This FAQ covers ENISA's Good Practice Guide on Security Incident Reporting

Why did ENISA conduct a Good Practice Guide on Reporting Security Incidents?

Reporting security incidents plays an important role in enhancing the resilience of public communications networks. The more we know about major incidents the better we understand the threat environment. This enhances our ability to respond to future cases and strengthens our contingency plans and procedures.

The European Commission already highlighted the importance of incident reporting in a number of important policy documents. Actually, the newly adopted Telecom Package[1] introduces through article 13a and b mandatory reporting of major incidents.

What where the main objectives of the Good Practice Guide?

The main objective of the guide was to identify good practices on that topic and share them with policy makers of Member States throughout the EU. This could help Member States to improve existing reporting schemes or assist them in creating these based on good practices of others.

ENISA's role in facilitating this kind of cooperation and knowledge-sharing is emphasized and reinforced in recent EU statements, including the communication on CIIP, and now in the new reformed telecoms package.

Why is the focus on resilience so important?

The European Commission and the Member States pay increasing attention to the resilience of public electronic communications networks with the aim of ensuring that the infrastructure fulfils its role as a fundamental platform for European societies, economies and institutions.

How was the good practice guide on incident reporting developed?

ENISA performed an extensive stock taking of Member States activities with the aim to identify and analyse existing practices for incident reporting procedures. The report was prepared by surveying and interviewing public authorities, network operators, IT industry players, and network security experts about their experiences, expertise, and

[1] http://ec.europa.eu/information_society/policy/ecomm/tomorrow/index_en.htm

recommendations for effective practices in planning and implementing incident reporting procedures.

Is there a need for a good practice guide?

One of the key findings of the stock taking was that the incident reporting schemes varies a lot from one Member State to another. Some of the Member States have extensive systems although they too vary a lot, while others have yet to launch one.

Why is effective reporting so important?

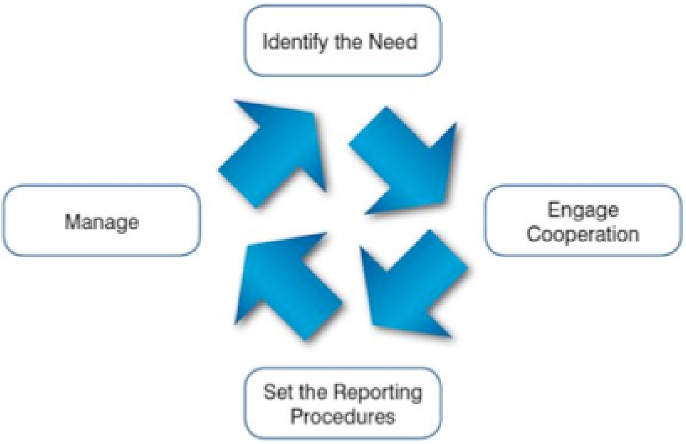
Basically, reporting is the cornerstone of a data collection framework. It is a clear need, since those Member States with little incident reporting in place, or with insufficiently effective schemes, have a need to introduce or adapt their schemes. But it is also an opportunity, since the existence of several diverse schemes in various locations provides many examples of types of schemes, approaches, objectives, procedures, etc.

Incident reporting ensures:

- ✓ quick dissemination of information among interested parties
- ✓ a coordinated response
- ✓ access to a wide pool of expertise about such incidents
- ✓ that national authorities can follow up with the infrastructure managers in a regulatory capacity
- ✓ threat analysis
- ✓ identification of good response and recovery practices

What are the steps in incident reporting?

Based on the analysis ENISA sees incident reporting as a lifecycle that involves the following phases:



Will the incident reporting across the EU improve?

There is a great deal of reason for optimism on several issues, especially after the implementation of article 13 a and b. First, national authorities should be able to implement effective incident reporting schemes. Also, national network resilience will increase as a result. International cooperation will be a facilitator of this development, as well as benefiting from it. These steps will play a useful part in the wider initiative to increase resilience of critical information infrastructure. And finally, these steps will play a useful part in the wider efforts to increase international cooperation among stakeholders in the efforts to increase network resilience.

What are ENISA's conclusions and recommendations?

As Europe's countries, institutions, businesses, and societies become increasingly dependent on information infrastructure, they must ensure the resilience of that infrastructure.

When it comes to incident reporting the study revealed that there is inconsistency in the implementation of early warning systems, information sharing, and coordination for incident response. Yet there is an enormous wealth of knowledge and experience with incident reporting in several Member States, from which others can learn. This report summarizes the variety of approaches encountered in a way that is intended to be useful both to the stakeholders launching a new reporting scheme, and to those trying to improve the standing procedures.

For full reports:
http://www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms

For further details contact:
Evangelos OUZOUNIS, Program Manager - Resilience and CIIP Program
Evangelos.Ouzounis@enisa.europa.eu

Ulf Bergstrom, ENISA's Spokesman
press@enisa.europa.eu, Mobile: +30 6948 460143