ENISA National Cyber Security Strategies workshop

Minutes of the workshop

Brussels, 27th September 2012

Contributors to the meeting minutes

ENISA would like to recognise the contribution of PwC Netherlands that prepared these minutes in collaboration with and on behalf of ENISA.

Agreements or Acknowledgements

ENISA would like to thank all the participants to the National Cyber Security Strategies Workshop for their contribution and for the valuable inputs provided during the event.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contents

1 Introduction

1.1 Overview

On the 27th September 2012, ENISA organised a National Cyber Security Strategies Workshop.

The **aim of the workshop** was to:

- present the existing national cyber security strategy documents within the European Union and in other countries;
- discuss and validate the initial findings and recommendations included in the ENISA draft deliverable 'Good Practice Guide on Cyber Security Strategies';
- debate key elements of a National Cyber Security Strategy;
- relate this project with the European Commission's efforts to develop an EU wide Cyber Security Strategy.

Around thirty five people participated at the workshop representing public institutions and private organisations across Europe.

The format and the agenda of the workshop were planned to encourage an open dialog amongst the workshop participants. This dialog allowed the participants to discuss the most relevant cyber security topics and to gather the opinions and inputs of the attendees to be further processed and include in the ENISA final deliverable which publication is foreseen in Q4, 2012.

The agenda of the workshop was the following:

10:00 - 10:15	Registration and coffee	
10:15 - 10:30	*ENISA Good Practice Guide on Cyber Security Strategies*	*Evangelos Ouzounis, ENISA*
10:30 - 11:00	*The European Strategy for Cyber Security*	*Ann-Sofie Ronnlund, DG CONNECT*
11:00 - 11:30	Coffee Break	
11:30 - 12:00	*Comparative Analysis of National Cyber Security Strategies*	*Laurent Bernat,* OECD
12:00 - 13:00	*Panel I*: *The process for developing and implementing a national cyber security strategy*	*Chair:* Dr. Frederick Wamala (Author of the 'ITU National Cyber Security Strategy Guide') *Panel members:* Christian Daviot (French Network and Information Security Agency, France) Helena Raud (Department of State Information Systems, Estonia) Peter Wallström (Swedish Post and Telecom Authority, Sweden)
13:00 - 14:00	Lunch	
14:00 – 14:45	*Panel I*: The process for developing and implementing a national cyber security strategy - *continuation*	
14:45 - 15:15	Coffee Break	
15:15 - 17:00	*Panel II: Scope and elements of a National Cyber Security Strategy*	*Chair:* Marc Henauer (MELANI Operation and Information Center) *Panel members:* Dr. Günther Welsch (Federal Office for Information Security, Germany) David van Duren (National Cyber Security Centre, The Netherlands)
17:00 - 17:15	Wrap up and Next steps	*Nicole Falessi,* ENISA

2 Morning Session-Presentations

Dr. Evangelos Ouzounis, Head of CIIP and Resilience Unit at ENISA, opened the workshop. The initial findings of the ENISA draft deliverable 'Good Practice Guide on Cyber Security Strategies' was presented. In particular, the presentation provided an overview of: a) content, scope and target audience of the ENISA draft deliverable b) methodology used to collect data c) the cyber security strategy lifecycle model d) objectives of the workshop.

Ann-Sofie Ronnlund, Policy Officer – Unit H. 4 Trust & Security, DG CONNECT, presented the strategic priorities and actions of the European Strategy for Cyber Security, the main objectives of the legislative proposal on Network and Information Security and the public

consultation open until 15 October on 'Improving Network and Information Security in the EU'.

Laurent Bernat, Policy Officer – OECD Secretariat, presented the commonalities amongst National Cyber Security Strategies, emerging trends and action plans and some considerations by non-governmental stakeholder. Their study will be used as one of the basis for the upcoming review of the OECD Network and Information Security Guidelines that will be decided in October.

3 Morning Session – Panel I

After the morning presentations the discussion continued within Panel I: *The process for developing and implementing a national cyber security strategy.* Chair of Panel I was **Dr. Frederick Wamala**, Cyber Security Advisor, UK and members of the panel were **Christian Daviot** Strategy Advisor at French Network and Information Security Agency, France - **Helena Raud** National Cyber Security Co-ordinator-Ministry of Economic Affairs and Communications, Estonia and **Peter Wallström** Senior Adviser at the Network Security Department of the Swedish Post and Telecom Authority, Sweden.

The topic of Panel I has been introduced by Dr. Frederick Wamala through the presentation of the ITU National Cyber Security Strategy Guide highlighting how to get started and define the scope (Strategy development process) and who to involve and how (Cyber Security stakeholders). The Estonian and French National Cyber Security Strategies have been discussed. Peter Wallström presented the evolution of government cyber security strategies in Sweden. Earlier studies and inquires to develop the Swedish Strategy have been presented together with the strategic objectives, areas and principles of the Strategy for Societal Information Security 2010-2015.

The discussions of Panel I started before lunch and continued right after lunch. The topics discussed during the morning and afternoon session has been summarised below.

3.1 Topics for discussion and key findings – Panel I

1) <u>How to get started in developing a National Cyber security Strategy</u>

A Cyber Security Strategy should be country specific. Relevant national characteristics, the structure and governance in place in each country should be taken into consideration when developing the Strategy. The strategy should start with clear objectives i.e. how cyber security supports relevant national interests such as national security, economy, diplomacy and the promotion of national values. National threats, risks and critical information infrastructure protection should be taken into account. The cyber-crime topic should be part of the overall framework of a strategy but should not be the only focus. Organised crime groups are just one of six typical cyber threat sources. Other threat sources could include nation states, hacktivists, extremist organisations and disaffected employees. Different events trigger the

adoption of cyber security strategies. For example, a panellist noted that in their country a cyber-attack heightened focus on strategy creation. In particular, national cyber strategists should specify how cyber insecurities threaten national interests. Since the dependency on CII is not uniform across countries, it is important to determine the extent to which the cyber threats affect each country's interests. The level or intensity of the impact should determine the level of resources – legal, technical, procedural, organisational and capacity building – a country invests in cyber security activities.

Points were raised regarding the issue of risk analysis from a social economic perspective, which focus on the social and economic costs incurred by the economy at large when there is a disruption of a given infrastructure. This is an issue that goes much beyond what is traditionally considered the national interests (usually evaluated by a public body). In order to make an assessment of the social and economic costs the private sector and also the academia, the consumers have to be involved from the very beginning of the process. The pint is that the involvement of the private is not only due to the issue of property or knowledge

2) How to involve the private sector and incentivize collaboration?

The panel highlighted the inevitability of public-private partnership owing to the reality that neither government nor the private sector can resolve cyber security issues alone. Using the RACI[1] responsibility assignment matrix, the panel noted that whilst partnership is crucial, it is important to stress that the Government is accountable for Critical Information Infrastructure Protection (CIIP). Accountability for CIIP lies with the Government because the disruption of CII systems and services could lead to wide-ranging implications on public services, economic activities and national security. The public sector has unique contributions to make to the public-private partnership. These include: (a) devising legal tools that boost collective cyber security; (b) ability to maintain focus on cyber security issues that interest the private sector; (c) capacity to provide cyber security research incentives; and (d) access to classified intelligence sources that may generate unique information about cyber threats. The RACI matrix recognises the private sector is a major player within the national cyber security execution process with roles ranging for responsible, consulted and informed. Whilst national conditions differ, the private sector is usually responsible for implementing the requirements of the cyber security strategy under the law. Additionally, the private sector has unique incident response expertise as owners/operators of CII. The private sector should be smartly engaged in order to acquire knowledge to successfully execute the strategy. It is important to create commitment within the private sector by building trust and demonstrating the value of the public-private collaboration. In small EU countries, small private companies are not typically involved in the process; only critical services providers are included.

3) How to strike a balance between regulatory and voluntary approaches

[1] Responsible, Accountable, Consulted and Informed (RACI)

In the US forums are created for companies to produce industry best practices and standards. This prevents the industry sector to become over regulated. Some countries follow or are in favour of a trust based relationship – with minimum regulation - with the private sector which collaborates and is consulted by the government. Other countries follow a more strict/regulatory approach. The bottom line is that different legislative approaches and legal systems across EU should be investigated.

4) What are the top three KPIs for evaluating a strategy?

There are different ways of measuring the success of a strategy. However, the panel expressed concern that typical indicators tend to measure the current state i.e. retrospectively. The ideal situation is to evaluate the strategy looking forward rather than backwards. A public body such as a national cyber security focal point should be accountable for evaluating the success of the strategy's implementation. The public body may appoint an independent/third party organisation to undertake the actual evaluation work on its behalf. Alternatively, under self-regulatory regimes, the public body may work with industry associations to require self-reporting from CII owners and operators. The action plan should be dynamic and be adapted to the threats scenario which is constantly changing. In this sense, if metrics are adopted to evaluate a strategy, they should also be adapted and updated based on the current threats scenario. What is important is to focus on the threats sources rather than merely methods. Also, without a transparent and independent evaluation, a given strategy will never be sustainable in the long term and even worse no one will be able to manage it.

5) Should a National Cyber Security Strategy be made public?

Publishing a National Cyber Security Strategy is needed to show which direction a country is taking. Nevertheless, the panel noted that it is common practice not to disclose sensitive parts of the national cyber security strategy in particular areas dealing with national security. Public versions of the strategy also tend to focus on the broad vision rather than the real steps of the action plan. A panellist noted that crucial parts of their country's national cyber security strategy are written in a local language. The view at the workshop that cyber security strategy documents should be published was not unanimous. There are various valid and credible reasons (e.g. security, political etc) as to why a country might not publish a strategy document on cyber security. In such cases, aspects of the strategy can tactically be made available through public awareness campaigns.

4 Afternoon session – Panel II

After the second part discussion of the first panel, the discussions continued with Panel II: *Scope and elements of a national cyber security strategy*. Chair of Panel II was **Marc Henauer**, Head of MELANI Information and Operation Center, Switzerland and members of the panel were **Dr. Günther Welsch**, Head of Division 'Coordination and Governance' at the Federal Office for Information Security, Germany and **David van Duren**, Senior Policy advisor - Cyber security policy unit - Ministry of Security and Justice, The Netherlands.

Marc Henauer started by presenting the Swiss Cyber Strategy, its challenges, the logic framework, and the fundamental principles e.g. the followed risk management approach where the CEOs are responsible to take all the necessary measures to protect themselves from cyber security threats. David van Duren has then presented the Dutch Strategy highlighting goals and principles, lines of action and the cyber security threat assessment. Following, the German Strategy has been presented by Dr. Günther Welsch explaining the philosophy behind the strategy, its key elements and top priorities.

4.1 Topics for discussion and key findings – Panel II

1) How to facilitate the correct perception of cyber security issues?

The perception of cyber security issues might be influenced by vested interests just like many other areas. The aim is to collect facts in order to improve the perception of the problems. The lack of information and facts could be provided by a well- functioning CERT community which could provide structured information on threats. Given the different approaches to cyber security across EU countries, dialogue is a key element in creating a common understanding. Cyber Security is an international phenomenon which requires international cooperation and being internationally proactive. In this regard, one of the experts mentioned that in his country the information collection and analysis process is centralized in order to get a clear and complete picture of the issues. The implementation of mechanisms for centralizing information exchange could facilitate a correct understanding of the cyber security issues. It should be made sure though those mechanisms will not only trigger internal engagements within companies but also at a sectorial level (information exchange). Self-responsibility should apply to the private sector for sharing information. Awareness and knowledge are also relevant in order to create a mutual understanding in relation to the importance of cyber security and the issues at stake. Focus should be directed at awareness raising activities and trainings. Particularly this should be done by targeting all levels of society involving and educating citizens from an early age. Challenges still exist when it comes to the issue of aggregated situational awareness that usually is referred when we discuss information sharing and cooperation.

2) Should incident reporting be mandatory or voluntary?

One of the ideas raised during the discussions was that information should be shared on a voluntary basis and a mandatory/regulatory approach should be used only in case the voluntary one turns out to be a non- feasible option. One incentive to facilitate information sharing is the creation of a trustworthy environment as most of the risks are borne by the private sector and the consumers. In this regard, in relation to incident reporting there should be not only one entity/channel to report to but it should also be made sure that the information provided will be accordingly addressed and followed up. Following up is necessary in order to provide value for companies which share information.

5 Next steps

ENISA has informed the participants of the workshop that the inputs provided during the day will be further analysed and included in the ENISA final Report in order to enrich the content of the draft – previously circulated to the speakers of the workshop - and to particularly focus on the improvement of the recommendations included in the deliverable. The final report will be published before the end of 2012 on the ENISA website.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu