

ACTION PLAN

Digital Wallonia Agency



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: L'Agence du Numérique

Country: Belgium

NUTS2 region: Wallonia

Contact person:

Jeremy Grandclaudon
Jeremy.grandclaudon@adn.be
+32 473 491 170

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:

Digital Wallonia – Digital Strategy for Wallonia

DETAILS OF THE ACTIONS ENVISAGED

ACTION 1: Raising the Adoption and Visibility of an Economic Instrument (Cyber Vouchers)

The background

Keep It Secure (KIS) was created to strengthen the Digital Wallonia Strategy, especially on two axes:

1. Facilitate access to finance at each stage of the business lifecycle.
2. Stimulate the growth of start-ups and SMEs through public action.

It is a Walloon-dedicated cybersecurity mechanism running since 2017. The action itself is working as expected by creating and curating a list of dedicated cyber security experts that SMEs can call when needed.

If they call an expert from the list, they can benefit for security vouchers, covering up to 75% of the costs of the expert's intervention. There are limitations on the type of intervention covered: only the initial security audit and following remediations will be eligible. Any recurrent costs or hardware purchased will not be eligible.

We have still one issue: SMEs barely use the cyber voucher and barely call upon the KIS experts.

After multiple interactions with the project's partners during the official meetings and one-to-one discussions, we have identified that, even if the voucher mechanism is sound, we did not have

the right tools and actions in place to reach the targeted community and ensure the full success of our policy.

When looking at Brittany and other project members, we are still missing some tools to help us make our ecosystem more alive and connected. A thriving ecosystem is a cornerstone for the Digital Strategy Wallonia where we aim to structure, streamline, and animate the digital ecosystem.

We are missing a holistic ecosystem for cybersecurity: the providers are there, with a good representation, but the SMEs are not involved enough and do not receive enough information and awareness about the need of cybersecurity and the voucher mechanism.

To address the identified issue, we have decided to implement an adapted version of the CyberBreakfast initiative from Brittany.

The original version of this event was destined to bring together cybersecurity experts for networking and collaboration. Our ecosystem in Wallonia is quite different and probably not yet mature enough to host this type of event.

Our version will keep the original spirit, but our main goal will be to bring together the cybersecurity service providers from KIS and any type SMEs to discuss cybersecurity. Each Cyberbreakfast will tackle a specific topic or problematic, focused on the SMEs needs, with security providers able to propose quick and concrete actions to strengthen security and the cyber voucher as a potential solution.

The action

We will divide this action in three major parts:

1. Thorough mapping of our cyber ecosystem and its components

We are not starting from scratch but there are obviously some gaps that need to be identified and closed before going further. We are already launching questionnaires via our partners and mapping the major actors in research and education.

The results will need analysis to ensure we have well defined our targets. We have planned several meetings to discuss them with our partners and stakeholders to refine the action further.

2. Shaping the action and communication

Once the target is well defined, we will begin to select topics (several of them are already ready) that can bring together SMEs and Cybersecurity providers around the table. We will create specific contents with our partners via workshops (private and academic) to animate and support the discussion, with a strong focus on the cyber voucher as a solution for a SME to improve its cybersecurity. The biggest unknown is the COVID-19 situation. Obtaining good results from an online Cyberbreakfast will be a lot tougher than in person but we are planning for both instances anyway. An adequate platform (Zoom, Airmeeet...) will be selected if the sanitary conditions do not improve but this is the least favourite scenario albeit the more realistic one. We are, at the same

time, actively looking for a convenient venue so we can be ready if the COVID-19 situation improves.

We are preparing a communication campaign on multiple medias (mailing, website, social media, radio...) targeting SMEs and their needs on cybersecurity. Other cybersecurity topics will be covered in the campaign but the Cyberbreakfasts will be one of main initiatives put forward. Part of the content already exists and will be updated with the help of our partners and stakeholders.

3. Starting the action and follow-up

We will start with the Cyberbreakfasts at the rate of one per month, for a duration of 1h30 (1h presentation and 30min of networking). The first ones will be probably held with a reduced audience to gauge the reactions, especially if we use the online format. We will adjust accordingly with the help of our partners and stakeholders.

Every month, we will choose a topic in cybersecurity, close to the SMEs' concerns and a speaker from the industry (the KIS providers are a perfect pool of experts) or the academic world (via the research centres or universities). We will book a proper location and provide a light breakfast to ease the networking.

This action will have impact on our Digital strategy. This kind of event is important in order to gather enough information and feedback regarding the efficiency of our Digital Wallonia Strategy. In this case, we are trying to create another "bridge" between offer and demand and if successful, this type of event will become part of our Digital Strategy.

Another goal of these events is to gather information and interact with our stakeholders regarding the state of our Digital Wallonia Strategy and what kind of improvements we can perform on the cyber vouchers initiative. The identified modifications will be discussed between our agency (AND) and the regional administration (SPWEER). The potential

modifications will cover topics such as eligibility, the type of services performed via the cyber voucher scheme, etc. If a modification is approved, it will be recorded and diffused via a modification in the ministerial decree governing the voucher scheme.

Players involved

The players involved are divided in three categories:

1. Private actors

- Infopole cluster TIC

This partner is the Walloon network for IT professionals and has been involved with us since the beginning of Keep It Secure. They provide us with an efficient way to contact IT companies in Wallonia and test some of our ideas before reaching out to the public.

- Cyber security coalition

The Cyber Security Coalition is a unique partnership between players from the academic world, the public authorities, and the private sector who join forces in the fight against cybercrime. They will help us regarding the content and speaker selection.

- European Cyber Security Organisation (ECSO)

2. Public actors

- Agence du Numérique (ADN)

The Agence du Numérique (AdN) is a subsidiary of the Walloon Agency for Enterprise and Innovation (AEI). AdN is responsible for implementing the Digital Wallonia strategy, which has the following objectives:

- Fast-tracking Wallonia's participation and integration in the digital economy.
- Encouraging the development of a real Walloon digital industry, producing goods and services with high added value.

- Integrating digital technology for the growth and competitiveness of enterprises.
- Developing a digital culture among the public and more specifically young people in Wallonia as part of their education and training.
 - Walloon administration

They are the responsible for the cyber voucher distribution and will be instrumental in all changes in our Policy.

- Centre for Cyber Security Belgium (CCB)

The Centre for Cyber Security Belgium is the central authority for cyber security in Belgium. It will draft a national Cyber Security policy and encourage all relevant Belgian governmental departments to make an adequate and integrated contribution. We will collaborate with them on multiple topics, including content, pool of experts, and communication.

3. Research centres

- Centre of Excellence in Information and Communication Technologies (CETIC)

As an applied research centre in the field of ICT, CETIC's mission is to support economic development by transferring the results of the most innovative research in ICT to companies, particularly SMEs. They are one of the two key partners for KIS and will also provide content and experts for this action

- Multitel Innovation Center

The mission of Multitel consists, as a priority, in helping Walloon companies to integrate effectively new technologies in their products, processes and services, in order to improve their competitiveness and to reach a sustainable economic prosperity. They are one of the two key partners for KIS and will also provide content and experts for this action.

4. Universities

- UCL

The university welcomes 32,000 students in seven locations in Brussels and Wallonia. Its main campus is in the pedestrianised city of Louvain-la-Neuve. The university offers courses in all disciplines, from bachelor's degree to doctoral degree level, as well as many lifelong learning programmes. They will provide experts and an academic perspective on topics such as cryptography or malware analysis.

- UMONS

The University of Mons, abbreviated to "UMONS", is one of five academic centres set up in the Wallonia-Brussels Federation as part of the restructuring of higher education, and is one of the founding members of the Pôle hainuyer, a cluster of hautes écoles, universities and other establishments. They will be solicited for experts and some content preparation.

- UNamur

The University campus is situated in the centre of the city of Namur, the capital of Wallonia (the French speaking region in Belgium), which is close to other major centres like Brussels. With 40 different programmes at the Bachelor, Master and Doctorate levels, the UNamur welcomes over 4,900 students in six Faculties: Arts, Law, Economics, Social Sciences and Business Administration, Computer Science, Medicine and Sciences. They will provide an academic perspective on several topics, and potential speakers.

Timeframe

This action will be held during 2021 and will continue if our indicators are good. We are already busy with the first action and our mapping should be ready for Q2. The communication campaign is under development and should start in Q3.

The discussion with our partners and stakeholders is ongoing (choosing the first

experts, topics...) and will intensify beginning of Q3.

The first Cyberbreakfast should be held before the end of Q3.

Summary:

1. Thorough mapping of our cyber ecosystem and its components → Before end of Q2
2. Shaping the action and communication → Mid Q3
3. Starting the action and follow-up → End of Q3.

Cost

Human resource:

Salary of cybersecurity expert ADN: +-100K€, already approved in the ADN's budget

Speaker expenses : 3000€ (500€ per event, 6 events planned)

Material, events, and licences

Platform costs : 1500€ per year

Event venue cost: TBD, the Covid-19 situation is still too cloudy at the moment.

Funding sources

The cost to implement this action will be supported using a dedicated budget inside our agency (ADN). We are financed by the Walloon government to create, develop, and maintain the Digital Strategy and this action falls within our scope and can make use of the already approved budget.

A maximum of 30K€ is forecasted for this particular action.

Monitoring and indicators

- Number of cyber vouchers used by SMEs (measurement unit: n° of cyber vouchers)
- Number of SMEs attending the Cyberbreakfast (measurement unit: n° of SMEs)
- Number of Cybersecurity providers attending the Cyberbreakfast (measurement unit: n° of companies)

ACTION 2: Creation of a Call to Projects to Improve the Cybersecurity Level of SMEs and Setup of a Better Matchmaking Between Cybersecurity Providers and SMEs in Need of Cybersecurity Services

The background

Keep It Secure-KIS was created to strengthen the Digital Wallonia Strategy, especially on two axes:

1. Facilitate access to finance at each stage of the business life cycle.
2. Stimulate the growth of start-ups and SMEs through public action.

It is a Walloon dedicated cybersecurity mechanism running since 2017. The action itself is working as expected by creating and curating a list of dedicated cyber security experts that SME's can call when needed.

If they call an expert from the list, they can benefit for security vouchers, covering up to 75% of the costs of the expert's intervention. They are limitations on the type of intervention covered: only the initial security audit and following remediations will be eligible. Any recurrent costs or hardware purchased will not be eligible.

We have still one issue: SME's barely use the cyber voucher and barely call upon the KIS experts.

After multiple interactions with the project's partners during the official meetings and one-to-one discussions, we have identified that, even if the voucher mechanism is sound, we did not have the right tools and actions in place to reach the

targeted community and ensure the full success of our policy.

Several regions such as Castilla y Leon or Brittany have implemented an acceleration program or a call for digital innovation projects to boost cyber initiatives or products creation. This action will be inspired from these good practices but modified to fit our needs and ecosystem.

Our goal will be to develop a call to projects, involving each time an SME with a concrete need in cybersecurity and a cybersecurity provider. The SME will have to submit a convincing case toward a committee who will assess the proposal based on several criteria.

If selected, the committee will determine the best cyber provider able to help the SME during the implementation of the proposal. The cyber vouchers will be used to finance the complete project or part of it, depending on the type of needs and the scope. The same limitation described before about the Cyber vouchers still apply.

The action

This action will be divided in three parts:

1. Creation of the selection committee and the creation of a list of cyber providers

With the KIS initiative, we have already a pool of providers with a solid expertise in Cybersecurity for SMEs. We will need to create a shortlist of partners willing to be involved in the project (already ongoing).

Within our network of partners, we have several actors ready to help us build the selection committee. They need to help us assess the quality of the SMEs' "project" and find the best way/actor to help it. Once the selection is done and the collaboration ongoing, the committee will monitor the result of the "project".

2. Putting in place the action's organisation and the communication campaign

Once the right partners are selected, we will put in place the processes needed to receive, evaluate and follow-up on the SME's case. The idea is to stay as fast and agile as possible – the purpose of this action is not to create brand new projects, it is to implement the Digital Wallonia Strategy via the strengthening of the SME's cybersecurity, using the cyber voucher.

We will launch a dedicated communication campaign, based on experience and personas close to the SME's needs. We will use social media, mailing, Digital Wallonia website and the network of our partners (federal level, universities, network of businesses...).

3. Start of the action and follow-up

As soon as the action is launched and we receive the first applications, we will move to give a quick response to the candidates and initiate the first collaboration. We will probably have to adjust parts of the action "on the fly", depending on the type of cases and candidates received.

We will ask of the candidates to give us a feedback about the implementation to correct our course of action if needed and to provide (if possible) a

success story that will be use in future communication and awareness campaign.

Players involved

1. Private actors

- Infopole cluster TIC

This partner is the Walloon network for IT professionals and is involved with us since the beginning of Keep It Secure. They provide us with an efficient way to contact IT companies in Wallonia and test some of our ideas before reaching out to the public.

- Cyber security coalition

The Cyber Security Coalition is a unique partnership between players from the academic world, the public authorities, and the private sector to join forces in the fight against cybercrime. They will help us regarding the communication and to reach potential candidates.

- European Cyber Security Organisation (ECSO)

2. Public actors

- Agence du Numérique (ADN)

The Agence du Numérique (AdN) is a subsidiary of the Walloon Agency for Enterprise and Innovation (AEI). AdN is responsible for implementing the Digital Wallonia strategy, which has the following objectives:

- Fast-tracking Wallonia's participation and integration in the digital economy.
- Encouraging the development of a real Walloon digital industry, producing goods and services with high added value.
- Integrating digital technology for the growth and competitiveness of enterprises.
- Developing a digital culture among the public and more specifically young

people in Wallonia as part of their education and training.

- Walloon administration

They are the responsible for the cyber voucher distribution and will be instrumental in all changes in our Policy.

- Centre for Cyber Security Belgium (CCB)

The Centre for Cyber Security Belgium is the central authority for cyber security in Belgium. It will draft a national Cyber Security policy and encourage all relevant Belgian governments departments to make an adequate and integrated contribution. We will collaborate with them on multiple topics, including content, pool of experts, and communication.

Research centres

- Centre of Excellence in Information and Communication Technologies (CETIC)

As an applied research centre in the field of ICT, CETIC's mission is to support economic development by transferring the results of the most innovative research in ICT to companies, particularly SMEs. They are one of the two key partners for KIS and will also provide help for the creation and running of the selection committee and experts for this action

- Multitel Innovation Center

The mission of Multitel consists, as a priority, in helping Walloon companies to integrate effectively new technologies in their products, processes and services, in order to improve their competitiveness and to reach a sustainable economic prosperity. They are one of the two key partners for KIS and will also provide help for the creation and running of the selection committee and experts for this action.

Universities

- UCL

The university welcomes 32,000 students in seven locations in Brussels and Wallonia. Its main

campus is in the pedestrianised city of Louvain-la-Neuve. Our university offers courses in all disciplines, from bachelor's degree to doctoral degree level, as well as many lifelong learning programmes. They will provide help for the creation and running of the selection committee.

- UMons

The University of Mons, abbreviated to "UMONS" is one of five academic centres set up in the Wallonia-Brussels Federation as part of the restructuring of higher education, and is one of the founding members of the Pôle hainuyer, a cluster of hautes écoles, universities and other establishments. They will provide help for the creation and running of the selection committee.

- UNamur

The University campus is situated in the centre of the city of Namur, the capital of Wallonia (the French speaking region in Belgium), which is close to other major centres like Brussels. With 40 different programmes at the Bachelor, Master and Doctorate levels, the UNamur welcomes over 4,900 students in six Faculties: Arts, Law, Economics, Social Sciences and Business Administration, Computer Science, Medicine and Sciences. They will provide help for the creation and running of the selection committee.

Timeframe

The preparation of this action will be started end of 2021 or beginning of 2022.

We are already busy reaching to our partners for the constitution of the selection committee and the curated list of cybersecurity providers.

Summary:

- Creation of the selection committee and the creation of a list of cyber providers → end of Q4
- Putting in place the action's organisation and the communication campaign → Q2 2022

- Starting the action and follow-up → Q3 2022.

Cost

Human resource:

Salary of cybersecurity expert ADN: +- 100K€ and already approved in the ADN's budget

Selection Committee members: no cost foreseen

Material, events and licences

Communication campaign: This action will be part of a wider communication campaign, with a separate budget.

Platform costs : 1500€ per year

Event venue cost: TBD, the Covid-19 situation is still too cloudy at the moment.

Funding sources

There will be two different sources :

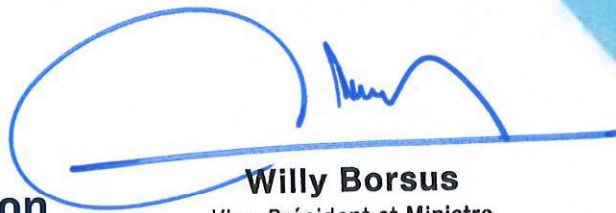
1. The cost to implement this action will be supported using a dedicated budget inside our agency (ADN). We are financed in by the Walloon government to create, develop and maintain the Digital Strategy and this action falls within our scope and can make use of the already approved budget. We have a 10K forecast for this particular action, for the beginning.
2. Budget allocated by the Walloon region to finance the cyber vouchers scheme

Monitoring and indicators

- Number of cyber vouchers used by SMEs (measurement unit: n° of cyber vouchers)
- Number of SMEs participating in this action (measurement unit: n° of SMEs)

Date 9/12/2021.

Signature



Stamp of the organisation

Willy Borsus
Vice-Président et Ministre



CYBER
Interreg Europe



European Union
European Regional
Development Fund