ACTION PLAN FOR A STRONGER CYBERSECURITY INDUSTRY

in the Stockholm Region

Region Stockholm

Action Plan for a Stronger Cybersecurity Industry
RS 2024-0587

Action plan under the Business and Growth Strategy for the Stockholm Region
RS 2020-0780

November 2024

Graphic design and production: Luxlucid

Introduction

THE ACTION PLAN FOR A STRONGER CYBERSECURITY INDUSTRY IN THE STOCKHOLM REGION is based on the Business and Growth Strategy for the Stockholm Region, and will contribute to the vision of the Stockholm region as Europe's most attractive metropolitan region. The action plan is limited to the cybersecurity subset of the ICT, tech and digitalisation priority area, which is one of four smart specialisation areas that have been identified as strategically important for public research and innovation efforts in the Stockholm region[1].

Cybersecurity as a competitive advantage for the Stockholm region

The need for cybersecurity is intensifying as digitalisation accelerates and AI and digital tools are increasingly applied in both the public and private sectors. In 2021, 76 percent of Sweden's entrepreneurs were affected by cybercrime at least once, with almost half not fully recovered one year after the attack[2]. The estimated costs of cybersecurity breaches at Swedish companies amounted to around SEK 30 billion in 2021, double the figure for 2019[3].

Cybersecurity is a shared responsibility that requires cooperation to strengthen society's defence capabilities against cyberattacks. This cooperation between sectors must clearly define roles and responsibilities to effectively build a strong and growing cybersecurity industry in the Stockholm region.

The Stockholm region is home to cutting-edge research and expertise in cybersecurity, as well as several fast-growing companies in the field. There is potential to develop a strong cluster, bringing together academic knowledge and entrepreneurial and practical expertise. In providing the necessary security and confidence in technologies and services, cybersecurity is also crucial for the development of other specialised areas.

There is a need for a comprehensive approach to the growth and overall needs of the cybersecurity sector in the Stockholm region. The industry has highlighted the need for new approaches to education and training to fill the current skills gap. Cooperation between educational institutions, private companies and the public sector is essential to ensure that training programmes are relevant, and to enable graduates to quickly enter the world of work. Neutral meeting places are needed in which different sectors can meet and discuss cybersecurity-related issues, and where academia and the business community can engage on challenges and shared solutions for a stronger cybersecurity industry in the Stockholm region.

[1] Read more about the Business and Growth Strategy for the Stockholm Region and smart specialisation on page 8.
[2] Swedish Federation of Business Owners: Är det it-säkert? (Is it cybersecure?), 2022
[3] Stockholm Chamber of Commerce: Cyberbrott mot svenska företag (Cybercrime against Swedish companies), 2022

Production

This action plan has been produced in consultation with Kista Science City, which in turn has held dialogues and meetings with representatives from both regional and national actors, including companies, trade associations, universities, research institutes and other relevant stakeholders. Relevant studies and reports have also been used to inform the development of this action plan.

Implementation

The smart specialisation action plans are implemented in collaboration between Region Stockholm and actors relevant to the smart specialisation area in question. Implementation of the action plans is coordinated within relevant groupings or networks. If necessary, a coordination group is formed. In accordance with the recommendations from the European Commission, initiatives and development in the priority areas for smart specialisation must be continuously monitored and evaluated. Region Stockholm does this within the framework of action plan follow-up and feedback to the government. If necessary, the activities of the action plans are adjusted during follow-up.

Goals and activities

For the Action Plan for a Stronger Cybersecurity Industry in the Stockholm Region, three goals and associated activities have been formulated based on the vision and goals for the development of the Stockholm region set out in the Business and Growth Strategy:

GOAL 1:

Develop an internationally attractive cybersecurity cluster in the Stockholm region

Activities:

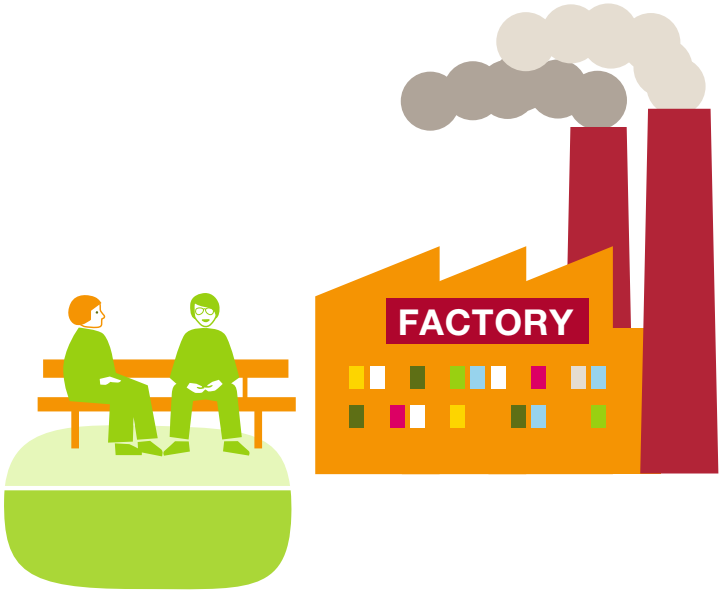
1. Survey and needs analysis: Conduct a detailed survey of all relevant actors (companies, organisations, academic institutions) to identify their activities, needs and challenges and see how these can be addressed via regional interventions. Analyse the data collected to identify trends, clusters and emerging opportunities, and to categorise the type of cybersecurity companies.
2. Report: Publish and communicate a report containing the results of the survey, highlighting relevant areas in cybersecurity, growth trends and the Stockholm region's international position of strength in this area. The analysis is to provide an idea of the current conditions for continued growth within the region and international competitiveness.
3. Identification of initiatives and partnerships: Identify current and future initiatives and possible partnerships that could encourage the development of the sector, including international cooperation.
4. Clustering activities: Organise and facilitate forums, events and roundtable discussions aimed at strengthening networks and collaboration within the cybersecurity cluster. Organise regular workshops and seminars to share knowledge and good practice.
5. Development of an attractive cluster platform: Create a platform for cybersecurity companies to showcase their expertise, foster cooperation and facilitate international exposure and business opportunities, as well as interact with the public sector. Examples might include introducing annual cybersecurity competitions in which individuals and start-ups can present solutions to genuine cybersecurity problems.
6. Targeted initiatives for SMEs: Develop targeted initiatives to help SMEs improve their cybersecurity position, for example through cybersecurity audits and training programmes.
7. Guidance on public funding: Provide guidance and support to businesses and organisations to leverage public funding, in particular from the EU, with the aim of strengthening the position and development of businesses for increased exports and investment. (Key national partners: Cybernoden and NCC-SE – Sweden's National Coordination Centre for Research and Innovation in Cybersecurity).
8. Internationalisation support: Analyse existing relevant internationalisation support and identify any need for new support and advisory programmes for companies looking to expand internationally. Work with regional and national actors to develop and provide potential new support.
9. Highlighting role models and success stories: Actively communicate cybersecurity success stories and role models to inspire and showcase opportunities within and/or outside the Stockholm region.

GOAL 2:

Capacity to develop and attract highly qualified cybersecurity expertise is strengthened in the Stockholm region

Activities:

1. Identify the skills supply needs of businesses and actors: Conduct a survey of all relevant actors (companies, organisations, academic institutions) to identify their current and future skills needs.
2. Analysis of existing training programmes: Conduct a detailed review of current training programmes related to cybersecurity to identify gaps and opportunities for improvement.
3. Proposals for improved cooperation to enhance skills: Develop proposals for closer cooperation between industry and the education sector, including internships, guest lectures and project work directly responding to industry needs.
4. Access to the right skills: Develop initiatives to support small, innovative companies in the Stockholm area to find staff with the right cybersecurity skills.
5. Proposals for improved cooperation in the recruitment of international talent and cutting-edge expertise: Develop proposals on how regional and national actors can work together to attract more international talent and expertise in cybersecurity to Sweden and the Stockholm region.
6. Development of new educational and training initiatives: Collaborate with educational institutions to create new programmes and courses that are directly aligned with industry requirements, including lifelong learning and training opportunities. (Key national partner: Cybercampus)
7. Explore opportunities to develop new educational and training programmes: Explore opportunities for academia and education providers to develop new cybersecurity education programmes such as vocational cybersecurity courses based on industry needs.
8. Incentives to stimulate the growth of talent: Analyse current opportunities and identify possible new ways to stimulate talent growth in cybersecurity, including students from undergraduate up to postgraduate level.



GOAL 3:

Value-adding partnerships contribute to new innovative cybersecurity solutions

Activities:

1. Creation of a Co-lab: Develop opportunities for cybersecurity companies to collaborate, exchange ideas and develop new innovative solutions with other stakeholders from both the public and private sectors.
2. Co-location opportunities: Provide a hub where these cooperative partners can meet face-to-face to work intensively on innovation and product development.
3. Stakeholder engagement: Invite representatives from the public and private sectors and other relevant stakeholders to work together to identify challenges that can be solved through new technologies and innovation.
4. Innovation through greater resilience in the public sector: Develop joint offers for public actors in the Stockholm region to boost skills and resilience in cybersecurity.
5. Support measures for innovative enterprises: Develop and implement actions that directly support businesses in developing new products and services, including support for prototyping and validation of digital solutions. For example, in other smart specialisation areas:
   - Life science, care and health: developing cybersecurity solutions to protect sensitive data and systems in the health sector.
   - Industrial transition through sustainable production: ensuring cybersecurity in the transition to sustainable production and Industry 4.0.
   - Climate and environmental initiatives for sustainable urban development: integrating cybersecurity into the development of sustainable urban projects and infrastructure.
6. Procurement as a catalyst for innovation: Use public procurement as a tool to drive innovation by setting requirements and allowing scope for innovative solutions in procurement processes.
7. International cooperation: Connect and collaborate with other leading cybersecurity nodes globally to exchange knowledge, experience and create opportunities for joint innovation and research projects and collaborations.

Smart specialisation in the Stockholm region

The Business and Growth Strategy for the Stockholm region, which is also the region's Research and Innovation Strategy for Smart Specialisation, was adopted in June 2021. The Business and Growth Strategy is a concretisation of the Stockholm Region's Development Strategy RUFS 2050, and will contribute to the vision of the Stockholm region as Europe's most attractive metropolitan region and the following goals:

- a leading growth and knowledge region
- an open, gender equal, equitable and inclusive region

A strategic direction with four focus areas has been identified based on global trends, the strengths and challenges of the Stockholm region, extensive analyses and broad dialogue with the region's actors through discussions, workshops and written input. The four strategic focus areas to strengthen and develop are:

- Research, innovation and smart specialisation
- The competitiveness of small and medium-sized enterprises (SMEs)
- Internationalisation, exports and investments
- Strategic skills provision

In connection with the 2014–2020 Structural Funds period, the EU Commission launched the concept of regional research and innovation strategies for smart specialisation as a condition for funding initiatives for research, innovation and technological development via the European Regional Development Fund (ERDF). The aim is to identify and prioritise a limited number of key areas where public funding for research and innovation is expected to have the greatest benefit, and where regional actors have the right conditions to develop international competitiveness.

Based on regional areas of strength in business, research and the public sector, a regional analysis and buy-in process was initiated in 2015, through which four smart specialisation areas were identified as strategically important for public research and innovation initiatives in the Stockholm region. In many cases, these are clearly anchored in various regional city centres and their research and innovation environments or clusters. These prioritised areas are:

- Life science, care and health (there is a specific strategy for this area: Life Sciences Strategy for the Stockholm Region RS 2019-0751).
- ICT, tech and digitalisation
- Industrial transition through sustainable production
- Climate and environmental initiatives for sustainable urban development

The areas prioritised for smart specialisation will be strengthened and developed through actions from the four strategic focus areas.

To achieve the vision and objectives above, several actors may need to take action, both within their own organisations and jointly. Action plans are being developed with a number of more specific goals and activities to create collaborative arenas for coordinating implementation.