National Cyber Security Centre
Ministry of Justice and Security

Starting a regional collaboration

Guide

Roadmap regional collaboration

The NCSC and its partners have created a roadmap to help you get started with a regional collaboration. In this roadmap, you will find three stages including concrete steps your organisation can undertake to create a successful regional collaboration.

Stage 1: **Explore**

Take time to make essential design choices:

- Identify enthusiastic organisations that are able to generate momentum.
- Organise a kick-off meeting for the leading group.
- Aim to get as much alignment as possible by discussing objectives, ambitions and needs.

Stage 2: **Develop**

Validate your ideas within a larger group and broaden support:

- Meet and intensify your relation with the different organisations in your regional cooperation.
- Establish a decision-making structure and organise financing and capacity.
- Ensure the cooperation has internal and external support.

Stage 3: **Action**

Expand the leading group into an interactive community:

- Create a roadmap with the activities for the first year.
- Continue to build the cybersecurity community within your regional ecosystem.
- Get inspiration from other regional collaborations.

Starting a regional collaboration

Collaboration within a regional ecosystem is an excellent way to increase the digital resilience of your organisation through a network of contacts nearby. And this can in turn boost the security of other organisations in your region.

Trust is key to exchanging knowledge and experiences in relation to cybersecurity, and with physical proximity trust is quick to establish and easy to maintain. This means collaborating within your regional ecosystem often opens up great opportunities. This guide highlights the experiences within a number of Dutch regional ecosystems in the cybersecurity domain.

Target audience

This guide is aimed at businesses and organisations looking to join forces within their region in order to enhance their digital resilience.

The following parties have contributed to this guide

Cybersecurity Center Maakindustrie, Cybersafety Noord-Nederland, Cyber Synergie Schiphol Ecosysteem (CYSSEC), Cyber Weerbaarheidscentrum Brainport (CWCB), Eindhoven Cyber Security Group (ECSG) and FERM-Rotterdam.

This guide is the result of a collaboration between

the National Cyber Security Centre (Ministry of Justice and Security) and the Digital Trust Center (Ministry of Economic Affairs and Climate Policy).

"Before organisations recognise the need for these types of initiatives, they must first acknowledge there is a need to strengthen their digital resilience."

CYSSEC

What do we mean by a regional ecosystem?

A regional ecosystem is based on the concept of ecosystems in nature. A natural ecosystem is a network of relationships between living organisms, characterised by a dynamic equilibrium, capacity for self-recovery and resilience to cope with a certain level of disruption. A 'cyber' ecosystem[1] is comparable with this. It encompasses a large number of diverse groups – private businesses, government bodies, individuals, processes and smart devices – which interact with each other for a range of purposes. Connected information infrastructures, processes, data and communication technologies create dependencies between these diverse groups.[2]

Sharing information is both an opportunity and a threat in an ecosystem. When information is exchanged and systems and processes are linked, new opportunities are generated for improving effectiveness and efficiency, as well as the development of new products. Yet those opportunities also mean an increase in the size of the attack surface, and more potential vulnerabilities and other challenges in maintaining the availability, integrity and confidentiality of ICT infrastructure.

Given the extent to which modern society has become digitised, it is no longer sufficient to look solely at our own digital security. Our investments in enhancing digital resilience must not only be focused on our own organisations, but also on the region within which we operate.

'The Port of Rotterdam is an ecosystem which links together a great number of businesses in some form or other, both physically and digitally. Disruptions can have a major impact on the process that allows secure and smooth entry to, and exit from, the port and of course also secure and smooth loading and unloading. We forge connections online as well as offline so we can guarantee the digital security of our businesses and the port together. We are FERM. That is not an acronym, but our Rotterdam way of expressing that we are resilient."

FERM-Rotterdam

A regional ecosystem is built up of organisations who besides operating from the same region have other things in common. Due to those shared interests within a region, creating an ecosystem that has digital resilience requires collaboration. Key to this is looking beyond the boundaries of our own organisations. This is the only way to counter digital threats within a region together.

1 https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

2 https://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf

Reasons to cooperate within your regional ecosystem

Collaboration within a regional ecosystem brings the following benefits:

- Learning from each other boosts your own digital resilience, along with that of your partners.
- It increases the awareness of digital threats within your regional ecosystem.
- Disruption to business continuity and loss of sensitive data or other damage (including to your reputation) can be prevented by giving each other timely warnings of potential attacks, using the expertise of colleagues and through the shared purchasing of solutions.
- If an incident occurs, there is a network of specialists close at hand who understand your circumstances and your type of organisation.
- It is beneficial to the business climate and it provides a wide range of challenging work in the cybersecurity domain which makes it easier to retain specialists within the region.
- It creates a secure environment which enables partners to exchange valuable information.
- There is a clear understanding of the dependencies of other organisations and systems within the ecosystem, meaning measures can be taken to reduce risks.

"The world around us has changed and our collective awareness of this is far from sufficient. Security must be comprehensible and accessible for all."

Cybersafety Noord-Nederland

How to start a collaboration within a regional ecosystem

A prerequisite for a good collaboration is that organisations already have basic measures in place for mitigating digital threats.[3]

When starting a regional cybersecurity ecosystem, the challenge lies in bringing together all the knowledge and expertise that is available. This often already adds up to more than you might think. Joining forces helps to elevate that knowledge and expertise to a higher level.

If your sights are set higher and your aim is to also safeguard business continuity, it is necessary to look beyond the results your own organisation can deliver. The key concern in case of an incident that impacts multiple organisations within a regional ecosystem, is having the ability to recover quickly. This is what collaboration in a regional ecosystem is all about.

The following sections outline specific steps that can be helpful when establishing a collaboration within your regional ecosystem. Remember that each partnership requires a customised approach, so the sequence of these steps can differ.

"CWCB was established to help small vendors (start-ups and SMEs) in their supply chain to also increase their resilience to digital attacks. Our initial group counted 11 members (ranging from start-ups to multinationals) and we are continuing to grow at a steady pace."

Cyber Weerbaarheidscentrum Brainport

Stage 1: Explore

Take time to make essential design choices

A key success factor for starting up regional collaboration is having a number of organisations that are willing to drive the collaboration forward. This could be by making time and resources available that enable the partnership to get off the ground.

Identify enthusiastic organisations

Organisations especially suitable for a leading role include those that are able to generate momentum and have a wide reach both inside and outside of the regional ecosystem. In this preparatory phase, keep the leading group small. A small leading group allows a certain level of trust to be quickly achieved, which in turn inspires confidence among other organisations in the region. Those organisations will be more inclined to join than with a leading group which covers too many different fields and sectors.

Possible candidates for the leading group include:
- central government, provinces and municipal authorities;
- security regions;
- police regions;
- major companies within a region;
- banks and insurance companies;
- branch organisations and interest groups;
- employers' or employees' associations;
- regional development companies.

When attending network meetings and conferences, sound out colleagues from these organisations about any interest in a regional collaboration in the area of cybersecurity. Also consider using existing partnerships within a region, such as those with a focus on physical security or innovation. In these cases, ensure there are clear agreements on who will take responsibility for which areas. Linking up with an existing partnership can offer a good route to realising your ambitions.

Consider discussing regional collaboration within an ecosystem on a small scale, such as with a colleague. Or deliver a presentation within your own organisation on regional collaboration in the field of cybersecurity. In raising awareness about the issue, use figures such as statistics on digital threats and the economic losses resulting from digital attacks, and provide examples of recent incidents.[4] There are also successful existing collaborations within Dutch ecosystems which you could use as an example.

3 https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html

4 https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html

"At the start, the key thing is to get everyone on the same page, which takes a lot of time and explanation. Linking up with existing partnerships can give you a head start here. We used BOOST, the Smart Industry network in the eastern Netherlands, which already sees businesses cooperate closely with local and other government bodies, interest groups and knowledge institutes."

Cybersecurity Center Maakindustrie

"ECSG came about as a result of a call for cybersecurity collaboration among the existing Eindhoven Manufacturing Group (consisting of approximately 70 executives)."

Eindhoven Cyber Security Group

Organise a kick-off meeting for the leading group

Once you have identified organisations that are willing to set to work, an initial meeting should be planned. This could be an informal meeting. Use this meeting of the brand-new leading group to get to know each other, and learn about the motivation and interests of each member.

Also use this meeting to start outlining the challenges. Aim to get as much alignment as possible by discussing the following topics:

Objectives and ambitions of the collaboration

- Define why the group has decided to take action.
- Define what each organisation wants to achieve through its membership of the collaboration and the role it envisions for itself.
- What are the joint objectives of the partnership?
- What arguments would persuade other organisations to join?
- What are the aims and next steps in the short term?

Needs and common factors

- Define the needs of your own organisation.
- Define the needs of the other organisations in the regional ecosystem.
- Define what connects the organisations in the regional ecosystem.
- Define the shared digital challenges within the regional ecosystem.
- Are lots of similar systems being used? Do organisations share physical or digital connections? What are the known dependencies?
- What would be realistic, achievable and logical in terms of the scope of collaboration?
- What is the cybersecurity maturity level within the regional ecosystem?

"Here in the eastern Netherlands we started out as a small core group and we then looked to expand and inspire others. We also made extensive use of declarations of intent, in order to reach as many prospective members that could also be potential investors."

Cybersecurity Center Maakindustrie

Stakeholder and SWOT analysis

Conduct a concise stakeholder and SWOT analysis to build a basic understanding of the stakeholders and existing partnerships within the region. Use the following questions and the afore-mentioned methods of analysis to guide you:

- Who are the key stakeholders in the area of cybersecurity within the regional ecosystem?
- Does the group know of any cybersecurity specialists in other organisations who may be willing to contribute or who should definitely be involved?
- Are the right people involved?
- What are the boundaries of the regional ecosystem? How many organisations are included?
- What type of organisations will initially be eligible for participation? Will the collaboration focus on large corporates, SMEs or start-ups, or perhaps a combination of these?
- Could the regional ecosystem be subdivided into sectors, supply chains or maturity levels?
- Are there any existing partnerships or other regional organisations that could play a facilitating role?
- What makes the collaboration in the regional ecosystem unique?

At the start, be modest when setting ambitions. If the initial ambitions are too wide-ranging, organisations may quickly drop out. If the ambitions are high, results will be more difficult while requiring a great deal of time and money. Start by focusing specifically on current needs and link them to activities that provide tangible results. Celebrating success, however small, will help to bring the group together.

"Begin in a small group and help each other straightaway by offering specific advice on current issues. This immediately generates tangible results and added value. If you also establish good rules and a structured set-up, everything else will follow."

Cyber Weerbaarheidscentrum Brainport

Stage 2: Develop

Validate your ideas within a larger group and broaden support

Within the leading group, begin with a round of introductions based on the stakeholder and SWOT analysis to get further acquainted with the regional ecosystem. Approach conversations with an open mind and make sure to include all the information that is already known about the ambitions, objectives and needs of the other organisations in the leading group.

Bring more organisations into the collaboration

Step by step, expand the leading group adding enthusiastic organisations that also want to contribute. Design a flyer or a presentation in which you briefly explain the initiative. Then take this to a network meeting in your region. Tools such as these will help kindle enthusiasm in other organisations and encourage them to become active participants in the initiative. Give an example of how an incident would impact your own organisation and highlight the interdependencies and possible impact for the region. This provides new organisations with reasons to invest in the regional ecosystem. As an alternative, you could develop a fictitious scenario which visualises the impact of a cybersecurity incident within the regional ecosystem.

At the same time, it is important for the leading group to consider how to steer the collaborative efforts. There must be sufficient support among the participating organisations for expanding and maintaining the regional ecosystem.

Establish a decision-making structure and organise financing and capacity

Ensure that individual organisations from the leading group free up capacity (in terms of hours and staff) so time can be spent on setting up the collaboration and getting things moving. It is possible to achieve a great deal in this phase without any expenditure. As the first successes materialise and organisations are able to see that the efforts are bearing fruit, there will be greater incentive for them to contribute financially. Discuss the following questions within the leading group:

Responsibilities, roles and coordination

- Which party or parties will take the lead in the collaboration? Will this include all the organisations currently in the leading group?
- Do all the organisations in the leading group have an influence on the direction and results of the initiative?
- Which role(s) would each of the organisations involved prefer?
- Who will lead the project and who will be able to influence its direction?
- Who will the lead partners be accountable to with regard to the choices made? And in what way will they render account?

Financing and capacity

- Are all the organisations currently at the table able to contribute equally and are they in fact able to take a leading role?
- How will the collaboration go about organising the working hours that are needed in order to take action? Will members contribute a sum, is there a participant who is able and willing to provide the (initial) financing, or will members provide capacity?
- Will each of the members of the leading group make an equal contribution or will there be a small number of lead partners working with a flexible layer of collaborative partners?
- Can one or more organisations within the leading group offer capacity? Or will capacity be sourced elsewhere?

Linking up with existing structures is key, as this prevents duplication of effort and promotes coordination. Time and money are allocated much more readily to ideas with a solid foundation, rather than those that have yet prove themselves.

"Explain that cybersecurity can also bring opportunities and do not focus solely on the vulnerabilities. This will deter those who have little affinity with the topic."

Cybersecurity Center Maakindustrie

"Our advice would be not to overcomplicate matters. Just bring people together and get them to exchange information and support each other. This immediately generates enthusiasm and provides them with a specific direction, which encourages them to invest time and resources of their own."

Cyber Weerbaarheidscentrum Brainport

Ensure the collaboration has internal and external support

It is key to have support and commitment at various levels within each of the participating organisations. Experience shows this helps to give the collaboration another push in the right direction. In order to ensure this, it is necessary to demonstrate how collaboration will help to boost the digital resilience of your own organisation and that of the regional ecosystem as a whole. Specify and illustrate what added value you are able to offer the relevant organisations. The ideas, objectives and ambitions must be supported at management level to ensure time, funds and resources are actually allocated.

Once you have mobilised support at various levels, this must be formalised by signing a joint kick-off statement or declaration of intent. Another good opportunity for generating awareness around the collaboration is to seek publicity, via a kick-off event or otherwise. Using a kick-off event to publicly sign the declaration of intent will inspire other organisation to also become members.

"We increased our reach by organising a number of meetings for businesses, approaching the local press and asking several front runners from the regional business community to highlight the importance of the initiative within their own networks. A member of Provincial Executive of Overijssel also put in a great deal of effort to gaining access to major investors to secure private financing."

Cybersecurity Center Maakindustrie

All of which goes to say: raise awareness in your region.
Suggestions:

- Appoint a spokesperson and contact person for interested parties inside and outside of the regional ecosystem. At FERM-Rotterdam, for example, the Harbour Master fulfils the role of Port Cyber Resilience Officer.
- Set up a website and use it to publish current information and regular updates on the collaboration and progress made in relation to the expansion (see also Stage 3).
- Raise your profile by joining national awareness campaigns related to cybersecurity, such as Alert Online.[5]
- Organise your own event linked to a current theme that will attract attention in the region, such as a hackathon for children.
- Contact ecosystems who have reached a more advanced stage and exchange experiences on how to put a regional ecosystem on the map.

"At the outset, ensure the collaboration focuses on practical matters as much as possible. Do not spend time setting up a detailed governance model, but do ensure responsibilities are clear so that the collaboration develops. This could involve appointing someone to act as champion and facilitator."

NCSC

Stage 3: Action

Expand the leading group into an interactive community

In the previous stage, the leading group determined the initial outlines of the initiative and identified lead partners making time, funds and/or resources available to get things of the ground. Now the time for action has come. Do not set the bar too high initially, have the courage to try out new ideas, keep an open mind about feedback and adjust plans if necessary.

Experience has shown that the first year is mostly about building up a network within the regional ecosystem. The participating organisations want to learn more about each other and their respective needs and increase cybersecurity awareness within their organisation step by step. Stage 3 will look at how to create further structure within the initiative and establish a community.

Draw up a roadmap for the regional ecosystem together

Develop a shared vision. Begin by drawing up a roadmap which briefly outlines the activities you want to carry out in the first year. It is necessary to evaluate this outline repeatedly with the organisations in the regional ecosystem and make refinements and adjustments. Partnerships will face ups and downs, as is in the nature of things. Recognise that not each activity will have immediate appeal. This is why it is important to keep an open mind and learn from feedback from other organisations within the collaboration. Circumstances can mean plans need changing, so be flexible and adapt.

The roadmap could be structured in line with the incident response model (prevent, detect, respond, recovery) or according to the different levels of knowledge and experience that were identified in the exploration phase. Also bear in mind that it is not necessary for everyone to participate in each aspect. It is better to harness the energy of organisations around topics that have the most relevance for them.

Carry out activities that match the level and the phase that the region and the partnership have reached. Suppose one of the ambitions formulated is to establish a collective Computer Security Incident Response Team (CSIRT).[6] As this requires a high maturity level and a high level of trust among the participating organisations, this is generally not a realistic goal in the first year.

5 Visit https://www.alertonline.nl/en/home for further details.

6 Visit https://www.ncsc.nl/english/cooperation for additional tips on establishing a collective CSIRT.

Take enough time to get a proper overview and understanding of the issues in the region, in order to ensure the activities will gain traction and generate results. Provide regular progress updates to the leading group, so they can monitor the bigger picture and keep track of all the activities.

Continue to build the cybersecurity community within your regional ecosystem

Celebrate your successes, however small, with the organisations in the collaboration. Visible successes and tangible results help to build support within the regional ecosystem, mobilising stakeholders and sustaining the development of the regional ecosystem.

"Ensure that your activities involve the education sector in particular, both at senior secondary vocational level (MBO) and higher professional education level (HBO). Identify and work with a fixed contact within the educational sector who contributes ideas and participates in developments. This is a win-win for the educational sector and business community alike."

Cybersafety Noord-Nederland

A website is a very helpful resource when building the community and promoting further collaboration.[7] The website can be used to present different types of information, including:

- big and small successes;
- a meetings and events calendar;
- cybersecurity tips;
- tools and scans;
- cybersecurity updates;
- publicly available products and news in the field of cybersecurity.

"Our experience is that websites and platforms must be easy to use and offer practical information in order to be successful. It can be worthwhile to link up with existing platforms or make use of existing information."

CYSSEC

Platforms like these can develop into a secure environment where organisations can exchange confidential and other information. The platform can be used to contribute or obtain information and it provides a communication channel for all the participating organisations.

Take inspiration from what others are doing

The examples below are activities undertaken by existing regional ecosystems. These are provided as inspiration in developing your own initiative. They can also serve as a framework for structuring your own initiative.

Organise cybersecurity meetings

Organise meetings on a regular basis for the network. Invite one or more engaging speakers (cybersecurity specialists or leaders in other regional ecosystems) and select a topic that reflects the members' interests and concerns. These meetings will help to raise awareness, generate support and build a community in the area of cybersecurity.

"Link up with existing meetings, that is our key takeaway from organising the Cyber Roadshow. Especially SMEs will generally not attend events specifically focusing on cybersecurity."

Cybersafety Noord-Nederland

"Our most successful sessions are those we organise with parties from the ecosystem itself. Sessions like these enable them to discuss their own ideas, challenges and knowledge. They also provide insight into topical issues and allow truly valuable partnerships to be forged."

CYSSEC

"The Port Cybercafés provide a meeting place for port entrepreneurs. They can enjoy a drink together and benefit from an engaging, informative programme on practical topics in cybersecurity that are relevant to the port area, such as storage spoofing. In this way we simultaneously enhance our digital and social network."

FERM-Rotterdam

7 Visit https://ferm-rotterdam.nl, https://cyssec.nl and www.digitaltrustcenter.nl for additional information.

Organise a joint exercise in the regional ecosystem

It can be worthwhile to organise joint exercises for supply chains or other groups that share digital or physical links within the region.[8] This does not necessarily have to be a large-scale ICT simulation. A tabletop exercise following a scenario can also act as a powerful tool.

"In 2018 we will be organising the second Cybernautics exercise. This involves close collaboration between partners in the nautical field in order to jointly tackle a cyber crisis. The exercise is highly valued within the ecosystem."[9]

FERM-Rotterdam

In the event of an incident, it is crucial to be able to act quickly. This can only happen if the parties have considered this in advance, and are familiar with and have direct access to one another. Joint exercises are also useful, so that everyone is familiar with the approach to crisis resolution. In an ideal situation, cyber exercises should be held on a regular basis. This enables the parties involved to build a routine. In the longer term, crisis management exercises provide a suitable stepping stone for reaching clear agreements on collaboration during ICT incidents.

Encourage information sharing within the regional ecosystem

The Information Sharing and Analysis Centre (ISAC) model[10] is a suitable tool for information sharing based on trust, shared interests and equality. These three values are all prerequisites for sharing sensitive business information.

Scan

Carry out a scan of the ICT systems, hardware and software, and make sure to include the work processes and staff. Arrange for as many members as possible to carry out this scan. Where are the weak links? Alternatively, the partnership could purchase an easy-to-use self-assessment tool or scan that allows members to check whether they have the basics covered and their current level of digital security.

Organise 'friendly hacks' among members

A friendly hack can be used to form an accurate picture of the security status in a business. This involves a reliable and specialised organisation investigating the website and ICT environment of a partner in the ecosystem, either at no cost or for a reduced fee. Businesses can then take the lessons learned from a friendly hack to improve their security. After all, when an organisation participating in the regional ecosystem boosts its own security, this will have a positive impact on the other organisations.

The Digital Trust Center website lists a number of collaborative partnerships in regional ecosystems and their plans for the years ahead.

8 Visit https://www.ncsc.nl/english/cooperation for the Guide *Starting a Supply Chain Collaboration*, which offers additional suggestions on exercises within supply chains.

9 https://ferm-rotterdam.nl/nl/nieuws/cybernautics2017-rotterdamse-haven-oefent-cyberweerbaarheid

10 The Guide *Starting an ISAC* is available at https://www.ncsc.nl/english/cooperation.

Publication
National Cyber
Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl/english/cooperation
samenwerken@ncsc.nl
@ncsc_nl

October 2018