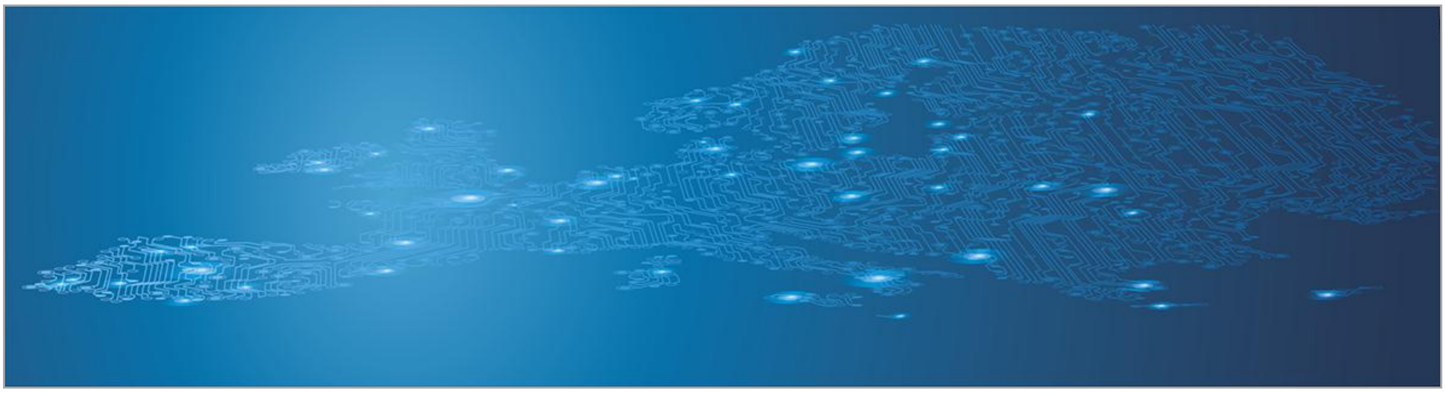

National-level Risk Assessments

An Analysis Report – executive summary

November 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

Executive summary

This report is based on a study and analysis of approaches to national-level risk assessment and threat modelling for cyber security which was conducted between April and October 2013. ENISA aims to provide an evidence-based methodology for establishing a National-level Risk Assessment in order to contribute to the wider objective of improving national contingency planning practices (NCPs)[1]. This report will help towards rationalising national risk assessments in EU Member States in order to reduce or eliminate vulnerabilities of critical Information and Communication Technology (ICT) services and infrastructures. This objective was articulated in the February 2013 European Cyber Security Strategy and thus sits within broader EU-wide efforts to improve crisis cooperation activities.

This report should be of use to policy-makers who are charged with implementing a CIIP or cyber security risk assessment programme. In addition, other interested parties may include regulators, researchers and senior industry representatives from Critical Information Infrastructure sectors.

In this study we have analysed current National-level Risk Assessment practices in around twenty countries and tried capture the main aspects of the implementation of their National-level Risk Assessments. Which of these aspects are most effective in a particular country depends to a certain extent on important administrative, economic, legal and cultural factors such as the dependence of society on cyberspace; the way in which government activities are conducted and the pre-existing state of the art in information security risk management. It is also important that National-level Risk Assessment programmes should be linked to a national cyber security strategy. A high-level cyber security strategy, clearly owned, can provide the context and ultimate rationale for a National-level Risk Assessment programme.

There are a number of permutations or variations in National-level Risk Assessment which may be implemented depending on the specific context of the country. Such possible options have been listed in this report, with clear guidelines for National-level Risk Assessment programme manager on how to identify these local specificities and requirements.

Regarding the identification of threats and modelling we have found that the most important are:

- articulated in a high-level strategy,
- based on scenarios,
- described qualitatively or quantitatively.

Concerning approaches to the conduct of a National-level Risk Assessment, they can be performed:

- through a formalised central framework or approach (a one-size-fits-all), or
- based on a decentralised model where each actor prepares their own risk assessment to be integrated by a coordinating authority.

Finally, national-level risk management methodologies may be based upon:

- Scenario-based approaches where actors are gathered together to consider scenarios in the round; such scenarios describe risks as a narrative and label them by applying simple categories of likelihood and impact (low, medium, high),
- Quantitative approaches which apply ordinal thresholds (e.g. a risk is classed severe if it affects 1 in 20,000), or

[1] For more on this topic see ENISA's Guide for National Contingency Plans: http://www.enisa.europa.eu/c3e/national-contingency-plans

- Approaches which combine elements of all of the above (for example, using scenarios and then qualitative and quantitative methods).

Key challenges

We have identified a number of key challenges for National-level Risk Assessment programmes, including:

- The lack of a harmonised national framework for cyber security, particularly with regard to terminology;
- Incomplete and diverse risk assessment methodologies (especially in the pan-European context);
- The lack of comprehensive methods to address threats;
- The need for effective risk management and preparedness capacity and skills;
- The need for more information sharing between different actors involved in a National-level Risk Assessment

Common lessons

The lessons learned are grouped into the following areas:

- The need to leverage international best practice, as many countries had visited others to learn about risk analysis practices;
- The importance of establishing effective collaboration between the public and private sectors, especially where in some cases the private sector owns considerable parts of the infrastructure;
- Finally, the need for effective critical information infrastructure approaches to be tailored to each national context.

Current priorities of National-level Risk Assessment programmes

Countries reported that they were focusing upon a number of priorities in the near to medium term, including the following:

- Improving understanding of threats and their effects upon society;
- Better incident management;
- Greater stakeholder involvement and information sharing;
- Improved national CIIP frameworks;
- Seeking further EU guidance and support.

In conclusion we can see that understanding of the national approach to cyber security and how risk decisions are taken in different countries is important to ensure that the results of any National-level Risk Assessment reach key decision-makers at the right time. It is also clear that there are a variety of approaches and levels of sophistication used in National-level Risk Assessments. **Qualitative** tools appeared to be preferred due to the complexities of understanding risk in the cyber domain. Depending on the preconditions regarding implementation, risk assessment could be performed using a **common set of methods** or in a more **decentralised fashion**. Challenges included the **diversity of methodologies** and approaches to National-level Risk Assessments (which highlights the need for this guidance document) as well as the complexities of **public–private cooperation**. As might be expected, many countries studied drew lessons from others when preparing their National-level Risk Assessment programmes. Some countries had identified priorities that they were seeking to focus on, including greater understanding of threats, improved stakeholder engagement and better national CIIP frameworks.

Recommendations

Based on an analysis of the data gathered we recommend the following:

1. Member States should understand better the underlying cyber threats and risks that they face and the impact to society.
2. Member States are advised to integrate National-level Risk Assessment into the lifecycle of NIS incident management and cooperation plans and procedures.
3. Member States should expand public–private sector dialogue and information sharing.
4. A practical step-by-step guide on how to perform National-level Risk Assessments should be developed, tested and maintained. Such a guide should be piloted by countries at the early stages of preparing their own National-level Risk Assessment programme. ENISA or another international institution would be appropriate bodies to oversee this action.
5. A catalogue of scenarios to help Member States in their National-level Risk Assessments should be established at EU level. Such a catalogue could be based on work already being done at ENISA on the threat landscape[2] and incident reporting[3].
6. The EU community of practitioners with an interest in cyber National-level Risk Assessments should be established and strengthened as information exchange platform, e.g., within the framework of the European Commission's NIS Platform[4].
7. Risk analysis expertise must be shared from other domains that assess complex cross-border risks, such as border security, financial services, aviation or public health for example within the European Commission's NIS Platform and other activities organised by ENISA.

[2] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment

[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting

[4] http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi, 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu