Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

COEUS TRAINING TRANSCRIPTS

Video lectures support material

Table of Contents

Introduction to Corporate Digital Responsibility..... 6
Introduction to Cybersecurity..... 19
Cybersecurity Ecosystem..... 24
Cyber Threats vs. Cyber Attacks..... 27
Security Architecture and Protective Measures..... 32
Cybersecurity in SMEs: Case Studies..... 36
Digital Inclusion and Accessibility..... 38
Digital Sustainability..... 45

CORPORATE DIGITAL RESPONSIBILITY

Introduction to Corporate Digital Responsibility

Katerina Fotova Čiković
University North, Croatia

Transcript 1–7 | Slides 1–69 | Voice-over script

Slide 1

Hello and welcome to the Introduction to Corporate Digital Responsibility Lectures. My name is Katerina Fotova Čiković and I am Assistant Professor at Economy Department at University North in Croatia. It is my great pleasure to host you and introduce you to the concept of CDR (Corporate digital responsibility).

Slide 2

What to expect from this lectures? Well, the lectures are structured to offer you knowledge, previous experiences and case studies regarding the application of CDR thus far.

In the first lecture, we will cover an introduction to the COEUS project. Thereafter, we would define CDR and explain the differences between CDR and CSR (Corporate Social Responsibility). In the third part, the ESG term and concept are introduced, together with its connection to the CDR. Next, we move on to the EU legislative related to CDR + GDPR (i.e. the Digital Act). Thereafter, we cover the inevitable subject of CDR profitability and the benefits & costs of CDR implementation, and we end with a short summary.

Slide 3

The COEUS (i.e. COrporate digital responsibility skills in central EUropean Smart specialisation) project is funded by the second Interreg Central Europe 2021-2027 call of the 2021-2027 programming period. COEUS aims to address the challenge of not only ensuring the achievement of digitization in Central Europe (CE), but also achieving it with social, economic, technological and environmental responsibility. It does this by supporting corporate digital responsibility (CDR) skills for traditional and innovative SMEs, with a focus on smart specialization priorities for digitalisation.

COEUS uses transnational cooperation to jointly design and co-implement a transnational pilot to test and validate the CDR program for upskilling/retraining SMEs. In parallel, the project builds the capacities of public bodies and stakeholders to support the adoption of CDR skills.

Moreover, COEUS is the first transnational project in the program area that deals with all areas of the relatively new and complex topic of CDR.

Slide 4

The project started in May 2024 and it will end in October 2026.

Slide 5

There are 7 partners from 6 countries working on this project. The lead partner organisation is Digital Innovation Hub from Slovenia.

Slide 6

So, let us dive in to the subject! The world is currently facing many challenges. We live in a hectic time when climate changes are an inevitable subject; there is an uncontrolled marine pollution, loss in biodiversity and an extreme usage of natural resources.

Slide 7

On the other hand, digitalization or the use and adoption of digital technologies – is driving massive economic, social and environmental changes. The future of humanity and the health of planet Earth depend to a large extent on how we undergo this digital transformation. We have an opportunity to drive this transformation in a manner that helps build a healthier, safer, cleaner and more equitable future, rather than one of exacerbated environmental degradation, inequality and social division.

Moreover, the digital transformation and the ever-evolving and occurring new technologies are putting established ways of doing business to the test. This offers opportunities, but also harbours risks. Companies have to be aware of their digital responsibilities to shape the process of digitalisation and guarantee it serves the best interests of citizens.

Slide 8

The digital transition brings new hope, but also raises new questions, as to what its environmental and social consequences are? Moreover, what are the consequences regarding the work organisation and professional relations? These are the questions that linger in societies nowadays, and the COEUS project aims to support small and medium organisations to meet legal requirements and make digital responsibility a normal part of their day-to-day business.

Slide 9

So let’s define the Corporate Digital Responsibility (hereafter the CDR). 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.

CDR is first and foremost a voluntary commitment by organisations in representing societal interests and to inform “good” digital corporate actions and digital sustainability (i.e., using data and algorithms) via collaborative guidance on addressing social, economic, and ecological impacts on digital society.

Even though, in theory, it sounds obvious, in practice, it is not so easy to achieve, particularly for SMEs.

Slide 10

What is a digitally responsible company? How would we define it? To simplify it, consider it as an organisation that responds in line with the sustainable development goals when it comes to regulatory, ethical responsibility, societal and environmental responsibility.

Slide 11

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

Moreover, there are 3 dimensions when innovating in the ICT, and these dimensions follow the process from digitization (technical dimension), to digitalisation (social behavioural dimension) to digitalisation and corporate digital responsibility (social ethical dimension).

Slide 12

What is the difference between CDR and CSR (i.e. Corporate Social Responsibility)?

Slide 13

As stated in many scientific studies and reviews, the main distinction between CDR and CSR is given by the role that technology plays in the respective concept. Moreover, it is safe to assume that CDR is a part of CSR.

Slide 14

As shown in this Figure by Pelters (2021), the so-called “Sustainability square” represents the transition from CSR to the CDR concept. What is shown here, is actually a reminder that CDR practices integrate economic, social and ecological aspects into both physical living and digital living environment.

Slide 15

In this figure introduced by Wynn & Jones (2023), the main parameters of CDR are shown. As seen in the graphical presentation, employees (through upskilling and redeployment, information transparency and access and cultural change and process re-design), customers (through building trust, data protection, privacy and security, and customer engagement) and other stakeholders are included and vital for successful implementation of CDR practices.

Slide 16

This is also emphasized in the CDR Manifesto.

Slide 17

So let's give a few examples on real-life CDR practices.

In the implementation stage, the CDR manager is responsible for creating and implementing a conscientious CDR policy (a company guideline to promote corporate digital responsibility). In this stage, it is vital to decide whether you want to make digitalization in your company sustainable and responsible?

As for the data protection procedures, the most pivotal question of handling private data revolves around the procedures that cover how you can collect and evaluate data securely.

When using Artificial Intelligence, the most important task of the AI manager is to implement it and accompany such transformation safely and responsibly in the spirit of corporate digital responsibility.

Slide 18

An excellent example of a successful real-life CDR implementation is the German company Zalando. In an interview from July 2022, Miss Darija Braeuniger, Senior Lead Public Affairs DACH at Zalando, explained how German companies and the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV) are working together to share best practices in the digital world when it comes to areas such as Data Privacy, Sustainability and Diversity & Inclusion.

The German CDR code has a section that focuses on making sure data is used in a way that customers expect and are aware of, and Zalando is achieving this by offering an experience of trust and processing customer data in accordance with all applicable data protection laws on national and EU level. This is vital for digital native companies such as Zalando.

A very insightful example is mirrored in the way in which Zalando tries to mitigate the fear of data misuse is the size recommendations. Size is very personal — it can be related to your health, mental wellbeing and physical goals — so somebody telling you what is and is not your size can be quite intrusive.

When Zalando gives size recommendations, they are accompanied by a little info icon that simply tells you what data is used to make this recommendation: learnings from your returns or feedback from other customers who have purchased the brand. By informing the customer very plainly with a simple sentence they know where the data comes from and there is no uncomfortable speculation.

Slide 19

On the other hand, there are many potential misleading and negative experiences with digitalization, including harm to customers and unwanted societal consequences. This is highlighted in the paper of Hartley, Kunz & Tarbit (2023), where they state that the unchecked proliferation of new technologies and AI systems continues to raise pressing societal concerns about biases, fairness, and transparency. For example, AI-powered technologies such as service robots are fraught with privacy concerns related to surveillance and the capture and retention of customer data (including consumer facial recognition data) without expressed permission.

This was the case of Goldman Sachs and the Australian government. 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.

Slide 20

So here’s an example of each of the CDR dimensions. For instance, when considering an organization’s relationship with people and society, with topics such as data privacy protection and aspects related to digital diversity and inclusion, such as bridging the digital divide between geographies, social classes, and age demographics, when imperfections occur, it is important to address customers questions. 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.

When considering the economic dimension of CDR, it usually concerns the responsible management of the economic impacts of digital technologies and includes topics such as the 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.

A good example is the Swiss holistic natural cosmetics and anthroposophical medicines company, Weleda, that claims that any use of robotic process automation would not result in staff reductions or job losses. Affected employees would be upskilled and transferred into other functions.

Slide 21

When it comes to the technological dimension of CDR, it assumes 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 deep fake videos can also have harmful effects on society. A good real-life example is the German telecommunications company Deutsche Telekom, which encourages its employees to follow corporate ethical guidelines related to AI engineering and usage.

Last but not least, the environmental dimension of CDR concerns the link between digital technologies and the physical environment, and tackles issues of responsible recycling or the disposal of old computer equipment. A good example here is the financial services group UBS, which committed to net zero Scope 1 and 2 emissions by 2025, and thus leverages connected sensors in its physical infrastructure to reduce their energy consumption and measure carbon emissions more effectively.

Slide 22

This table from Lobschat et al. (2021) provides an example of activities and potential concerns in the example of wearable personal health devices that illustrate the four stages (namely, the Creation, Operation and Decision-Making, Inspection and Impact Assessment and Refinement) and discusses the potentially relevant ethical considerations that emerge in the respective context.

In turn, these considerations need to be reflected in specific CDR norms that seek to guide and inform behaviors across levels. As a special form of refinement, CDR norms must also cover the retirement of digital assets. Notably, CDR norms should specify how long collected customer data are kept on file, as highlighted in current discussions about the “right to be forgotten” on the Internet.

Retirement considerations also apply to digital technologies per se, especially when these have become systemic or infrastructural, in that they set out ways to avoid being locked into a system as well as fail-safe conditions and procedures.

Slide 23

Service organizations have many touchpoints in a customer's journey with vast opportunities to capture data, deploy technology, and generate insights. These capabilities have led to new digital service ecosystems with the service firm in the center orchestrating value creation, exchange and capture, and governing the ecosystem of customers, complementors, and external business partners.

This figure presents the model introduced by Wirtz et al. (2022), where they examine the central value exchanges present within the digital service ecosystem. This ecosystem depicts the service firm's business model from two sides: a front- and back-end with related flows of money, service, data, insights, and technologies.

The front-end consists of the customer-facing side containing the service delivery system and customer interface, while the back-end covers the service firm's relationship to business partners. The dynamics within this ecosystem are fundamental to understanding the origins of CDR issues.

The discussion on the digital service ecosystem shows that service firms will face CDR issues not only in their interactions with customers (front-end), but also in the back-end with their many and varied supply chain, technology, and other business partners. There is the potential for significant value creation and capture, and as service firms have effectively become private regulators of their ecosystems, they are at risk of abusing that position for their own advantage and create CDR issues.

Slide 24

We now move forward and tackle the scholarly literature regarding CDR and CSR i.e. what is thus far found.

Slide 25

For instance, when surveying the Clarivate Scopus and the Web of Science databases with the keywords/keyphrase "CSR (Corporate Social Responsibility)", there are 36.176 and 43.288 papers, respectively.

Slide 26

When this search is narrowed to the implementation to SMEs, there are only 361 paper in the Clarivate Scopus database and 481 paper in the Web of Science database.

Slide 27

What is most interesting, as found in the paper of Oduro, Bruno & Maccario (2021), even though the scholarly literature on CSR in SMEs is ever-growing, the knowledge around this subject is still very fragmented across scientific journals, sectors, disciplines, and cultural and geographical contexts.

Slide 28

These findings reveal rather interesting new insights as follows: the CSR research in SMEs is rapidly growing 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, CSR green practice and ethics studies are preponderately Europe-centric, multi-sectoral, and atheoretical; and there is a limited adoption and development of novel theories and linkage between the conceptual and empirical studies.

Slide 29

In this figure, a wordcloud of the surveyed relevant published papers regarding the CSR in SMEs is presented. The words with biggest font are words that are mostly used in the surveyed papers.

Slide 30

As for CDR, when surveying the Clarivate Scopus and the Web of Science databases with the keywords/keyphrase “CDR (Corporate Digital Responsibility)”, there are 843 and 1.042 papers, respectively. This survey reveals the novelty of CDR among scholars and researchers.

Slide 31

When diving deeper and analysing these papers, we see on the right that most of these published papers revolve around the US, i.e. the authors affiliations are from the US (114 papers), then China with 110 papers, UK with 95 papers, Germany with 72 and Italy with 48 papers. So, it is safe to assume that CDR in SMEs is a subject that is relevant to scholars from developed (mostly Western) economies.

Slide 32

An analysis on the time of publication reveals that there is an uprising trend of popularity of this subject, where the most of the papers were published in 2023, and each consecutive year, the number of papers increased.

Slide 33

As for the subject area, when tackling “CDR” with “entrepreneurship”, only 30 papers were hit in the Scopus database, most of which were written in the subject area of Business, Management and Accounting (18 papers), Economics, Econometrics and Finance (10 papers) and 7 papers per each subject area: Computer Science, Engineering and Social Sciences.

Slide 34

As for the Web of Science database, there were 1042 hits with the keyphrase “corporate digital responsibility”. There is a visible growing trend of published papers throughout the years, which again shows the novelty and the rise in popularity of this subject.

The research areas in which most of these papers are published are Business Economics, Environmental Sciences Ecology and Science Technology.

Slide 35

When combined with the keyword “entrepreneurship”, there are only 72 results in the Web of Science database, most of them published in 2023 in Business Economics area.

Slide 36

Lastly, the combination of CDR and SME in both these databases reveal very modest literature published on this subject, i.e. only 9 papers in the Clarivate Scopus and 16 papers in the Web of Science database, or a total of 25 papers.

Slide 37

Again, in this figure, a wordcloud of the surveyed relevant published papers regarding the CDR in SMEs is presented. The words with biggest font are words that are mostly used in the surveyed papers. This wordcloud could reveal the trends in this research area.

Slide 38

The CDR Manifesto was introduced in 2021, when 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.

Slide 39

The CDR Manifesto is based on seven principles as shown in the figure.

Slide 40

The first principle is the principle of Purpose and Trust, which sheds light on transparency, publishing the corporate/entrepreneurial purpose and advocating trust as a key ingredient for employees, customers and shareholders.

The second CDR core principle is the Fair and Equitable Access for all, which implies inclusive and accessible products and services for all, responsible employment and promotion of justice, equity, diversity and inclusion altogether.

Slide 41

The third principle of CDR is the promotion of societal wellbeing, which actually implies strong privacy, responsible data practices, and promotion of digital maturity skills and digital wellbeing.

The fourth CDR principle is the consideration of the economic and societal impact, which includes transparency with all stakeholders regarding third party data, and a creation and implementation of a plan for sustainable and responsible automation.

Slide 42

The fifth CDR principle promotes acceleration of the Impact Economy Progress, which assumes investment in sustainability, environmental and societal impact returns. This principle also promotes acceleration of sustainable consumer behaviors.

The sixth CDR principle focuses on a creation of a Sustainable Planet to Live, which implies innovation and positive impact beyond corporate boundaries.

Slide 43

The last, but not least, seventh CDR principle revolves around reducing Tech's Impact on Climate and the Environment, which basically comes down to planning and implementing

an environmental IT strategy and consistent measurement and minimisation of energy use, and moving towards renewable energy.

Slide 44

Before we move to the next lecture, a short summary of the thus far lectures and a figure by Merbecks (2023), which very clearly shows the path each organisation goes from digitization to corporate digital responsibility. The first phase, digitization, includes innovation in ICT but only as a technical dimension. The second phase, digitalisation, includes a social behavioural dimension as well, and the third phase, i.e. Digitalisation and responsibility includes the social ethical dimension on top of the other dimensions. This last phase incorporates the CDR as a concept.

Slide 45

The next lecture revolves around the concept of ESG and its connection to CDR.

Slide 46

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.

Slide 47

ESG stands for environmental, social, and governance, and represents a holistic framework that measures the sustainable and ethical behaviour of a business. The criteria ensure that a business is being socially responsible and held accountable, which is in the best interest of shareholders and potential investors.

The environmental component of the framework considers the impact and contribution that a business can have on the natural world, including but not limited to waste and pollution management, Resource management, Greenhouse gas emissions (GHGs), Energy efficiency and Deforestation.

The social component of the framework assesses how a business treats and protects its employees, suppliers, customers, and the public by considering diversity, equity, and inclusion, working conditions, data protection, privacy, customer satisfaction, local communities, whereas the governance component of the framework examines how the business policies itself through tax strategy, executive remuneration, donations and political lobbying, corruption and bribery and board diversity and structure.

Slide 48

There is a lingering question regarding AI hovering above SMEs. In the age of artificial intelligence, how effectively are tech companies acknowledging their CDR?

The CDR core principles encompasses certain aspects, and are particularly relevant to deploying artificial intelligence (AI), which is considered “the most disruptive technology innovation of our lifetime”. However, matters such as governance, environmental responsibility and the imbalance of power continue to be neglected.

Slide 49

Deutsch Telekom, for example, argued that its approach to digital responsibility was focused on “human-centred technology” and built on a series of foundations, namely, laws and regulations, human rights, and culture and values, and two principles: 1) data privacy and security and 2) transparency and dialogue.

Slide 50

The House of Digital Responsibility of Deutsch Telekom focuses on human-centered technology. They claim to act responsibly in both the analog and digital spheres. This attitude is their protective roof. People are behind all the stakeholder groups at our company: customers, employees, shareholders, partners, and society as a whole.

Slide 51

In regards to AI, Google acknowledged that the future development of “AI is dynamic and evolving, and we will approach our work with humility, a commitment to internal and external engagement, and a willingness to adapt our approach as we learn over time”. The company added that it recognised that “AI technologies raise important challenges that we need to address clearly, thoughtfully, and affirmatively”.

Microsoft offered details of its “Responsible AI Standard” – the company’s internal playbook for responsible AI – which “shapes the way in which we create AI systems, by guiding how we design, build and test them”, and of its “Responsible AI Impact Assessment Template”.

More generally, regarding digital technology deployment, IBM argued that “customers, employees, and even shareholders are more frequently demanding that organizations not only take a principled stance on current concerns, but also follow through with meaningful actions that lead to clear outcomes”.

Slide 52

In this Table, which was introduced in the paper of Scarpi & Pantano (2024), the key elements for AI retail service automation are presented. It focuses on different aspects, such as consumer complaints management, improving personalization, merging and managing data from different sources and development of new prediction models.

Slide 53

The following figure by Scarpi & Pantano (2024) shows the Artificial Intelligence Responsibility in Retail Service Automation from both consumers and retailers perspective and summarizes the CDR considerations mentioned above and graphically

summarizes the relationship between the AI intelligence types, the CDR tools and solutions.

Slide 54

What follows is a lecture revolving around the Digital Act – the EU legislative related to CDR (Regulation (EU) 2022/2065.

Slide 55

The Digital Services Act – or shortly DSA is the most important and most ambitious regulation in the world in the field of the protection of the digital space against the spread of illegal content, and the protection of users' fundamental rights. There is no other legislative act in the world having this level of ambition to regulate social media, online marketplaces, very large online platforms (VLOPs) and very large online search engines (VLOSEs) and as of 17 February 2024, the DSA rules apply to all entities.

Slide 56

So what are the key goals of the Digital Services Act? The DSA protects consumers and their fundamental rights online by setting clear and proportionate rules. It fosters innovation, growth and competitiveness, and facilitates the scaling up of smaller platforms, SMEs and start-ups. The roles of users, platforms, and public authorities are rebalanced according to European values, placing citizens at the centre.

Slide 57

What the new rules mean for users, businesses and platforms? For users, the Digital Services Act and Digital Markets Act create a safer and more open digital space for all users, where their fundamental rights are protected and where they have access to quality digital services at lower prices.

For businesses, the Digital Services Act and Digital Markets Act create a level playing field that will allow innovative digital businesses to grow within the single market and compete globally.

For platforms, the Digital Services Act and Digital Markets Act set a high global benchmark for regulating digital services with clear obligations tailored to the importance of the online platforms.

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.

Slide 58

What the new Digital Services Act changes? They bring more user empowerment; strong protection of minors; more diligent content moderation, less disinformation; more transparency and accountability and a better risk assessment.

Slide 59

What's in it for SMEs? There are many changes and opportunities for SMEs, for instance new opportunities for businesses, greater transparency when it comes to working with the gatekeepers (Amazon, Google etc.), clearly-defined procedural rules that will ensure quick decisions translated in speedy advantages for both business users and consumers,

access to more information regarding how their products or services are performing on third party platforms, increased competition etc.

Moreover, the new rules will make it easier for smaller businesses and new entrants to grow and expand, and compete with gatekeeper platforms and start-up and new businesses will emerge and grow, and will create new jobs, thanks to a level playing field.

Slide 60

As a summary, the Digital Services Act package includes the Digital Services Act and the Digital Markets Act.

The Digital Services Act will bring many benefits to all the included entities. Business users who depend on gatekeepers to offer their services in the single market will have a fairer business environment.

Innovators and technology start-ups will have new opportunities to compete and innovate in the online platform environment without having to comply with unfair terms and conditions limiting their development.

Consumers will have more and better services to choose from, more opportunities to switch their provider if they wish so, direct access to services, and fairer prices.

Gatekeepers will keep all opportunities to innovate and offer new services. They will simply not be allowed to use unfair practices towards the business users and customers that depend on them, in order to gain an undue advantage.

Slide 61

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018.

The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. 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.

Slide 62

The GDPR defines individuals' fundamental rights in the digital age, the obligations of those processing data, the methods for ensuring compliance and the sanctions for those breaching the rules.

Slide 63

This next lecture revolves around the profitability of CDR implementation, the benefits & costs of CDR implementation.

Slide 64

We acknowledge that it's not always easy for SMEs to allocate the necessary resources to establish and maintain a strong CDR culture. Investing in CDR has uncertain ROI outcomes

such as avoidance of legal and reputational risks and potential long-term enhanced brand equity when consumers recognize and value good CDR practices of the firm.

The organizational objectives are often opposed to the adoption of good CDR practices. The resultant tensions can be viewed as trade-offs that service firms need to navigate in order to be profitable yet ethical.

We call that the Service Firm’s CDR Calculus and argue that firms weigh the benefits and costs of good CDR to determine how much they will engage in CDR-positive practices. This figure provides an overview of the benefits and costs of good CDR for service firms.

Slide 65

It is vital for SME management and owners/entrepreneurs recognize the power of CDR. Namely, the Corporate Digital Responsibility practices can improve a company's competition for scarce resources along the dimensions of trust, digital readiness, allocation, responsible innovation, risk and sense-making purpose.

Slide 66

The CDR calculus presented in this figure encapsulates the firm’s tensions and trade-offs between the implementation of digital technologies to meet organizational goals and gain consumer insights to the increased CDR concerns and costs. As depicted in the figure, the calculus weighs the advantages against the pitfalls of following robust CDR practices, providing insights into cost-benefit analysis incurred by firms.

The CDR Calculus illustrates the overall costs, both direct and indirect, associated with implementing and embracing effective CDR, in comparison to the benefits that a company can gain. Here, the value derived from ‘good’ CDR is dependent upon intensity of opportunity cost trade-offs made by the firm in their quest for market growth.

Slide 67

Finally, a short summary: The act of being ‘responsible’ suggests that certain requirements or expectations are met. To be considered as ’digitally responsible’, companies must adopt CDR practices that help them minimize both intended and unintended risks.

CDR should not only be seen as a tool for risk management, but also to generate opportunities and benefits that have positive impacts on stakeholders. However, CDR practices often focus on reducing negative impacts for firms. Fig. 3 outlines the key managerial practices that underpin a robust CDR culture within firms.

Slide 68

The behaviors and attitudes of managers and employees at all levels of the organization should be aligned with the specific norms and practices established by the organization in relation to CDR. The establishment of a robust CDR culture acts as an enabler of managerial practices that support CDR and mitigate risks within firms.

To enact this, firms need to consider how they can 1) restructure current processes and responsibilities within various organizational units, 2) strengthen data management and governance practices, and 3) invest in managerial and employee competencies and training aligned with CDR needs.

It’s not surprising that CDR needs to be adopted as an evolutionary process, not merely a static practice. It is also not a siloed organizational strategy or governance structure but rather a philosophy that underpins the organization’s culture.

Corporate culture is a critical building block for CDR, with shared CDR values and specific CDR norms as well as CDR artifacts and behaviors recognized as key drivers.

Slide 69

Thank you very much for your time, focus and attention. We hope you gained a lot of new insights into CDR implementation in your business. We wish you a successful implementation of the CDR and the best of luck!

CORPORATE DIGITAL RESPONSIBILITY

Introduction to Cybersecurity

Dr. Tomislav Horvat
University North, Croatia

Transcript 8 | Voice-over script

Slide 1 — Introduction to Cybersecurity

Welcome to our first session on cybersecurity. Today, we are going to explore what cybersecurity really means and why it is so important, especially for small and medium-sized enterprises.

It is my pleasure to introduce you to our comprehensive series on cybersecurity in SMEs. My name is Dr. Tomislav Horvat, an assistant professor at University North, Croatia. Throughout this course, I will guide you through a range of topics designed to equip you with the knowledge and tools needed to protect your organization.

Slide 2 — Hackers

First, let's start by understanding the term "hacker." Over the decades, the meaning of the word "hacker" has evolved significantly.

The first recorded use of the term "hack" in the context of technology dates back to the 1950s at the Massachusetts Institute of Technology (MIT). It was used by the Tech Model Railroad Club to describe playful and clever technical work. The members of the club, who were also early computer enthusiasts, began using "hack" to refer to their innovative modifications and experiments with technology.

Later, more precisely in the 1990s, films like "Hackers" published in 1995 and "The Matrix" published in 1999, contributed significantly to the public's perception, showing hackers as rebels or techno-wizards capable of effortlessly gaining access to any system.

Initially, hackers were seen as individuals who made creative, often harmless modifications to technology. However, over time, the media shaped the image of hackers into something more sinister, often depicting them as mysterious, highly skilled individuals capable of performing seemingly extraordinary accomplishments with computers.

Today, we use the term "hacker" to describe a broad spectrum of individuals, ranging from malicious cybercriminals, also known as black hats, to ethical hackers, also known as white hats, who work to improve security.

Slide 3 — Types of Hackers

As already mentioned there are different kinds of hackers in the world of cybersecurity, each with their unique motivations and skills. First, we have Script Kiddies, or hobbyists, who are inexperienced hackers using pre-made tools to exploit vulnerabilities without fully understanding the technology.

Next are Hacktivists, who are politically or socially driven hackers, using their skills to target organizations and governments to promote their beliefs, often through actions like website defacement or denial-of-service attacks.

White Hat Hackers, also known as ethical hackers, are those who work legally to identify and fix security flaws, often hired by organizations to improve their cybersecurity.

Grey Hat Hackers operate in a murky area between ethical and unethical, as they might break into systems without permission but usually report the issues they find.

Black Hat Hackers are those who engage in malicious activities, breaking into systems for personal gain, stealing data, or causing damage.

Finally, we have State-sponsored Hackers, who work on behalf of governments to conduct activities like cyber espionage, surveillance, or even cyber warfare.

These different types of hackers highlight the diverse motivations and skills present in the cyber landscape, each presenting unique challenges and considerations for cybersecurity professionals..

Slide 4 — History of Cybersecurity

Now, let's focus on the history of cybersecurity and its evolution over time, highlighting only key events and concepts that have shaped this field.

Let's start with a significant turning point - The Morris Worm. The Morris Worm of 1988 marked a major turning point as one of the first significant cyberattacks, impacting ARPANET computers. A coding flaw caused widespread crashes, exposing system vulnerabilities and leading to the creation of the first CERT. Legal action was also taken against its creator, Robert Tappan Morris, under the Computer Fraud and Abuse Act.

In the 1990s, the Internet's growth introduced new challenges, prompting antivirus and firewall development in response to threats like the "ILOVEYOU" virus, which caused billions in damages. Early 2000s attacks, like the SQL Slammer worm, highlighted the need for stronger security and raised public awareness.

By the mid-2000s, cybersecurity became a priority for businesses and governments. The PCI DSS was introduced in 2004 to protect consumer data, while social media's rise created new risks, requiring advanced security strategies.

The 2010s saw a rapid growth in attack surfaces with mobile devices and IoT. Major breaches like Sony in 2014 and Equifax in 2017 highlighted cybersecurity’s impact on privacy and security. AI and machine learning also began enhancing threat detection.

The 2011 Stuxnet attack on Iran's Natanz nuclear facility was pivotal, showing that cyberattacks could cause physical damage. This sophisticated attack reshaped national approaches to cyber defense.

The rise of cloud computing transformed data storage and processing, providing flexibility but introducing new security challenges like data privacy and compliance. Companies adapted with specialized cloud security protocols.

Digital transformation, with IoT, AI, and big data, has expanded the attack surface, creating new cybersecurity challenges. Companies now invest in stronger security protocols, employee training, and incident response plans to counter evolving threats.

In summary, cybersecurity has evolved with technological advances and emerging threats, from the Morris Worm to cloud computing and digital transformation. Looking forward, innovations like quantum computing and blockchain will further strengthen defenses.

Slide 5 — What is Cybersecurity

Now, let’s focus on the core concept of cybersecurity. In today’s digitally driven world where technology touches every aspect of human lives, cybersecurity has emerged as a critical concern for people, organisations and countries. The reliance on digital systems has transformed how people communicate, conduct business and manage their personal lives, offering unprecedented convenience and efficiency. However, digital transformation also brings with it significant risks and challenges that cannot be ignored.

In the context of Information technology, the term "cybersecurity" consists of two words — "cyber" and "security." Each of these words has a specific meaning that together define the scope and goal of cybersecurity.

The word "cyber", originates from "cybernetics", refers to the science of communication and automatic control systems in both machines and living organisms.

In the IT context, "cyber" refers to the digital world, all digital aspects involving computers, networks, software, the internet, and all associated technologies, cyberspace, the virtual environment created by interconnected computer networks that serves as the global framework for sharing and accessing data, enabling seamless interaction between individuals, organizations, and systems worldwide and connected technologies, more precisely all devices and technologies that connect and communicate via the network, including smartphones, computers, servers, Internet of Things devices and other digital systems.

On the other hand, the word "security" in the IT context refers to data protection, preserving the confidentiality, integrity and availability of information, system protection, maintaining the functionality and security of computer systems and networks, and threat prevention and response, more precisely, proactive and reactive measures to detect, prevent and respond to cyber threats which includes the use of security tools, procedures and policies to manage security incidents.

Combined, "cybersecurity" refers to the protection of digital space and all connected systems, devices and data from cyber threats.

Slide 6 — Definition of Cybersecurity

In simple terms, cybersecurity refers to the protection of our digital world, including computers, networks, software, and internet-related activities. As our reliance on digital systems grows, from conducting business to managing our personal lives, the risks and challenges associated with it also increase.

Imagine a world where sensitive data is routinely stolen, businesses are paralyzed by ransomware and critical infrastructure is sabotaged by malicious actors. This is not a distant dystopian future but an ongoing present reality that many have already faced. Small and medium-sized enterprises, often lacking robust security measures, are particularly vulnerable. They become easy targets for cybercriminals who exploit their

limited resources and knowledge, resulting in significant financial losses, reputational harm, and in many cases, business closure.

Slide 7 — Understanding Cybersecurity

Cybersecurity covers a wide range of practices, from protecting data integrity and ensuring privacy to protecting networks and systems against unauthorized access. It demands a collaborative effort across all levels of society, combining technical solutions with the promotion of a culture of awareness and constant vigilance.

This lecture series aims to provide a thorough overview of what cybersecurity entails for SMEs, highlighting its importance, the different types of threats they face and the measures that can be taken to protect against them. By understanding the key concepts and challenges of cybersecurity, SMEs can better prepare themselves to navigate the digital world safely and securely.

Slide 8 — The Goal of Cybersecurity

As already stated, cybersecurity is a vast and ever-evolving field dedicated to safeguarding systems, networks, and programs from digital attacks. These attacks typically aim to gain unauthorized access to sensitive data, alter or destroy information, extort money, or disrupt regular business operations.

Now, let’s dive into what we mean by 'cybersecurity.' At its core, cybersecurity is the practice of protecting internet-connected systems, including hardware, software, and data, from cyberattacks.

The goal of cybersecurity is to protect the confidentiality, integrity, and availability of information. This is done by implementing security measures that prevent unauthorized access to sensitive data, maintain its accuracy and consistency over time, and ensure that authorized users can access the information promptly and reliably when required.

Slide 9 — Cybersecurity Key Components

Also, cybersecurity is composed of several key components, technical security which involves protecting networks, computer systems, and applications using tools like firewalls, antivirus software, and encryption, physical security referring to protection of physical devices and infrastructure from unauthorized access using measures as security cameras, locks, and access control systems, and last but not least, administrative security which involves policies, procedures, and guidelines that regulate the use and protection of information resources, including security policies and incident response plans.

Slide 10 — Importance of Cybersecurity

Now, we’ll discuss why cybersecurity is crucial for small and medium-sized enterprises (SMEs). With limited resources, SMEs are more vulnerable to the severe impacts of cyber incidents. Here’s why cybersecurity is essential for these businesses.

First, let's talk about Financial Protection. Cyber attacks can cause significant financial losses for SMEs, with average costs ranging from $84,000 to $148,000 due to data theft or ransom payments. Business interruptions can worsen these losses, temporarily or

permanently halting operations. Recovery expenses and lost productivity during downtime can also severely impact small businesses.

Next, let's move on to Reputation Protection. Trust is crucial for SMEs. A security breach can harm client trust and partner relationships, which are vital for their success. Weak security can damage reputation with lasting effects, but proactive communication about measures helps maintain trust.

Now, let's consider Legal Compliance. Compliance is essential, not just a best practice. Regulations like GDPR ensure data privacy, with non-compliance risking fines and legal action. Some industries like healthcare and finance have stricter standards, and proper certifications build client trust and open market opportunities.

Lastly, we have Business Continuity. For SMEs, maintaining operations is crucial. Cyber attacks disrupting essential systems can be devastating, particularly with limited resources. Recovery planning reduces impact and speeds up business restoration, while redundancy, such as backups, ensures continuity.

In summary, cybersecurity is not just a technical issue for SMEs—it's about safeguarding their finances, reputation, legal compliance, and operational continuity. For small businesses, a strong cybersecurity strategy can mean the difference between recovery and severe setbacks after an incident.

Slide 11 — Conclusion

In conclusion, cybersecurity is vital in our digital world, shielding individuals, organizations, and nations from evolving threats. Understanding its history, threats, and goals is key to creating strong defenses, especially for vulnerable SMEs. Join us for the next modules, where we'll address challenges, solutions, and best practices to help you confidently tackle cybersecurity.Thank you for your attention.

CORPORATE DIGITAL RESPONSIBILITY

Cybersecurity Ecosystem

Dr. Tomislav Horvat
University North, Croatia

Transcript 9 | Voice-over script

Slide 1 — Module 1: Cybersecurity Ecosystem

Welcome to the second part of Module 1, which continues our introduction to cybersecurity. In the first part of Module 1, we discussed the basics of cybersecurity, focusing on its definition, importance, and evolution. We also examined the role of hackers, their different types, and how their activities shape cybersecurity challenges.

My name is Dr. Tomislav Horvat, an assistant professor at University North, Croatia.

Slide 2 — Cybersecurity ecosystem

To understand the broader landscape of cybersecurity, we need to explore what is known as the cybersecurity ecosystem and what exactly does this ecosystem include.

A cybersecurity ecosystem is defined as a complex network of interconnected software, hardware, network resources, and users that function together as a cohesive unit. This ecosystem encompasses a wide array of components, including applications, operating systems, devices, cloud services, and the interactions between them. It's not just about the technology—it's also about the people involved, such as developers, end-users, service providers, and other stakeholders like ethical hackers who contribute to and use these technologies.

The cybersecurity ecosystem seeks to create a seamless, integrated environment that enhances functionality, user experience, and innovation. However, challenges like security vulnerabilities, data privacy concerns, and reliance on specific technologies can lead to monopolistic practices, restricting competition and innovation.

As already stated, the ecosystem of cybersecurity is a complex and interconnected network of technologies, processes and stakeholders aimed at protecting digital assets from cyber threats. While ecosystems can be intricate, we'll streamline our focus to five key areas: Threat Actors, Cyber Threats, Security Measures, Regulations and Standards, and Incident Response.

Slide 3 — Threat Actors

First, Threat Actors—these are the drivers behind cyber incidents, and include the following groups or individuals:

Cybercriminals, individuals or groups who seek financial gain through various illegal activities, often exploiting vulnerabilities for monetary profit.

Hacktivists, individuals or groups who leverage hacking skills for activism, targeting systems to make political or social statements.

Nation-state actors, individuals or groups who operate with the backing of governments, engaging in cyber espionage or disruptive activities aimed at influencing global politics.

Insiders, also individuals or groups who remain a significant risk, as they may, whether intentionally or by accident, leak information or disrupt systems.

Slide 4 — Cyber Threats

Next, Cyber Threats, which encompass the tools and tactics used to breach systems such as 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 into revealing sensitive information like passwords or financial details, Ransomware, type of malware that encrypts a victim's data and demands payment for the decryption key to restore access, and finally DDoS attacks, attacks that overwhelm a network or server with excessive traffic, causing it to become slow or unavailable to legitimate users.

Slide 5 — Security Measuers

In terms of Security Measures part of cybersecurity ecosystem are Firewalls and Intrusion Detection Systems (IDS) which form the first line of defense by monitoring and filtering traffic to detect and prevent unauthorized access. Encryption ensures that even if data is intercepted, it remains unreadable without the correct decryption key and finally Antivirus software which plays a crucial role in identifying and removing malicious software from individual systems.

Slide 6 — Regulations and Standards

The next key area of the cyber security ecosystem are Regulations and Standards which guide the organizations how to manage cybersecurity. Regulations like GDPR and HIPAA enforce strict data protection and privacy protocols while standards such as PCI-DSS and ISO/IEC 27001 set the framework for secure handling of sensitive information, ensuring that companies maintain robust information security practices.

Slide 7 — Incident Response

Lastly, let's touch on Incident Response, the critical process of managing security incidents which consists of few steps. Detection is the first step during which identifying anomalies that indicate a potential breach is crucial. From there, containment and eradication focus on isolating the threat and removing its cause. Recovery restores systems to normal operation, ensuring they are secure and functional, while post-incident analysis is key for learning from each event, identifying gaps, and improving future response strategies.

Focusing on these five areas clarifies cybersecurity dynamics and their impact on system security, with real-world scenarios and advanced strategies shaping our approach.

Slide 8 — Estimated Global Costs of Cybercrime

Now, let's focus on estimated global costs of cybercrime. Statista estimates global cybercrime costs have soared from $860 billion in 2018 to a projected $23.84 trillion by 2027, underscoring the need for stronger cybersecurity. These costs include direct expenses like ransom and indirect losses such as legal fees, productivity loss, and reputational damage, making robust cybersecurity essential.

Increasing complexity of cyber threats makes investing in cybersecurity essential for protecting data, minimizing losses, maintaining trust, and ensuring resilience. Proactive steps like updates, advanced threat detection, and incident response plans help reduce risks, making cybersecurity a priority in the digital era.

Slide 9 — Cyber Insurance

As digital threats become more sophisticated, cyber insurance has emerged as a key strategy for managing risk in today's digital age. Let's break down what it is, what it covers, and why it's so critical.

What is Cyber Insurance? It's coverage that protects against the costs of cyberattacks, including recovery, legal fees, and reputational damage. It's become essential as more organizations rely on digital systems.

Key Components of the Cyber Insurance are Liability Coverage which covers legal costs from lawsuits, settlements, and fines after a data breach, especially when customer data or intellectual property is exposed.

Then First-Party Coverage. It handles direct losses like data recovery, system repairs, business interruption, and even ransom payments.

Incident Response Support. It offers access to cybersecurity experts, legal counsel, and PR professionals during and after a breach, helping restore normal operations quickly.

And finally Risk Management. Insurers often provide risk assessments and resources, like employee training and security audits, to help prevent future incidents.

As we can see Cyber insurance helps organizations manage the financial, operational, and reputational impacts of cyber incidents, enabling faster recovery and is essential for modern risk management as cyberattacks increase.

Slide 10 — Conclusion

In conclusion, cybersecurity is vital in today's interconnected world, safeguarding information, preventing losses, and maintaining trust. As threats grow, neglecting security costs more than investing in it. Proactive measures reduce risks, fostering trust and safety. Let's build on these principles in the next modules. Thank you for your attention.

CORPORATE DIGITAL RESPONSIBILITY

Cyber Threats vs. Cyber Attacks

Dr. Tomislav Horvat
University North, Croatia

Transcript 10 | Voice-over script

Slide 1 — Module 2: Cyber Threats vs. Cyber Attacks

Welcome back to our cybersecurity series. In this second module, we'll delve into a critical aspect of cybersecurity: understanding the differences between cyber threats and cyber attacks. Recognizing these distinctions is essential for building an effective defense strategy, as it allows you to anticipate potential risks and respond more proactively.

I'm Dr. Tomislav Horvat, an assistant professor at University North, Croatia, and I'll be guiding you through this session as we explore how threats and attacks differ, the typical sources of each, and how this knowledge can strengthen your organization's cybersecurity approach. Let's get started!

Slide 2 — Cyber Threats vs. Cyber Attacks

First, it's crucial to understand the difference between cyber threats and cyber attacks to build a solid cybersecurity foundation. Cyber threats represent potential risks—anything that could endanger information systems or data, such as malware, phishing schemes, software vulnerabilities, or social engineering tactics. These threats are passive in nature, holding the potential for harm without directly causing it.

On the other hand, cyber attacks are deliberate actions taken by individuals or organizations to exploit these threats. Unlike passive threats, attacks are active and intentional, aiming to disrupt, damage, or steal information. Examples include ransomware attacks, where data is held hostage, and DDoS attacks, which overwhelm systems to deny access.

By distinguishing these two concepts, you gain insight into both the passive and active elements of cybersecurity, setting the stage for identifying and responding to risks effectively.

Slide 3 — Cyber Threats Types

Now, let's focus on basic cyber threats types. As already mentioned, cyber threats can take many forms, each with distinct features and potential consequences.

In cybersecurity, we categorize the primary types of cyber threats into five main groups: malware, phishing, social engineering, distributed denial of service (DDoS) attacks, and insider threats. Each of these categories represents a unique approach to compromising systems and data, and understanding them is crucial for effective defense.

Slide 4 — What is Malware

Now, let’s begin with the first type of cyber threat - malware.

Malware, short for "malicious software," is designed to harm, steal data, or disrupt normal computer operations. It comes in various forms, each with specific methods of attack.

Viruses - These attach to legitimate programs and spread whenever those programs are executed. They require user interaction to propagate.

Worms - Unlike viruses, worms are self-replicating and spread across networks independently, without needing user action.

Ransomware - This type of malware encrypts data on infected systems and demands a ransom payment to decrypt the data.

Spyware - Spyware works covertly, tracking and recording user activities without their awareness, often used to steal sensitive information.

Slide 5 — Examples of Malware Attacks

Throughout history there are many examples of malware attacks. Now we will mention only the most significant ones to raise awareness about the importance of defense against such attacks.

The most famous example of malware attack is definitely WannaCry from 2017. This was a massive ransomware attack that affected thousands of computers worldwide. WannaCry exploited a vulnerability in the Windows operating system to spread. Once it infected a machine, it encrypted the files and displayed a message demanding a payment in cryptocurrency to unlock them. Not only did it encrypt data, but it also rendered the computers unusable, essentially locking users out until the ransom was paid or the system was restored from a backup.

Another example is ILOVEYOU (2000), one of the most damaging viruses of its time. It spread via email with the subject line ‘ILOVEYOU’ and an attachment named ‘LOVE-LETTER-FOR-YOU.txt.vbs.’ Once opened, the virus ran a script that overwrote files, including images and documents, and then sent itself to all contacts in the user’s address book. This caused severe data loss, system instability, and major network slowdowns due to the flood of emails. Both individuals and businesses were affected, leading to significant financial and operational disruptions.

These examples highlight the variety and severity of cyber threats and the importance of preventive measures and regular backups to mitigate such risks.

Slide 6 — What is Phishing?

Next is phishing, a 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. Phishing attacks often appear to be from trusted sources, making them particularly dangerous.

The primary types of phishing include:

Email Phishing - Generic fake emails that appear to be from reputable organizations.

Spear Phishing - Highly targeted phishing attempts aimed at specific individuals or organizations, often using personalized information.

Whaling - Phishing attacks directed at high-ranking individuals within organizations, such as executives, due to the potential for high-value information.

Slide 7 — Example of Phishing Attacks

Throughout history there are many examples of phishing attacks.

A notable example of phishing is the PayPal Phishing Scam. In this case, attackers sent emails that appeared to be from PayPal, urging recipients to verify their accounts or warning that their accounts had been compromised. When users clicked on the link, they were redirected to a fake website mimicking PayPal's login page. Upon entering their credentials, victims unknowingly gave attackers access to their accounts, leading to unauthorized transactions and potentially even identity theft. This scam not only led to financial losses and privacy issues for the victims but also underscored the importance of user awareness in detecting phishing threats.

This example shows how phishing can result in both financial damage and loss of personal information, stressing the importance of vigilance and education to recognize and respond to suspicious communications.

Slide 8 — What is Social Engineering?

Another type of cyber threats is social engineering. Social engineering is a type of cyber threat that manipulates individuals into revealing sensitive information or performing actions that compromise security. Rather than exploiting technical vulnerabilities, social engineering takes advantage of human psychology to breach defenses.

Key tactics used in social engineering include:

Pretexting - The attacker creates a fabricated scenario to obtain confidential information by pretending to be someone trustworthy.

Baiting - The attacker offers something desirable to lure the victim into providing sensitive information.

Tailgating - The attacker physically follows an authorized person into a secure area without proper access credentials.

Slide 9 — Example of Social Engineering

A common example of social engineering is phone scams, where 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. Once in, attackers can install malware, steal information, or demand payment for fake repairs. Victims often suffer financial losses, identity theft, and emotional distress, while also losing trust in legitimate tech support services.

This example highlights how social engineering can cause severe financial and emotional harm, emphasizing the need for awareness and caution when dealing with unsolicited calls or offers.

Slide 10 — What is Distributed Denial of Service (DDoS)?

Next are Distributed Denial of Service (DDoS) attacks. DDoS attack uses numerous infected devices, known as a botnet, to flood a target system with fake traffic, making it inaccessible to legitimate users. DDoS attacks come in several types:

Volumetric Attacks: These flood the network with large volumes of fake traffic.

Protocol Attacks: These exploit weaknesses in network protocols to overwhelm resources.

Application Layer Attacks: These target specific applications or services within the system.

Slide 11 — Example of DDoS Attack

A well-known example is the 2016 Dyn Attack, which targeted the DNS provider Dyn using a botnet of IoT devices infected with Mirai malware. This led to 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.

Slide 12 — What is Insider Threats?

Last but not least are 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. These threats are divided into two types:

Malicious Insiders: Individuals who intentionally seek to harm or steal information from the organization.

Unintentional Insiders: Individuals who inadvertently compromise security through negligence or lack of awareness.

Slide 13 — Example of Insider Attack

A key example of an insider threat is Edward Snowden in 2013. As a former NSA contractor, he leaked top-secret documents on U.S. government surveillance, including metadata collection and access to data from companies like Google and Facebook. His actions 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.

Slide 14 — Interesting Facts About Cyber Threats

Now, let's focus on some interesting facts about cyber threats and real-world examples that highlight their impact, especially on small and medium-sized enterprises (SMEs).

Let's start with interesting facts. Every day, over 350,000 new malware samples are detected, illustrating the rapid growth of malicious software. Phishing remains a major concern, with about 12% of users clicking on phishing links, often leading to data breaches. Social engineering is another prominent threat, accounting for 70% to 90% of all malicious data breaches. DDoS attacks are disruptive, with an average duration of 12 hours, and insider threats can be costly, with an average incident cost of $11.5 million.

Slide 15 — Example of Ransomware Attack

To understand these threats better, let’s look at some additional real-world examples:

Ransomware Attack on ABC Manufacturing: A phishing email led to a ransomware attack that encrypted critical data, halting production for days and costing $50,000 in ransom. Key takeaways include the need for employee training on phishing awareness, multi-factor authentication, and regular data backups.

Data Theft at XYZ Marketing: A disgruntled former employee stole sensitive client data and sold it to a competitor, resulting in financial losses and reputational damage. This incident underscores the importance of promptly revoking access for terminated employees, implementing role-based data access, and regularly reviewing security policies.

DDoS Attack on E-Shop Ltd.: A botnet flooded this retailer’s servers, disrupting online sales and affecting customer trust. This example highlights the need for DDoS protection, regular resilience testing, and scalable IT infrastructure.

These facts and examples remind us that cyber threats are real and that proactive measures can significantly reduce their impact on businesses.

Slide 16 — Conclusion

In conclusion, this module has explored the critical differences between cyber threats and cyber attacks, providing insights into their characteristics, examples, and potential impacts. Understanding these concepts is essential for building effective defense strategies and fostering awareness of the evolving cybersecurity landscape. By examining real-world examples like WannaCry, ILOVEYOU, and the Dyn Attack, we've highlighted the importance of vigilance, preventive measures, and robust security practices.

Thank you for joining this session. In the next module, we’ll dive into Security Architecture and Protective Measures, where we’ll explore the frameworks and strategies that underpin a strong cybersecurity defense. See you then!

CORPORATE DIGITAL RESPONSIBILITY

Security Architecture and Protective Measures

Dr. Tomislav Horvat
University North, Croatia

Transcript 11 | Voice-over script

Slide 1 — Security Architecture and Protective Measures

Welcome back to our cybersecurity series. In Module 3, we covered the key differences between cyber threats and cyber attacks, their sources, and their role in strengthening cybersecurity strategies.

Now, we'll focus on security architecture and proactive measures, exploring how to build defenses and prevent risks from escalating into attacks.

I'm Dr. Tomislav Horvat, an assistant professor at University North, Croatia. Together, we'll explore how a well-structured security framework and proactive planning can significantly enhance your organization's cybersecurity resilience. Let's get started!

Slide 2 — Security Architecture

There are many different ways to defend against cyber threats, and today's focus is on some of the most critical tools like firewalls - a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules, antivirus software - a program designed to detect, prevent, and remove malware from computers and networks, and intrusion detection and prevention systems, shortly IDS and IPS, - security tools designed to detect and respond to unauthorized or malicious activities on a network. These technologies form the core of a strong security architecture, offering protection against both internal vulnerabilities and external threats.

Slide 3 — Firewalls

Let's start with firewalls. Firewalls act as the first layer of defense by creating a barrier between trusted internal networks and external, untrusted sources. Their primary role is to manage network traffic, ensuring only authorized access is permitted.

There are several types of firewalls, each tailored to specific security requirements. For instance, packet-filtering firewalls examine and block unauthorized data packets, while stateful inspection firewalls track the state of active connections. Next-generation firewalls (NGFWs) go a step further, offering advanced capabilities such as inspecting encrypted traffic and integrating intrusion prevention systems.

Slide 4 — Antivirus Software

Next on the list is antivirus software, a vital tool for detecting and removing malware, including viruses, ransomware, and spyware.

Antivirus solutions use methods like signature-based detection, which identifies known threats. For example, a financial firm uses antivirus software to detect and remove known threats.

On the other hand, heuristic-based detection antivirus software analyzes behavior to uncover new or unknown threats. For example, a tech startup can use antivirus software to block unknown threats.

Real-world applications showcase how these tools prevent both common and sophisticated attacks.

Slide 5 — Intrusion Detection and Prevention Systems (IDS/IPS)

Moving forward, intrusion detection and prevention systems (IDS/IPS) come into play. IDS monitors network traffic for unusual activity, flagging potential threats, while IPS goes a step further by blocking these threats in real time.

There are two types of Intrusion Detection and Prevention Systems. Network-Based IDS/IPS which monitor traffic across the network, identifying suspicious activity that may indicate an attack. These systems can detect a wide range of attacks by analyzing network traffic patterns and anomalies.

The second type is Host-Based IDS/IPS, which monitors activities on individual devices to detect threats at the host level. It identifies issues like unauthorized file changes or suspicious processes and is effective against insider threats and non-network-based attacks.

Whether network-based or host-based, these systems provide a critical layer of security, ensuring that malicious activity is detected and stopped before it causes harm.

Slide 6 — Backup, data recovery, and network security management

After introducing the essentials of firewalls, antivirus programs, intrusion detection and prevention systems, we now move on to another critical set of topics in security architecture: backup, data recovery, and network security management. These elements are vital for ensuring the resilience of IT systems and minimizing the impact of cyber incidents.

Let’s start with backup, which is the process of creating copies of data to prevent its loss due to hardware failure, cyberattacks, or accidental deletions.

Effective backup strategies include full backups, which create a comprehensive data copy; incremental backups, which save only the changes since the last backup; and differential backups, which capture all changes since the last full backup. Best practices, like the 3-2-1 rule, ensure backups are stored across different media and locations, safeguarding data even in the face of catastrophic events.

Slide 7 — Data Recovery

Next security architecture issue is data recovery. Data recovery is about restoring lost or corrupted data from backups. A robust recovery plan ensures that organizations can quickly resume operations after an incident. Regularly testing recovery procedures is critical to ensure that systems function correctly when recovery is required, minimizing downtime and operational disruption. Here’s a fun fact: Did you know that 30% of people

have never backed up their data? It’s a surprising statistic, especially when you consider how much we rely on our devices and data every day.

Again, the best solution has proven to be the 3-2-1 rule, a widely recommended backup strategy. It ensures data protection by maintaining multiple copies across different locations and media types, effectively safeguarding against various types of failures.

Slide 8 — Network Security Management

Moving forward, network security management encompasses measures to protect a network from unauthorized access and attacks.

Let’s talk about some key security measures, starting with network segmentation, which involves dividing a network into isolated sections. This approach helps contain potential breaches and limits their impact on other parts of the network.

Next is encryption, a method for securing data by ensuring that it cannot be accessed without the appropriate decryption keys, keeping sensitive information safe even if intercepted.

We also have VPNs (Virtual Private Networks), which create secure, encrypted communication channels—especially important for remote users accessing company resources.

Finally, there are access control policies, which regulate user access to sensitive resources based on their roles and permissions, ensuring that only authorized personnel can access critical information.

Slide 9 — Preventive Measures

Building on previous discussions about firewalls, antivirus programs, intrusion detection and prevention systems, backups, and network security management, we now turn our attention to the broader concept of protective measures and their integration into a cohesive cybersecurity strategy.

Each element—detecting threats, securing networks, or ensuring data recovery—forms a multi-layered defense. These components must align within a comprehensive framework to address organizational vulnerabilities. Firewalls and intrusion detection and prevention systems prevent unauthorized access, while backups ensure critical data remains secure and accessible after incidents.

Slide 10 — Prevention Measures (2)

In addition to these technologies, preventive measures play a crucial role in strengthening an organization's cybersecurity posture:

Employee education is essential for reducing human errors and mitigating risks such as phishing and social engineering. Regular training sessions help staff recognize and respond to cyber threats effectively.

Regular system and software updates ensure that vulnerabilities are patched promptly, reducing the risk of exploitation. Automated update systems are particularly effective in maintaining up-to-date security.

Log monitoring and analysis provide early detection of potential threats. Using tools like Security Information and Event Management (SIEM) systems helps identify patterns or anomalies, enabling swift responses.

Security system testing, such as penetration tests and simulations, ensures that current measures are effective and highlights areas needing improvement.

These steps emphasize building a proactive cybersecurity culture where employees contribute to threat awareness and prevention, fostering resilience and reducing attack risks.

Slide 11 — Conclusion

Cybersecurity is an ongoing process, requiring constant adaptation through monitoring, assessments, and policy updates to keep defenses effective.

In conclusion, combining advanced strategies with preventive measures enables organizations to build resilient security. This holistic approach ensures asset protection and operational stability. Thank you for watching. In the next module, we will examine two detailed examples that illustrate the practical application of cybersecurity strategies.

See you then!

CORPORATE DIGITAL RESPONSIBILITY

Cybersecurity in SMEs: Case Studies

Dr. Tomislav Horvat
University North, Croatia

Transcript 12 | Voice-over script

Slide 1 — Cybersecurity in SMEs (case studies)

Welcome back to our cybersecurity series. So far, we've explored key cybersecurity concepts, including firewalls, antivirus software, IDS/IPS, backups, and network security management, focusing on building a strong theoretical foundation.

Today, we'll shift from theory to practice by examining two case studies: SweetBites Bakery and TechRise Solutions. These examples will demonstrate how cybersecurity principles can be applied in small and medium-sized enterprises to address unique challenges and protect their operations.

I'm Dr. Tomislav Horvat, an assistant professor at University North, Croatia, and I'll guide you through these examples of implementing cybersecurity strategies in SMEs. Let's get started!

Slide 2 — SweetBites Bakery

First, let's start with the example of SweetBites Bakery, a family-owned business that began with a simple goal: to make and sell homemade cakes locally. Initially, it operated out of a home kitchen, relying on word-of-mouth to attract customers.

However, as the bakery's popularity grew, the family decided to expand by creating an online presence. They launched a website, started taking online orders, and actively engaged with customers through social media platforms like Instagram and Facebook.

As their online business grew, SweetBites opened a successful physical store with public Wi-Fi, QR code menus, and an online reservation system, but this expansion brought challenges in managing customer data and securing both digital and physical operations.

SweetBites Bakery's growth mirrors many small businesses, facing risks like data breaches, public Wi-Fi vulnerabilities, and website threats. This case study examines their cybersecurity strategy to protect operations and maintain customer trust.

Slide 3 — Cybersecurity Plan

Next, we'll present a 5-step cybersecurity plan for SweetBites Bakery. This plan starts with basic security practices to counter immediate threats and evolves to manage complex risks, ensuring protection of operations and assets from cyber threats.

Let's start with the first step in SweetBites Bakery's cybersecurity plan: Securing Passwords and User Access. This involves using strong passwords, enabling two-factor authentication (2FA), and implementing role-based access control (RBAC) to limit access to necessary systems. Tools like password managers and individual accounts further enhance security and simplify access management.

The second step is Protecting the Website, Online Shop, and Reservation System. SweetBites Bakery should use SSL certificates, a Web Application Firewall (WAF), and regularly update software to safeguard against threats like SQL injection and XSS, protecting customer data and operations.

The third step is Securing the Network and Public Wi-Fi by segmenting public traffic from internal systems, ensuring customer activities don't affect sensitive systems, and using WPA3 encryption and VLANs for added security.

The fourth step is Regularly Backing Up and Protecting Data. Automated backups of critical information, stored locally and in the cloud with encryption, ensure data recovery after incidents like ransomware or hardware failures. Regular testing prevents data loss.

The fifth step is Training Employees and Monitoring Security. Regular training on phishing and secure practices, along with simulations, keeps employees prepared, while system monitoring ensures quick threat detection and response.

By following these five steps, SweetBites Bakery can build a robust cybersecurity framework that evolves with its growth, ensuring both digital and physical operations remain secure against a wide range of cyber threats.

Slide 4 — TechRise Solutions

The next example is TechRise Solutions. TechRise Solutions started as a small, family-run technology business focused on delivering custom software to local clients, operating from a garage with a few computers and a basic network.

First, as the company gained clients, it expanded by hiring employees and adopting cloud infrastructure to meet data needs, introducing vulnerabilities like securing client information and cloud protection.

Next, with the team growing to 50 employees, many working remotely, the cybersecurity landscape became more complex. The company had to focus on securing remote work environments, ensuring compliance with industry regulations, and defending against advanced cyber threats.

Finally, TechRise transitioned from a small, local operation to a thriving technology company with a national client base. This growth required implementing a comprehensive cybersecurity strategy to protect its cloud infrastructure, web applications, and increasing digital assets.

Slide 5 — Cybersecurity Plan

In conclusion, we've covered four comprehensive modules that provided a strong theoretical foundation in cybersecurity, exploring key concepts, threats, and protective measures. Through the case studies of SweetBites Bakery and TechRise Solutions, we demonstrated the practical application of these principles, from securing systems and data to training employees and managing risks. This holistic approach equips businesses with the knowledge and tools to strengthen their digital defenses and ensure operational resilience.

Thank you for your attention and engagement. I hope this series has been insightful and provided practical tools to enhance your cybersecurity understanding and build stronger defenses.

CORPORATE DIGITAL RESPONSIBILITY

Digital Inclusion and Accessibility

Josip Hrgović
University North, Croatia

Transcript 13 | Voice-over script

Slide 1 — Introduction

Hello everyone, and welcome!
My name is Josip Hrgović, and I'm a teacher at University North. I've always been fascinated by how new technologies influence our everyday lives and shape our behavior—especially when it comes to ethical decision-making. This curiosity guided me toward exploring Corporate Digital Responsibility, where businesses of all sizes, from large corporations to small and medium-sized enterprises, share the responsibility of using digital tools ethically and transparently.

In today's talk, I will focus on Digital Inclusion and Accessibility, and highlight how these aspects are crucial for everyone to benefit from current technological advancements. Whether it's designing websites that people of all abilities can use or ensuring fair access to digital resources, we must keep responsibility at the forefront of innovation. In this sense, SMEs play a pivotal role: they are the backbone of many economies, and their active participation in inclusive and ethical digital practices can significantly influence the well-being of both customers and communities.

I'm excited to share my insights and look forward to hearing your perspectives as we explore how ethical, inclusive technology can lead to more responsible and sustainable growth—both for individuals and for organizations of all sizes. Thank you for joining me, and let's get started!

Slide 2 — What is Digital Inclusion and Accessibility?

Let's start by looking at the meaning of these two terms. Digital Inclusion basically means making sure that everyone—no matter where they live, how much money they make, or what their physical or cognitive abilities might be—can enjoy the benefits of modern technology. Accessibility is closely related, but focuses more on designing digital products and services so people with different needs or disabilities can use them easily. When we put these ideas together, our goal is clear: technology should be available and user-friendly for absolutely everyone.

Now, let's talk about some practical ways to make this happen. I want to share a few approaches that any organization—whether we're talking about large corporations or small and medium-sized enterprises (SMEs)—can follow:

Make Your Website Accessible

Use clear headings and descriptive text, so screen readers can help visually impaired users find what they need.

Include alternative text (alt text) for images, so people who can't see the images can still get the information.

Check that your colors and fonts are easy to read, and that pages can be navigated using just a keyboard.

Provide Alternative Formats

If you have videos, offer captions or transcripts for viewers who can't hear audio.

Give people different file formats for documents (like PDF or Word) to accommodate various devices and screen readers.

Design for Different Devices and Connection Speeds

Make sure your websites and apps work smoothly on mobile phones, because that's the only internet access some folks have.

Keep your pages lightweight and fast to load, as not everyone has a strong internet connection.

Education and Training

Offer basic digital skills training for anyone who might need it, including your customers, employees, or local community members.

Provide step-by-step instructions or video tutorials so people can learn at their own pace.

Use Clear, Inclusive Language

Write in plain, understandable language without too much jargon.

Consider offering content in multiple languages if you're serving diverse communities.

Test with Real Users

Invite people with different abilities to try out your website or app and then gather their feedback.

Use that feedback to make improvements, because real-world input is the best way to uncover what might not be working well.

Adopt Accessibility Policies and Standards

Familiarize yourself with guidelines like the Web Content Accessibility Guidelines (WCAG) to ensure you're on the right track.

Incorporate these guidelines early in your planning, so accessibility isn't just an afterthought.

Collaborate with Experts

Don't be afraid to ask for help from accessibility consultants, nonprofits, or advocacy groups. They can offer valuable insights and advice.

Join industry forums or groups focused on inclusive design to learn about best practices.

Offer Multiple Support Channels

Make it easy for people to reach you—whether that's by phone, chat, email, or social media—so everyone can choose the option they prefer.

Train your customer support teams to understand assistive technology, so they know how to help users who need specific accommodations.

Continuous Improvement

Keep track of where users run into trouble by looking at analytics or simply asking for feedback.

Remember, technology changes fast, so stay updated on new tools and standards that can help you remain accessible.

What's great about these steps is that they benefit everyone. When we ensure our digital products and services are easier to use, we're not only supporting people with specific needs; we're also creating a better user experience for all. And small and medium-sized enterprises, in particular, have the agility to adopt these practices quickly and set an example that can spread throughout their communities.

By staying committed to Digital Inclusion and Accessibility, we make our digital world more open and equitable, while also strengthening our organizations' reputations and relationships with the people we serve. Ultimately, it's about creating a future where no one feels excluded from the possibilities technology can offer.

Slide 3 — Why is Digital Inclusion Important for SMEs?

Now, let's talk about why Digital Inclusion and Accessibility matters so much for SMEs in the European Union.

First off, the EU is a highly diverse environment. We have people from different cultural backgrounds, speaking multiple languages, and experiencing varied levels of digital literacy. Across all member states, the aim is to make sure that nobody is left behind in the digital age.

1. Meeting Legal and Policy Requirements

In the EU, there's a growing focus on legislation and standards that push for accessibility in both public and private sectors. You might have heard of initiatives like the European Accessibility Act or the Web Accessibility Directive—these require organizations to make their digital services accessible to all users, including those with disabilities. While these rules mainly apply to public sector bodies, they also create a broader culture of accessibility that SMEs should be mindful of to stay competitive and avoid future legal pitfalls.

2. Tapping into a Larger Customer Base

By investing in digital inclusion, SMEs can open their doors to potentially millions more people who might otherwise struggle to access goods or services. Think about seniors who might have difficulty navigating complicated websites, or people with visual or hearing impairments who need adapted content. Making your website and apps user-friendly for them doesn't just meet an ethical obligation—it can expand your reach and win new customers across the continent.

3. Boosting Reputation and Customer Trust

European consumers increasingly care about how companies treat their customers and communities. When SMEs prioritize accessibility, it sends a powerful message that they're forward-thinking, customer-centric, and ethical. This can build brand loyalty and trust. In a crowded market, that positive reputation can be a real differentiator—especially for smaller businesses trying to stand out from bigger competitors.

4. Encouraging Innovation

Accessibility often fosters more innovative design. When you're creating apps, products, or websites that need to work for a wide range of users, you and your team start thinking more creatively about user experience. This can lead to ideas that are more intuitive, streamlined, and efficient for everyone—ultimately raising the overall quality of what you offer.

5. Aligning with EU Core Values

In the EU, there's a strong commitment to values like inclusion, diversity, and social cohesion. SMEs, being at the heart of local communities, have an important part to play in turning these values into practical action. By promoting digital inclusion, you help drive the EU's broader mission of strengthening unity and equal opportunity—something that benefits society and the economy at large.

6. Attracting and Retaining Talent

Finally, consider that employees also benefit from an inclusive digital environment. When your internal systems are accessible and user-friendly, you're creating a workplace that appeals to a wider pool of talent. People with varying abilities will feel more comfortable applying for jobs, and you'll see higher satisfaction and productivity among current staff when their tech tools just "work."

In short, making your products and services accessible to all isn't just a nice-to-have—it's increasingly becoming essential for SMEs in the EU. By embracing digital inclusion, you align with European values, broaden your customer base, stand out among competitors, and stay one step ahead of evolving legal requirements. It's truly a win for everyone: your business, your customers, your employees, and the communities you serve.

Slide 4 — Steps for Implementation

Here's a simple, step-by-step roadmap for how a typical European small or medium-sized enterprise (SME) can start making its digital services more accessible to everyone. I'll use everyday language, so it's easy to follow.

1. Assess Your Current Digital Platforms

What to do:

Begin by taking a close look at your website, mobile apps, and any other digital channels you use.

Use free or paid accessibility checkers (like WAVE or Axe) to get an initial idea of where the problems might be.

Note down any pages or functions that users often complain about or that seem confusing.

Why it matters:

This "health check" helps you figure out which parts of your digital presence need the most work right away.

It also gives you a baseline, so you can measure improvements later on.

2. Train Your Team on Inclusion and Compliance

What to do:

Organize short workshops or training sessions about digital inclusion and relevant EU accessibility standards (like the Web Content Accessibility Guidelines, or WCAG).

Encourage everyone—developers, designers, managers, and even customer support—to attend and learn the basics.

Share easy-to-understand guides and checklists.

Why it matters:

Accessibility is a team effort. If only one person knows what to do, it won't stick.

Training ensures everyone uses the same language and understands the same goals.

3. Identify Gaps in Digital Accessibility

What to do:

Compare your "health check" results with accessibility standards.

Figure out what specific issues might be preventing people with disabilities or low digital skills from using your platforms.

Some common trouble spots include hard-to-read text, images without descriptions, or forms that don't work well with screen readers.

Why it matters:

By pinpointing exactly where the problems lie, you save time and resources.

You'll also ensure that the improvements you make have the most impact.

4. Set Goals Aligned with Accessibility Standards

What to do:

Decide on clear, measurable goals—for example, "By the end of this quarter, all images on our website will have alt text," or "We will meet at least WCAG 2.1 Level AA on our main website by year's end."

Break these goals into smaller tasks that can be assigned to specific team members.

Why it matters:

Having realistic, bite-sized targets keeps everyone focused and motivated.

It also makes it easier to track progress and celebrate milestones along the way.

5. Prioritize Actions Based on Impact

What to do:

Look at your list of issues and figure out which problems affect users the most.

Tackle the most urgent or widespread challenges first, such as fixing crucial parts of your website (e.g., main navigation menu, customer login, payment process).

Why it matters:

By focusing on the areas that make the biggest difference, you'll quickly see improvements in user satisfaction.

This also shows your customers and stakeholders you're serious about making changes.

6. Implement Inclusive Design for Products and Services

What to do:

When creating or updating digital products, use inclusive design principles from the start.

Focus on clear layouts, easy navigation, and well-structured content.

Make sure your color choices offer enough contrast, and your fonts are large and clear.

Why it matters:

Inclusive design means creating solutions that work for as many people as possible, right from the beginning.

This reduces the need for major fixes or redesigns later on.

7. Partner with Experts and Stakeholders

What to do:

Consider reaching out to accessibility consultants, local disability advocacy groups, or tech specialists who can provide hands-on support.

Involve community members who have firsthand experience with accessibility barriers and can offer valuable insights.

Why it matters:

Outside expertise can help you avoid common pitfalls and save time.

Bringing real users into the process guarantees you're solving actual challenges, not hypothetical ones.

8. Deploy Tools and Best Practices

What to do:

Put known accessibility features in place, such as:

Alt text for images so screen readers can describe them to visually impaired users.

Keyboard navigation to ensure people who don't use a mouse can still navigate your content.

Transcripts or captions for videos so users who are deaf or hard of hearing can follow along.

Use responsive design techniques so your platform works well on different screen sizes and speeds.

Why it matters:

These core practices are the building blocks of accessible digital platforms.

They're also relatively straightforward to implement, giving you a quick win in your accessibility journey.

9. Test Platforms with Diverse User Groups

What to do:

Invite people with different abilities—like visual or hearing impairments, limited mobility, or even low digital literacy—to test your site or app.

Encourage them to share honest feedback about what works and what doesn't.

Document everything and address the issues.

Why it matters:

Real-world testing shows you how actual users interact with your platform.

It uncovers usability barriers that automated tests or internal reviews might miss.

10. Regularly Review Your Progress

What to do:

Schedule regular check-ins (e.g., monthly or quarterly) to see how you're doing against your goals.

Update team members and stakeholders on what's been fixed, what's still pending, and any new issues that have come up.

Why it matters:

Accessibility is an ongoing effort—it's not something you do once and forget about.

By reviewing regularly, you ensure that progress doesn't stall and that you keep up with new standards or technologies.

11. Gather User Feedback and Continuously Improve

What to do:

Open lines of communication, such as feedback forms on your website or email surveys, where users can report any difficulties.

Keep refining your platforms, adding new improvements, and staying current with the latest accessibility tools.

Why it matters:

Listening to your community helps you stay on track and provides ideas for future enhancements.

Continuous improvement fosters a culture of inclusion, which benefits everyone—customers, employees, and the broader community.

By following these steps—assessing your current situation, training your team, setting clear goals, and continuously testing and improving—you'll create digital platforms that truly work for everyone. This approach not only helps you meet evolving EU accessibility requirements, but it also strengthens your reputation as a business that cares about all of its customers. And in the long run, offering inclusive, user-friendly experiences can open your doors to new markets and opportunities, making it a win-win for both your SME and the diverse communities you serve.

Slide 5 — Conclusion

At the end of the day, Digital Inclusion and Accessibility aren't just buzzwords—they're essential steps toward creating a fair, open, and successful digital environment for everyone. By understanding why inclusion matters, assessing and improving your current platforms, training your team, and continuously seeking feedback, your SME can stay aligned with EU values and emerging accessibility standards.

This process isn't a one-time project—it's an ongoing commitment to ensuring your products and services are easy to use for people of all backgrounds and abilities. Not only does this strengthen trust among customers, employees, and partners, but it also sets

your organization apart as one that genuinely cares about the well-being of its community.

In short, by making digital spaces accessible to all, you create real value for your business while contributing to a more inclusive society—a true win-win for everyone.

CORPORATE DIGITAL RESPONSIBILITY

Digital Sustainability

Josip Hrgović
University North, Croatia

Transcript 14 | Voice-over script

Slide 1 — Introduction

Hello everyone, and thank you for joining me today!
My name is Josip Hrgović, and I'm a lecturer at University North. Over the years, I've explored how technological changes can reshape society and influence our behavior—especially when it comes to making ethical decisions. This path led me to study Corporate Digital Responsibility (CDR), a concept that looks at the ways organizations use technology responsibly and sustainably.

Today, we're focusing on Digital Sustainability—an issue that's especially important for small and medium-sized enterprises (SMEs) in the European Union. In many ways, SMEs are the backbone of the EU economy, and how they adopt digital tools can have a big impact on everything from local communities to broader European policies. By understanding digital sustainability, we can encourage growth and innovation while also respecting the environment, data privacy, and ethical guidelines.

I'm excited to share some insights on how we can balance cutting-edge technology with mindful practices that benefit both our businesses and the societies we serve. So, let's dive in!

Slide 2 — What is Digital Sustainability?

Digital sustainability is all about using technology in a way that not only meets our current needs, but also preserves resources and opportunities for future generations. It's a mindset that encourages us to consider the environmental and social impacts of every digital tool or platform we use. When we talk about digital sustainability, we're really focusing on how to minimize our technological footprint while still taking advantage of all the benefits that innovation can bring.

A key part of this discussion involves energy-efficient IT systems. Imagine if every server and device in our offices were optimized to run using as little power as possible. That might mean switching to more efficient hardware, making sure systems go into sleep or standby mode when they're not in use, or using virtualization to reduce the total number of physical servers you need. In many cases, simply setting up regular maintenance and updates can also help—older, neglected devices often end up wasting more energy than you'd expect. When small and medium-sized enterprises embrace these changes, the cumulative effect across the EU can be huge, both in terms of cost savings and environmental impact.

Another important angle is e-waste management. We live in a world where devices get replaced more quickly than ever, so we end up with piles of outdated phones, laptops, and other gadgets. Digital sustainability asks us to think carefully about what happens to all that hardware. One approach is to extend device lifecycles by repairing or upgrading

components instead of tossing an entire machine. When a device really has reached the end of its life, it's essential to recycle it through certified programs that safely extract reusable materials and handle hazardous elements properly. Doing this prevents harmful substances from ending up in landfills and encourages the reuse of valuable metals and plastics, reducing the need for brand-new resources.

We also need to consider the adoption of sustainable software and cloud solutions. Not all software is created equal—some platforms are designed with efficiency in mind, meaning they use fewer server resources, while others might be massive energy hogs. By picking software that's optimized for lower power consumption and by working with cloud providers that rely on renewable energy, we can dramatically cut back on our environmental footprint. At the same time, cloud computing itself can reduce the number of physical machines an organization needs to maintain, which is particularly beneficial for SMEs that don't always have the budget or space for large-scale data centers.

So, in practical terms, digital sustainability might involve a few key measures. We might start by auditing our current systems to see how much energy they're using and then look for ways to optimize or replace the worst offenders. We can set up clear policies for upgrading and recycling old devices, and make sure we're collaborating with trustworthy e-waste management partners. When choosing new software, we can prioritize solutions that don't require unnecessary power or resources, and if we're moving operations to the cloud, we can opt for providers that demonstrate their commitment to using green energy sources.

For small and medium-sized enterprises within the EU, these steps are particularly important because they contribute to broader sustainability goals set at both the national and European levels. Even small changes, when added up, can make a substantial difference across the continent. Ultimately, digital sustainability isn't just about being "green"—it's about finding a healthier, more responsible way to use technology that benefits our businesses, our communities, and the planet we all share.

Slide 3 — Why Digital Sustainability is Important for SMEs?

When we talk about why digital sustainability matters for small and medium-sized enterprises, we're essentially recognizing that SMEs make up the backbone of many economies—especially in the European Union. Even though each individual business might not use as many resources as a global corporation, the collective impact of thousands of SMEs is enormous. By embracing digital sustainability, these companies can not only reduce their environmental footprint but also tap into a wealth of practical benefits such as cost savings, improved reputation, and compliance with emerging regulations.

One major advantage is that energy-efficient and sustainable practices often translate into reduced operational costs. For instance, keeping software and hardware optimized helps prevent those annoying overheads that creep up when servers run around the clock or devices operate inefficiently. Many SMEs find that by swapping out old hardware for more efficient equipment, or by consolidating their digital processes in the cloud, they can drastically cut electricity expenses. Choosing eco-friendly cloud providers or implementing a robust e-waste management plan doesn't just help the planet; it can also strengthen a company's bottom line. Plus, when you advertise that your business is

environmentally responsible, it resonates with customers who are increasingly eco-conscious themselves.

Digital sustainability also helps SMEs stay on the right side of regulations. The EU, for example, has set certain standards and goals to curb electronic waste and encourage cleaner energy use, and it's likely that these requirements will become even stricter over time. By getting ahead of the curve and adopting things like certified recycling processes or energy-saving technologies now, you're not just avoiding potential fines or reputational damage—you're positioning your business as a forward-thinking leader that can adapt quickly to new legislation. And that leads to another benefit: competitive advantage. It's easier to stand out in a crowded market when you can point to tangible efforts like refurbishing older devices, ensuring responsible disposal of outdated hardware, or optimizing server usage to reduce carbon emissions.

Another reason digital sustainability is so important for SMEs is that it fosters innovation and encourages a culture of continuous improvement. You might, for example, decide to audit your entire IT setup to figure out where you're wasting energy, storage space, or resources. This exercise doesn't just help the environment; it usually leads to a more streamlined and cost-effective operation as you uncover hidden inefficiencies. You might switch to cloud services that run on renewable energy, invest in software that's designed to minimize energy use, or institute a policy that encourages employees to switch off equipment when it's not in use. All of these steps help cultivate a mindset in which every team member feels responsible for the business's environmental footprint, creating a ripple effect that can lead to smarter decision-making at every level of the organization.

Ultimately, digital sustainability is about more than just meeting a social or environmental obligation—it's a forward-looking approach that benefits SMEs on multiple fronts. By reducing costs, appealing to eco-conscious customers, staying compliant with regulations, and inspiring ongoing innovation, SMEs that prioritize digital sustainability aren't just doing "the right thing." They're also building resilient businesses that can thrive in a marketplace where environmental responsibility is increasingly valued by consumers, employees, and policymakers alike. And when you multiply that effect across the many SMEs operating throughout the EU, you end up with a significant positive impact that helps us move toward a more sustainable future together.

Slide 4 — Steps for Implementation

Let's talk about the concrete steps involved in making digital sustainability a reality, especially for small and medium-sized enterprises. I'll walk you through a practical, straightforward process that anyone can follow, even without a specialized technical background.

First, it's crucial to educate employees about sustainable practices. This goes beyond sending out a few emails or handing out pamphlets; it means hosting interactive workshops, providing online training modules, or even inviting sustainability experts to speak with your team. The more your employees understand why digital sustainability matters and how their daily actions can make a difference, the stronger your overall strategy will be.

Next, you need to analyze your digital footprint and resource consumption. Essentially, this involves taking stock of the hardware, software, and energy resources your

organization uses. You might start by tracking how much electricity your servers consume, the extent of your cloud usage, and the volume of electronic waste you produce each year. This data gives you a baseline for future improvements, so you know exactly where you're starting from.

Once you have that information, it's time to define measurable sustainability objectives. Maybe you want to reduce your energy consumption by 20% over the next year, or you're aiming to recycle at least 80% of your outdated hardware. Whatever your goals might be, make sure they're both realistic and specific—this way, you can track your progress more accurately and keep everyone aligned.

With your objectives in place, you can prioritize initiatives like energy efficiency and e-waste management. Think about where you can get the quickest or largest benefits. For instance, if you know your servers are guzzling electricity, focusing on upgrading them or moving to the cloud might be your best first move. Alternatively, if you generate a lot of electronic waste, setting up a robust recycling system might be at the top of your list.

After that, it's important to optimize energy consumption in IT operations. This can involve simple steps like switching to LED lighting in server rooms, scheduling regular maintenance to keep hardware running smoothly, or consolidating servers and using virtualization to reduce the total number of physical machines. You'd be surprised at how quickly these tweaks can add up to significant energy savings.

Of course, you can't talk about digital sustainability without discussing how to implement effective e-waste recycling programs. Here, you'll want to partner with certified recyclers who follow proper guidelines for disposing of hazardous materials and recovering useful components. Some organizations also donate older but still functional devices to schools or nonprofits, extending their lifecycle before they end up in a recycling facility.

A big piece of the puzzle is to partner with green technology providers. Not all tech suppliers are committed to sustainable practices, so it pays to do a bit of homework. Ask prospective vendors about their energy sources, carbon footprint, and recycling policies. By choosing providers that share your values, you can ensure that your entire supply chain—and not just your own operations—supports a greener future.

To really make this initiative a success, you'll want to engage with stakeholders for sustainable development. That includes talking with local communities, customers, suppliers, and even your own employees. Listen to their ideas, incorporate their feedback, and keep them in the loop about your progress. This approach not only builds trust but can also spark fresh insights you might not have considered otherwise.

As you put these strategies into action, remember to use analytics to track and report on sustainability efforts. Whether it's an internal dashboard that monitors energy usage or quarterly reports outlining how much e-waste you've recycled, data is your friend. Sharing these metrics—both internally and with the public—demonstrates accountability and helps you measure whether you're hitting those goals you established early on.

Finally, never forget to refine strategies based on feedback and results. Digital sustainability isn't a one-and-done project; it's an ongoing commitment that evolves over time. As technology changes and your organization grows, you may need to revisit your

objectives, upgrade your policies, or adopt new innovations. The key is to stay flexible, keep learning, and continually look for better ways to reduce your environmental impact while still running a successful, dynamic business.

By following these steps—educating your team, analyzing resource use, setting clear objectives, and then continuously monitoring and improving your approach—you'll be well on your way to establishing a culture of digital sustainability that benefits both your organization and the world around you.

Slide 5 — CONCLUSION

As we wrap up this discussion on digital sustainability, it's clear that embracing responsible and energy-efficient technologies isn't just about ticking boxes—it's a powerful way to protect our environment, streamline operations, and build stronger relationships with customers and communities. Whether we're adopting more efficient servers, recycling old devices, or choosing green technology partners, every step we take brings us closer to a future where our digital tools have a far smaller impact on the planet. By continuing to educate our teams, setting clear goals, and regularly measuring our progress, we can ensure that sustainability remains a core value in our organizations. Ultimately, these efforts not only benefit our businesses here and now, but also help preserve resources and opportunities for generations to come.