enisa
European Network and Information Security Agency

Critical Information Infrastructure:

How to successfully be prepared for emergency situations

Steve Purser
Head of Technical Competence Department

June 2011

Agenda

- ENISA’s Activities
- Supporting the CIIP Action Plan.

Who are we?

- The European Network & Information Security Agency (ENISA) was formed in 2004.
- The Agency is a *Centre of Expertise* that supports the Commission and the EU Member States in the area of information security.
- We facilitate the exchange of information between EU institutions, the public sector and the private sector.

Activities

- The Agency’s principal activities are as follows:
  - Advising and assisting the Commission and the Member States on information security.
  - Collecting and analysing data on security practices in Europe and emerging risks.
  - Promoting risk assessment and risk management methods.
  - Awareness-raising and co-operation between different actors in the information security field.

II. Supporting the CIIP Action Plan

The Commission CIIP Communication

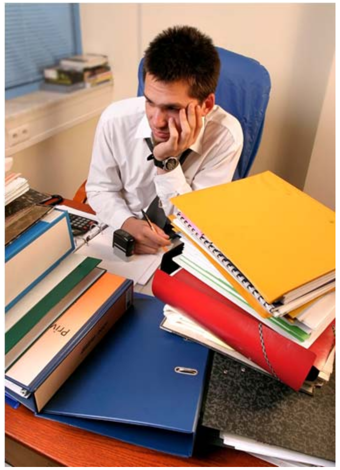
- "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" – published 30 March.
- Strengthens the role of ENISA.
- Activities within the scope of the European Program for Critical Infrastructure protection (EPCIP).
- Proposes five areas, or 'pillars', of action.
- ENISA is explicitly called upon to contribute to three of these areas.

The Role of ENISA

- ENISA's role is to proactively support Member States in achieving the objectives of the CIIP action plan.
- Member States must take the lead in addressing the issues.
- ENISA is currently supporting the CIIP action plan in a number of ways:
  - Assisting Member States in the planning process.
  - Setting up mechanisms to facilitate the establishment and day-to-day running of key instruments (European Forum for IS, EP3R, ...).
  - Providing input in the form of studies and best practices.

EFMS

- The European Forum for Member States builds on national approaches to CIIP.
- It will be used to foster common understanding of the issues and strategies for dealing with them.
- ENISA is supporting this initiative in the following way:
  - Assisting the Commission and Member States in defining a roadmap for the EFMS.
  - Ensuring exchange of expertise on policy and operational aspects.
  - Provision of good practice guides as a starting point.
  - Identifying significant risks and proposing suitable mitigation strategies.



EP3R

- The European PPP for Resilience will provide a framework for supporting collaboration between public and private sectors on NIS policy issues.
- There are many challenges in establishing such a PPP, but we can learn a lot from national initiatives.
- ENISA is supporting this initiative in the following way:
  - Summarising lessons learned from national PPPs.
  - Identifying challenges and obstacles.
  - Working together with Member States to identify a common approach.
  - Supporting the creation and day-to-day running of EP3R

www.enisa.europa.eu

First Pan European Exercise

- Table top exercise
- Incidents affecting all Member States
- Tested only communication aspects
- Involvement of public authorities/bodies only
- Concentrated on members of the CIIP community – no political escalation
- Test Carried out on 4 November 2010

Objectives

- Increase understanding of how cyber incidents are handled by Member States
- Test communication points and procedures between participating Member States
- Build trust among participants - help to establish mutual support procedures
- Create a CIIP community with a focus on exercises
- Highlight interdependencies between MS across Europe

Objectives - Measures

- Measures to test:
  - The contact points in the MS.
  - The communications channels and the type of data exchanged over these channels.
  - The understanding that MS have of the role and mandate of their counterparts in other MS.

The Scenario

- The scenario was not the focus of the test but was used to support the test.
- Based on a Cyber Incident.
  - The impact is on IP networks - large operators – cross country interconnections.
  - We assume that voice (PSTN/Mobile) communications are not affected.
  - Similarly, supporting facilities, such as power supply are not affected.
- Implemented as 320 injects.

Participation

- All EU Member States and 3 EFTA countries (Switzerland, Norway, Iceland) participated
- Profile of Participants:
  - Ministries, National Regulatory Agencies, CIIP and Information Security related organisations, CSIRTs and other related stakeholders
  - 70 organisations and 150 experts
- The role of ENISA was to help Member States to prepare - facilitation and project management.
- The role of the JRC was to provide scientific and technical support for the exercise itself.

Findings – Planning & Structure

- Planning phase benefited from the interaction among the participants and was key to success.
- The exercise was very resource intensive.
- The technical exercise set-up, the participants training and the Dry Run were also key success factors.
- The exercise set-up and scenario were well-chosen and enabled a varied level of activity throughout the exercise.
- Having Member State moderators in the same room as the players was very useful.

Findings – Building Trust

- Member States should develop the contacts made to establish a solid CIIP network.
- Member States should continue to organise pan-European exercises in the area of CIIP.
- Future exercises could involve a pre-exercise conference.
- ENISA should:
  - Facilitate the establishment of an information exchange mechanism.
  - Facilitate the creation of smaller sub-groups focusing on specific topics.
- Member States should:
  - Organise debriefing with their players in order to build trust.

Findings – Understanding

- The exercise increased the understanding of the MS on how incidents are handled.
- A deeper understanding could have been reached if national pre-exercise workshops had been conducted in the planning phase.
- Aligning procedures between MS would be a useful step towards pan-European crisis management.
- National contingency plans should be developed and tested on a regular basis.
- Procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be developed and tested in future exercises.

Findings – Points of Contact

- The ability to find the relevant points of contact varied between and within Member States.
- In the event of a real crisis, 55% of Member States were NOT confident that they could quickly locate the appropriate contact in another Member State.
- The most important characteristics of a useful directory are to be available, up-to-date, clear, well-structured and contain detailed information.
- ENISA should make directory information available via the exercise portal.
- The dialogue on Single Points of Contact should continue.

Main Recommendations

- The main recommendations that arose out of the exercise are as follows:
- Future exercises should involve the private sector.
- Lessons-learned should be shared with other national or international exercises.
- Member States should be well-organised internally:
  - E.g. By developing national contingency plans.
- A roadmap for pan-European exercises and preparedness should be created.
  - This will include the definition of Standard Procedures.

CYBER EUROPE 2012 - Next Steps

- Second pan European CIIP exercise
  - Official kick off in May 2011.
  - Liaising with other activities related to exercises will be key to success.
- Draft list of Standard Operating Procedures.
- Draft longer term Roadmap for Exercises
- Next Planning Workshop will be held in June.