI is changing companies. Accompanying this transformation safely and responsibly in the spirit of corporate digital responsibility is the job of an AI manager.

https://ihk-kompetenz.plus/wissenswertes/corporate-digital-responsibility-cdr-definition/

Real-life CDR implementation examples

Zalando publishes first Corporate Digital Responsibility Report in partnership with the German government



The CDR code has a section that focuses on making sure data is used in a way that customers expect and are aware of, how is Zalando doing this?

Internet users sometimes fear that they are being tracked and their data is being used, but they don't know how and what for exactly. For Zalando it is very important to offer an experience of trust. We process customer data in accordance with all applicable data protection laws on national and EU level.

https://corporate.zalando.com/en/company/zalando-publishes-first-corporate-digital-responsibility-report-partnership-german

Real-life examples

It is essential for organizations to be aware that digitalization can lead to negative impacts if misused, including harm to customers and unwanted societal consequences.

For example, **Goldman Sachs** faced public backlash after being investigated for discrimination arising from their algorithm which was providing women with lower lines of credit than men.

Further, incidences such as the ‘Robot debt’ debacle by the **Australian government** resulted in lower socio-economic residents being forced to repay erroneous welfare repayments, causing bankruptcy, psychological stress and even reports of suicide as a result of the algorithmic anomalies that underpinned the repayment demands.



Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*, *53*(2), 101056.

Real-life CDR implementation examples

Social This involves an organization's relationship with people and society. Topics include data privacy protection and aspects related to digital diversity and inclusion, such as bridging the digital divide between geographies, social classes, and age demographics.

Example: When online insurance applications are denied with Swiss insurance company **Die Mobiliar**, the affected individual has the right to speak to an employee to understand the reasoning behind the decision.

Economic This concerns the responsible management of the economic impacts of digital technologies. Topics include replacement of existing jobs by robots and the creation of the new digital-era jobs that are enriching and fulfilling. Questions include how firms share the economic benefits of digitalization with society at large.

Example: **Weleda, a Swiss holistic natural cosmetics** and anthroposophical medicines company, has said that any use of robotic process automation will not result in staff reductions or job losses. Affected employees would be upskilled and transferred into other functions.

Real-life CDR implementation examples

Technological This is linked to the responsible creation of the technologies themselves. For example, biased or inaccurate AI decision-making algorithms can lead to unfair or discriminatory practices. Other technologies such as so-called deepfake videos can also have harmful effects on society.

Example: Employees of German telecommunications company Deutsche Telekom are encouraged to follow corporate ethical guidelines related to AI engineering and usage.

Environmental This concerns the link between digital technologies and the physical environment, including issues of responsible recycling or the disposal of old computer equipment. Another consideration is limiting power consumption for firm activities.

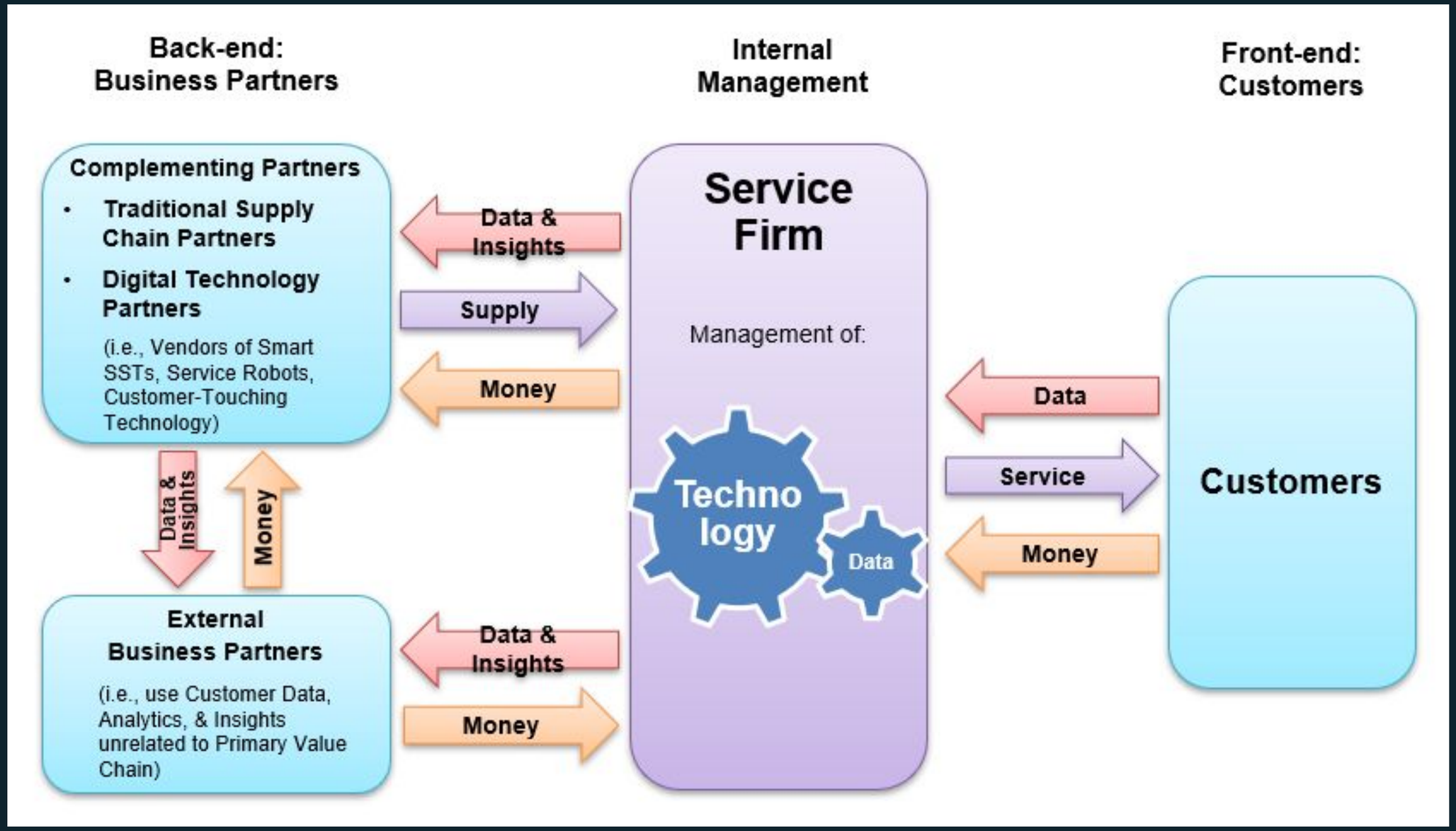
Example: By committing to net zero Scope 1 and 2 emissions by 2025, financial services group UBS leverages connected sensors in its physical infrastructure to reduce their energy consumption and measure carbon emissions more effectively.

https://swiss-digital-initiative.org/wp-content/uploads/2022/11/SDI_IMD-CDR-Report_2022.pdf

Table 2. Activities and Potential Concerns in the Example of Wearable Personal Health Devices

	Creation	Operation and Decision-making	Inspection and Impact Assessment	Refinement
Activities	• Designing the wearable device (e.g., wristband) and deciding which sensors to use • Building software and deciding which sensors of the host device (e.g., smartphone) to use • Deciding which existing personal health data on the host device to use • Building a data and prediction model for data analysis • Capturing of data from the user • Inferring health data from other sources (e.g., social media) • Deciding on storage location of data and data ownership	• Ongoing and continued collection of user data • Analyzing user preferences and routines (e.g., exercise regime) • Compiling data into comprehensive user profile • Matching of user characteristics to other users based on selected variables • Probabilistically extrapolating unobservable data (e.g., future development of health) and future events (e.g., health incidents) • Making recommendations to the user on health-related issues	• Analyzing users' progress vis-à-vis their goals / intentions • Assessing health advice • Analyzing customer complaints (e.g., on social media) • Inspecting algorithms and analytics to understand decision models • Benchmarking with technological progress and legislation • Assessing wider network of stakeholders (e.g., third-parties interested in data) • Analyzing of unintended effects (and ability to discover these)	• Refining analytics / algorithms (even re-training if need be) • Refining decision rules: deciding when what recommendation is given to users • Implementing additional safety / security measures for users' data • Deciding which new data need to be collected and which data need to be discontinued / deleted • Improving algorithms and predictive models
Potential Concerns	• Users are not given fair chance at informed consent to collect data • Privacy concerns not considered • Data accuracy not considered • Over-collection of unrelated data (e.g., by using additional sensors in host device) • "Coerced" data provision by customer to gain customization, convenience, promotions • Safekeeping of data (data breach; hacking; identity theft)	• Lack of transparency of data collection (e.g., which sensors) and analytics (e.g., why specific recommendations were made) • Lack of transparency and control to potential and current users about how data are used • Algorithmic decisions / recommendation lack validity (accurately reflecting underlying truth) • "Hidden agenda" / unrelated variables infused into analytics	• Lack of transparency in algorithms leaves systemic biases undetected • Security concerns due to outdated technology or algorithms (e.g., data not stored securely) • Lack of contingency governance (e.g., who owns data in case company is being bought) • Decisions / recommendations based on outdated medical advice • Unintended discrimination, biases (e.g., gender, ethnicity)	• Right to "forget" not followed; data are kept without clear retirement dates • Technology embodies sustained biases, discrimination, etc. • Technology cannot be retired because data has become systemic (e.g., health devices required for insurance coverage) • Data ownership changes without clear information to users (e.g., data acquisition)

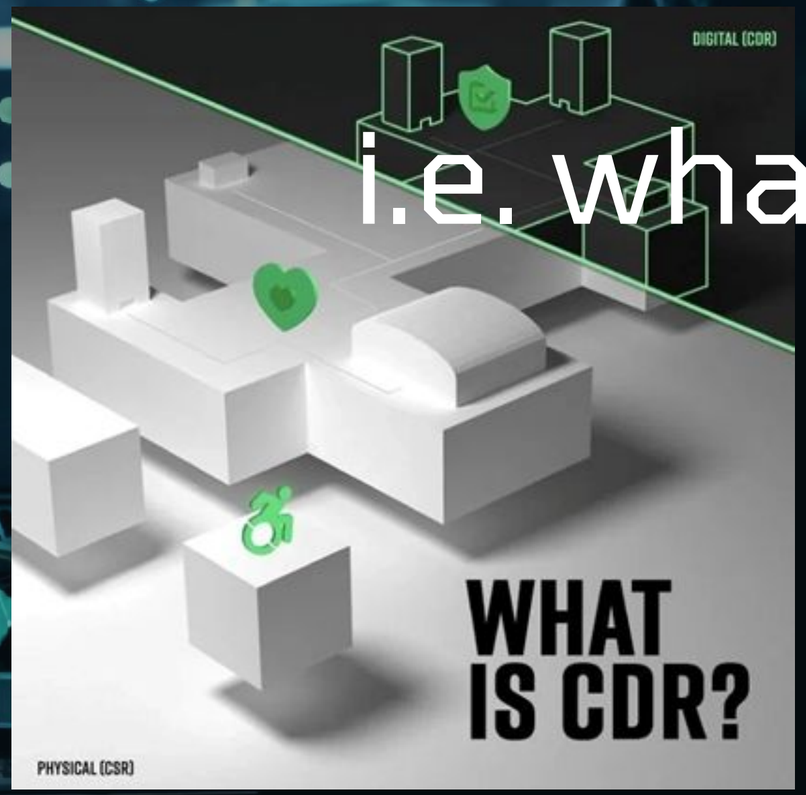
Lobschat, Lara & Mueller, Benjamin & Eggers, Felix & Brandimarte, Laura & Diefenbach, Sarah & Kroschke, Mirja & Wirtz, Jochen. (2021). Corporate Digital Responsibility. Journal of Business Research. 122. 875-888. 10.1016/j.jbusres.2019.10.006.



Source: Wirtz, Jochen, Werner Kunz, Nicole Hartley, and James Tarbit (2022), “Corporate Digital Responsibility in Service Firms and their Ecosystems”, Journal of Service Research, published online first, https://doi.org/10.1177/10946705221130467.

CDR vs. CSR: the scholarly literature

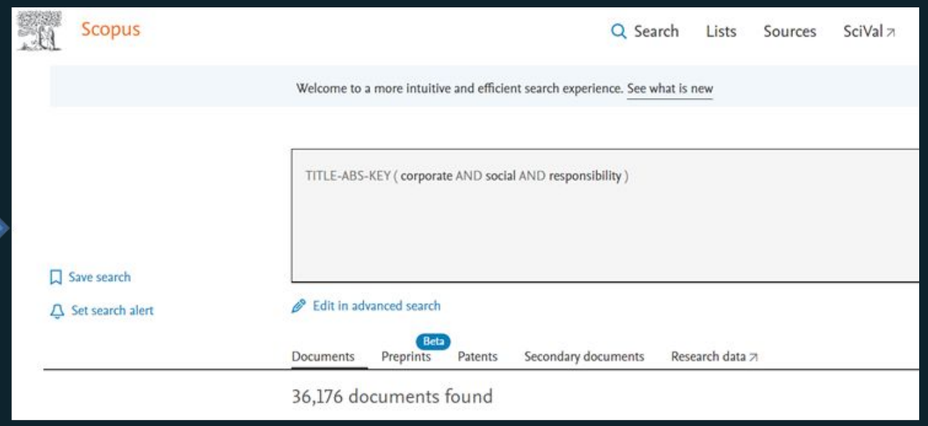
i.e. what is thus far found



CSR (Corporate Social Responsibility)

Scopus

36.176 papers



Clarivate Web of Science™

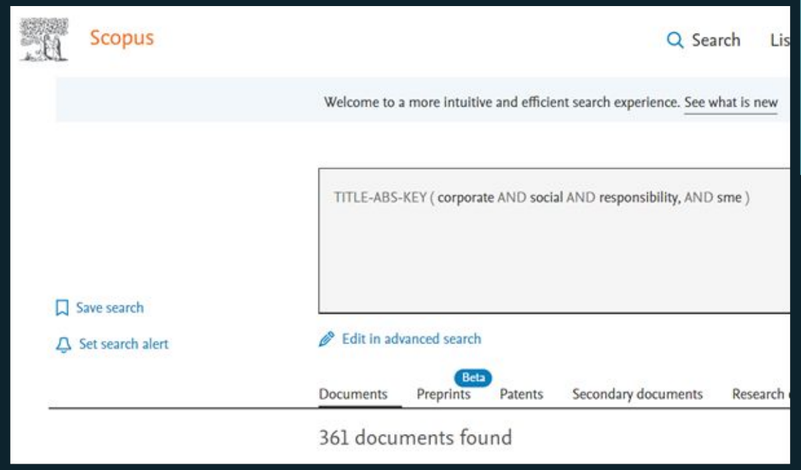
43.288 papers



CSR in SMEs

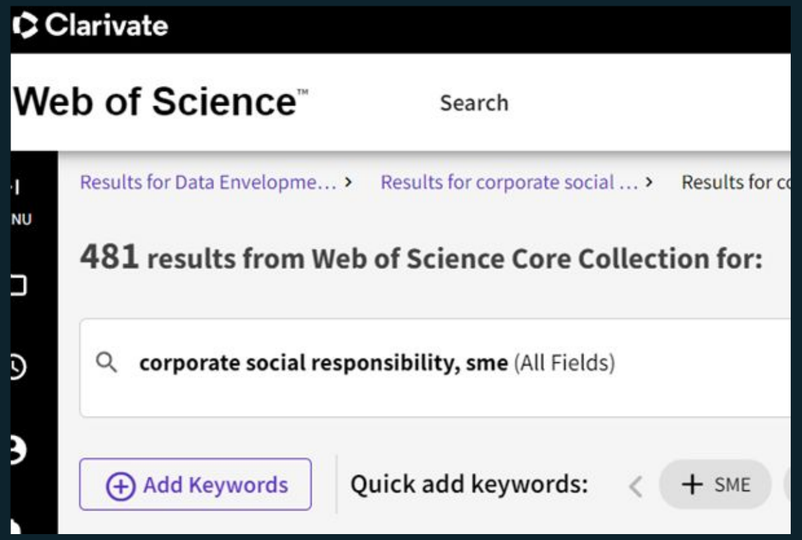
Scopus

361 papers



Clarivate Web of Science™

481 papers



CSR in SMEs

- Scholarly discourses on CSR in SMEs are rapidly growing in volume in recent years; yet knowledge in this field of inquiry **is fragmented** across scientific journals, sectors, disciplines, and cultural and geographical contexts.

Oduro, S., Bruno, L., & Maccario, G. (2021). Corporate social responsibility (CSR) in SMEs: what we know, what we don't know, and what we should know. Journal of Small Business & Entrepreneurship, 36(2), 207–238. https://doi.org/10.1080/08276331.2021.1951064

Findings show that:

- CSR research in SMEs is **rapidly growing** with over 136 peer-reviewed articles published in the last decade, appears significantly in top tier journals, and empirically based;
- **quantitative surveys and panel study designs** dominate the field over other methodological designs such as qualitative case studies and conceptual models;
- **firm performance** (financial, non-financial, and both) is the topic/theme frequently investigated, followed by drivers/antecedents, perception/knowledge awareness, and CSR green practice and ethics, in that order
- studies are preponderately **Europe-centric, multi-sectoral, and atheoretical**;
- there is a limited adoption and development of novel theories and linkage between the conceptual and empirical studies.

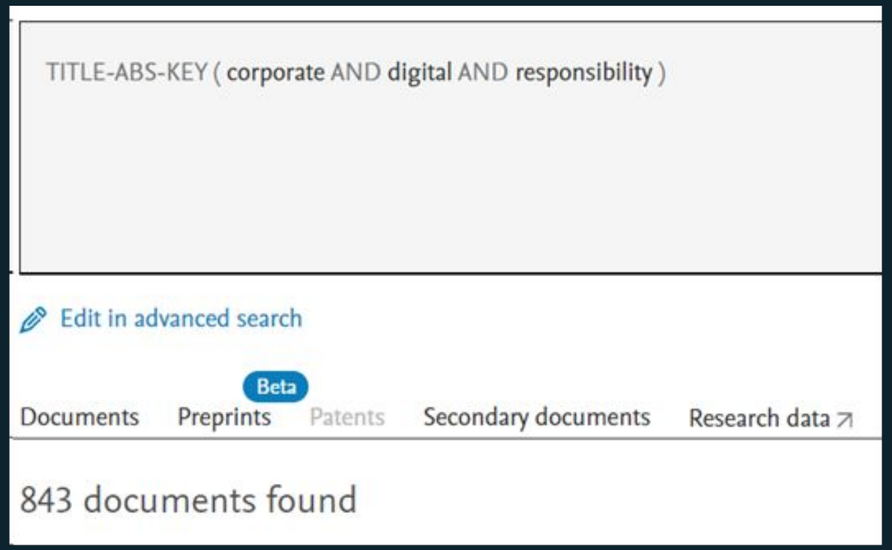
CSR in SMEs - wordcloud



CDR

Scopus

843 papers



Clarivate Web of Science™

1042 papers



Scopus

TITLE-ABS-KEY (corporate AND digital AND responsibility)

Edit in advanced search

Documents | Preprints (Beta) | Patents | Secondary documents | Research data

843 documents found

Country/territory

United States	114
China	110
United Kingdom	95
Germany	72
Italy	48

Show all

Scopus

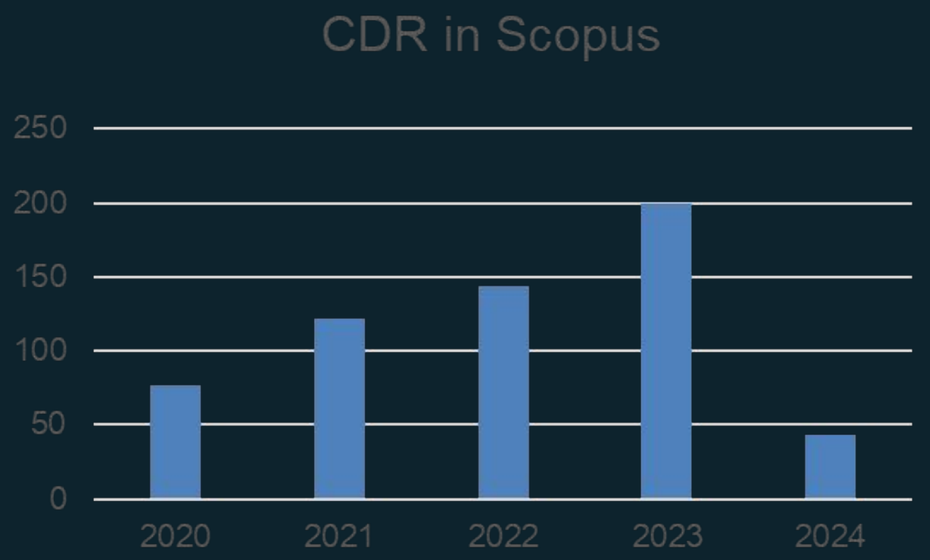
TITLE-ABS-KEY (corporate AND digital AND responsibility)

Edit in advanced search

Beta

Documents Preprints Patents Secondary documents Research data

843 documents found



Scopus

TITLE-ABS-KEY (corporate AND digital AND responsibility, AND entrepreneurship)

Edit in advanced search

Documents | Preprints (Beta) | Patents | Secondary documents | Research data

30 documents found

Subject area

- [ ] Business, Management and Accounting 18
- [ ] Economics, Econometrics and Finance 10
- [ ] Computer Science 7
- [ ] Engineering 7
- [ ] Social Sciences 7

Clarivate
Web of Science™

1,042 results from Web of Science Core Collection fo

corporate digital responsibility (All Fields)

Research Areas

Business Economics	464
Environmental Sciences Ecology	187
Science Technology Other Topics	156
Engineering	97
Communication	95

2024	31	2016	35	2007	3
2023	222	2015	32	2005	2
2022	183	2014	20	2001	1
2021	133	2013	18	2000	1
2020	132	2012	8	1999	1
2019	76	2011	4	1998	2
2018	87	2010	4	1996	1
2017	42	2009	3	1991	1

Clarivate
Web of Science™

72 results from Web of Science Core Collection for:

corporate digital responsibility, entrepreneurship (All Fields)

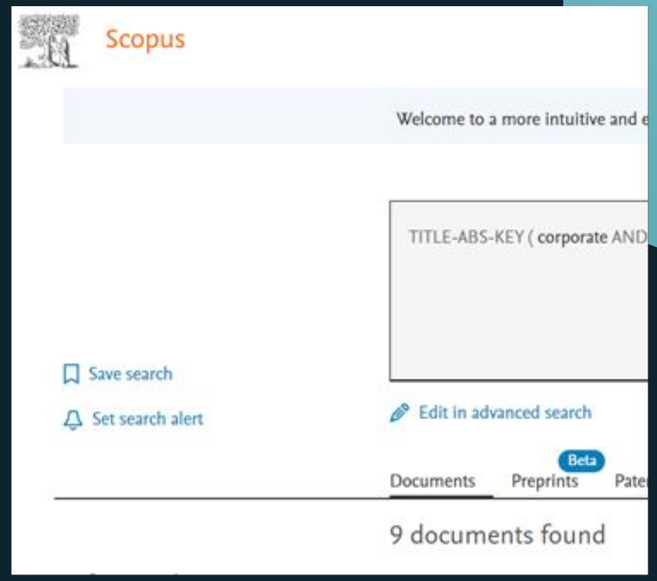
Research Areas

Business Economics	48
Environmental Sciences Ecology	15
Science Technology Other Topics	12
Development Studies	4
Public Administration	3

CDR + SMEs

Scopus

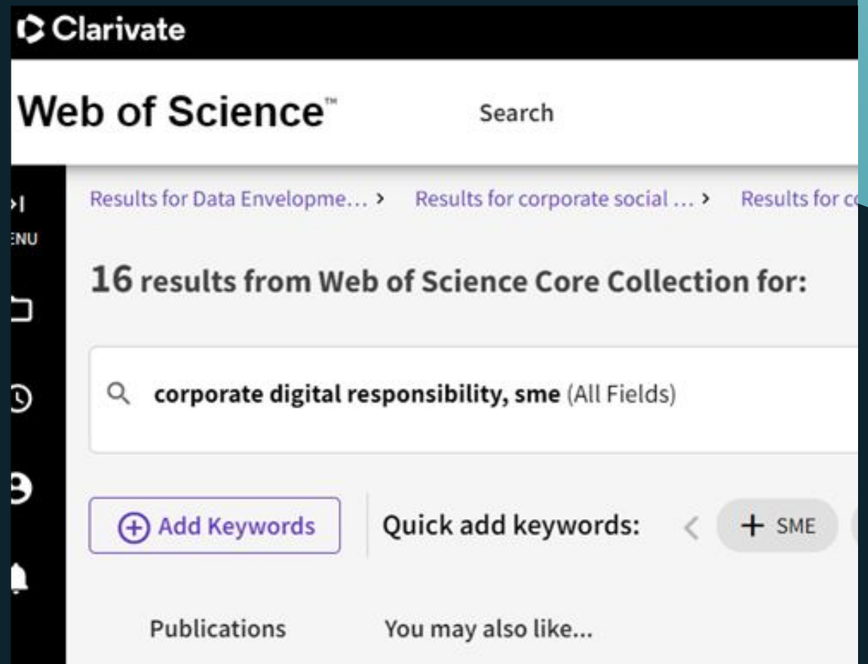
9 papers



Clarivate Web of Science™

16 papers

25 papers

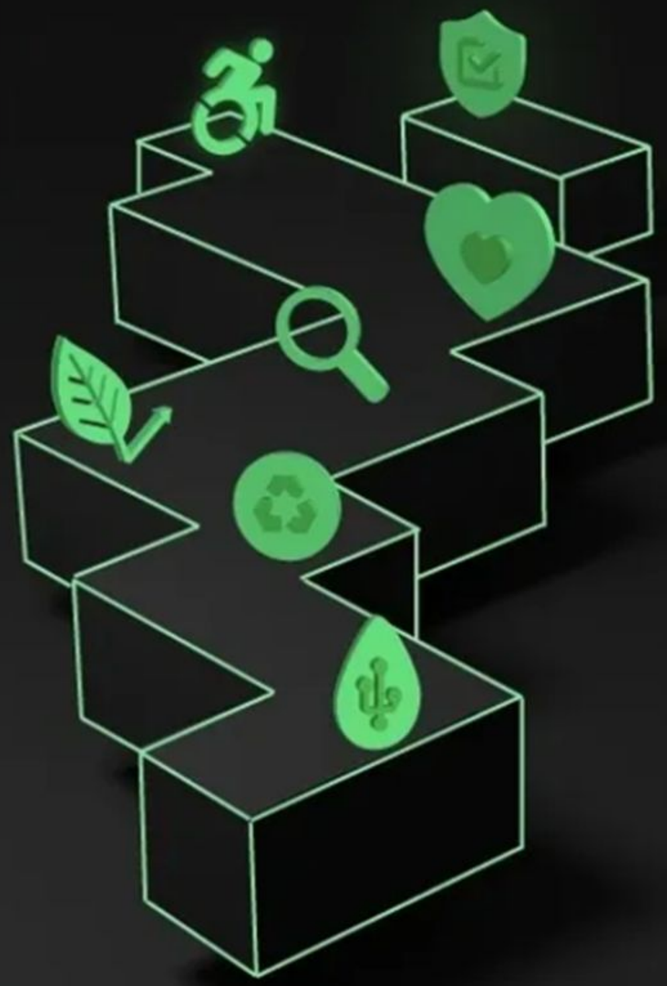



FRAMEWORK ANALYSIS
ENVIRONMENTAL
SECTOR
SME'S
BUSINESS
DIGITALIZATION
IMPROVE
PERFORMANCE
INNOVATION
REDUCTION
DEVELOPMENT
SIZED
PERCEIVED
ORGANIZATIONAL
ENTERPRISES
ETHICAL
SMES
STUDY
MEDIUM
KNOWLEDGE
TECHNOLOGY
OWNER
DIGITAL
CSR
COMPETITIVE
SUSTAINABLE
SMALL
ONE
COMPLEX
LABEL
CLIMATE
POSITIVE
ACTIONS
IMPACT
FOCUS
EFFECT
ROLE
CORPORATE
DRIVER
CASE
ALSO
WORK
MEDIA
SME
SOCIAL
EMERGING
ECONOMY
TWIN
THEORY
PACE
MORAL
CAN
STAKEHOLDER
CULTURE
RESPONSIBILITY
RESEARCH
SUSTAINABLE
ADVANTAGE
ACCEPTANCE
DIGITAL
INFORMATION
CONSTRUCTION
LEADERSHIP
REFLECTIVENESS
EMISSION
SIMULATION
KEYWORDS
PROCESS
SOCIAL
EMPLOYEES
RELATIONSHIP
EXPLAIN
OUTCOME
MANAGERS
BEHAVIOR
PRO
CORPORATE
ARTICLE
EVIDENCE
TECHNOLOGICAL
MODEL
RESPONSIBILITY
USING
AMONG
SUSTAINABILITY
CAPACITY
LACK
LABELING
FRAMEWORK
TEST
ABSORPTIVE
MEDIATION
ENGAGEMENT
TOWARD
IMPLICATIONS
RESOURCES
PRODUCT
FIRM IMPACT

The International CDR Manifesto

- During 2021, an international group of academics, corporate practitioners and published authors collaborated to aggregate their existing work into a single, international definition that pulls the best from each to build a set of principles to guide you on your Digital Responsibility journey.





CDR PRINCIPLES

1. PURPOSE AND TRUST
2. FAIR AND EQUITABLE ACCESS FOR ALL
3. PROMOTE SOCIETAL WELLBEING
4. CONSIDER ECONOMIC AND SOCIETAL IMPACT
5. ACCELERATE PROGRESS WITH IMPACT ECONOMY
6. CREATING A SUSTAINABLE PLANET TO LIVE
7. REDUCE TECH IMPACT ON CLIMATE AND ENVIRONMENT

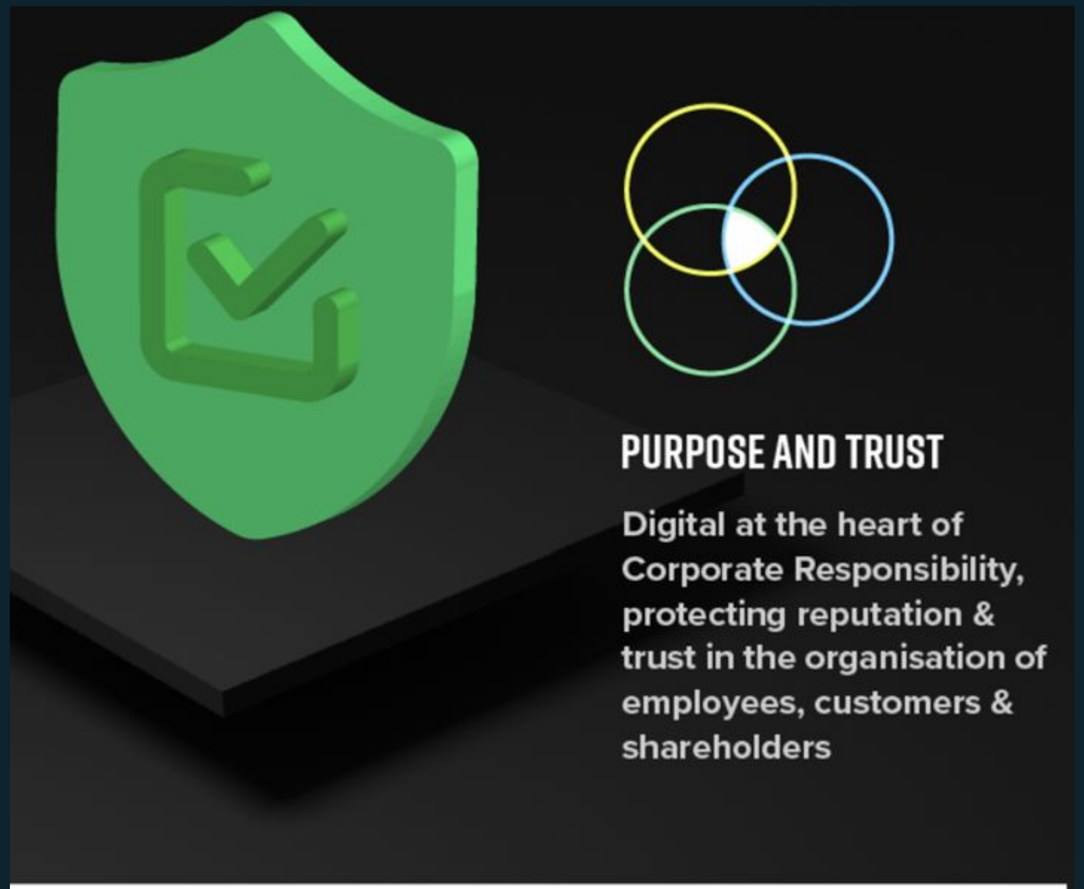
CDR

The Seven Core Principles of the International definition of Corporate Digital Responsibility

The CDR Manifesto

The International CDR Manifesto – the 7 core principles

1. Purpose and Trust



PURPOSE AND TRUST

Digital at the heart of Corporate Responsibility, protecting reputation & trust in the organisation of employees, customers & shareholders

HOW

- Publish digital responsibility code
- Publish corporate purpose
- Implement strong responsible digital governance
- Comply with, and advocate for stronger responsible regulation

2. Fair and Equitable Access for All



FAIR AND EQUITABLE ACCESS FOR ALL

Justice, Equity, Diversity and Inclusion drives a need to engage different stakeholders, like customers & employees, effectively in the use of digital technologies

HOW

- Accessible and inclusive products and services
- Promote justice, equity, diversity and inclusion
- Responsible employment rights

The International CDR Manifesto

- the 7 core principles

3. Promote Societal Wellbeing



PROMOTE SOCIETAL WELLBEING

Protect data and personal privacy, empower people to engage and develop skills, and protect from harm to improve reputation and trust

HOW

- Implement strong privacy
- Implement responsible data practices
- Promoting digital maturity skills
- Promoting digital wellbeing

4. Consider Economic and Societal Impact



CONSIDER ECONOMIC & SOCIETAL IMPACT

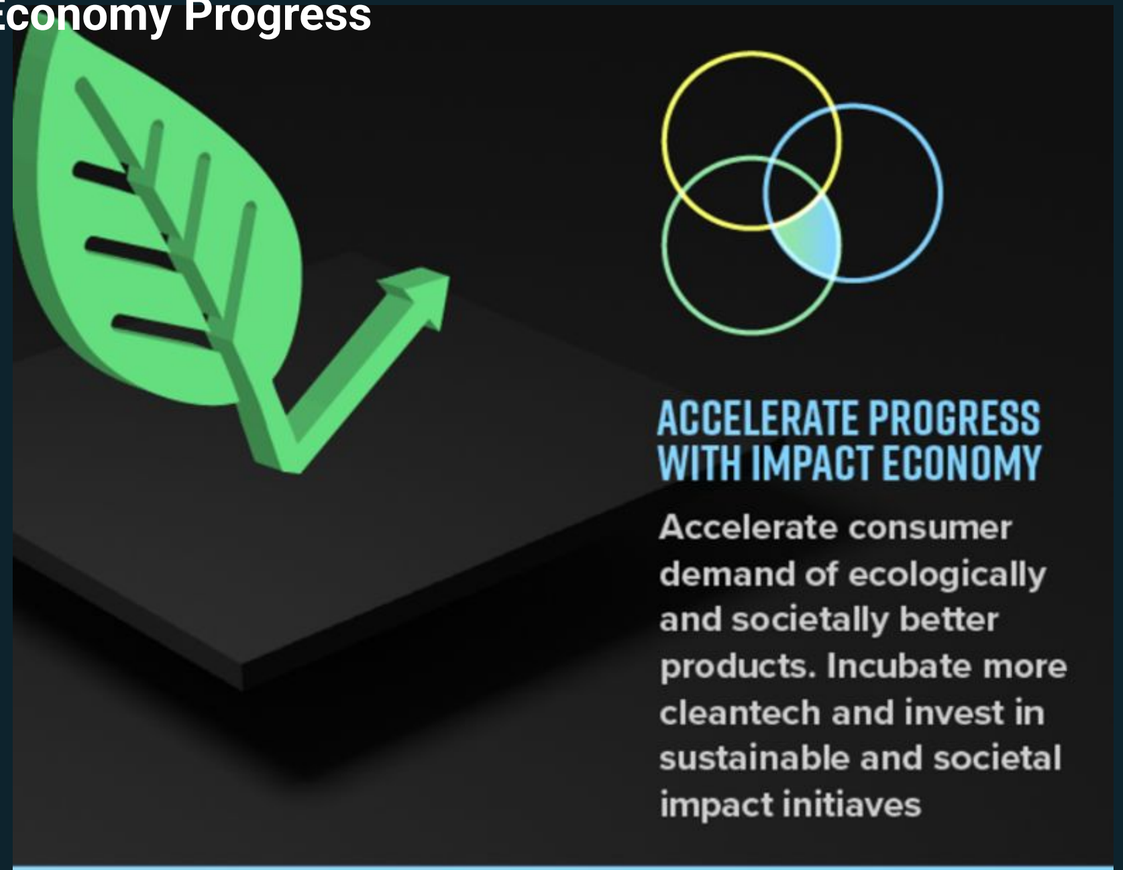
Reputational need to consider the economic and societal impact of decisions within the organisation

HOW

- Plan for sustainable and responsible automation
- Transparency with stakeholders with verifiable third party data
- Share digital economic benefits with relevant stakeholders

The International CDR Manifesto – the 7 core principles

5. Accelerate Impact Economy Progress



ACCELERATE PROGRESS WITH IMPACT ECONOMY

Accelerate consumer demand of ecologically and societally better products. Incubate more cleantech and invest in sustainable and societal impact initiaves

HOW

- Invest in sustainability, environmental and societal impact returns
- Accelerate & innovate sustainable consumer behaviours
- Use only verifiable carbon offset credits

6. Create a Sustainable Planet to Live



CREATING A SUSTAINABLE PLANET TO LIVE

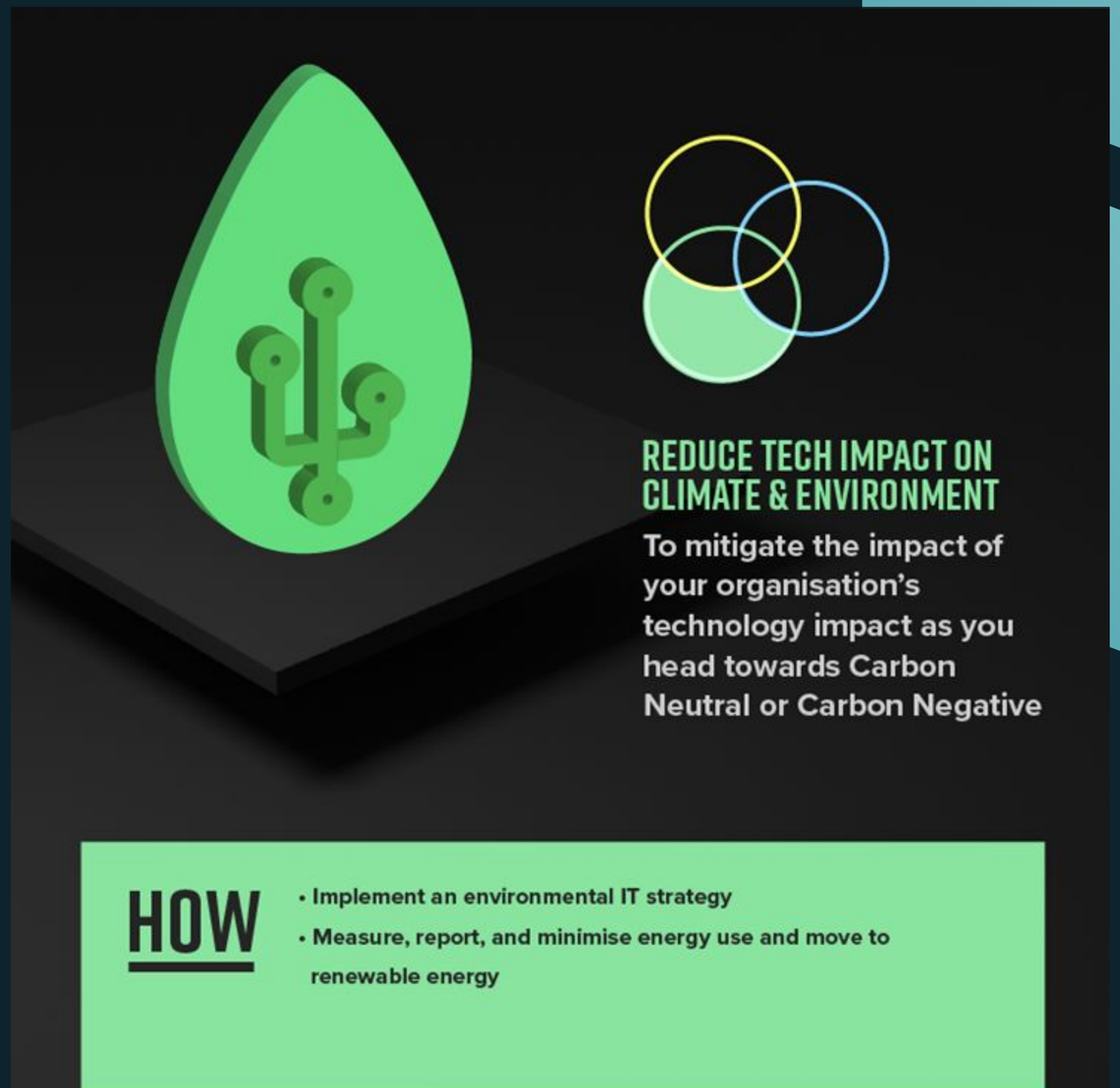
To move beyond Carbon Neutral or Carbon Negative, creating a more positive impact on the planet than your organisational scope using digital products & services

HOW

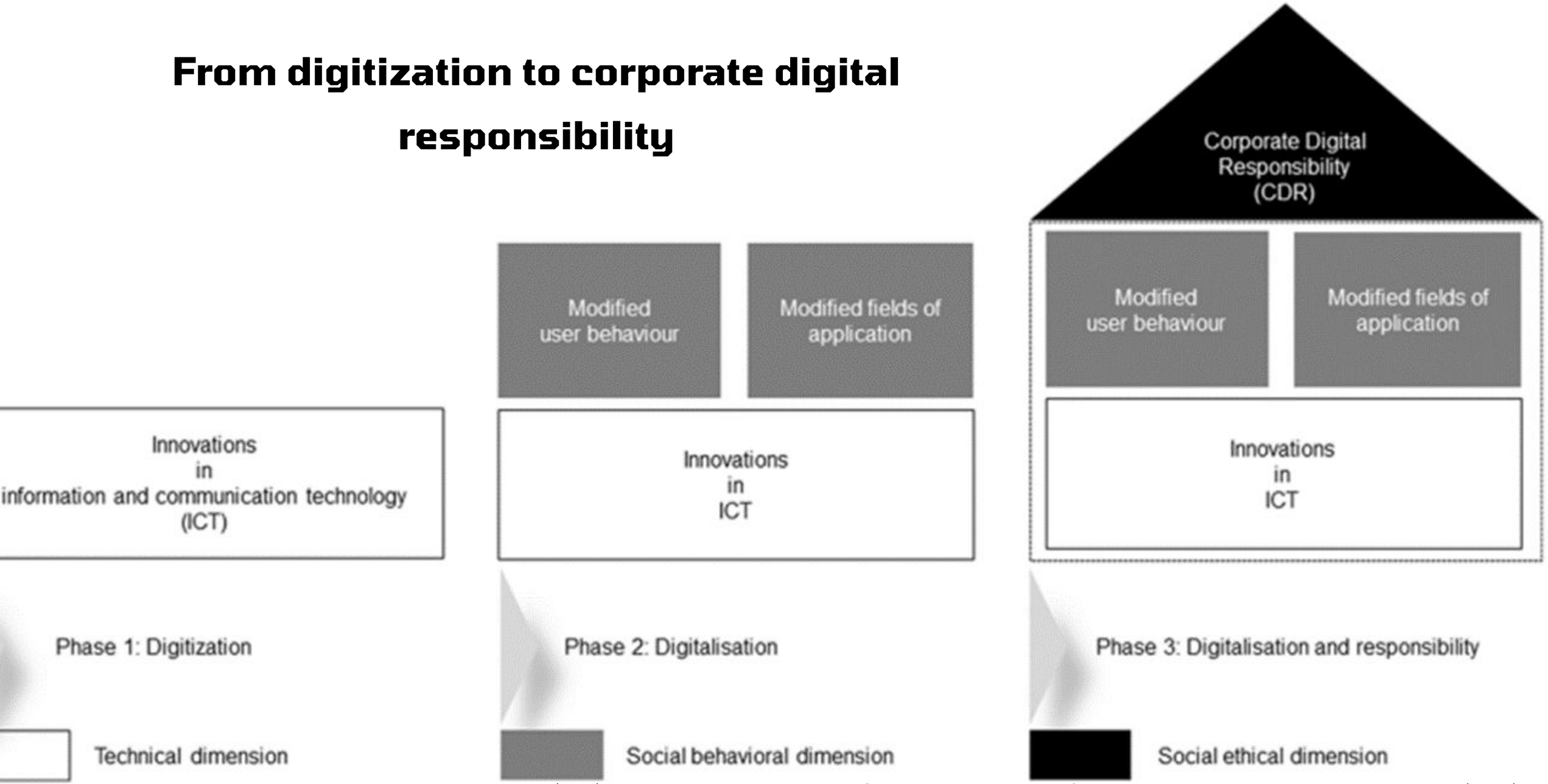
- Report business impact against certified third party assessments
- Innovate and positively impact beyond corporate boundary

The International CDR Manifesto - the 7 core principles

7. Reduce Tech's Impact on Climate and the Environment



From digitization to corporate digital responsibility



•SOURCE: Merbecks, U. Corporate digital responsibility (CDR) in Germany: background and first empirical evidence from DAX 30 companies in 2020. J Bus Econ (2023). https://doi.org/10.1007/s11573-023-01148-6

Module 4: ESG and its connection to CDR



As part of the initiative for sustainable development of the economy, three basic groups of goals have been determined that are being attempted to be achieved.

These are **environmental, social and governance** goals abbreviated ESG. ESG practice includes and cares about the way companies deal with climate change, the way they take care of their employees and other interested parties, but also about the company's corporate culture and its management. The ever-increasing global attention and focus on environmental, social, and governance (ESG) issues led to the development of the Corporate Sustainability Reporting Directive (CSRD) which will ensure reporting on all sustainability topics (environmental, social and governance factors).
ESG is a new way of thinking and therefore doing business in order to ensure a green and sustainable future.

ESG principles were coined back in 2004 at The UN Global Compact summit, as a commitment of twenty major financial companies to start integrating social, environmental and governance problems into investment analysis and decision-making (United Nations Global Compact, 2023).

The **environmental (E)** aspect includes environmental matters that may have a positive or negative influence on financial outcomes such as the risks of climate change, the need for waste reduction, and environmentally friendly products.

Social (S) includes social matters that may influence an entity positively or negatively such as the working environment and communication.

Governance (G) includes governance matters in terms of positive or negative impact on all interested parties such as corporate structure, transparency of information and rewarding system (Li et al., 2021).

United Nations Global Compact (2023). The Global Compact Leaders Summit 2004 – Final Report available at https://d306pr3pise04h.cloudfront.net/docs/news_events%2F8.1%2Fsummit_rep_fin.pdf

Li, T. T., Wang, K., Sueyoshi, T., & Wang, D. D. (2021). ESG: Research progress and future prospects. Sustainability, 13(21), 11663.

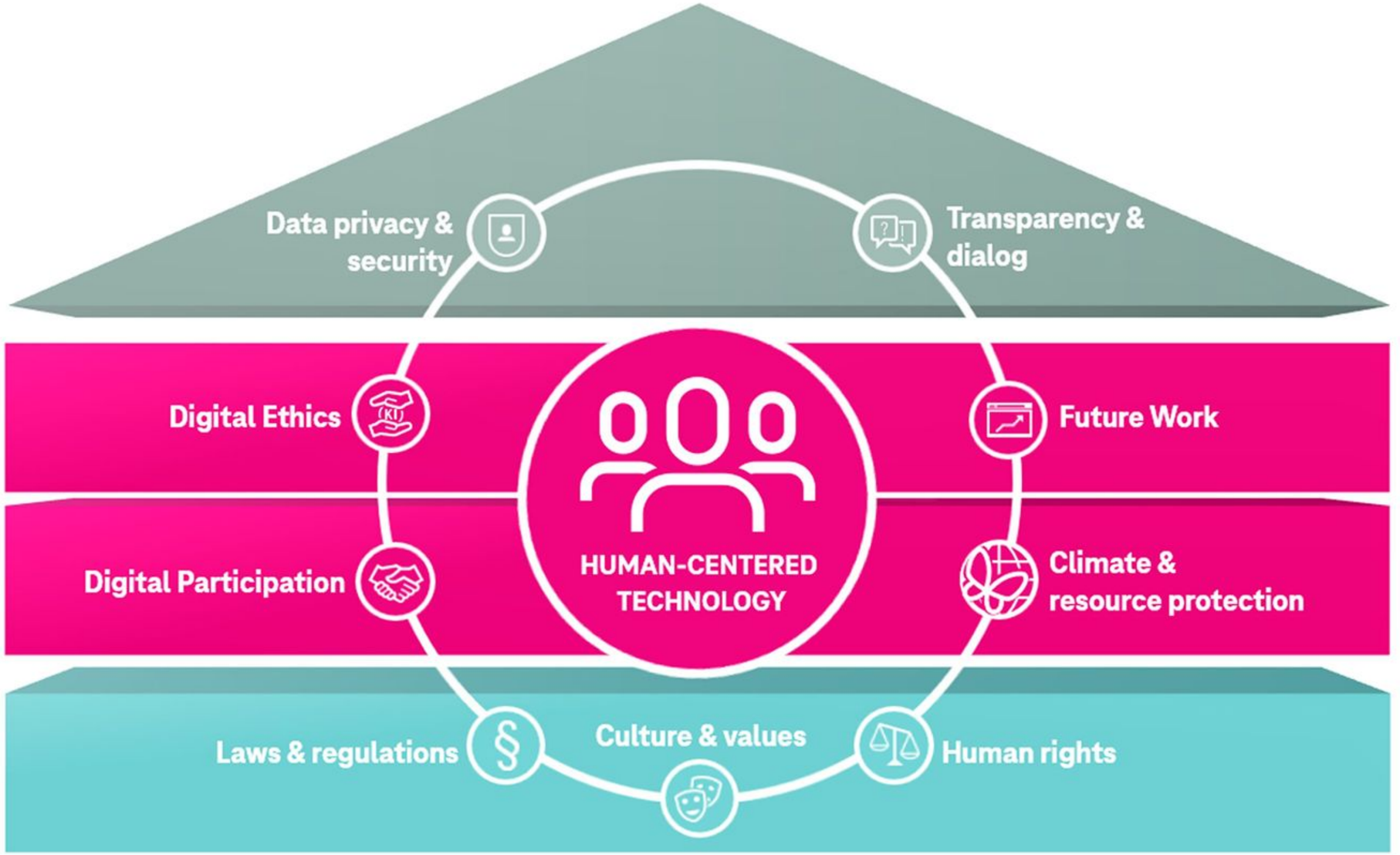
Corporate digital responsibility in the age of artificial intelligence

- **Key question:** How effectively are tech companies acknowledging their CDR?
- - there are increasing worries regarding AI labs being '*locked in an out-of-control race*' to develop and deploy increasingly powerful systems that no one – including their creators – can understand, predict or control

SOURCE: https://theacademic.com/artificial-intelligence-corporate-digital-responsibility/

Best practice – real-life examples

Deutsche Telekom - CDR



The House of Digital Responsibilityin Deutsche Telekom

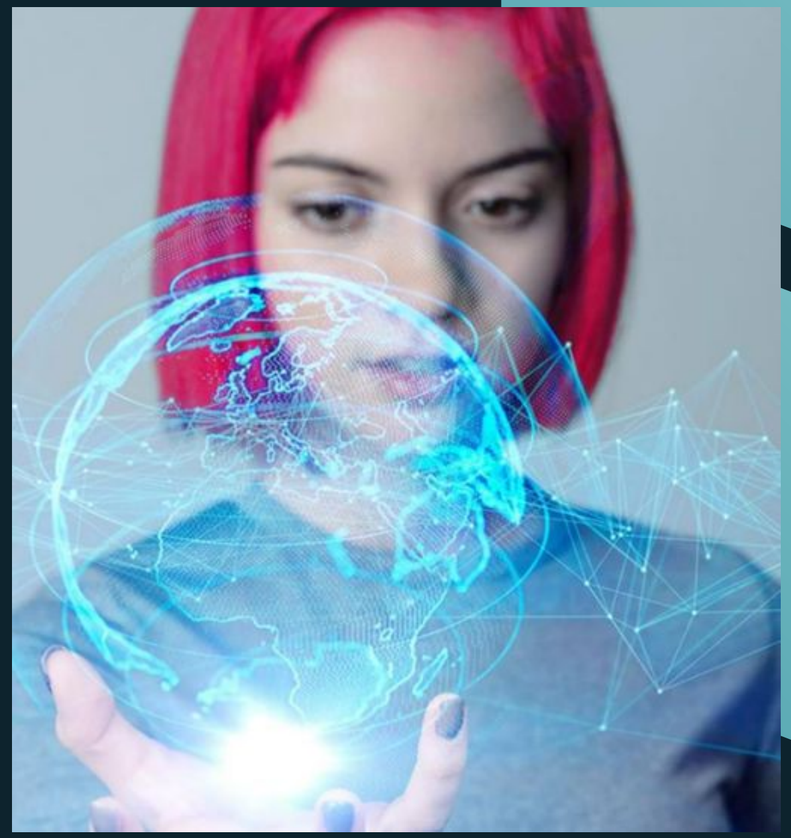
Our actions are based on our firm foundation and our principles. We focus on technologies for people and with people. We currently categorize these actions in four areas:

Digital Ethics – Ensuring sovereignty and supporting people are our focus. We design digital technologies responsibly.

Digital Participation – Deutsche Telekom wants everyone to take part in the digital society. Everyone should have access to the many opportunities afforded by digitalization.

Future Work –Digital responsibility at Deutsche Telekom means thinking about future work as part of its dynamic transformation process and ensuring that despite all the changes, people remain the focus of all decisions.

Climate and resource protection – Protecting the climate together and using resources responsibly – with and through digitalization.



Corporate Digital Responsibility @Deutsche Telekom

Our definition of digital responsibility

IBM

Google

Microsoft

Acting with digital responsibility

Corporate Digital Responsibility @Deutsche Telekom is the result of our CDR community. Contact persons and experts from all Board of Management departments have contributed and continue to contribute to the discussion. Based on our analysis of numerous documents, qualitative surveys, and detailed interviews, we have identified a large number of activities that help foster our digital responsibility. Further activities are already being planned in the various departments.

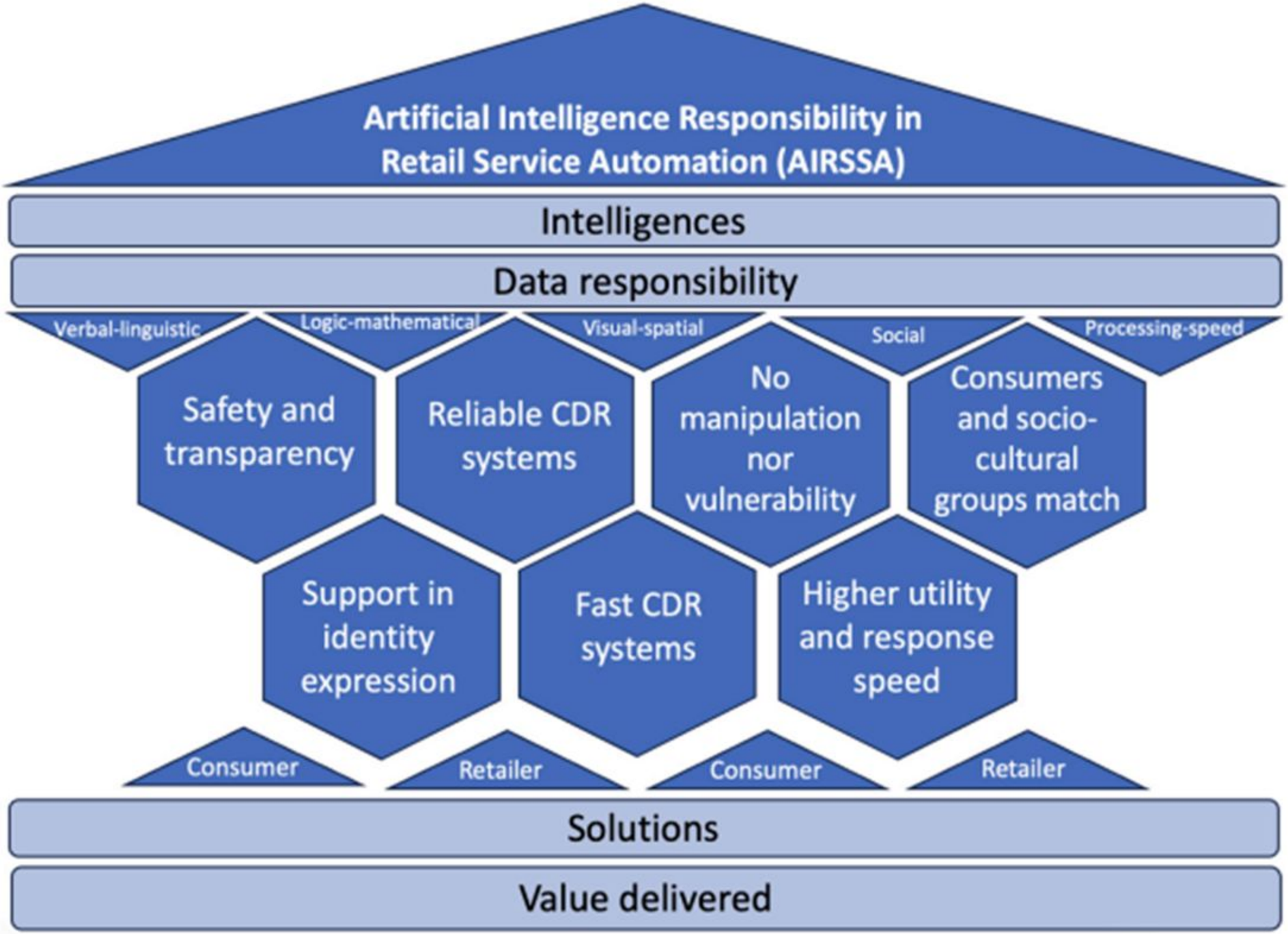
We see taking digital responsibility as a dynamic process and constant evolution. We will report on new and expanded activities and measures on a regular basis, because meeting our high standards for responsible digitalization is an ongoing challenge and duty – **one that we gladly face**.

Key elements for AI retail service automation.

Potential advantages for retailers	AI service automation tools	Potential privacy and ethical concerns for consumers
Adopting new ways for replying to consumers' complaints (automatization via social media and online chatbot)	Machine learning algorithms	Potential non-deterministic behavior of the AI (i.e., how will the AI evaluate the importance of the complaint of a certain consumer and consequently accommodate the response if the complaint is slightly different from the one used for training?), which results in a possible lack of validity
Improving personalization (including recommendations, notifications, and products)	Machine learning algorithms	Lack of data transparency in collection, storage, and usage
Capturing and merging data from different sources, including in-store proximity sensors, CCTV, online interactions, mobile apps	Facial recognition systems, iBeacon and RFID	Lack of data transparency in collection, storage, and usage, and a limited possibility to delete or remove past data
Developing new prediction models	Machine learning algorithms and big data analytics	Lack of data accuracy leading to systemic biases undetected

AI for intelligent retail service automation

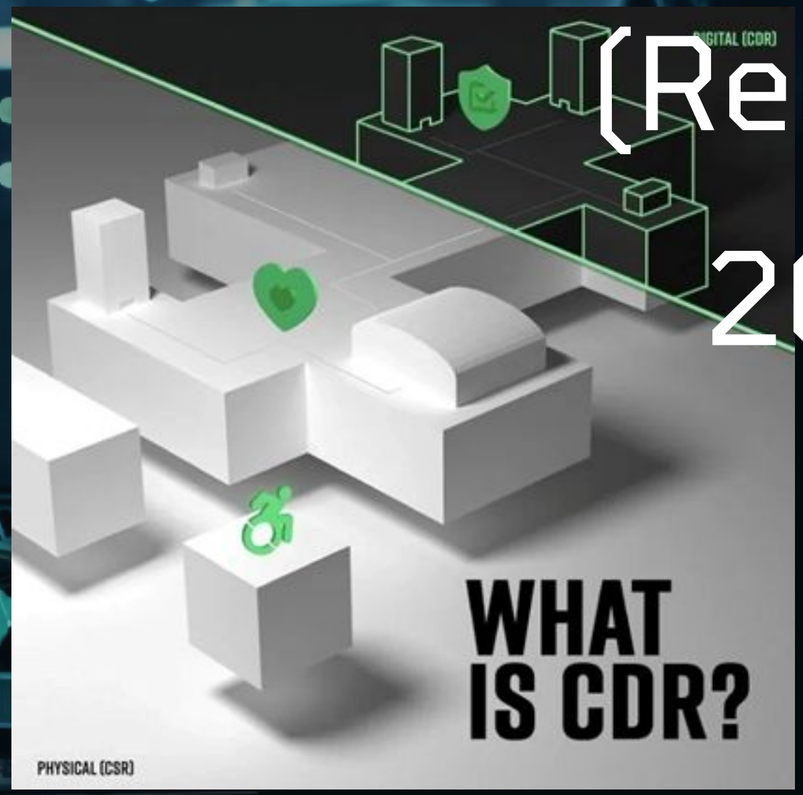
SOURCE: Scarpi, D., & Pantano, E. (2024). “With great power comes great responsibility”: Exploring the role of Corporate Digital Responsibility (CDR) for Artificial Intelligence Responsibility in Retail Service Automation (AIRRSA). Organizational Dynamics, 53(2), 101030.



Artificial Intelligence Responsibility in Retail Service Automation (AIRRSA), from consumers and retailers perspective.

Scarpi, D., & Pantano, E. (2024). “With great power comes great responsibility”: Exploring the role of Corporate Digital Responsibility (CDR) for Artificial Intelligence Responsibility in Retail Service Automation

Lecture 5: Digital Act – EU legislative related to CDR (Regulation (EU) 2022/2065)



The Digital Services Act - DSA

The DSA regulates **online intermediaries and platforms** such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.

Its main goal is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment.

As of 17 February 2024, the DSA rules apply to all platforms. Since the end of August 2023, these rules had already applied to designated platforms with more than 45 million users in the EU (10% of the EU's population), the so-called Very large online platforms (VLOPs) or Very large online search engines (VLOSEs).

What are the key goals of the Digital Services Act?



For citizens

- better protection of fundamental rights
- more control and choice
- stronger protection of children online
- less exposure to illegal content



For providers of digital services

- legal certainty
- a single set of rules across the EU
- easier to start-up and scale-up in Europe



For business users of digital services

- access to EU-wide markets through platforms
- level-playing field against providers of illegal content



For society at large

- greater democratic control and oversight over systemic platforms
- mitigation of systemic risks, such as manipulation or disinformation

SOURCE: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

What the new rules mean for users, businesses and platforms

Europe fit for the Digital Age: New online rules for businesses

The same rules will apply in the entire Union and will be the basis of a large domestic market for digital services to grow and prosper. Cross-border digital trade in the single market is expected to increase up to 2%

Small players will have legal certainty to develop services and protect users from illegal activities and they will be supported by standards, codes of conduct and guidelines

Small and micro-enterprises are exempted from the most costly obligations, but are free to apply the best practices, for their competitive advantage

Support to scale-up: exemptions for small enterprises are extended for 12 months after they scale past the turnover and personnel thresholds that qualify them as small companies

What the new rules mean for users, businesses and platforms (pt. 2)

Europe fit for the Digital Age: New online rules for businesses

- Removing disincentives for companies to take voluntary measures to protect their users from illegal content, goods or services
- Businesses will use new simple and effective mechanisms for flagging illegal content and goods that infringe their rights, including intellectual property rights, or compete on an unfair level
- Businesses may also become ‘trusted flaggers’ of illegal content or goods, with special priority procedures and tight cooperation with platforms
- Enhanced obligations for marketplaces to apply dissuasive measures, such as "know your business customer" policies, make reasonable efforts to perform random checks on products sold on their service, or adopt new technologies for product traceability

DSA: What’s in it for SMEs?

- Open up new opportunities for businesses, who will be able to innovate and compete against gatekeepers’ own services in equal terms.
- Consumers will be able to see which are the best options available and not just those that the gatekeepers want them to see.
- Business users will know what to expect when dealing with gatekeepers.
- Gatekeepers will know the clear obligations applicable to them.
- Clearly-defined procedural rules will ensure quick decisions that will translate in speedy advantages for both business users and consumers.

- It will allow businesses to have access to more information on how their products or services are performing on third party platforms
- No more unfair ranking of gatekeepers' own services and products compared to those offered by other businesses on the same platform
- Businesses will be able to more easily attract consumers who can no longer be locked in by gatekeeper platforms
- The new rules will make it easier for smaller businesses and new entrants to grow and expand, and compete with gatekeeper platforms.
- Increased competition can be expected to lead to greater innovation potential amongst smaller businesses as well as improved quality of service, with associated increases in consumer welfare.

The Digital Services Act package includes:

a. The Digital Services Act,

b. The Digital Markets Act.

The Digital Markets Act (DMA) affects “gatekeeper platforms” like Google, Amazon and Meta, and covers the need for user consent before processing personal data for targeted advertising. It is interesting that most of the companies that are affected by the Digital Markets Act and the Digital Services Act are based in the United States of America.

If you believe that the sanctions for GDPR violations are very strict (up to 4% of global annual turnover), you will be surprised with the sanctions for Digital Services Act violations (up to 6% of global annual turnover), and the sanctions for Digital Markets Act violations (up to 10% of global annual turnover, or up to 20% in case of repeat offence.)

The General Data Protection Regulation - GDPR

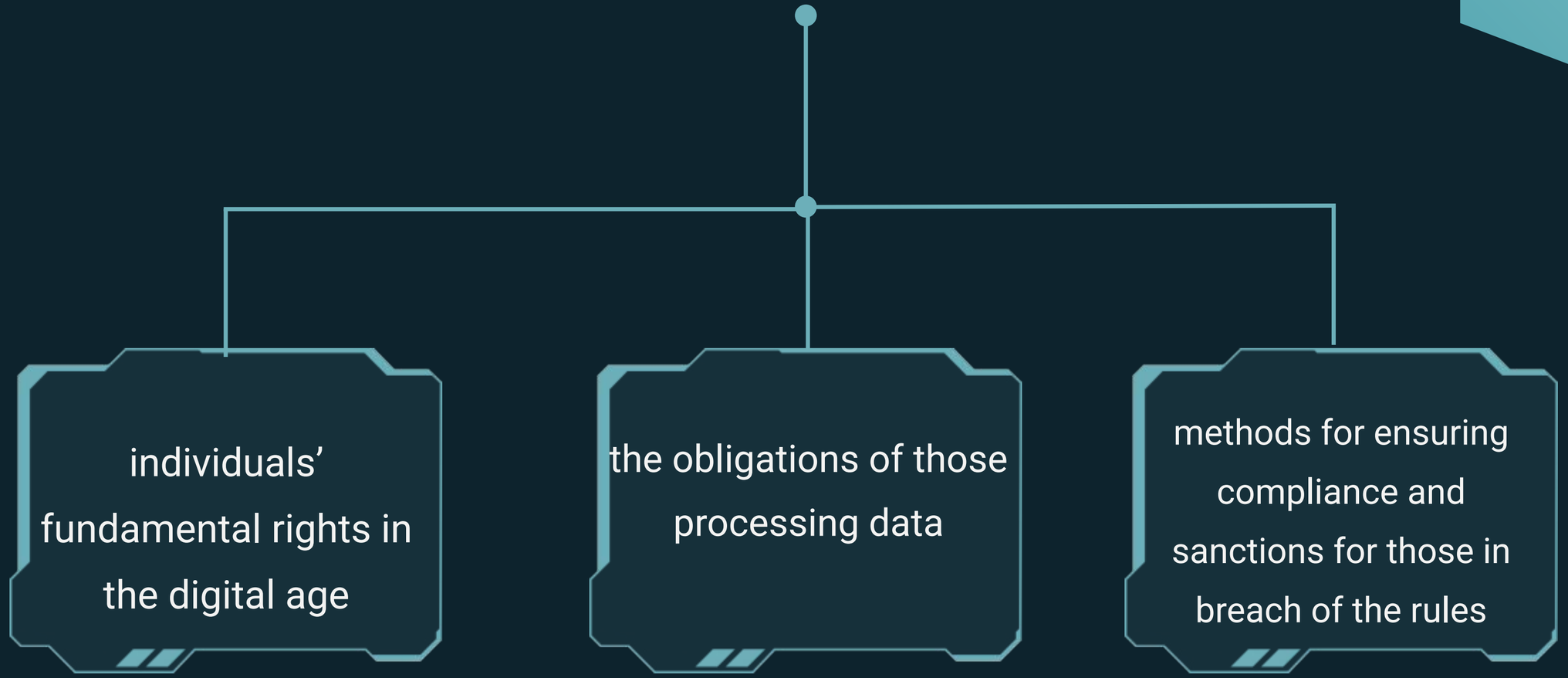
The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. The EU general data protection regulation (GDPR) governs how the personal data of individuals in the EU may be processed and transferred.

- entered into application **on 25 May 2018**

Why is everyone so familiar with the GDPR?

- The fines for violating the GDPR are very high. There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages.

The GDPR defines:



Module 6: Is CDR profitable?

Benefits & costs of CDR implementation



Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

CDR Calculus

Value of Good CDR = **Benefits** − **Opportunity Costs / Costs of Good CDR**

Benefits

Mitigation of CDR Risks

- Legal risks
- Reputational risks
- Regulatory risks

Brand Equity and Trust

"Warm glow" of being a good organization builds brand equity in:

- Consumer markets
- Labour markets
- Partner and supplier ecosystem

Opportunity Costs / Costs of Good CDR

Lost Incremental Revenues

- Contribution (sales, cross-and up-selling)
- Price discrimination
- Churn prediction and prevention
- Revenues from new services
- Revenues from data, insights, and services sold to 3rd parties

Reduced Customer Experience

- Customization and personalization
- Convenience, accessibility, and speed of service

Untranslated Potential Cost Savings

- Optimized and automated service processes
- Compliance to service processes and policies
- Risk assessment, and fraud detection and prevention
- Optimized supply chain

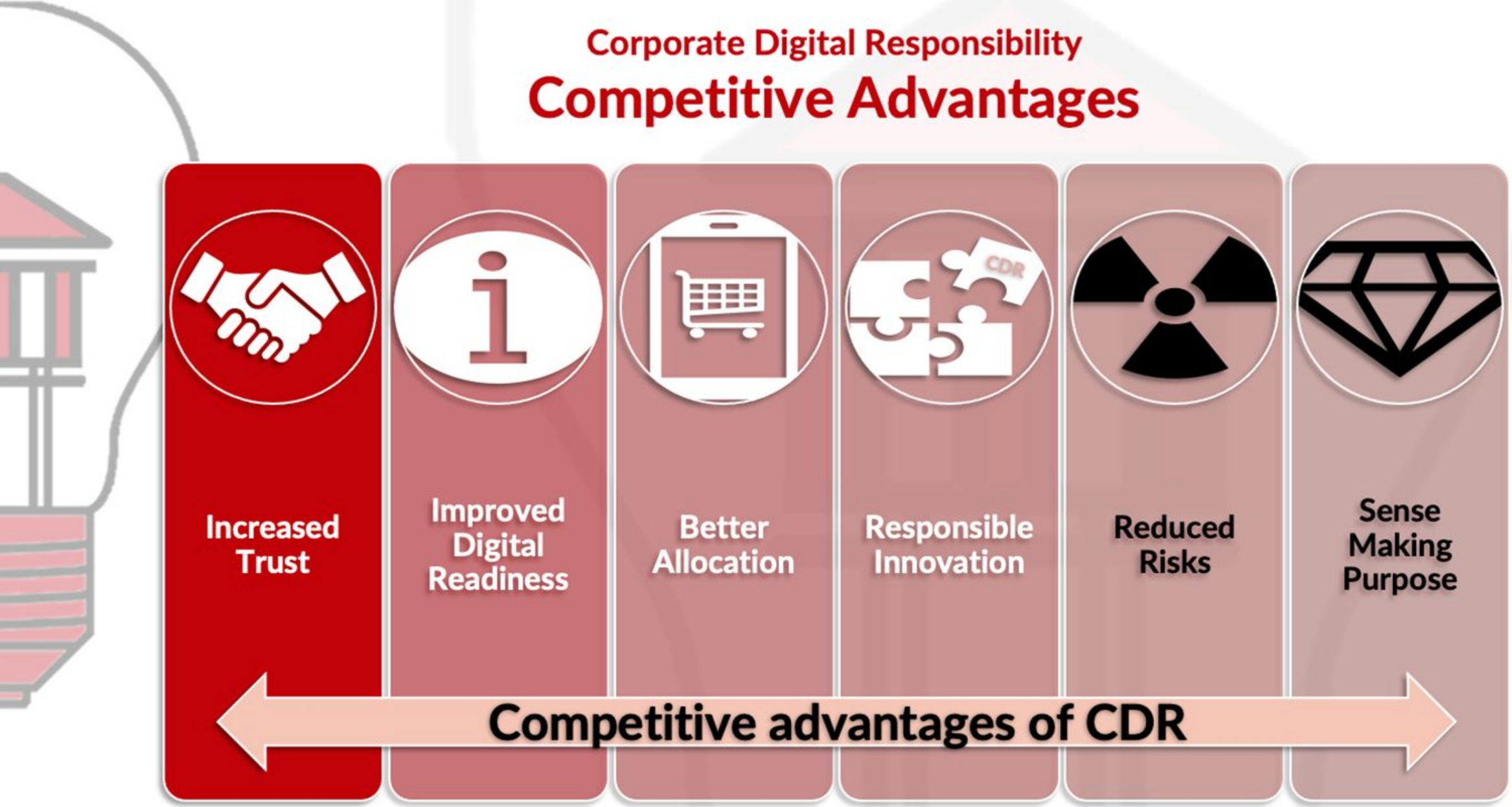
Cost of Robust CDR

- Cost of building a CDR culture and norms
- Cost of a CDR management structure, unit, and team (incl. staffing for CDR activities and CDR training and development)
- Cost of governance (internally and business partner ecosystem)

SOURCE: https://www.servsig.org/wordpress/2023/04/corporate-digital-responsibility-cdr-in-the-age-of-ai-why-do-service-firms-engage-in-poor-cdr-practices/

Corporate Digital Responsibility

Competitive Advantages

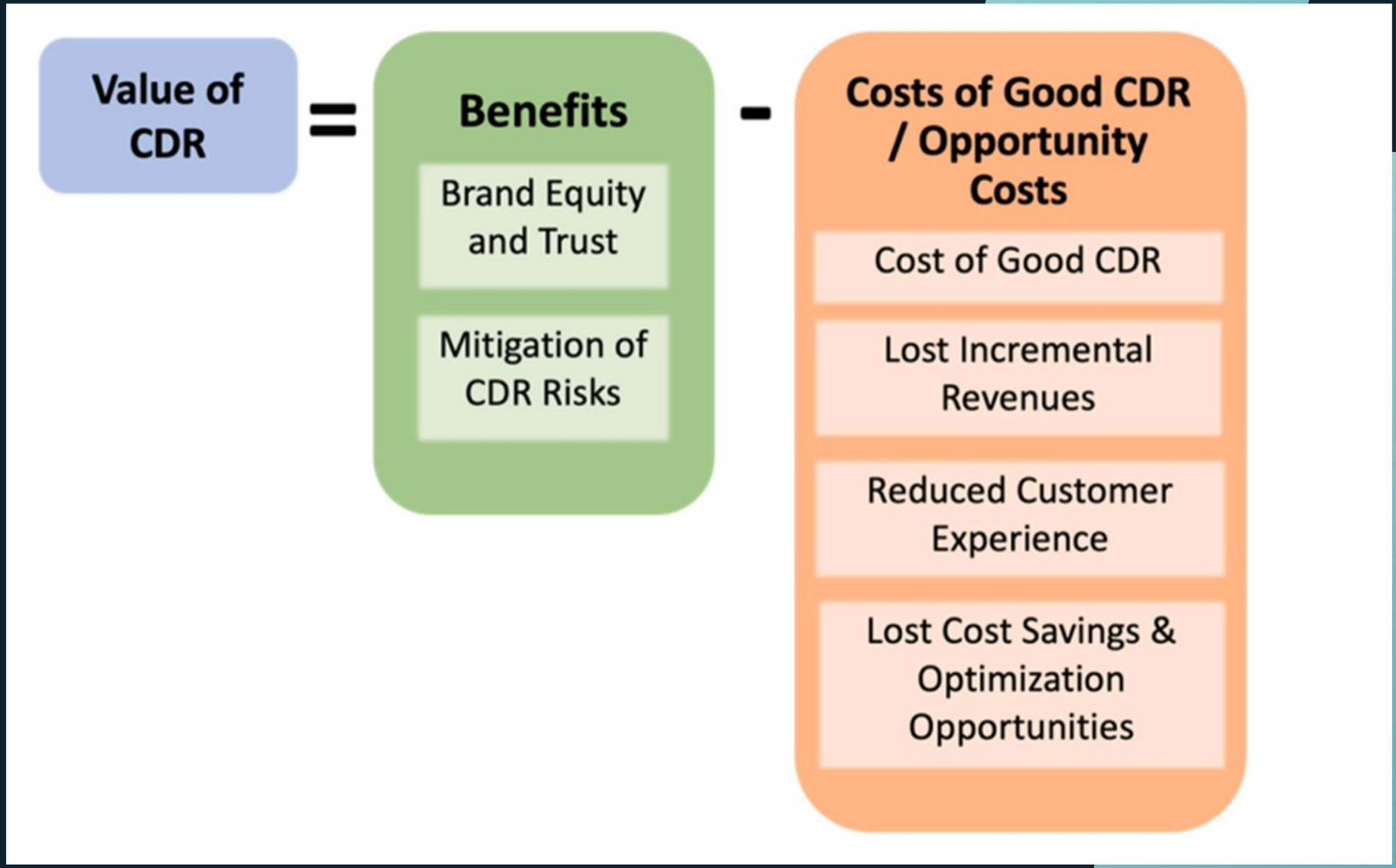


2@3A BANK'S CONSULTING

www.2at3a.com

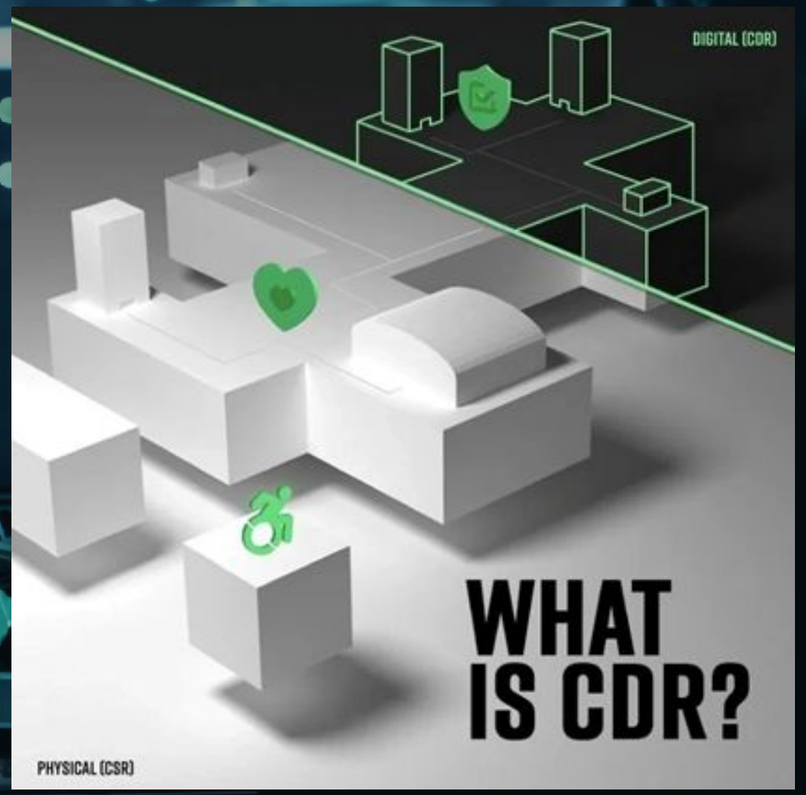
Corporate Digital Responsibility can improve a company's competition for scarce resources along the dimensions of trust, digital readiness, allocation, responsible innovation, risk and sense-making purpose.

The CDR calculus

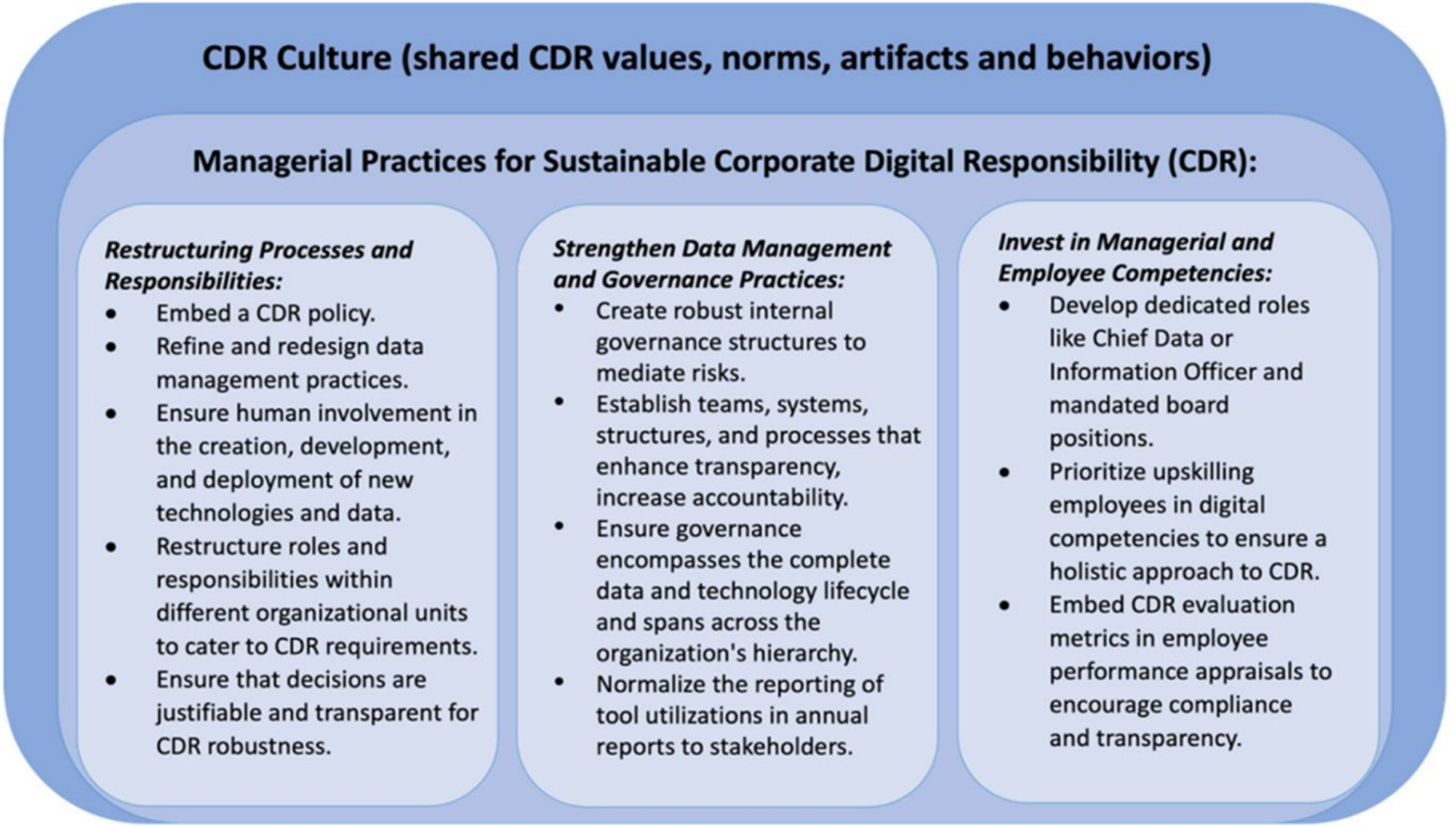


•Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. Organizational Dynamics, 53(2), 101056.

Module 7: Summary



Managerial Practices for Sustainable CDR



Thank you for your time and attention!

Module 1.1: Introduction to Cybersecurity

For Small and Medium-Sized Enterprises (SMEs)

Presenter:

Dr. Tomislav Horvat

University North,

Croatia

Interreg CENTRAL EUROPE

Co-funded by the European Union

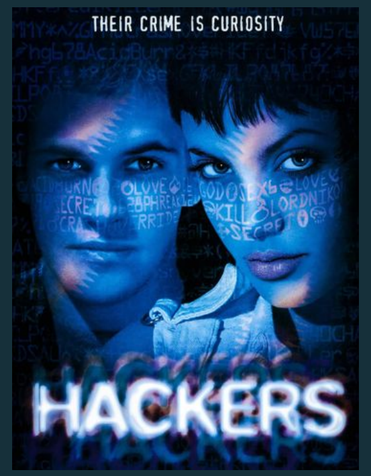
COEUS

Hackers

Hackers

The term "hack" originated at MIT, meaning playful and clever technical modifications by early tech enthusiasts.

1950



1995



1999

Term "Hacker" today refers to individuals from malicious cybercriminals (black hats) to ethical hackers (white hats).

2024

Types of Hackers today

Types of Hackers today

01 Script Kiddies, or hobbyists - inexperienced hackers who use pre-made tools to exploit vulnerabilities without fully understanding the technology

02 Hacktivists - politically or socially driven, target organizations and governments to promote their beliefs (website defacement, DDoS attacks, ...)

03 White Hat Hackers - work legally to identify and fix security flaws, often hired by organizations to improve their cybersecurity

04 Grey Hat Hackers - operate between ethical and unethical, break without permission but usually report the issues they find

05 Black Hat Hackers - malicious hackers break into systems for personal gain, stealing data and causing damage

06 State-sponsored Hackers - conduct cyber espionage, surveillance, and cyber warfare on behalf of governments



History of Cybersecurity

History of Cybersecurity

The Morris Worm (1988)

A pivotal moment in cybersecurity, exposing system vulnerabilities, prompting the creation of the first CERT, and resulting in legal action under the Computer Fraud and Abuse Act.

2010s

Mobile devices and IoT expanded attack surfaces, high-profile breaches underscored cybersecurity’s impact on privacy, and AI began enhancing threat detection.

"ILOVEYOU" virus

The Internet’s growth led to the antivirus and firewalls development, while major early 2000s attacks underscored the need for stronger security measures and increased public awareness.

The 2011 Stuxnet attack

The Stuxnet attack on Iran's Natanz facility was pivotal, demonstrating cyberattacks' potential for physical damage and reshaping national defense strategies.

Digital transformation

Expanded the attack surface, prompting companies to invest in enhanced security protocols, employee training, and incident response plans.

Mid-2000s

Cybersecurity became a priority, with the PCI DSS introduced in 2004 for data protection and the rise of social media demanding advanced security strategies.

The rise of cloud computing

Transformed data storage and processing, offering flexibility but introducing challenges in data privacy and compliance, leading companies to adopt specialized security protocols.

What is Cybersecurity?

What is Cybersecurity?

Cybersecurity

What is Cybersecurity?

Cybersecurity

Originally cybernetics, refers to the science of communication and automatic control systems in both machines and living organisms.

Refers to data protection, ensuring confidentiality, integrity, and availability; system security, maintaining functionality; and proactive/reactive measures for cyber threat management through security tools, procedures, and policies.

What is Cybersecurity?

Cybersecurity

Cyber + security = combined refer to the protection of our digital world, including computers, networks, software, and internet-related activities.

Definition of Cybersecurity

Definition of Cybersecurity

Cybersecurity refers to the protection of our digital world, including computers, networks, software, and internet-related activities.



Sensitive data is routinely stolen



Businesses are paralyzed by ransomware



Critical infrastructure is sabotaged by malicious actors

Understaning Cybersecurity

Cybersecurity covers a wide range of practices.



Protecting data integrity



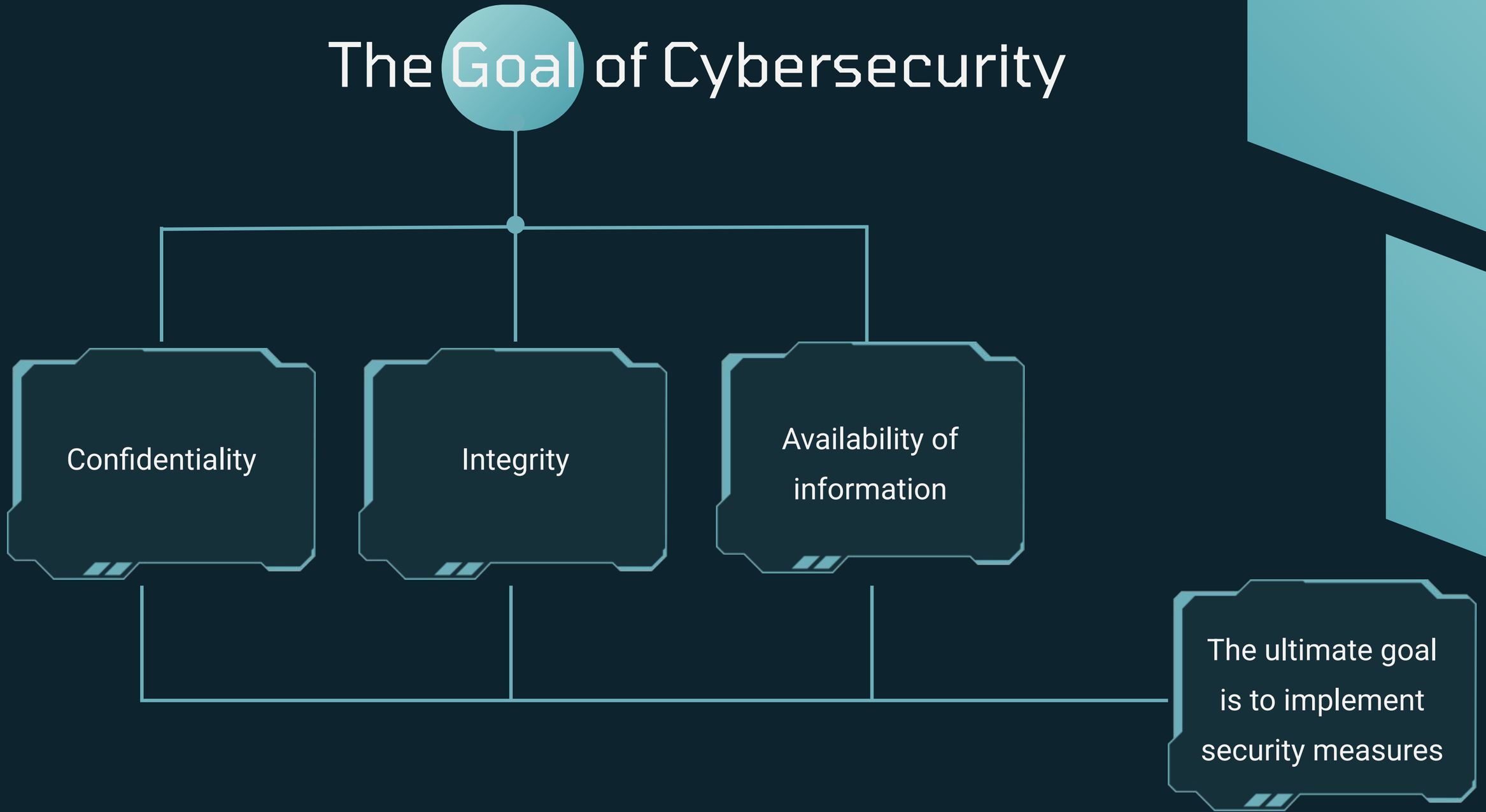
Ensuring privacy



Protecting networks and systems against unauthorized access

The Goal of Cybersecurity

The Goal of Cybersecurity



Importance of Cybersecurity

Importance of Cybersecurity

Financial Protection

- cyber attacks cost between $84,000 and $148,000
- business disruptions, recovery costs, and lost productivity, ...

Reputation Protection

- trust is vital for SMEs
- a damaged reputation can have lasting effects
- communication helps SMEs maintain client trust

Legal Compliance

- compliance is a legal necessity
- GDPR protect data privacy, and non-compliance can lead to fines and legal action

Business Continuity

- keeping operations running is crucial
- recovery planning minimizes impact and speeds up return to business

- cybersecurity isn’t just a technical issue for SMEs—it’s about protecting their finances, their reputation, their legal standing, and their ability to keep the doors open



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Conclusion



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Thank You for Your attention!



Module 1.2: Cybersecurity Ecosystem

For Small and Medium-Sized Enterprises (SMEs)

Presenter:

Dr. Tomislav Horvat

University North,

Croatia

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

What is Cybersecurity Ecosystem ?

Cybersecurity Ecosystem

A cybersecurity ecosystem is defined as a complex network of interconnected software, hardware, network resources, and users that function together as a cohesive unit.

=

Technological components

Applications, operating systems, devices, cloud services, and the interactions between them.

+

People involved

Developers, end-users, service providers, and other stakeholders like ethical hackers who contribute to and use these technologies.

Cybersecurity Ecosystem

The ecosystem of cybersecurity is a complex and interconnected network of technologies, processes and stakeholders aimed at protecting digital assets from cyber threats.

Five key areas:

01 Threat Actors

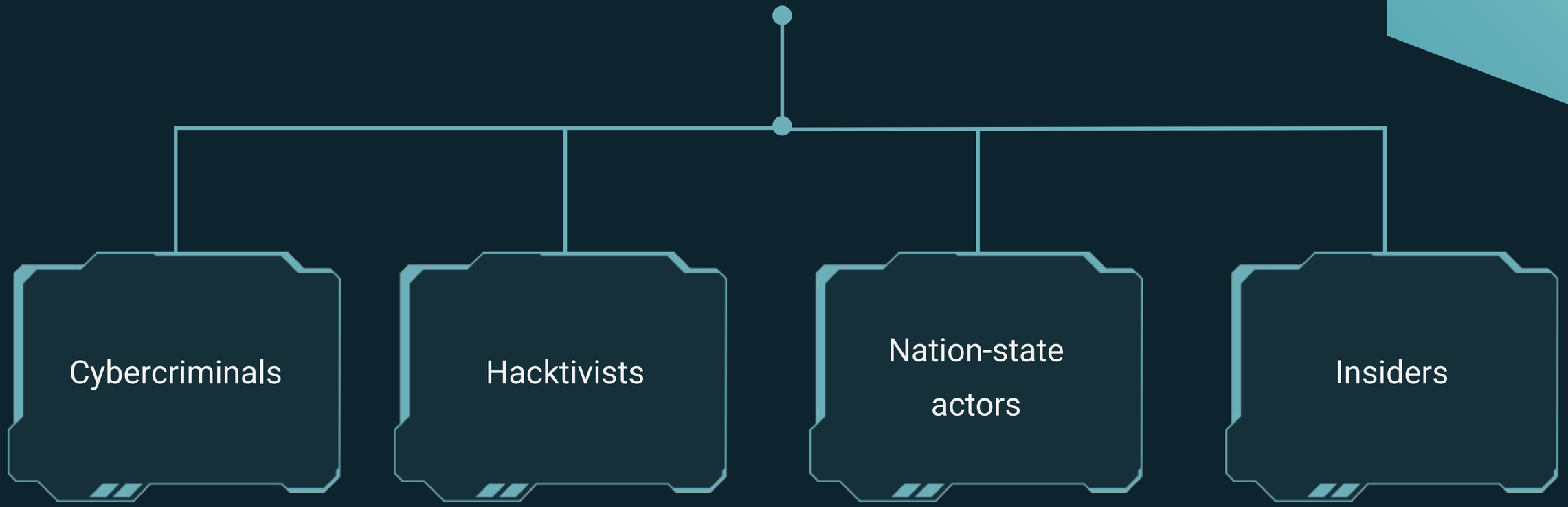
02 Cyber Threats

03 Security Measures

04 Regulations and Standards

05 Response

Threat Actors



Cyber Threats

Malware

A software designed to harm, exploit, or gain unauthorized access to computer systems.

Phishing

A scam where attackers pose as trustworthy entities to trick people.

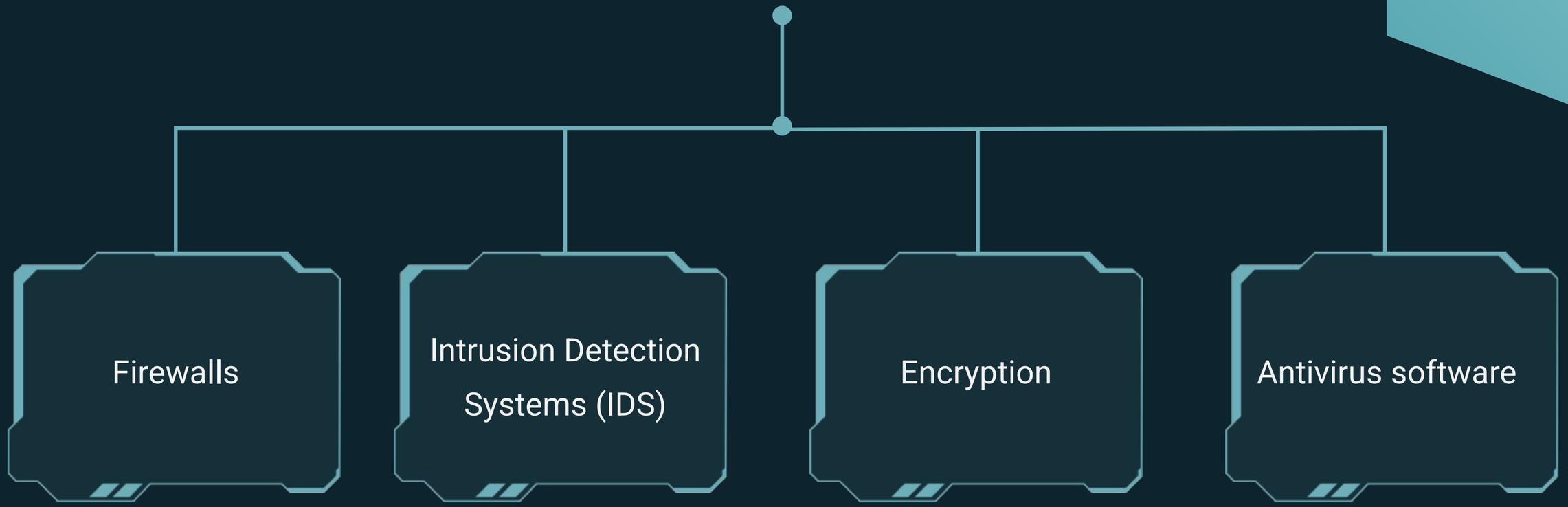
Ransomware

Type of malware that encrypts a victim’s data and demands payment for the decryption key.

DDoS attacks

Attacks that flood a network or server with excessive traffic, making it slow or unavailable.

Security Measures



Regulations and Standards

GDPR and HIPAA

Enforce strict data protection and privacy protocols.

PCI-DSS and ISO/IEC 27001

Framework for secure handling of sensitive information, ensuring that companies maintain robust information security practices.

Incident Response

Detection

First step during which identifying anomalies that indicate a potential breach is crucial.

Containment and Eradication

Isolating the threat and removing its cause.

Recovery

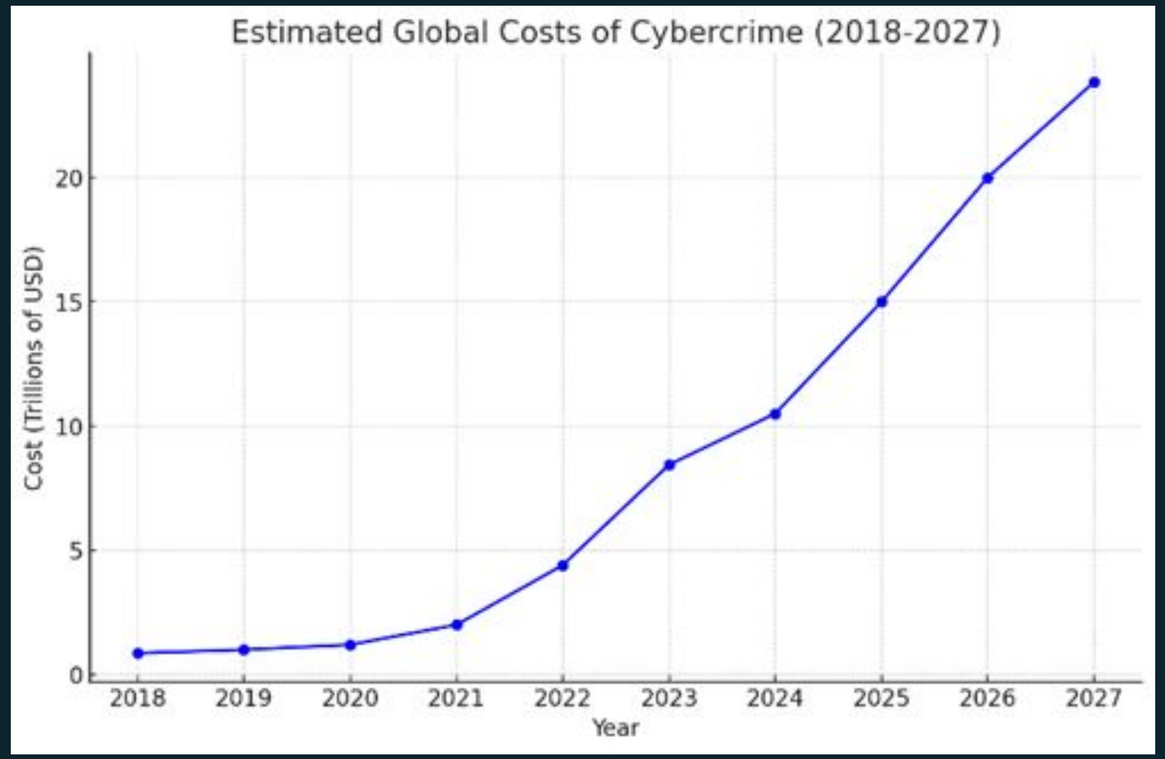
Restores systems to normal operation, ensuring they are secure and functional.

Post-Incident Analysis

Learning (identifying gaps, improving future response strategies).

Estimamted Global Costs of Cybercrime

- Statista estimates global cybercrime costs have soared from $860 billion in 2018 to a projected $23.84 trillion by 2027



Source: Statista

What is Cyber Insurance?

Cyber insurance is coverage that protects against the costs of cyberattacks, including recovery, legal fees, and reputational damage.

Liability Coverage

Covers legal costs from lawsuits, settlements, and fines after a data breach.

First-Party Coverage

Handles losses like data recovery, system repairs, business interruption, and even ransom payments.

Incident Response Support

Offers access to experts, legal counsel, and PR professionals.

Risk Management

Provide risk assessments and resources, like employee training and security audits.



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Conclusion



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Thank You for Your attention!



Module 2: Cyber Threats vs. Cyber Attacks

For Small and Medium-Sized Enterprises (SMEs)

Presenter:

Dr. Tomislav Horvat

University North,

Croatia

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Cyber Threads vs Cyber Attacks

Cyber Threats

- represent potential risks
- malware, phishing, software vulnerabilities, or social engineering tactics
- passive in nature

VS

Cyber Attacks

- deliberate actions taken by individuals or organizations to exploit these threats
- active and intentional
- ransomware attacks, DDos attacks

Cyber Threats Types

Cyber Threats Types

01 Malware

02 Phising

03 Social Engineering

04 Distributed Denial of Service (DDos)

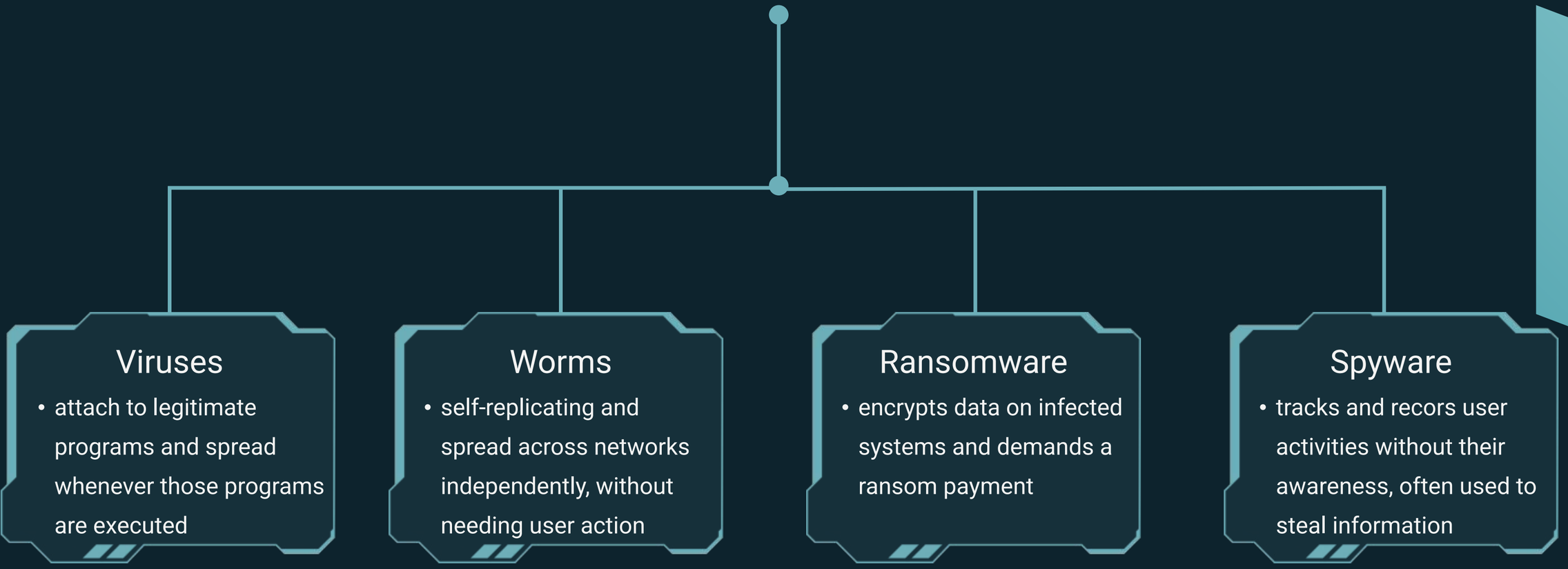
05 Insider Threats



What is Malware?

What is Malware?

Malware, short for "malicious software," is designed to harm, steal data, or disrupt normal computer operations.



Examples of Malware Attacks

Examples of Malware Attacks

01

WanaCry (2017)

- massive ransomware attack that affected thousands of computers worldwide
- once it infected a machine, it encrypted the files and displayed a message demanding a payment in cryptocurrency to unlock them
- rendered the computers unusable, essentially locking users out until the ransom was paid or the system was restored from a backup

02

ILOVEYOU (2000)

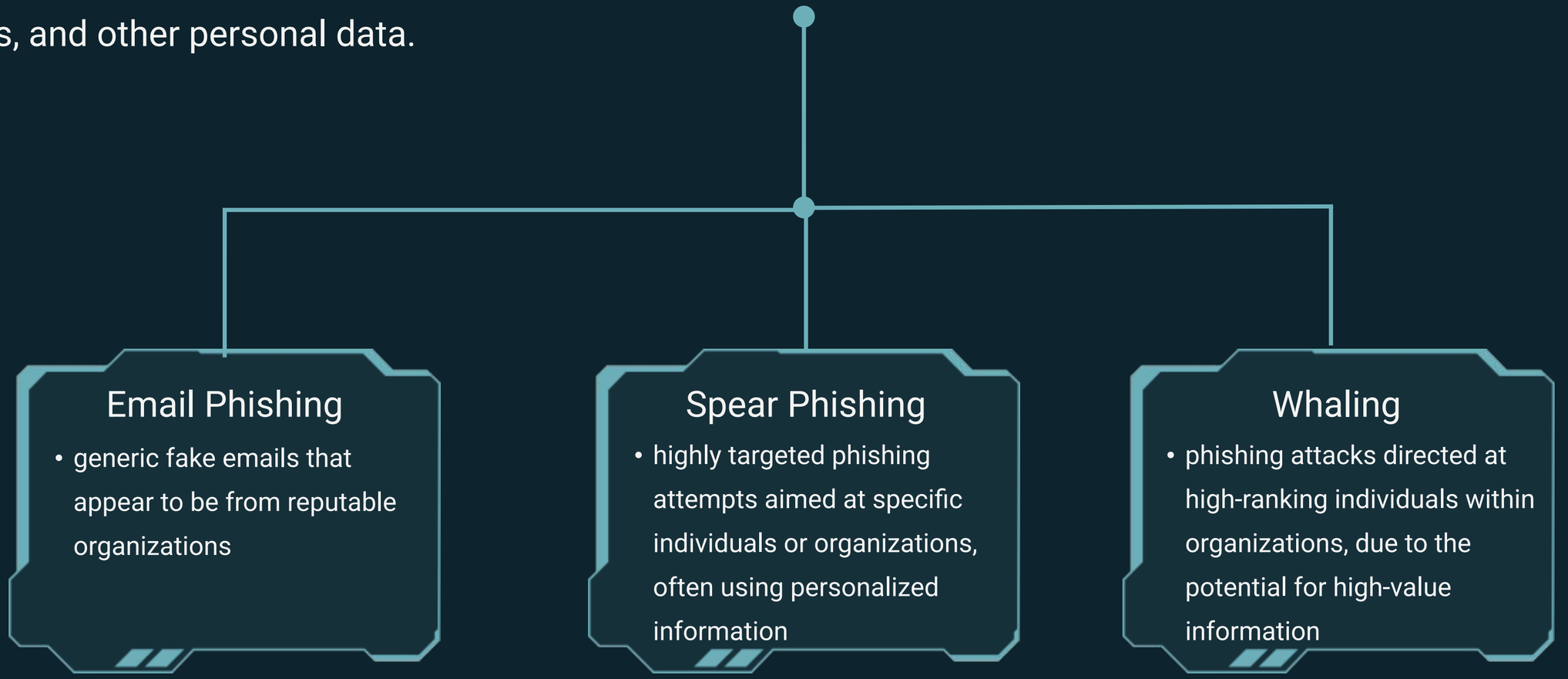
- circulated by sending an email with the subject "ILOVEYOU" and an attachment
- once opened, the attachment ran a script that overwrote files and then sent itself to all contacts in Microsoft Outlook address book
- infected computers experienced data loss from file overwriting, system instability, and severe network slowdowns due to the mass distribution of emails



What is Phishing?

What is Phishing?

Phishing is type of cyber threat that uses deceptive communication, typically through emails, to trick individuals into revealing sensitive information, such as passwords, credit card details, and other personal data.



Example of Phishing Attack

Example of Phishing Attack

01

PayPal Phishing Scam

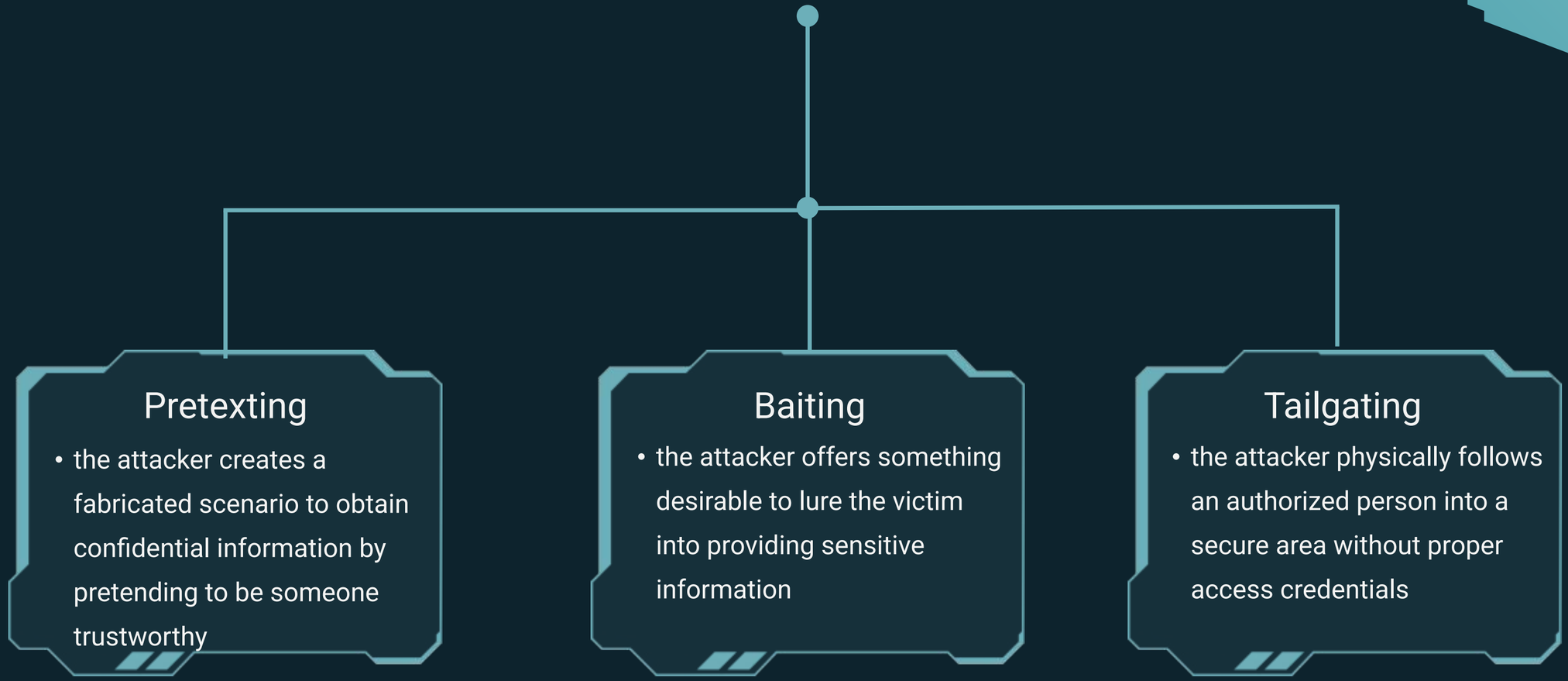
- attackers sent emails that appeared to be from PayPal, urging recipients to verify their accounts or warning that their accounts had been compromised
- users were redirected to a fake website mimicking PayPal's login page
- victims unknowingly gave attackers access to their accounts, leading to unauthorized transactions and potentially even identity theft



What is Social Engineering?

What is Social Engineering?

Social engineering is a type of cyber threat that manipulates individuals into revealing sensitive information or performing actions that compromise security.



Example of Social Engineering

Example of Social Engineering

01

Phone Scams

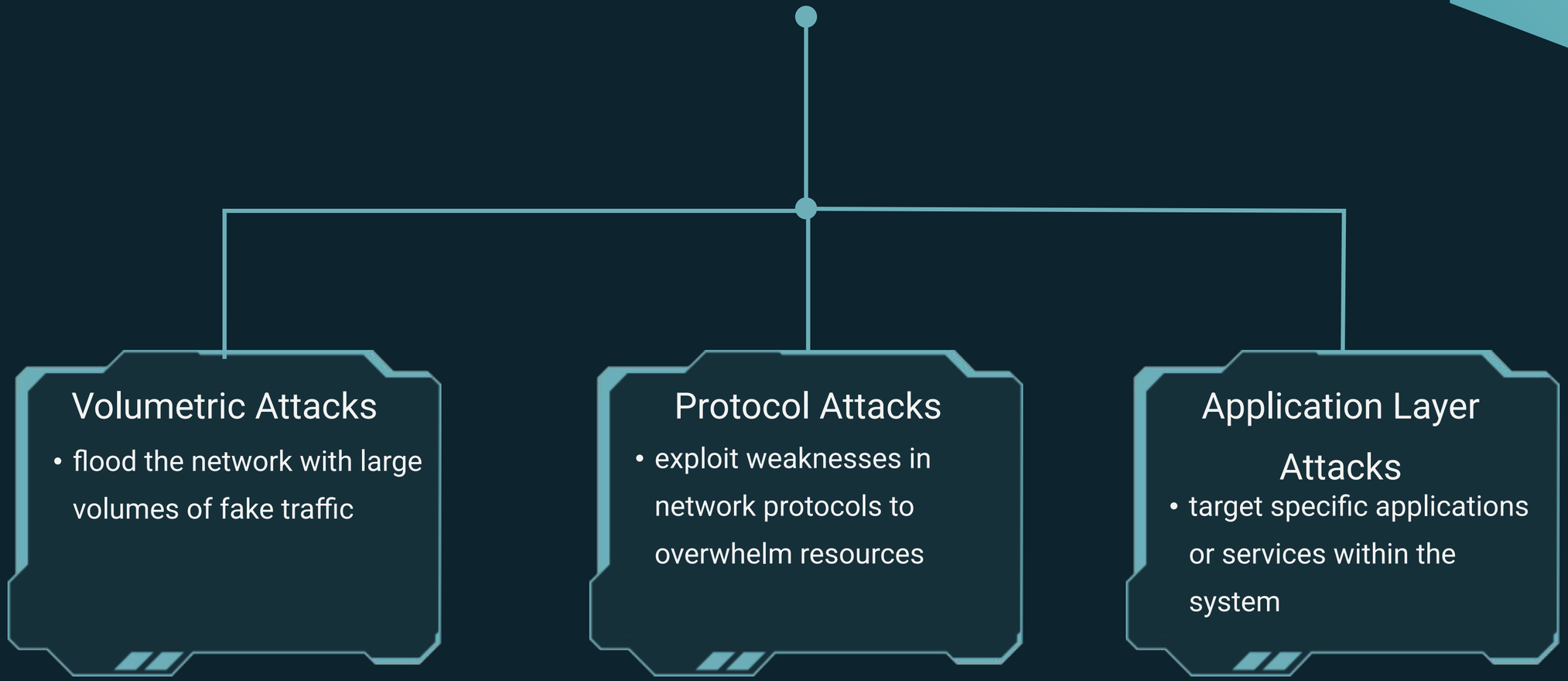
- attackers impersonate tech support from companies like Microsoft, IBM or an Internet Service Provider
- they claim the victim's computer is compromised and instruct them to install remote access software
- attackers can install malware, steal information, or demand payment for fake repairs --> financial losses, identity theft, emotional distress, while also losing trust in legitimate tech support services



What is Distributed Denial of Service (DDoS)?

What is Distributed Denial of Service (DDoS)?

DDoS attack uses numerous infected devices, known as a botnet, to flood a target system with fake traffic, making it inaccessible to legitimate users.



Example of DDoS Attack

Example of DDoS Attack

01

Dyn Attack (2016)

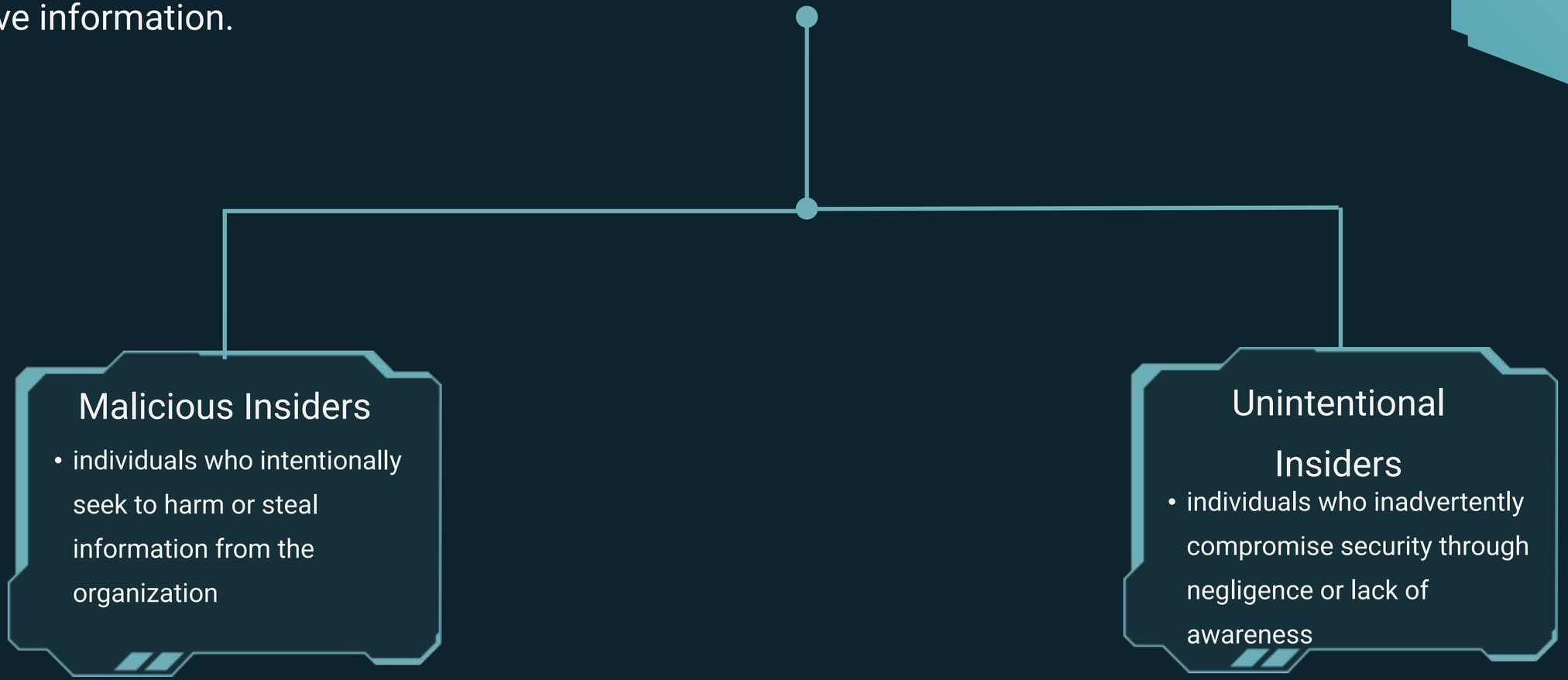
- targeted the DNS provider Dyn using a botnet of IoT devices infected with Mirai malware --> major disruptions on sites like Twitter, GitHub, and Netflix, causing internet outages in the U.S. and Europe for hours
- the attack exposed IoT vulnerabilities and highlighted the critical role of DNS providers in internet stability, leading to advancements in IoT security and DDoS mitigation strategies



What is Insider Threats?

What is Insider Threats?

Insider Threats are risks that originate from within an organization, typically involving employees, former employees, contractors, or business partners who have access to sensitive information.



Example of DDoS Attack

Example of DDoS Attack

01

Edward Snowden (2013)

- a former NSA contractor leaked top-secret documents on U.S. government surveillance, including metadata collection and access to data from companies like Google and Facebook
- ignited global debates on privacy, prompted U.S. intelligence reforms, and underscored the serious impact of insider threats, accelerating the push for stronger encryption and data security



Interesting Facts About Cyber Threats

Interesting Facts About Cyber Threats

Every day, over 350,000 new malware samples are detected

Phishing remains a major concern, with about 12% of users clicking on phishing links.

Social engineering is a major threat, causing 70% to 90% of data breaches.

DDoS attacks are disruptive, with an average duration of 12 hours

Insider threats can be costly, with an average incident cost of $11.5 million

Example of Ransomware Attack

Example of Ransomware Attack

01

Ransomware Attack on ABC Manufacturing

- a phishing email caused a ransomware attack, encrypting critical data and halting production for days, resulting in a $50,000 ransom payment
- key takeaway – employee training on phishing awareness is essential to prevent such incidents
- implement multi-factor authentication and regular data backups to mitigate risks



Example of Insider Attack

Example of Insider Attack

02

Data Theft at XYZ Marketing

- a disgruntled former employee stole sensitive client data and sold it to a competitor, leading to financial losses and reputational damage
- highlights the importance of promptly revoking access for terminated employees
- emphasizes implementing role-based data access and regularly reviewing security policies



Example of DDoS Attack

Example of DDoS Attack

03

DDoS Attack on E-Shop Ltd.

- a botnet attack flooded the retailer's servers, disrupting online sales and damaging customer trust
- highlights the importance of implementing DDoS protection and regular resilience testing
- emphasizes the need for scalable IT infrastructure to handle such attacks





Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Conclusion



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Thank You for Your attention!



Module 3: Security Architecture and Protective Measures

For Small and Medium-Sized Enterprises (SMEs)

Presenter:

Dr. Tomislav Horvat

University North,

Croatia

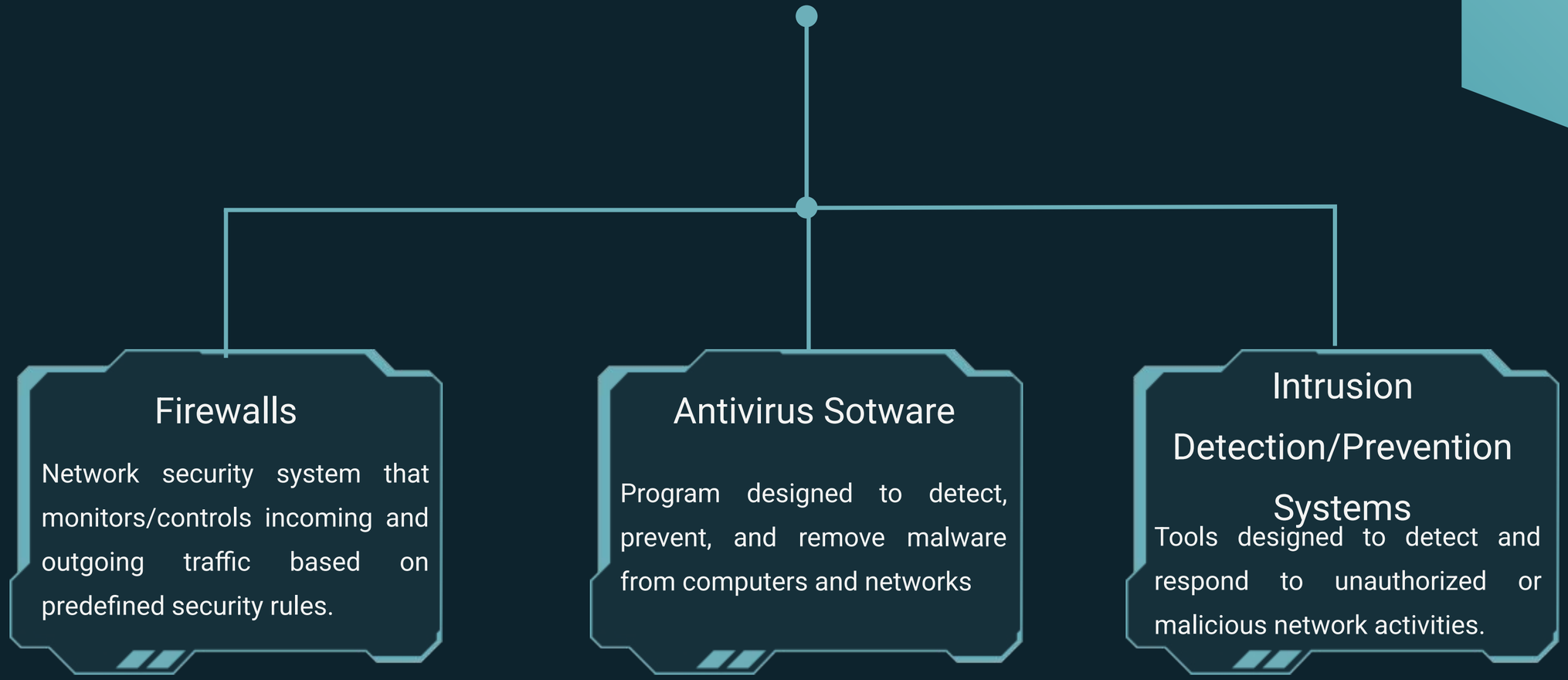
Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Security Architecture

Security Architecture



Firewalls

Firewalls

01 Act as the first layer of defense by creating a barrier between trusted internal networks and external, untrusted sources

02 Primary role is to manage network traffic, ensuring only authorized access is permitted

- Packet-Filtering Firewall
- Stateful Inspection Firewall
- Next-Generation Firewall (NGFW)



Antivirus Software

Antivirus Software

01

A vital tool for detecting and removing malware, including viruses, ransomware, and spyware.

Signature-Based Detection

Heuristic-Based Detection



Intrusion Detection and Prevention Systems

Intrusion Detection and Prevention Systems (IDS/IPS)

01 IDS (Intrusion Detection System) monitors network traffic for unusual activity, flagging potential threats.

02 IPS (Intrusion Prevention System) block threats in real time.



Network-Based IDS/IPS

Monitor traffic across the network.

Host-Based IDS/IPS

Monitors activities on individual devices.

Backup, Data Recovery and Network Security Management

Backup

01

Backuping is process of creating copies of data to prevent its loss due to hardware failure, cyberattacks, or accidental deletions.

Full Backup

Comprehensive data copy.

Incremental Backup

Saves only the changes since the last backup.

Differential Backup

Captures changes since the last full backup.



02

3-2-1 rule - ensure backups are stored across different media and locations (best practice)

Data Recovery

01 Data recovery is restoring lost or corrupted data from backups.

02 Backup frequency — according to research, 30% of people have never backed up their data.

03 3-2-1 rule - ensure backups are stored across different media and locations (best practice).



Network Security Management

01

Network security management encompasses measures to protect a network from unauthorized access and attacks.

Network Segmentation

Dividing a network into isolated sections to contain breaches.

Encryption

Securing data so that it remains inaccessible without the proper decryption keys.

VPNs (Virtual Private Networks)

Ensuring secure, encrypted communication channels, particularly for remote users.

Access Control Policies

Regulating user access to sensitive resources based on roles and permissions.



Proactive Measures

Preventive Measures

01

Preventive measures play a crucial role in strengthening an organization's cybersecurity posture.

Employee Education

Regular System and Software Updates

Log Monitoring and Analysis

Security System Testing





Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Conclusion



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Thank You for Your attention!



Module 4: Cybersecurity in SMEs (case studies - implementation)

For Small and Medium-Sized Enterprises (SMEs)

Presenter:

Dr. Tomislav Horvat

University North,

Croatia

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

SweetBites Bakery

SweetBites Bakery

01 Family-owned business with a simple goal to make and sell homemade cakes

02 As the bakery grew, the family expanded online with a website, orders, and social media

03 With their store opening, SweetBites faced cybersecurity challenges in securing customer data, Wi-Fi, and online systems



Cybersecurity Plan

Cybersecurity Plan

01 **Secure Passwords and User Access** – use strong, unique passwords, enable two-factor authentication (2FA), and implement role-based access control (RBAC)

02 **Protect the Website, Online Shop, and Reservation System** – implement an SSL certificate, use a Web Application Firewall (WAF), and regularly update software

03 **Secure the Network and Public Wi-Fi** – use network segmentation, enable WPA3 encryption, and implement VLANs to isolate sensitive data

04 **Regularly Back Up and Protect Data** – automate data backups, develop a disaster recovery plan, and use encryption to protect backup files

05 **Train Employees and Continuously Monitor Security** – conduct regular cybersecurity training, perform phishing simulations, and use continuous monitoring tools to detect threats



TechRise Solutions

TechRise Solutions

01 TechRise Solutions, a small family-run business, started in a garage delivering custom software to local clients with a basic network setup.

02 With growth, TechRise hired employees and adopted cloud infrastructure, introducing vulnerabilities in client data and cloud security.

03 With 50 employees, many remote, cybersecurity grew more complex, requiring secure remote work, regulatory compliance, and defense against advanced threats.

04 TechRise grew from a local business to a national tech company, requiring robust cybersecurity to protect its cloud, applications, and digital assets.



Cybersecurity Plan

Cybersecurity Plan

01 **Strengthen Passwords and Access Controls** - use strong passwords, MFA, and RBAC to prevent unauthorized access and password attacks

02 **Secure Cloud and Web Applications** - encrypt data, use WAFs, implement SSL, and conduct regular security audits

03 **Protect Remote Work** - Use VPNs, EDR solutions, and MDM to secure remote devices and connections

04 **Implement Backups and Disaster Recovery** - Automate backups, create a DRP, and use immutable backups to recover data quickly

05 **Monitor Systems and Train Employees** - provide regular training, monitor systems with SIEM tools, and conduct phishing simulations





Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Conclusion



Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Thank You for Your attention!



DIGITAL SUSTAINABILITY, INCLUSION AND ACCESSIBILITY

Josip Hrgović, PhD

Assist. Prof., University North, Croatia

kcikovic@unin.hr

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Learning Outcomes

- Ability to educate employees on sustainable digital practices (energy-efficient IT, optimized software use, e-waste management)
- Knowledge of digital inclusion strategies and WCAG standards
- Expertise in integrating inclusive design principles into business practices
- Skills to guide teams in personalized, user-friendly interface design
- Capacity to identify and implement external collaboration opportunities

Key Challenges for SMEs

- **Limited resources** (financial and human)
- **Lack of expertise** in complex digital systems
- **Infrastructure constraints** (technology, security, maintenance)
- **Data protection and privacy requirements** for maintaining consumer trust

- Digital Inclusion and Accessibility in the Context of SMEs and CDR
- How SMEs can ensure equal access to digital tools, services, and products
- Enhances market position, reputation, and customer satisfaction while fulfilling a legal obligation



Learning Outcomes

- Ability to educate employees on sustainable digital practices (energy-efficient IT, optimized software use, e-waste management)
- Knowledge of digital inclusion strategies and WCAG standards
- Expertise in integrating inclusive design principles into business practices
- Skills to guide teams in personalized, user-friendly interface design
- Capacity to identify and implement external collaboration opportunities

Learning Outcomes

- Ability to educate employees on sustainable digital practices (energy-efficient IT, optimized software use, e-waste management)
- Knowledge of digital inclusion strategies and WCAG standards
- Expertise in integrating inclusive design principles into business practices
- Skills to guide teams in personalized, user-friendly interface design
- Capacity to identify and implement external collaboration opportunities

Learning Outcomes

- Ability to educate employees on sustainable digital practices (energy-efficient IT, optimized software use, e-waste management)
- Knowledge of digital inclusion strategies and WCAG standards
- Expertise in integrating inclusive design principles into business practices
- Skills to guide teams in personalized, user-friendly interface design
- Capacity to identify and implement external collaboration opportunities

Thank you for your time and attention!