Global Good Practices

Practice: **Assess national cybersecurity capacity using a maturity model**

#MaturityModel

Capacity building is most effective when it builds on existing capacities. How can we have a better picture of current capacities and capabilities? Assessing national cybersecurity capability and readiness using a maturity model provides a comprehensive review of existing capacities which can be further developed, and offers recommendations for setting priorities.

Related thematic areas:

Policy and strategy

Culture and skills

Standards

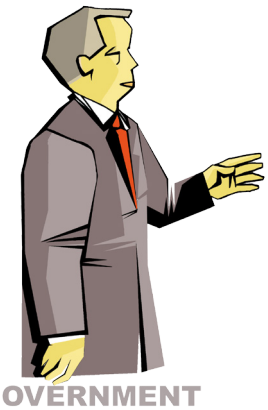
Cooperation and community building

Of particular interest to:

CIVIL SOCIETY

PRIVATE SECTOR

EXPERTS



GOVERNMENT

Description

As countries turn to planning their strategic cybersecurity steps, it is of the utmost importance to assess their existing capacities and capabilities. Using a cybersecurity **maturity model** allows governments to do a comprehensive review of a country's cybersecurity capacity, where it stands, what the gaps are and what concretely could be done to improve, and how to build capacity. Based on the results, policymakers and other stakeholders are able to set priorities for capacity building and investment.

Actors (or who this is for)

- Governments, and in particular, their agencies responsible for cybersecurity, or other institutions responsible for capacity building in this field.
- Regional and international organisations that wish to support the cybersecurity capacity building of their member states with a view to strengthening national, regional, and global cybersecurity.
- Academia, civil society, ISPs, and the banking sector – as participants in consultations.

The big picture

One of the key principles of capacity building is to work from existing capacities and an understanding of where further capacity is needed. Clearly, this requires that existing capacities are assessed and understood before planning how to build on them. The practice presented here addresses this requirement.

Another important aspect of this practice is its comprehensive approach, which corresponds with the recommendation that capacity building is carried out in a systematic way, based on multiple criteria. The methodology used should be developed through a broad, multistakeholder collaboration, and should be a publicly available resource.

Equally important is the local ownership of the review process. The responsible governments must make the decision to carry out the assessment, and are responsible for using the results for making decisions and implementing recommendations.

Instructions

The country decides to carry out an assessment of its cybersecurity capacity. It should then look into existing models and explore which is feasible for the country's situation and whether cooperation with the institutions that conduct and facilitate those assessments is possible.

The steps vary depending on a model. In the case of the Cybersecurity Capacity Maturity Model for Nations (CMM) by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, the assessment is carried out by a team of the

institution providing a maturity model - or one of its partners once a country has requested and agreed on an assessment. The country then forms a host team, typically within a commission or a ministry, that is responsible for the organisation of the consultations. Possible challenges in implementation are related to limited funding and human resources, or to lack of political will and momentum.

An assessment can produce measurements for comparing the country's readiness with that of other countries, or produce a ranking; yet different models may have different outputs. The main purpose of assessments may be to provide a country with a 'health-check' and recommendations for future capacity building.

Timing

Timing depends on the model of assessment. For instance, in the case of the CMM, the assessment is a comprehensive review process composed of three-day in-country stakeholder consultations, and a review report based on the collected evidences and including recommendations. The whole process takes approximately three months.

Upon an agreement concluded with a country to carry out the review, the process takes about **three to six-week** preparatory phase which includes the organisation of venue and equipment, the selection and invitation of participants and preparatory desk research etc.

The preparatory phase is followed by a **three-day** intensive in-country review consisting of 9-10 sessions with in total 10 stakeholder clusters (including among others public and private sector, critical infrastructure, law enforcement, academia, and civil society).

The final **six-week** phase consists of the analysis of the focus group interviews and the drafting of a detailed report including recommendations, which is performed by the research team. This report is reviewed by a board of experts before the draft is shared with the country representatives for comment, feedback, and distribution.

Examples

The GFCE initiative "Assessing and developing cybersecurity capacity" is based on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the GCSCC at the University of Oxford. The CMM was developed in consultation with more than 200 international experts from governments, international organisations, academia, the private sector, and civil society. It assists countries in understanding their priorities for investment and development by assessing cybersecurity capacity maturity across five dimensions: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory frameworks; and standards, organisations, and technologies.

The CMM deployment has been supported by the governments of the UK and Norway, and in cooperation with strategic partners such as the World Bank, the ITU, the CTO, and the OAS. It has been deployed in more than 50 countries to date. The

GCSCC is actively working on broadening the network of implementing partners and is currently developing a collaboration framework with regional partner institutions.

Countries interested in using this approach to assess their cybersecurity capacity maturity, and to plan further capacity building, can contact the GCSCC or one of its partners to discuss and initiate the process. For countries with limited means, there are possibilities for financial support which can be explored through the GCSCC. Once the review is agreed, the GCSCC or an implementing partner will guide the country through the process.

Other notable examples of maturity assessment are the ITU GCI, and the global CRI developed by the Potomac Institute. The GCI is a multistakeholder initiative to measure the commitment of countries to cybersecurity, through analysing five categories: legal measures, technical measures, organisational measures, capacity building, and cooperation. The CRI, on the other hand, is a methodological framework for assessing cyber readiness across five essential elements: cyber national strategy, incident response, e-crime and legal capacity, information sharing, and cyber research and development.

Source, support, and mentoring

The need for the use of methods such as the CMM, and their potential effectiveness is tackled in:

- Cyber Security Capacity: Does It Matter? A paper by William H Dutton and Ruth Shillair, Michigan State University – Quello Center, as well as Sadie Creese, Maria Bada and Taylor Roberts from the GCSCC: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-security-capacity-does-it-matter
- Cybersecurity Capacity Maturity Model for Nations: https://www.thegfce.com/initiatives/a/assessing-and-developing-cybersecurity-capability/documents/publications/2017/02/13/cybersecurity-cmm-for-nations

Several well documented examples of the CMM from countries are available online:

- Lithuania Cybersecurity Capacity Review 2017: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/lithuania-cybersecurity-capacity-review-2017
- Senegal: Cybersecurity Capacity Review 2016: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/senegal-cybersecurity-capacity-review-2016
- Madagascar: Cybersecurity Capacity Review 2016: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/cmm_rapport_final_cybersecurite_madagascar.pdf
- The UK Cybersecurity Capacity Review 2015: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/uk-cybersecurity-capacity-review-2015
- An example of follow-up steps taken on the basis of a review: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-%E2%80%93-what-followed-cmm-review

More information on the ITU GCI:

- GCI 2017 Report: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx
- Country profiles: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx

More information on the global CRI by the Potomac Institute:

- Cyber Readiness Index 2.0 model: https://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf
- Country profiles: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

More information on the GFCE work:

- Assessing and Developing Cybersecurity Capability initiative: https://www.thegfce.com/initiatives/a/assessing-and-developing-cybersecurity-capability

Contact points:

- Carolin Weisser (carolin.weisser@oxfordmartin.ox.ac.uk)
- Robert Collett (Robert.Collett@fco.gov.uk)