First Steps towards a National Cyber Risk Assessment

Cyprus Efforts in NRA and National Contingency Planning

Costas Efthymiou
Office of the Commissioner of Electronic Communications and Postal Regulation
http://www.ocecpr.org.cy

24 September 2013
Overview

- Digital Cyprus
- National Cybersecurity Strategy
- National Risk Assessment
  - Why?
  - How?
  - Expected Outcomes
- Next Steps
Information Society – Digital Cyprus

- Infrastructure and Services Development
- Application Development
- Access to Content
- Network and Information Security
- Citizen Participation
- Trust

First Steps towards a National Cyber Risk Assessment – Cyprus Efforts
National Cybersecurity Strategy

Legal Framework

Technical and administrative measures

Coordination of public stakeholders

Capability Development

Incident Response

Effective public-private collaboration
Comprehensive National Response

National Cybersecurity Strategy

National Cyber Risk Assessment

National Contingency Plan for Critical Information Infrastructures
Critical Information Infrastructures
Need for a National Risk Assessment

➢ State of the World

• Computer security is not a new field, but in our age it needs a high level of effective cooperation between stakeholders
• Use of Information and Communication Technology (ICT) in all areas of life
• Many new threats continue to emerge in cyberspace and with constantly increasing levels of complexity
  • Sabotage, theft, fraud, physical destruction, data loss, denial of service, loss of productivity and many more

➢ Large scale disruption can have effects on a national level
Assessment Targets – everything?

- What is different on the national level?
- Risks to what? Protect what?
How can we do this?

- Critical infrastructures (CIs) are largely dependent on each other
- Studying these interdependencies will help identify and categorise CII assets
- Interdependencies also exist on the incident response level

Modelling Interdependencies

Threat Evaluation

- Cyber threats that ‘everyone’ faces
- Threats specific to us – i.e. special considerations?

Scenarios

- Impact-based
- Service-based
- Asset-based
Expected Outcomes

- Aid identification and prioritisation of critical information infrastructures
- Solid basis for a comprehensive National Contingency Plan
- Complement national risk assessments in other areas
- Valuable input to a number of national cybersecurity strategy actions
Next Steps

➢ Stock taking:
   ➢ Existing risk assessments across the critical sectors
   ➢ Existing contingency plans

➢ Actions as above:
   ➢ Modelling Interdependencies
   ➢ Threat Evaluation
   ➢ Scenarios

➢ Coherent inclusion in **one** national cyber risk assessment
Thank You!

- OCECPR - [http://www.ocecpr.org.cy](http://www.ocecpr.org.cy)
- Costas Efthymiou
  - Tel. +35722693169 [costas.efthymiou@ocecpr.org.cy](mailto:costas.efthymiou@ocecpr.org.cy)