

ACTION PLAN

Košice IT Valley



European Union
European Regional
Development Fund



INTRODUCTION

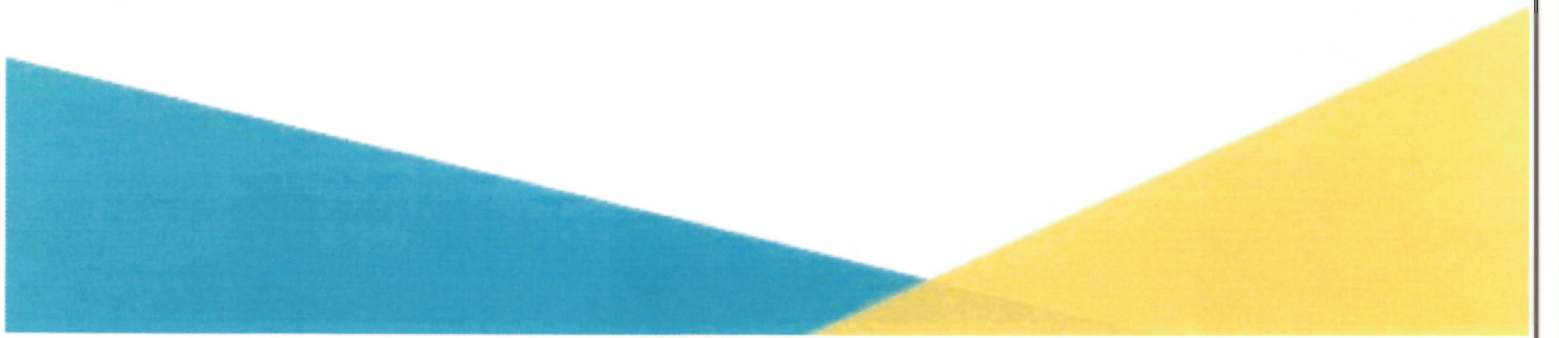
At a time of an evolving landscape of threats, cybersecurity's place at the top of the EU's political agenda raises no doubts. Since its first ever cybersecurity strategy adopted in 2013, the EU has adopted and initiated a number of policy measures to strengthen its cybersecurity capabilities and resilience against cyberattacks: NIS Directive, Digital Single Market Strategy, the proposal to create the European Cybersecurity Competence Centre and Network, the EU Cybersecurity Act, as well as the Digital Europe and the Horizon Europe programmes.

The current EU policies suggest that in the context of cybersecurity, the core players are Member States' national governments, supported by dedicated EU bodies, such as the European Union Agency for Cybersecurity (ENISA). However, because of its multifaceted and all-encompassing nature, cybersecurity policy requires a diversification of the actors involved in its implementation. On one hand, ensuring a close cooperation with the private sector has been recognised as an important step in strengthening the EU's cybersecurity, resulting in the contractual public-private partnership on cybersecurity signed with the European Cyber Security Organisation (ECSO) in 2016. But on the other hand, European regions have often lacked recognition as important cybersecurity actors.

Uniquely positioned, regions hold a privileged connection to their local ecosystems. They have the biggest potential to connect technology with end

users, to assist local small and medium enterprises (SMEs), and to provide them with business support and access to innovative technologies. Regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on solutions coming from third countries and non-European providers. In the near future, the EU cybersecurity landscape will be shaped by initiatives having a direct impact on regional ecosystems, such as the European Cybersecurity Competence Centre and Network, the European digital innovation hubs and renewed smart specialization strategy in each region. Interregional cooperation is therefore key to identifying solutions and moving towards a more integrated cybersecurity market.

The **CYBER project** has been initiated under the EU Interreg Europe programme and the European Regional Development Fund (ERDF) financial instrument to strengthen the local cybersecurity SMEs and to boost interactions among the European regional cybersecurity ecosystems. The lack of cooperation among different cybersecurity stakeholders and different ecosystems is identified as one of the challenges preventing local cybersecurity SMEs from scaling up and internationalising their business. To address this challenge, project partners work together through a series of interregional events to develop and implement regional action plans and concrete policy instruments.



The CYBER involves nine institutional partners, representing different EU countries and regions:

- **Bretagne Development Innovation agency (France),**
- **Institute for Business Competitiveness of Castilla y León (Spain),**
- **Tuscan Region (Italy),**
- **Digital Wallonia agency (Belgium),**
- **Brittany Region (France),**
- **Kosice IT Valley (Slovakia),**
- **Chamber of Commerce and Industry of Slovenia (Slovenia),**
- **Estonian Information System Authority (Estonia),**
- **the European Cyber Security Organisation (Belgium).**

CYBER overall objective is to boost competitiveness of cybersecurity SMEs, thanks to improved public policies. It involves public authorities that can help knock down barriers of market fragmentation, lack of coordination of regional actors and lack of skills. Medium-term aim is to ensure greater coherence between offer and market demand, with a chance to build up skills and merge competences. In the long term, by making the digital world safer, the CYBER initiative contributes to the development of the EU digital market.

During its first phase, CYBER focused on identifying main barriers: lack of coordination between relevant actors, market fragmentation and lack of skills. For each barrier, regional strengths, weaknesses, opportunities and threats were identified, using SWOT analysis. The aim was to identify characteristics and key services that an innovation ecosystem supporting SMEs in the cybersecurity sector should deliver. Based on their level of cyber-development, CYBER partners also identified good practices that represent strengths of their territories and potential solutions to other partners' needs. These good practices fall under two different groups of policy measures:

those that support the structure of the cyber innovation ecosystem and those that support advanced services provided within the ecosystem (such as labels, access to public and private funding, capacity building etc.). As a result of this interregional exchange process, good practices and solutions have been selected by partners in a perspective of transfer and adaptation and have been collected into **regional Action Plans**. These Actions Plans represent, for concerned regional authorities, a concrete road map for designing and targeting more and better funding to increase competitiveness of cybersecurity SMEs. Their relevance is also crucial within an EU context, as they provide inputs that can contribute to the European Investment for Growth and Jobs programme and the European Territorial Cooperation programme, as well as to address cybersecurity challenges through the newly proposed NIS2 Directive lenses. Produced by CYBER partners, these Actions Plans are therefore key documents both for regional cooperation across Europe and for policymaking at the EU level.



GENERAL INFORMATION

Name of the project: CYBER

Partner organisation: Košice IT Valley

Country: Slovakia

NUTS2 region: SK04 Východné Slovensko

Contact person:

Viktor Mitruk
Viktor.Mitruk@itvalley.sk
+42 19 48 412 650

Miriama Hučková
Miriama.huckova@itvalley.sk
+42 12 44 403 587



POLICY CONTEXT

The Action Plan aims to impact:

- Investment for Growth and Jobs programme
- European Territorial Cooperation programme
- [Other regional development policy instrument](#)

Name of the policy instrument addressed:

Smart Industry Strategy of the Slovak Republic



DETAILS OF THE ACTIONS ENVISAGED

ACTION 1: Revision of the Smart Industry Action Plan and New Approach for Support to Cybersecurity SMEs – Policy making Based on Evidence

The background

The government must understand the risks of cyber-attacks that threaten companies' property and reputations, especially SMEs. SMEs are the new big target for cyber-attacks. In Europe, in 2016, 60% of all cyber-attacks were aimed at SMEs. 68% of SMEs have no systematic approach to ensuring cybersecurity. 60% of SMEs who were victims of cyber-attacks did not recover and shut down within six months. SMEs see themselves confronted with a large variety of cyber threats.

In Slovakia, on the national level, cybersecurity faces a lack of attention that creates enormous vulnerabilities. Cybersecurity represents a significant unseen challenge at all levels of government and brings opportunities for new business.

During the seven first months of developing the Action Plan, we have organized five meetings with the local (cyber) ecosystem representatives. The essential partnership was with the government, the Ministry of Economy of the Slovak Republic, which is responsible for innovative SMEs on national level.

Together we defined three main challenges:

1. Old (not revised) strategic documents (valid until 2020)
2. The first Smart Industry Strategy addressed insufficiently the challenge of cybersecurity. Some of the actions supporting the cybersecurity of innovative SME's were proposed but implemented very poorly

3. Ministry of Economy is missing relevant data about the cybersecurity readiness of SMES that constrain making policies that are addressed and relevant.

In the CYBER project framework, we have decided to prepare a tool that can lead to effective policymaking based on evidence. Also, improving the information about the local market and company needs will help us to prepare policy recommendations which will reflect on actual challenges in cybersecurity. Jointly we would like to prepare, spread, and analyze the outcome of the online survey form. Concerning that, this action focuses on cooperation with the national body, not a regional government, which has no competence in cybersecurity.

Secondly, Košice IT Valley has agreed with the Technical University of Košice and the Managing Authority to organize an event called CyberBreakfast at the campus of the university. This event represents the value of the CYBER project's capacity for knowledge exchange, as Košice IT Valley had taken the idea for the Cyber Breakfast after hearing about the Brittany Region's success in a similar event. This breakfast is implemented with a few minor differences.

At the same time, we would like to state that the policy instrument has changed. The main reason for this change is that the Operational Program Research and Innovation, originally mentioned in the application form ended in 2020. After meetings with representatives of the Ministry of Economy of the Slovak Republic, we have decided to change the policy instrument to Smart Industry Strategy and its related action plan. Strategy

was prepared in 2016 in cooperation with National Security Office (NBÚ) and Computer Security Incident Response Team (CSIRST) and approved by government. The Action Plan was valid until 2020 and there is no following one.

Implementation of the Action Plan of Smart Industry until 2020 formed the basic precondition for a successful transformation of Slovak economy responding to digitalization of SMEs. Emerging digital technologies are opening tremendous market opportunities for SMEs and creating entirely new industries, but, in turn, raise vulnerability to digital security risks. From our point of view in the context of the COVID-19 pandemic, more businesses have been forced to operate online than ever before, and their reliance on digital infrastructure, cloud computing and software has increased, as the intensity of cyber-attacks. Many SMEs lack the awareness, resources or expertise to assess their digital risk exposure and to implement appropriate prevention and remediation measures which are more common among larger. As SMEs connect to the digital world and move towards new digital solutions, they will need to effectively manage cyber-risks to reap the benefits of the digital transition.

The Ministry of Economy suggests the launch of the revised Action Plan of Smart Industry in January 2023. The Managing Authority invited the cluster to become part of the forming working group to a new action plan which consists of representatives of different stakeholders.

The role of the cluster in the working group:

Kosice IT Valley will represent the challenges of stakeholders in cybersecurity from East Slovakia where the business environment is quite different than in the rest of the country. We agreed that Košice IT Valley will prepare a survey for companies to define the main challenges. By collecting and analyzing inputs from local stakeholders, we will prepare a set of recommendations for a revised Action Plan of Smart Industry. Working groups will meet regularly 3 times per year (starts in Autumn 2021).

Main goals:

- **Improved Governance** – By collecting data about the needs of SMEs we can improve the information about the local market and the needs of innovative SME which leads to better support on national level
- **Motivating SMEs to focus on cybersecurity threads**
- **Boosting Digital Transformation of the Society** - Preparations of two sets of policy recommendations:

- **Smart Industry Strategy**
- **Action Plan**
- **Supporting the development of cybersecurity within business community** - Share the results of the survey with the local cyber companies and managing authority- Cyber Breakfast - information for the local cyber value chain, to be properly informed about possible opportunities.

The Ministry of Economy has agreed as well to take into consideration the recommendations from the Cyber project during preparations of

- The new Operational Program in Slovakia within the programming period 2021 - 2027
- New calls to support the digitization of companies from the Recovery and Resilience Plan of the Slovak Republic
- Defining priority areas for new Regional Innovation Strategy (should take place throughout the 2021-2027 programming period)

Learning process:

We have been inspired by the Estonian Strategy at the partner meeting. Estonia is a leader in digital transformation and builds a friendly environment for innovative SMEs which reflected very well at the Cybersecurity Strategy of Estonia.

Also, we have adopted the vision represented by the Chamber of Commerce and Industry of Slovenia – Association of Informatics and Telecommunication. We agree that without a high level of cyber maturity of SMEs it is not possible to successfully realize the objectives of digital transformation. We had a bilateral (online) meeting with Digital Wallonia, which showed us an online tool which effectively collects data. It helps to provide a better understanding of actual maturity of cybersecurity ecosystem. We also learned from other partners, namely Britany's Cyberbreakfast, how to stimulate ecosystems for innovative SMEs, especially cyber SMEs. The idea is to focus on a specific group (SMEs) which we believe is the vital group to educate and take the data from to make necessary changes in the policy. Regarding that, we have decided to link Managing Authority, SMEs with the cyber specialists to define concrete measures which later on become a part of revised Action Plan. During the CyberBreakfast we will present the outputs of the survey, discuss and propose other actions. Furthermore, we will focus on the dissemination of knowledge to SMEs to address cyber risk within their development projects.

The action

- Studying Slovak national documents regarding the cybersecurity including the organisations and competences
- Defining stakeholders and key actors (Ministries, local players, universities...)
- SWOT analysis - The level of respond to current needs, new challenges in strengthening the cyber security of the Slovak Republic and define its starting points and goals.
- Identification of main problematic area for Slovak SMEs with partners – 6 threats
 - Internal Attacks
 - Phishing and spear phishing
 - Lack of Cybersecurity knowledge
 - Distributed Denial of Service (DDoS)
 - Malware
 - SQL Injection
- Bilateral online meeting with partner from Digital Wallonia, Mr. Jeremy Grandclaudon to learn about their online tool to collect data
- Preparation of the tool (online survey) – the tool should help to SMEs to underline their security gaps and (e.g. Secure Configuration, Malware protection, Awareness of Password weaknesses...).
- The survey can be completed in less than 10 minutes (as seen below)
- Spreading the online survey through members and central body - (in progress) We have already contacted the associations, chambers, and other organizations to spread the survey.
- Evaluation of Data and Roundtable with stakeholders – defining policy recommendations
- Policy recommendations for revised Strategy and its Action Plan: Support the Managing Authority in the renewal of the Cybersecurity Strategy and addressing the needs of innovative SMEs as the cornerstone of digital transformation of the society
- Webinars for stakeholders, focusing on students and women

SURVEY QUESTIONS (prepared in Slovak language)

1. Who is responsible for cybersecurity in your company?
2. Have you created security documentation for cybersecurity?
 - a. Is there a list of assets and risks?
 - i. Which assets are most important?
 - b. Do you have a plan for dealing with cybersecurity incidents?
 - c. Are employees demonstrably familiar with security policy?

3. Are you able to detect a cybersecurity incident in the subject?
 - a. How many cybersecurity incidents have you detected in the environment in the last six months?
 - i. If cybersecurity incidents have been identified, what and how have measures and lessons been implemented?
 - b. Is your company able to detect an internal attacker (internal employee)?
4. How much would it probably cost the subject to interrupt the activity due to a cyber attack for one week?
5. What is the percentage of cybersecurity funding out of the entity's total running costs?
6. Do you have recovery plans in place?
 - a. If so, are these plans regularly tested, e.g., also by a simulated incident?
7. Is there an active approach to employee training from a cybersecurity perspective?
8. How is the entity prepared for a security incident from the GDPR perspective?
9. What are the most serious cybersecurity threats to the subject identified (name 5)?
10. Do you have a specialized team for dealing with cybersecurity incidents?
 - a. If so, is this team available 24x7x365 days?
11. What are the currently implemented security measures of the entity for the area of cybersecurity?
 - a. At the level of end stations or user devices such as mobile phones and tablets.
 - b. At the network level.
 - c. At the level of infrastructure components (email server, web portal, etc.).
 - d. At the level of access from the external environment.
12. How is the company prepared for cybersecurity incidents by suppliers?
 - a. What types of access are granted to suppliers?
 - i. How are these approaches monitored and controlled?
 - b. How are suppliers' activities monitored and controlled?

Players involved

1. Ministry of Economy of the Slovak Republic – responsible for innovative SMEs

2. Technical University in Košice

3. Local SMEs

Timeframe

- Identification of main problematic area for Slovak SMEs - 31st September 2020
- Preparation of the tool (online survey) – the tool should help to SMEs to underline their security gaps as well as support the managing authority activities (e.g. Secure Configuration, Malware protection, Awareness of Password weaknesses...). Survey can be completed in less than 10 minutes. – 30th November 2020
- Spreading the online survey through members and central body – 30th August 2021
- Evaluation of Data, results will serve as a base for upcoming decisions about financial support tools – 1st October 2021
- Trainings – Creating a Culture of Awareness – November 2021
- Participation in policy working group – starting in Autumn 2021, ongoing in 2022
- Launch of the revised Action Plan of Smart Industry – January 2023

Cost

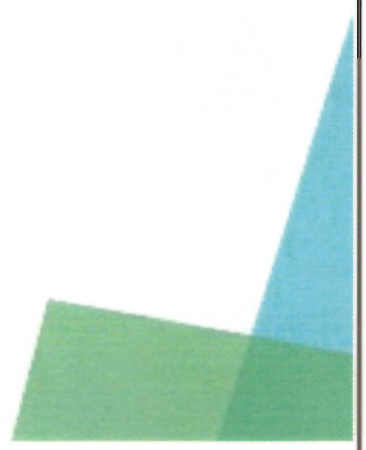
- Human resources
- Events and meetings

Funding sources


Own resources – membership fees

Monitoring and indicators

Number of local SMEs used online survey



Date 11.8.2021

Signature MARTIN SVOBODA 

Stamp of the organisation

MINISTERSTVO HOSPODÁRSTVA
Slovenskej republiky
Mlynské nivy 44/a
827 15 Bratislava 212
- 3220 -



European Union
European Regional
Development Fund