Brussels, 27th September 2012

ENISA's Guide to successful National Cyber Security Strategies

Dr. Evangelos Ouzounis
Head of CIIP and Resilience Unit
ENISA

ENISA Guide: content, scope and target audience

- ✓ *Objectives*
  - ✓ *provide useful and practical recommendations to targeted stakeholders on the development, implementation, assessment and maintenance of a national CSS strategy*

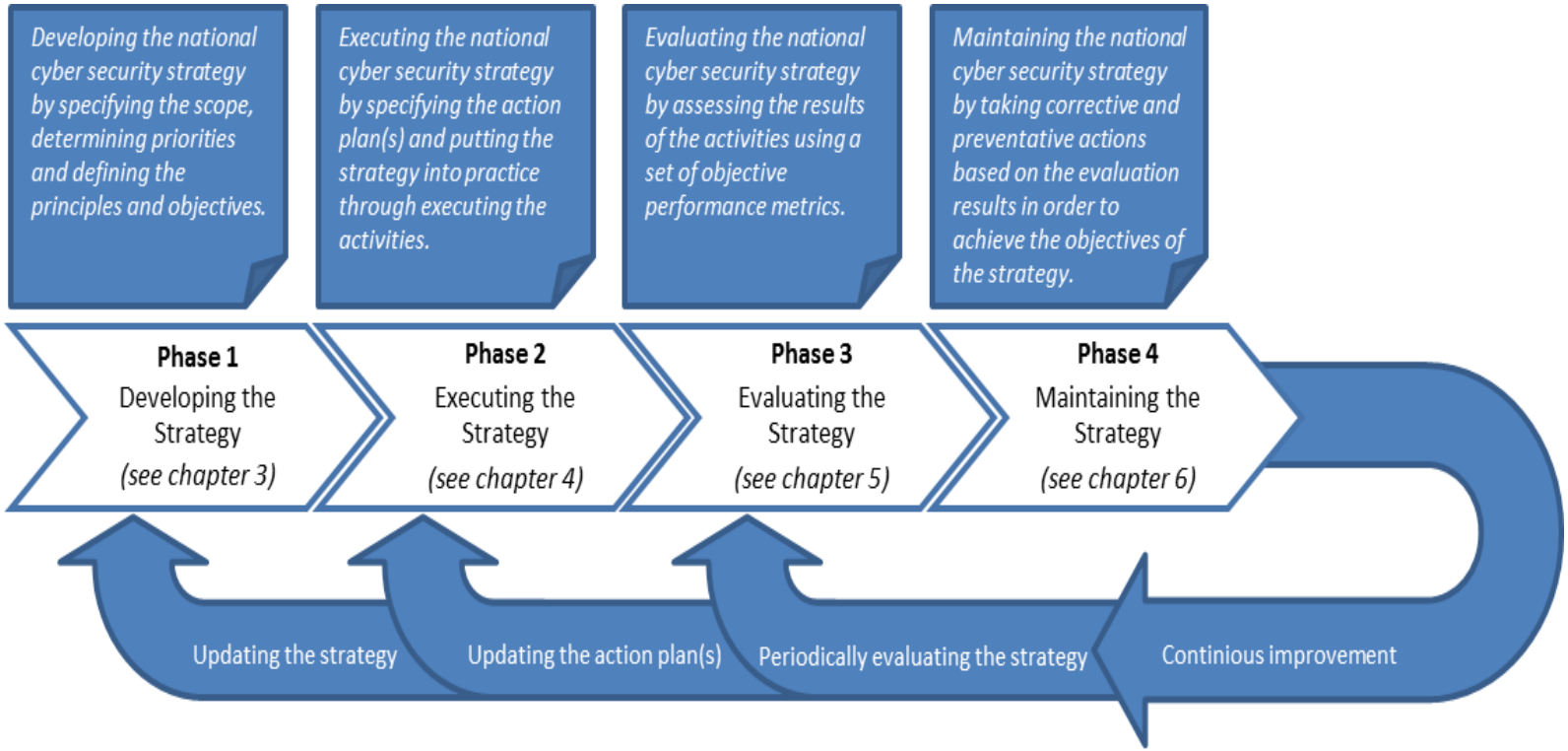
- ✓ *Key Elements*
  - ✓ *phases and elements of a lifecycle model*
  - ✓ *good practices, standards and policies*
  - ✓ *stakeholders and their roles*
  - ✓ *the challenges and barriers in developing, maintaining and implementing a CSS*

- ✓ *Targeted Stakeholders*
  - ✓ *Ministries, regulators, cyber security agencies, CERTs, national PPPs, ISPs, Cloud Computing providers, …*

Methodology

- ✓ *surveying and interviewing public authorities (such as Chief Information Security Officers, Chief Information Officers) and other IT/cyber security experts from various industry sectors*
- ✓ *a questionnaire has been distributed to experts from the Public Sector located primarily in the EU Member States (10 MSs) and in a non-EU country (Japan).*
- ✓ *17 Interviews have been performed with stakeholders from the private sector (such banking and telecom). The companies interviewed were located in 9 different MSs.*
- ✓ *A working group with experts from different EU and non EU MS that discussed the findings and made suggestions; they will also validate the final report*

Development Model



Phase 1: Developing the Strategy

Define priorities, principles and strategic objectives

An example: The vision, principles and objectives of the UK strategy

The vision for the UK in 2015 is "to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guide by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society."

The UK strategy includes the following objectives:

- ✓ ***Tackling cyber crime and making cyberspace secure in order to do business;***
- ✓ ***Being more resilient to cyber attacks and be able to better protect the interests of the UK in cyberspace;***
- ✓ ***Helping to shape an open, stable and vibrant cyberspace which the public can use safely and that supports open societies;***
- ✓ ***Having cross-cutting knowledge, skills and the capabilities to underpin all cyber security objectives of the UK.***

The UK strategy includes the following principles:

- ✓ ***A risk-based approach;***
- ✓ ***Working in partnerships;***
- ✓ ***Balancing security with freedom and privacy.***

Source: The UK Cyber Security Strategy

Phase 2: Executing the Strategy

Implement and enforce a governance framework in order to put the National Cyber Security Strategy into practice

An example: A governance framework in practice in The Netherlands

In the strategy of the Netherlands a public-private partnership has been created for the ICT Response Board which gives advice on measures to counteract major ICT disruptions to decision-making organisations. The Board began its activities in 2011 under the auspices of the National Cyber Security Centre.

Source: The National Cyber Security Strategy – Strength through cooperation, Ministry of Security and Justice, The Netherlands, The Hague, 2011.

Phase 3: Evaluating the Strategy

Evaluate whether the results correspond with the objectives

An example: United States - Cyber Storm

Cyber Storm, the US Department of Homeland Security's biennial exercise series, provides the framework for a government-sponsored cyber security exercise. An exercise as Cyber Storm delivers input for evaluating a strategy.

The Cyber Storm exercise series aims to strengthen cyber preparedness in the public and private sectors. The following activities are being carried out:

- ✓ ***Examine organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects;***
- ✓ ***Exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;***
- ✓ ***Validate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and***
- ✓ ***Examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.***

Source: Website of US Department of Homeland Security, Cyber Security, United States of America, 2012.

Phase 4: Maintaining the Strategy

Monitor the progress of the activities from the action plan

An example: The first and second national strategy on information security of Japan

In 2006 Japan released its first national strategy on information security. The strategy is based on a three-year plan from 2006 till 2009. In 2009 the strategy was evaluated and , based on the results, a second national strategy on information security was developed. The second strategy focuses on the time span from 2009 till 2012.

Source: The First National Strategy on Information Security - Toward the creation of a trustworthy society, The Information Security Policy Council, Japan, 2006. (2) The Second National Strategy on Information Security - Aiming for Strong "Individual" and "Society" in IT Age, National Information Security Policy Council, Japan, 2009.

Objectives of the Workshop

- ✓ *Debate about existing National Cyber Security Strategies*
- ✓ *Share expertise and knowledge from the MS who did it*
- ✓ *Identify good practices, barriers and challenges to help new MS to develop a CSS*
- ✓ *Validate ENISA's findings and/or propose new suggestions to be included in the guide*
- ✓ *Relate this work with Commission's efforts to develop an EU wide CSS*