ACTION PLAN

Tuscany Region

CYBER
Interreg Europe

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: Tuscany Region
Country: Italy
NUTS2 region: Toscana

Contact person:

Sauro Del Turco
Sauro.delturco@regione.toscana.it
055 4383048

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:

- ERDF Regional Operational Programme "Tuscany" 2014-2020 (Action 1)
- Digital Transition Policy of Tuscany Region (Action 2)

DETAILS OF THE ACTIONS ENVISAGED

ACTION 1: VOUCHER FOR CYBERSECURITY SOLUTIONS

The background

Since the very beginning of the CYBER project, partners discussed means of supporting companies. On the one hand, the aim was to create a stronger regional market for cybersecurity services. On the other, to incentivise all SMEs to invest and become more cyber secure. Among the many examples presented, two GPs appeared to be compatible with the approach already adopted by the Regional Government of Tuscany in relation to funding schemes for innovative services.

The first example is the GP “Keep it Secure” from Wallonia (Nantes Project meeting held in June 2019). They put in place a voucher system for SMEs with a specific focus on funding cybersecurity audits and assessments. This GP has many similarities with existing initiatives in Tuscany, but two main differences were identified and analysed. The first one referred to the selection of the service provider. While in Wallonia there is a register that lists all eligible providers, in Tuscany the SMEs are free to select their own service provider provided that they can demonstrate an adequate level of experience. The second main difference concerned the specific focus on cybersecurity, which was lacking in Tuscany.

This focus was also highlighted in the second GP: Cybersecurity Voucher, shared by the Chamber of Commerce of Slovenia (Webinar on Cybersecurity Vouchers - April 2020). This GP was included among the programmes activated by the Slovenian Digital Innovation Hub, funding system security reviews and penetration tests. Projects were very technical, funded to a max of 9.999,00 € and result-oriented. Eligible service providers were included in a list and validated by the programme.

The action

The Action ***Voucher for cybersecurity solutions*** consists of the following sub-actions :

- GPs exchange among partners
- defining change of funding scheme with the introduction of new services targeting cybersecurity in the regional catalogue of eligible services
- implementing the update of the regional catalogue with a call for proposals
- monitoring the progress of financed pilots focusing on cybersecurity

The Sector for digital transition and technological infrastructures of the regional government is the CYBER project partner. They are in charge of managing the regional Data Centre and, therefore, perfectly placed to understand and fight the cybersecurity risks from the Public Administration perspective. Exchange activities with other project partners helped to deepen the partners’ knowledge of the importance of incentivising awareness and investment at company level as well.

Thanks to CYBER, they initiated an important cooperation with the Regional Direction dealing with Enterprise Support, which is the ERDF Managing Authority in Tuscany. This Direction was involved in

the LOCKS meeting (the local stakeholder group active in the region), in the project meeting held in Leon (October 219) and in the virtual webinar on Cybersecurity vouchers organised in April 2020 by the Slovenian partner.

After analysing the Walloon and Slovenian schemes (KIS and Cybersecurity Voucher Good Practices), the Regional Government of Tuscany decided to modify their funding scheme aiming at contracting professional services to help SMEs increase their innovation levels. In this context, it was decided that the current selection modality for service providers, well known among beneficiaries and in place for a long time, was still the right fit for Tuscany. However, both experiences clearly demonstrated the success of a specific result-oriented focus on the cybersecurity aspect.

For many years, the Regional Government of Tuscany has directed ERDF money towards local small and medium enterprises (SMEs) to contract professional services aimed at increasing their innovation levels. The restricted list of services that are eligible for funding is included in a catalogue defined by the Regional Government. The catalogue represents the point of reference for eligibility, both in terms of activities and of funding rules.

Over the years, the catalogue has undergone many changes in order to meet the needs of the territory.

Based on the lessons learnt thanks to CYBER, the Direction for Enterprise Support of Tuscany Region, made the decision to add a cybersecurity focus in their catalogue.

In Tuscany, the topic had so far been included in the broader context of Industry 4.0, without an independent status.

The review process of the catalogue took place between May and July 2020 in cooperation with the University of Pisa, which was in charge of designing the new eligible service taking into account the GPs shared within CYBER, and the process completed in August 2020 with the approval of the renewed catalogue (Decree of Director n.12935 of 19th August 2020).

In this catalogue the new services focused on cybersecurity pilot solutions are classified as service B.6.8 and include solutions such as Security managed services and cloud security, System Integration, Security and risk assessment and penetration test, Security software and hardware, Threat intelligence.

This action can be categorised as a strategic change to the policy instrument that is also relevant to the improvement typology “new projects”.

The implementation of the change in funding scheme took place in September 2020 when a call for proposal based on the updated catalogue was published making use of ERDF money diverted to digitalisation measures in the framework of the COVID-19 emergency.

The call opened on 17/09/20 with a budget amounting to 10.000.000€. In two days, 312 proposals were submitted for a total funding request amounting to over 13.000.000€. Vouchers covering costs were made available to the selected proposals.

The pilot should be integrated within the company processes and production lines. Projects can last up to 12 months, with max eligible costs amounting to 60.000€, funded at 50% by the ERDF.

The number of projects including cybersecurity services are being monitored and the quality of their results assessed in cooperation with the Managing Authority. The monitoring process will take into consideration the number of projects submitted on cybersecurity services, the amount of funding requested, and the total funding approved (vouchers approved and financed) referring to the cybersecurity services.

The Sector for digital transition and technological infrastructures plans to work in cooperation with the Regional Direction dealing with Enterprise Support (MA) in order to:

- Collect data for the monitoring process (bimonthly calls scheduled with the MA to follow the process, from selection, to implementation and closure)
- Collect qualitative information on the projects (i.e. on specific topics tackled, impact on the company, etc.)
- Participate in follow up activities before the launch of similar calls or in the design process of the updated catalogue for the period 2021-2027.

Players involved

The stakeholders involved in this action are:

- Regional Authority: Managing Authority of ROP

- University of Pisa – Supporting in design the new eligible services targeting cybersecurity to be added in the regional catalogue
- All eligible entities, mainly SMEs.

Timeframe

The action 1 has been already implemented as the Catalogue was updated with new services for cybersecurity in August 2020 and in September the call for proposal was opened. Therefore, the policy change has been achieved in the 5th semester (August 2020) of the project.

The monitoring process was set up in order to be fully implemented when the approved cybersecurity projects will be implemented.

- GPs exchange among partners (June 2018 – November 2019)
- Defining change of funding scheme with the introduction of new services targeting cybersecurity in the regional catalogue of eligible services (December 2019 – May 2020)
- Implementing the update of the regional catalogue with a call for proposals (June 2020 – September 2020)
- Monitoring the progress of financed pilots focusing on cybersecurity (from October 2020 to end of the project)

Cost

In the call focusing on cybersecurity services, every project has an eligible budget of 60 thousand € funded at 50% by the ERDF.

Funding sources

ERDF funding

Monitoring and indicators

Tuscany Region has already started monitoring the implementation of the refereed action in order to assess the progress and define the impact. Tuscany Region will check and valuate how the action has been implemented and what are the results coming from this.

The monitoring system has already started monitoring the number of projects submitted on cybersecurity services, the amount of funding requested, the total funding approved (vouchers approved and financed) referring to the cybersecurity services.

For each project, the monitoring system aims at monitoring indicators according to the ROP Managing Authority monitoring system, Sistema Informativo Unico POR FESR 2014-2020. Exactly, the following indicators will be measured:

- SMEs that submit project on cybersecurity
- Type of cybersecurity services required
- Total approved fund
- Total financed fund

The monitoring process on the submitted projects (qualified service area 6) will be run every 6 months, in cooperation between the Direction for Enterprise Support and the Direction for Information Systems and Technological Infrastructures.

ACTION 2: Formalisation and Kick-off of the Regional Cybersecurity Ecosystem Coordination Mechanism

The background

In September 2020, after the Regional election, a new regional government took office in Tuscany. The new government has identified cybersecurity as an important priority of the regional ecosystem: its strategic position has risen due to the importance of the digitalisation process, also pushed by the Covid-19 emergency. In this new political context, the activities in the field of cybersecurity, are being restructured starting from the agreements already signed with the aim of making the cybersecurity ecosystem operational.

Inspired by connections and practices resulting from CYBER, the Regional Minister for Digitalisation intends to set up a coordination mechanism bringing together the existing public and private organisations active on the cybersecurity topic in the region.

In 2018, the creation of the Tuscany Cybersecurity Center (C3T) was proposed and approved by the Regional Government (see Decreto 4/2018). This Center consists of Universities and Research Centers operating in Tuscany. The C3T is in charge of awareness activities, scientific and technical support to SMEs and PA, research and technology transfer, training and education. It operates based on ad hoc funding agreements signed by different Regional departments, depending on the activities they intend to carry out. So far, only the Support for SMEs department, ERDF Managing Authority, has signed a funding agreement with C3T.

The C3T, together with Tuscany Region, is the backbone of the newly created ecosystem. Considering the above, the theoretical idea of a coordination mechanism involving different regional departments and the C3T was already included in the initial agreement signed in 2018. However, this has not become operational yet. As the involvement of both institutional and territorial stakeholders is fundamental, based on the ongoing CYBER experience, the new formalisation introducing new working group and the practical kick off of such a mechanism will be the focus of the current action.

By making the coordination mechanisms operational it will be possible to broaden the scope of C3T's activities, for instance: to observe the system in terms of risks/attacks, to provide local public bodies with solutions, to support in the regional cybersecurity policy in terms of stakeholder coordination, to train competence and update skills, do applied research but also contribute to the definition of the cybersecurity regional policy.

This ecosystem supports Tuscan SMEs from two directions. On the one hand, it aims to protect them from potential cyber threats, through policies, skills and research. On the other, it is an opportunity for SMEs working in computer engineering fields to discover new markets in the cyber security field.

The action

The formal output of this action consists of an act signed by the Regional Government approving and making operational the completed coordination mechanism proposed for the Tuscan cyber security ecosystem. Subsequently, ecosystem activities will be launched and monitored. The act will be proposed by the Digital Transition and Technological Infrastructures department and will contribute to the improvement of their Digital Transition Policy.

This action has been inspired by experiences shared by the partners from Brittany and Spain that showed how an advanced cybersecurity ecosystem works and develops to meet the need of the regional stakeholders.

In particular, Castilla y Leon provided useful insights in the process of creating an ecosystem sharing the most important initial steps that led to the success of their governance system. The partner answered a series of specific questions supporting Tuscany in drafting an effective proposal for the decision-making level.

Tuscany Region has decided to replicate 4 key features. This includes:

1. Begin the work by involving different departments of the Regional Authority - to enhance the involvement of a broader community active in several sectors thanks to a formalised structure.

2. Stimulating a large and strong presence of the local stakeholders (universities, different regional departments, associations of SMEs, SMEs, other public bodies) – to develop a critical mass useful for the implementation of the activities.

3. Creation of a Regional Cybersecurity Working Group for supporting operational coordination of activities – this will be done in continuity with the work of the Cyber LOCKS group, which was the first organised group of stakeholders involved at regional level on the cybersecurity topics.

4. Role of action leader assigned to the Regional Authority, in our case Tuscany Region.

The coordination mechanism will be based on 2 pillars:

- Decision-making role attributed to a Technical Coordination Board formed of 1 representative for the following Regional Departments: Digital transition and technological infrastructures; Support to SMEs; Research, Education and Vocational Training.
- Consultation body of experts called Regional Cybersecurity Working Group to gather feedback on needs and solutions from the territory.

On the one hand, the regional public administration system (Region, municipalities, universities, health institutions) is key in its decision-making and coordination role and also because it is in charge of providing support to regional SMEs.

On the other hand, different actors operating in Tuscany with different skills and visions on the cybersecurity sector, such companies, universities, business associations, should become an integral and active part of the ecosystem.

Players involved

The action will be run by Tuscany Region (Technological Infrastructure department, in cooperation with other departments) that is the lead of the action.

The other main partner involved is the C3T - Tuscany Cybersecurity Center. This Center consists of Universities and Research Centers operating in Tuscany. It has already collaborated with Tuscany Region and is an active actor of regional cybersecurity ecosystem.

Local stakeholders (SMEs, Association of SMEs, Education and Training Centres, etc.) provide support to the new institute's formalisation and activities.

Timeframe

The action will be run over the second phase of the project.

These are the steps to reach the goal of formalisation of the new governance structure:

- Meeting with regional actors from different departments of Tuscany Region (Research, Education and Vocational Training, Support to SMEs departments) – done in March 2021
- In the framework of CYBER Phase 1, organisation of the Tuscan Cybernight involving LOCKS members (SMEs and associations of SMEs), 3 departments of Tuscany Region and C3T to reinforce cooperation among different actors of regional ecosystem - done in May and June 2021
- Preparatory work to draft Regional act for the formalisation of the coordination mechanism and the activity plan - by October 2021
- Approval of the Regional act that sets up the governance structure based on 2 pillars - by December 2021:
    - The Technical Coordination Board (*Nucleo di coordinamento tecnico*) formed of 1 designated

representative from the following departments: Digital transition and technological infrastructures; Support to SMEs; Research, Education and Vocational Training.
    - The Regional Cybersecurity Working Group formed of regional stakeholders and inspired by the LOCKS meeting organised within the CYBER project
- Technical Coordination Board meeting – by the end of 2021
- Regional Cybersecurity Working Group meeting – first semester of 2022
- Ongoing monitoring until the end of Phase 2

Cost

Staff costs of civil servants working for the Regional Government

Funding sources

Not applicable

Monitoring and indicators

The monitoring process will be focused on following the evolution of the regional cybersecurity ecosystem measuring:

- No. of Technical Coordination Board meetings
- No. of Regional Cybersecurity Working Group meetings
- No. of stakeholders involved in the Regional Cybersecurity Working Group, including SMEs