enisa
European Network and Information Security Agency

National Cyber Security Strategies

Practical Guide on Development and Execution

December 2012

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

Follow us on Facebook Twitter LinkedIn Youtube and RSS feeds

ENISA project team

Nicole FALESSI, Resilience and CIIP Unit, ENISA
Razvan GAVRILA, Resilience and CIIP Unit, ENISA
Maj Ritter KLEJNSTRUP, Resilience and CIIP Unit, ENISA
Konstantinos MOULINOS, Resilience and CIIP Unit, ENISA

Contact details

For questions related to this report or any other general inquiries about the resilience programme please use the following contact address: **resilience [at] enisa.europa.eu**

Contents

Executive summary

In order to respond to cyber threats in a constantly changing environment, EU Member States need to have flexible and dynamic cyber-security strategies. The cross-border nature of threats makes it essential to focus on strong international cooperation. Cooperation at pan-European level is necessary to effectively prepare for, but also respond to, cyber-attacks. Comprehensive national cyber security strategies are the first step in this direction.

At a European and International level, a harmonised definition of cyber security is lacking.[1] The understanding of cyber security and other key terms varies from country to country. [2] This influences the very different approaches to cyber-security strategies among countries. The lack of common understanding and approaches between countries may hamper international cooperation, the need for which is acknowledged by all.

ENISA has developed this guidebook aiming to identify the most common and recurrent elements and practices of national cyber security strategies (NCSSs), in the EU and non-EU countries. ENISA has studied existing NCSS, in terms of structure and content, in order to determine the relevance of the proposed measures for improving security and resilience.

Based on this analysis, ENISA has developed a guide that is aimed at Member State policy makers interested in managing the relevant cyber security processes within their country.

Within this context, ENISA has identified a set of concrete actions, which if implemented will lead to a coherent and holistic national cyber-security strategy. It is worth noting that many of the components and issues that should be addressed in such a strategy are horizontal or can fall into more than one of the categories you will find in this guide.

This guide also proposes a national cyber-security strategy lifecycle, with a special emphasis on the development and execution phase. For each component of the strategy a list of possible and indicative Key performance indicators (KPIs) will be described in the chapter dedicated to the evaluation and adjustment of the NCSS. Senior policy makers will find practical recommendations on how to control the overall development and improvement process and how to follow up on the status of national cyber-security affairs within their country.

In early 2012, ENISA published a white paper on national cyber security strategies. The paper includes a short analysis of the status of cyber security strategies within the European Union and elsewhere. It also identifies common themes and differences, and concludes with a series of observations and recommendations.[3]

---

[1] *H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf,* Ten National Cyber Security Strategies: a comparison, *CRITIS 2011 –6th International Conference on Critical information infrastructures Security, September 2011.*

[2] *The definition of cyber space, cyber-attacks and cyber security policies also varies from country to country.*

[3] *ENISA,* National Cyber Security Strategies, *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber security-strategies-ncsss/cyber security-strategies-paper*

1 Introduction

During the last few decades new technologies, e-services and interconnected networks have become increasingly embedded in our daily life. Businesses, society, government and national defence depend on the functioning of information technology (IT) and the operation of critical information infrastructures (CIIs). Transportation, communication, e-commerce, financial services, emergency services and utilities rely on the availability, integrity and confidentiality of information flowing through these infrastructures.

As society becomes more and more dependent on IT, the protection and availability of these critical assets are increasingly becoming a topic of national interest. Incidents causing disruption of critical infrastructures and IT services could cause major negative effects in the functioning of society and economy. As such, securing cyberspace has become one of the most important challenges of the 21st century. Thus, cyber security is increasingly regarded as a horizontal and strategic national issue affecting all levels of society.

A national cyber security strategy (hereafter 'strategy') is a tool to improve the security and resilience of national information infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such, it provides a strategic framework for a nation's approach to cyber security.

EU Member States need to have flexible and dynamic cyber-security strategies to meet new global threats. In light of this, and to assist the EU Member States, the European Network and Information Security Agency (ENISA)[4] has developed this guide, which presents good practices and recommendations on how to develop, implement and maintain a cyber-security strategy.

Developing a comprehensive strategy can pose many challenges. A document that ticks all the right boxes for what should be included can be easily made. However, this is unlikely to achieve any real impact in terms of improving the cyber security and resilience of a country. To develop a strategy it is necessary to achieve cooperation and agreement from a wide range of stakeholders on a common course of action – this will not be an easy task. It should be realised that the process of developing the strategy is probably as important as the final document.

1.1 The European policy context

The main regulatory and policy statements governing activities in the cyber-security strategy field are briefly summarised below.

The Strategy for a Secure Information Society

[4] *https://www.enisa.europa.eu*

The purpose of this Communication was to revitalise the European Commission strategy set out in 2001 in the Communication *Network and Information Security: proposal for a European Policy approach*.[5]

The Council Resolution of December 2009

The Council Resolution on a collaborative European approach on Network and Information Security of 18 December 2009 provides political direction on how the Member States, the European Commission, ENISA and stakeholders can play their part in enhancing the level of network and information security in Europe.[6]

The Council conclusions on CIIP of May 2011

The Council Conclusions take stock of the results achieved since the adoption of the CIIP action plan in 2009, launched to strengthen the security and resilience of vital information and communication technology infrastructures.[7]

The Electronic Communications Regulatory Framework

The review of the EU electronic communications regulatory framework and, in particular, the new provisions of Articles 13a and 13b of the Framework Directive and the amended Article 4 of the e-Privacy Directive aim at strengthening obligations for operators to ensure security and integrity of their networks and services, and to notify breaches of security, integrity and personal data to competent national authorities.[8]

The CIIP Action Plan

The Commission Communication *Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience* calls upon ENISA to support the Commission and Member States in implementing the CIIP Action Plan to strengthen the security and resilience of CIIs.[9]

The Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security' adopted on 31 March 2011

This Communication takes stock of the results achieved since the adoption of the CIIP action plan in 2009 launched to strengthen the security and resilience of vital information and

---

[5] *European Commission,* A Strategy for a Secure Information Society – 'Dialogue, partnership and empowerment', *COM(2006) 251*

[6] *Council of the European Union,* Council resolution of 18 December, 2009 on a collaborative approach to network and information security, *(2009/C 321 01)*

[7] *Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)*

[8] *Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)*

[9] *European Commission, Commission Communication on Critical Information Infrastructure Protection,* Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, *COM(2009)149.*

communication technology infrastructures. The next steps the Commission proposes for each action at both European and international level are also described.[10]

Review of the Data Protection Legal Framework

On 25/01/2012, the European Commission published its proposal for a regulation on data protection. This regulation will replace the existing Data Protection Directive.[11]

The Single Market Act

In April 2011, the European Commission adopted a Communication, the Single Market Act, a series of measures to boost the European economy and create jobs. This notably includes the key action entitled 'Legislation ensuring the mutual recognition of electronic identification and authentication across the EU and review of the Directive on Electronic Signatures'.[12]

The Digital Agenda

The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, and provides an action plan for making the best use of information and communications technology (ICT) to speed up economic recovery and lay the foundations of a sustainable digital future.[13]

The Internal Security Strategy for the European Union

The Internal Security Strategy lays out a European security model, which integrates among other things action on law enforcement and judicial cooperation, border management and civil protection, with due respect for shared European values, such as fundamental rights. This document includes a number of suggested actions for ENISA.[14]

The Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary

This conference took place on 14-15 April 2011. On this occasion, the Vice President of the European Commission and Commissioner for the Digital Agenda, Ms Neelie Kroes, acknowledged the progress made by Member States but also called for further actions and stressed the importance of international cooperation. In particular, as a follow-up to the Conference, Ms Kroes called on ENISA to intensify its activity of promoting existing good

---

[10] Achievements and next steps: towards global cyber security, *adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)*

[11] *European Commission,* Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

[12] *European Commission,* Single Market Act – Twelve levers to boost growth and strengthen confidence – 'Working Together To Create New Growth'*, COM(2011)467 Final*

[13] *European Commission,* A Digital Agenda for Europe*, COM(2010)245, May, 2010.*

[14] *Council of the European Union,* An EU Internal Security Strategy, *(6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf*

practice by involving all Member States in a peer-learning and mutual support process with the aim to promote faster progress and bring all Member States on par. Ms Kroes called on ENISA to establish a highly mobile dedicated team to support such process.

European Strategy for Cyber Security

At the time of writing, the European Strategy for Cyber Security is still under development. The text that follows is therefore a reflection of the current state of affairs and may well change. The goal of the initiative is to propose a comprehensive cyber-security strategy for Europe.[15]

EC proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market

The aim of the European Directive 1999/93/EC on a community framework for electronic signatures was the legal recognition of electronic signatures.[16] Assessing the need for secure and seamless electronic transactions as well as the shortcomings of the Directive, the European Commission adopted on 4 June 2012 a proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market.[17]

1.2 Scope

This guide aims to provide useful and practical recommendations to relevant public and private stakeholders on the development, implementation and maintenance of a cyber-security strategy. More specifically the guide aims to:

- ✓ define the areas of interest of a cyber-security strategy;
- ✓ identify useful recommendations for public and private stakeholders;
- ✓ help EU Member States to develop, manage, evaluate and upgrade their national cyber security strategy;
- ✓ contribute to the Commission's efforts towards an integrated pan-European cyber security strategy.

The guide describes:

- ✓ a simplified lifecycle model for developing, evaluating and maintaining a national cyber-security strategy;
- ✓ the main elements of each phase;
- ✓ good practices, recommendations and policies for each step.

---

[15] Update on European Strategy for Cyber Security, http://www.europarl.europa.eu/document/activities/cont/201207/20120712ATT48826/20120712ATT48826EN.pdf

[16] http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

[17] http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

1.3 Target audience

The target audience of this guide is public officials and policy makers: that is, those who usually lead the process of developing a national cyber-security strategy. The guide also provides useful insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders. Typical examples include policy makers, regulators, telecommunication providers and internet service providers (ISPs), online banks, utility companies, computer emergency response team (CERT) experts and others.

1.4 Methodology

This guide was prepared by surveying and interviewing public authorities, chief information security officers, chief information officers, security architects and other IT/cyber security experts from various industry sectors about their experiences, expertise, and recommendations for effective practices in developing, implementing, evaluating and maintaining strategies.

A questionnaire was prepared and distributed to representatives of the public sectors of EU Member States and of countries outside the EU. Several interviews were performed with stakeholders from the private sector. The companies interviewed were located in nine different EU Member States.

Following completion of this research, the results were analysed, recommendations were identified, and these findings were then prepared in the form of this guide.

A validation workshop was organised to assess the ENISA initial findings in September 2012.[18] Inputs and comments gathered during the workshop were elaborated and included in this guide.

1.5 How to use this guide

This guide can be used in a number of ways:

- ✓ as a practical, step-by-step guide for creating a brand new cyber-security strategy;
- ✓ as an incentive for enhancing or complementing parts of an existing national cyber-security strategy;
- ✓ as a benchmark for checking the effectiveness of actions in existing national cyber-security strategies;
- ✓ as a basis for improving the maintenance of existing national cyber-security strategies.

[18] *ENISA's Workshop on National Cyber Security Strategies, Brussels, September 2012, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/ncss-workshop*

2 National cyber security strategy lifecycle

In this guide, there are *two key phases* in governing a national cyber security strategy:

- ✓ developing and executing the strategy:
- ✓ evaluating and adjusting the strategy.

This structure follows Deming's 'Plan-Do-Check-Act' (PDCA) model for governing a national cyber-security strategy. The PDCA model is also used to check and continuously improve strategies, policies, processes and products.[19]

In addition, three approaches can be pursued in governing a strategy:

- ✓ a linear approach: the strategy will be developed, implemented, evaluated and eventually terminated (or replaced);
- ✓ a lifecycle approach: the output of the evaluation phase will be used to maintain and adjust the strategy itself;
- ✓ a hybrid approach: several continuous improvement cycles on different levels may exist.

Based on insights from the surveys and interviews, we have adopted a lifecycle approach since it better fits the needs and nature of the requirements of a national cyber-security strategy. Normally such strategies should quickly respond and/or adapt their actions to emerging cyber-security issues and emerging threats.

This report is an overview and the accent is on the development and execution phase of the lifecycle. In addition, we present high-level suggestions of indicative key performance indicators that could be used for evaluation purposes. ENISA plans to further pursue this topic in the future, with a second edition that will focus on the evaluation and adjustment phase.

[19] *It is also commonly used for structuring information security management systems, ISO/IEC 27001:2005*

3 Develop and execute the national cyber-security strategy

This chapter will aim at providing guidance to the steering and editorial teams of the strategy on the main components and actions that should be considered during the development and execution phases. Each sub-chapter will focus on specific objectives that require attention and a non-exhaustive list of tasks required to meet these objectives. In this sense, these phases will outline the core of the overall 'national philosophy' on cyber security.

3.1 Set the vision, scope, objectives and priorities

The Oxford Dictionary defines a strategy as a plan of actions designed to achieve a long-term or overall aim.[20] The aim of a cyber security strategy is to increase the global resilience and security of national ICT assets, which support critical functions of the state or of the society as a whole. Setting clear objectives and priorities is thus of paramount importance for successfully reaching this aim.

Typical tasks to consider in this step are listed here.

- ✓ Define the vision and scope that set the high-level objectives to be accomplished in a specific time frame (usually 5-10 years).
- ✓ Define the business sectors and services in scope for this strategy.
- ✓ Perform a comprehensive national risk assessment for determining the objectives and scope of the strategy.
- ✓ Prioritise objectives in terms of impact to the society, economy and citizens.
- ✓ Take stock of the current situation (e.g. policy, regulatory, operational, etc.).
- ✓ Involve the right stakeholders from the very beginning of the process to gain early 'buy in'.
- ✓ Define a roadmap for the implementation of the strategy, which may involve the following steps.
    - Define concrete activities that would meet the objectives of the strategy.
    - Develop a governance framework for the implementation, evaluation and maintenance of the strategy.
    - Develop a master plan for the implementation of the strategy.
    - Develop concrete action plans for each activity.
    - Define the evaluation of the strategy and its main actions (e.g. which key performance indicators (KPIs)) will be performed and by whom.

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, guided by our core values of liberty,

[20] Oxford English Dictionary, OUP, Oxford; 7th edition, 2012.

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 that the public can use safely and that supports open societies;
- having the 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 – Protecting and promoting the UK in a digital world, Cabinet Office, United Kingdom, London, 2011.

An example: The use of an action plan to execute the Japanese strategy

In December 2000 Japan formulated the Special Action Plan on Countermeasures to Cyber-terrorism for Critical Infrastructures. The action plan provided a framework for public and private sector cooperation in protecting seven critical infrastructure sectors. Because of the rapid spread in IT use, increased IT dependence in the critical infrastructure sectors and increased interdependence between critical infrastructures, a new action plan was formulated based on the document 'Basic Concept on Information Security Measures for Critical Infrastructures' in September 2005.

In December 2005 the Action Plan on Information Security Measures for Critical Infrastructures was adopted. The action plan provided an overall plan for protecting critical infrastructures against IT-malfunctions. In February 2009 the Second Action Plan on Information Security Measures for Critical Infrastructures was adopted.

Source: (1) *Special Action Plan on Countermeasures to Cyber-terrorism for Critical Infrastructures*, Cabinet Secretariat, Japan, 2000; (2) *Action Plan on Information Security Measures for Critical Infrastructures*, The Information Security Policy Council, Japan, 2005; (3) *The Second Action Plan on Information Security Measures for Critical Infrastructures*, The Information Security Policy Council, Japan, 2009.

3.2 Follow a national risk assessment approach

One of the key elements of a cyber-security strategy is the national risk assessment, with a specific focus on critical information infrastructures. Risk assessment is a scientific and technologically based process consisting of three steps: risk identification, risk analysis and risk evaluation.[21] The scope of the assessment is to coordinate the use of resources and to monitor, control, and minimise the probability and/or impact of unfortunate events that might put at risk the objectives of the vision.

Risk assessments can provide valuable information for developing, executing and evaluating a strategy. By carrying out a national risk assessment and aligning the objectives of the strategy with national security needs, it is possible to focus on the most important challenges with regard to cyber security.

In most cases, governments adopt an all-hazard approach (i.e. incorporating all kinds of cyber threats such as cyber crime, hacktivism, technical failures or breakdowns) when assessing the risks at national level.

Typical tasks to consider in this step are listed below.

- ✓ Agree on a risk assessment methodology to use; if this is not possible, tailor an existing one to the specific needs of national risks.
- ✓ Follow an all-hazard approach to risk identification and assessment.
- ✓ Define critical sectors and establish a sector specific protection plan. Activities in this task might include the following.
    - Identify assets and services critical to the proper functioning of the society and economy.
    - Assess all risks affecting the critical assets, prioritise them according to their impact[22] and calculate the probability of being realised.
    - Engage the right private-sector stakeholders, share with them their risk assessments and correlate them with your findings.
    - Decide which risks you mitigate and how, which risks you accept, and which risks you do nothing about (and be clear why you make these decisions).
    - Develop a national risk registry to store the identified risks.
    - Define a recurring process for continually monitoring threats and vulnerabilities and updating the national threat landscape.

An example: A risk-based approach as a principle in the UK strategy

The UK strategy includes a risk-based approach as one of its three underlying principles. The strategy states that: 'In a globalized world where all networked systems are potentially vulnerable and where cyber-attacks are difficult to detect, there can be no such thing as

[21] *ENISA, Glossary, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary*

[22] *Various metrics can be used for the impact assessment e.g. monetary units, people affected.*

absolute security. We will therefore apply a risk-based approach to prioritizing our response.' Source*: The UK Cyber Security Strategy – Protecting and promoting the UK in a digital world*, Cabinet Office, United Kingdom, London, 2011.

3.3 Take stock of existing policies, regulations and capabilities

Before defining in detail the objective of the cyber-security strategy, it is important to take stock of the status of the key elements of the strategy at national level. At the end of this activity important gaps must be identified.

Typical tasks to consider in this step include the following.

- ✓ Take stock of existing policies developed over the years in the area of cyber security (i.e electronic communications, data protection, information security); bear in mind that cyber security is/should be part of an overall national security policy framework.
- ✓ Identify all regulatory measures applied in different sectors and their impact, so far, in improving cyber security (e.g. mandatory incident reporting in the electronic communications sector).
- ✓ Take stock of existing capabilities developed for addressing operational cyber security challenges (e.g. national or governmental CERTs).
- ✓ Identify existing soft regulatory mechanisms (e.g. public and private partnerships) and assess the extent to which these have achieved their goals.
- ✓ Analyse the roles and responsibilities of existing public agencies mandated to deal with cyber security policies, regulations and operations (i.e energy regulators, electronic communications' regulators, data protection authorities, national cyber crime centres); identify overlaps and gaps.
- ✓ Assess the extent to which the existing policy, regulatory and operational environment meet the objectives and scope of the strategy; If not, identify the missing elements.

An example: An essential principle in the Strategy of the Czech Republic

It is highly desirable to support all initiatives, be they of the state (civilian, police, military) or of commercial or academic sectors, which have already accomplished a lot in the field of cyber security. Such joint efforts have led to improved cyber security and in many cases prevented dispersion of resources and unnecessary duplication. Much of the ICT infrastructure and many related products and services are provided by the private sector. Mutual trust and sharing of information are essential conditions of successful cooperation between the private and the public sectors.

Source: *Cyber Security Strategy of the Czech Republic for the 2011–2015 period*, Czech Republic, 2011

3.4 Develop a clear governance structure

The cyber security strategy will succeed only if a clear governance framework is in place. A governance framework defines the roles, responsibilities and accountability of all relevant

stakeholders. It provides a framework for dialogue and coordination of various activities undertaken in the lifecycle of the strategy.

A public body or an interagency/interministerial working group should be defined as the coordinator of the strategy. This will be the entity that has the overall responsibility for the strategy lifecycle and the strategy documentation itself. The structure of the coordinating entity, its exact responsibilities and its relationships with the other stakeholders should be clearly defined.

Typical tasks to consider in this step are listed here.

- ✓ Define who is the ultimate responsible for the management and evaluation of the strategy; usually it is a cyber security coordinator – or the nation's chief information (systems) officer (CIO/CISO) – who is appointed by the prime minister/president and is ultimately responsible for managing the cyber-security strategy.
- ✓ Define the management structure i.e an advisory body that advises the cyber security coordinator of the strategy. Specify the governmental and private parties taking part in this structure. Usually this is done through a national cyber security council, which has members from both public and private sectors. Try to cover the widest spectrum of stakeholders involved.
- ✓ Define the mandate (e.g. roles, responsibilities, processes, decision rights) and tasks of this advisory body (e.g. it manages the national risk management, assesses and prioritises emerging threats, responds to critical situations, manages the progress of the strategy, engages relevant stakeholders, fosters international cooperation etc).
- ✓ Define or confirm the mandate and tasks of the entities responsible for initiating and developing cyber-security policy and regulation; explain how these interact with and/or contribute to the advisory body.
- ✓ Define the mandate and tasks of the entities responsible for collecting threats and vulnerabilities, responding to cyber attacks, strengthening crisis management and others; explain how these interact with and/or contribute to the advisory body. Typical examples include a national cyber security centre (NCSC) which is tasked with protecting the national (critical) information infrastructures.
- ✓ Properly analyse and define the role of existing, , national cyber security and incident response teams (CERT) in both public and private sectors. The national/governmental CERT may be tasked with monitoring activities, trusted information sharing, providing news on emerging threats and other critical information infrastructure protection activities. The CERT may play a key role in cooperating and sharing information with other similar organizations at national and international level.

An example: A governance framework in practice in The Netherlands

In order to be able to adequately respond to various threats and to be able to return to a stable situation in the event of a disruption of attack, various response activities are necessary. The relevant organisation will in the first instance itself deal with ICT incidents which lead to a

breach of the availability, integrity or availability of the network and information infrastructure. The government will respond adequately where incidents can lead to social disruption or harming of vital objects, processes or persons.

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 (NCSS) – Strength through cooperation*, Ministry of Security and Justice, The Netherlands, The Hague, 2011.

An example: Responsibility for UK cyber security

The Office of Cyber Security was formed in 2009 and became the Office of Cyber Security and Information Assurance (OCSIA) in 2010. OCSIA is located in the Cabinet Office and coordinates cyber security programmes run by the UK government including location of the National Cyber Security Programme funding.

The Cyber Security Operations Centre (CSOC) was formed in 2009. CSOC is housed with GCHQ and is responsible for providing analysis and overarching situational awareness of cyber threats.

The Centre for the Protection of National Infrastructure (CPNI) provides guidance to national infrastructure organisations and businesses on protective security measures, including cyber.

CESG is the National Technical Authority for Information Assurance and is situated within GCHQ. CESG provides information security advice and a variety of information assurance services to government, defence and key infrastructure clients.

Computer emergency response teams (CERTs) exist in a number of public and private sector organisations. GovCERTUK is responsible for all government networks, while CSIRTUK, CPNI's CERT, responds to reported incidents concerning private sector networks in the critical national infrastructure.

Source: *Cyber Security in the UK*, Postnote No 389, September 2011.

3.5 Identify and engage stakeholders

A successful cyber-security strategy requires proper co-operation between public and private stakeholders. Identifying and engaging stakeholders are crucial steps for the success of the strategy. Public stakeholders usually have a policy, regulatory and operational mandate. They ensure the safety and security of the nation's critical infrastructures and services. Selected private entities should be part of the development process due to the fact that they are likely the owners of most of the critical information infrastructures and services.

Typical tasks to consider in this step include the following.

- ✓ Identify the owners of all critical infrastructures and services. Typical examples include energy, transport, finance, telecommunications, etc.
- ✓ Identify public stakeholders responsible for initiating and developing cyber security policy and regulation e.g. national telecommunications regulator, centre for the protection of national infrastructures etc.
- ✓ Engage both public and private stakeholders in the process by clearly defining their roles and responsibilities (e.g. private stakeholders protect their infrastructures and there is a joint responsibility with regard to protecting national security).
- ✓ Define the appropriate incentives that allow private and public stakeholders to participate in the process (e.g. no costly regulations). Take into account the possible different or even conflicting interests of the public and private sector.
- ✓ Involve the right stakeholders at the right time in the process of developing the strategy. Stakeholder involvement is necessary from a strategy content point of view and in order to gain commitment for executing the strategy later on.
- ✓ Explain how and why these stakeholders contribute to the objectives of the strategy, the individual tasks and the actions plans (e.g. pursue a collaborative approach together with critical infrastructure owners and critical service providers in assessing threats and risks).
- ✓ Assign the government the role of a facilitator. The government can facilitate activities on a national level, such as information-sharing, (international) cooperation and risk management.
- ✓ Involve top-level representatives in order to create ownership and assign an alternate for each representative.
- ✓ Involve specific critical infrastructure owners instead of allocating responsibilities to a specific sector. By allocating responsibilities to individual companies, these can be held responsible and/or even accountable for not taking proper security measures.
- ✓ Include civil society (end users, civilians) in executing the strategy from an awareness point of view. By raising awareness at a national level, citizens will better understand cyber-security risks and this will enable them to proactively take measures to lessen or mitigate risks.
- ✓ Involve ministries with responsibility for security, safety, crisis management, such as defence, interior, foreign affairs, justice, national telecommunication regulator, data protection authority, and cyber crime unit in developing the strategy.
- ✓ Involve existing national CERTs or CERT communities (of companies) as they may be a critical part of the information-sharing capabilities on a national level.
- ✓ Involve national interest groups in order to incorporate the interest of different stakeholder groups.

An example: Development of the Estonian strategy based on input from state agencies and working groups

The Implementation Plan of Estonia's strategy was developed on the basis of proposals from different state agencies and working groups which have been set up for development of the strategy. Attention was given to the actions and funds needed to achieve the objectives of the strategy in its various fields of competence. Implementation plans have been developed for two periods: 2008–2010 and 2011–2013.

Source: Cyber Security Strategy, Cyber Security Strategy Committee, Ministry of Defence, Estonia, Tallinn, 2008.

3.6 Establish trusted information-sharing mechanisms

Information-sharing among private and public stakeholders is a powerful mechanism to better understand a constantly changing environment. Information-sharing is a form of strategic partnership among key public and private stakeholders. Owners of critical infrastructures could potentially share with public authorities their input on mitigating emerging risks, threats, and vulnerabilities while public stakeholders could provide on a 'need to know basis' information on aspects related to the status of national security, including findings based on information collected by intelligence and cyber-crime units. Combining both views gives a very powerful insight on how the threat landscape evolves.

These are the typical objectives of an information sharing scheme.

- ✓ Assess the impact of incidents (e.g. security breaches, network failures, service interruptions).
- ✓ Identify, analyse, and adopt in co-ordinated manner appropriate, sector-wide minimum security measures to manage the threats associated with the incidents.
- ✓ Set up internal and joint procedures to continuously review the implementation of adopted measures.
- ✓ Provide unique, strategic insights to policy and decision-makers.

Typical tasks to consider in this step include the following.

- ✓ Properly define the information-sharing mechanism and the underlying principles and rules that govern the mechanism (e.g. non-disclosure agreements, traffic-light protocol, antitrust rules)
- ✓ Follow a sector approach to information sharing (e.g. one information-sharing platform for ISPs, one for energy etc). Make sure that there is enough information flow among the different information-sharing schemes.
- ✓ Focus on strategic issues and critical threats and vulnerabilities (e.g. major/critical disruptions).
- ✓ Provide the appropriate incentives for stakeholders (mostly for private ones) to participate and share sensitive information (sharing with the community the results of the analysis).
- ✓ Make sure that the right experts with the right profile take part in the scheme. Normally participants are high-level security experts (e.g. CISOs) able to share information at corporate level.

- ✓ Decide whether experts from law enforcement, intelligence, national/governmental CERTs and relevant regulatory bodies should be present.
- ✓ Keep the size of the information-sharing scheme relatively small to allow trust among experts to flourish.
- ✓ Organise regular (face-to-face) meetings to share sensitive information. Government should facilitate the process and provide logistical support. The initiative could be chaired both by the public sector and industry to symbolise the joint responsibility of the two stakeholders' categories.
- ✓ Identify other relevant European or international trusted information-sharing communities and decide whether to engage with them to expand your level of understanding, or not to.
- ✓ Update the national risk registry and distribute the collected information, in an anonymous way, to appropriate targeted users through the early-warning systems.

An example: The German Strategy

Quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators enables the National Cyber Response Centre to analyse IT incidents and give consolidated recommendations for action. The interests of the private sector to protect itself against crime and espionage in cyberspace should also be adequately taken into account. At the same time respective responsibilities must be observed. Every stakeholder takes the necessary measures in its remit on the basis of the jointly developed national cyber security assessment and coordinates them with the competent authorities as well as partners from industry and academia.

Source: *Cyber Security Strategy of Germany*, Federal Ministry of the Interior, 2011

3.7 Develop national cyber contingency plans

National cyber contingency plans (NCPs) are the interim structures and measures for responding to, and recovering services following, major incidents that involve critical information infrastructures (CIIs).[23] A national cyber security contingency plan should be part of an overall national contingency plan. It is also an integral part of the cyber security strategy.

The objectives of a NCP are to:

- ✓ present and explain the criteria that should be used to define a situation as a crisis;
- ✓ define key processes and actions for handling the crisis;
- ✓ clearly define the roles and responsibilities of different stakeholders during a cyber-crisis.

[23] *ENISA,* Good Practice Guide on National Contingency Plans for CIIs*, 2012, available on request.*

An NCP should be developed within a lifecycle. In essence, the lifecycle is a quality assurance and management cycle for such plans. Following that, the main steps for developing the NCP are the following.

- ✓ Perform an initial risk assessment, which will cover the process of identifying threats and vulnerabilities and their potential impact and will define a set of priorities.
- ✓ Engage the relevant stakeholders in the process and make sure their roles and responsibilities are clear and not overlapping.
- ✓ Develop the standard operating procedures (SOPs) for use by all relevant stakeholders during different crises.
- ✓ Develop the necessary cooperation and response framework to be used e.g. capabilities, procedures, non-disclosure agreements (NDAs) etc.
- ✓ Define the procedures to be used for dealing with the media during emergency situations.
- ✓ Test, evaluate and adjust procedures, capabilities and mechanisms; one proven way of doing this is through cyber exercises.
- ✓ Train the personnel responsible for offering the capabilities.
- ✓ Organise and execute exercises that will evaluate the existing standard operating procedures, roles and responsibilities and communication mechanisms.
- ✓ Review the contingency plan taking also into consideration lessons learnt from cyber exercises.

For more information on this topic, please check ENISA's webpage Good Practice Guide on National Contingency Plans.[24]

3.8 Organise cyber security exercises

Exercises enable competent authorities to test existing emergency plans, target specific weaknesses, increase cooperation between different sectors, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience. Cyber exercises are important tools to assess preparedness of a community against natural disasters, technology failures, cyber-attacks and emergencies.

Typical objectives for this step are to:

- ✓ identify what needs to be tested (plans and processes, people, infrastructure, response capabilities, cooperation capabilities, communication, etc.);
- ✓ set up a national cyber exercise planning team, with a clear mandate;
- ✓ integrate cyber exercises within the lifecycle of the national cyber security strategy or the national cyber contingency plan.

Typical tasks to consider in this step include the following.

- ✓ Develop a mid-term vision with concrete objectives to be achieved.

[24] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/national-contingency-plans

- ✓ Identify the relevant public and private sector stakeholders to be involved in the process.
- ✓ For each cyber exercise do the following.
  - Define the manager(s) of the exercise.
  - Define concrete objectives to reach; always relate them to the parts of the contingency plans to be tested.
  - Establish a planning team that will prepare the exercise and decide on important issues.
  - Agree on the scenario of the exercise; make sure that the scenario is pragmatic and based on real incidents.
  - Agree on the evaluation and monitoring approach to be followed.
  - Define a clear media and public affairs strategy.
  - Agree on international cooperation and the observers program.
  - Identify and engage the players of the exercise.
  - Develop a training program that will familiarise the players with all aspects of the exercise.
  - Prepare and execute a dry run that will ensure that the exercise is properly prepared.
  - Run the exercise; evaluate and monitor its progress.
  - Organise a hot wash the day after the exercise and collect and consolidate the main conclusions and the lessons learned.[25]
  - Report about the achievements, key findings and lessons learnt. A small, summary report can be widely published while a detailed report can remain confidential between the players of the exercises.
  - Follow up the lessons learned and the key recommendations and make sure the targeted stakeholders implement them.
- ✓ Assess the impact of one or the series of cyber exercises and update your vision to better meet the needs of the cyber security strategy.

For more information on this topic, please check ENISA's publication *Good Practice Guide on National Exercises*.[26]

[25] *'Held immediately following an exercise, a hot wash is a facilitated discussion among exercise players from each functional area. It is designed to capture feedback about any issues, concerns, or proposed improvements.' Source:* Information Assurance Challenges in an International Environment, *IATAC, available online at* http://iac.dtic.mil/csiac/download/Vol12_No4.pdf

[26] *ENISA,* Good Practice Guide on National Exercises –Enhancing the Resilience of Public Communication Networks, *2009.* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises/national-exercise-good-practice-guide

3.9 Establish baseline security requirements

All relevant public and private organisations should take necessary measures to protect their information infrastructure from threats, risks and vulnerabilities identified after the completion of the national risk assessment. Baseline security requirements for a given sector define the minimum security level that all organisations in that sector should comply with. Such requirements could be based on existing security standards or frameworks and good practices widely recognised by the industry.

Defining a minimum set of security measures is a complex exercise that should take into account the following aspects: the different level of maturity among the stakeholders, the differences in terms of the operational capacity of each organization and the different standards existing in each critical sector under consideration.

Typical objectives of this phase should be to:

- ✓ harmonise the different practices followed by the organizations both in public and the private sector;
- ✓ create a common language between the competent public authorities and the organisations;
- ✓ Enable different stakeholders to check and benchmark their cyber-security capabilities;
- ✓ share information about the cyber-security good practices in every different industry sector;
- ✓ help the stakeholders to prioritise their investments on security.

Typical tasks to consider include the following.

- ✓ Review and then update the existing set of measures.
  - Identify the security measures that already described in the existing regulatory documents.
  - Identify the information security threats and then map these threats to the existing measures.
  - Identify the gaps and derive mitigation measures from the existing technical standards (like ISO27001, ISO27002, ISO27004, COBIT, ITIL). Where gaps are found, enhance the list of measures by taking into account the opinion of the experts and the relevant standards.
  - Update the relevant regulatory texts with the new measures.
- ✓ Create security maturity self-assessment tools and encourage the stakeholder to use them.
- ✓ Mandate information security audits to competent authorities based on the list of the minimum measures.
- ✓ Update the baseline requirements based on reported incidents of significant impact.

3.10 Establish incident reporting mechanisms

Reporting security incidents plays an important role in enhancing national cyber security. The more a person knows about major incidents the better they can understand the threat environment. Incident reporting and analysis helps in adjusting and tailoring the security measures list, referred to in the previous section, to the changing threat landscape. This way, the national preparedness, response and recovery capabilities are enhanced.

Typical tasks of this activity include the following.

- ✓ Identify the need for incident reporting by:
  - deciding whether there are incident reporting schemes within the already existing national, European and international cyber security landscapes, and identifying gaps and needs that are presently not addressed and that a new scheme will have to cover or satisfy;
  - identifying the types of incidents to be reported and the purpose of the new scheme;
  - outlining the reporting requirements, especially the scheme's constituency (the potential reporting parties), the reporting obligation and the thresholds beyond which incidents should be reported.
- ✓ Engage cooperation with the involved parties by;
  - making use of existing arrangements and resources;
  - formulating the value proposition of the scheme;
  - raising awareness of the threats;
  - building trust with the participants;
  - addressing the private stakeholders' concerns.
- ✓ Set the reporting procedures by:
  - setting reporting requirements;
  - defining the prioritisation of incidents;
  - establishing follow-up procedures;
  - developing media policies.
- ✓ Manage the scheme: when the reporting procedures are set and running, the responsible authorities will need to pay attention to scheme management. The tasks in this stage fall into three groups:
  - analysing and following up on individual incidents;
  - conducting statistical analysis of a series of incidents;
  - examining feedback to improve and evolve the scheme.
- ✓ Communicate the results of the analysis to the competent authority or authorities responsible for updating the set of minimum security measures.

An example: MIMER/GLU Sweden

For their telecommunications outage reporting scheme, the Swedish Post and Telecom Agency (PTS) coordinates and cofinances a public–private partnership formed together with the larger telecommunications operators in Sweden. The participants include between five

and seven large telecommunications operators and the members of the Swedish Urban Network Association. The total infrastructure handled within the partnership adds up to about 80%–90% within the country. Additional telecommunications operators should be able to participate in the future.

Source: *Good Practices on Reporting Security Incidents*, ENISA, 2009.

3.11 User awareness

Raising awareness about cyber-security threats and vulnerabilities and their impact on society has become vital. Through awareness-raising, individual and corporate users can learn how to behave in the online world and protect themselves from typical risks. Awareness activities occur on an ongoing basis and use a variety of delivery methods to reach broad audiences.[27]

Security awareness activities may be triggered by different events or factors, which may be internal or external to an organisation. Major external factors could include: recent security breaches, threats and incidents, new risks, updates of security policy and/or strategy. Among the internal factors are new laws, new governments etc.[28]

Principles to follow in order to support an awareness-raising programme include the following.[29]

- ✓ Define the target of the awareness-raising campaign (e.g. citizens, children, end-users).
- ✓ Develop mechanisms for reaching out to these communities.
- ✓ Identify common behavioural problems affecting the target audience or issues that the target audience should know about.
- ✓ Create the national information security unique identity: choose specific information security topics that support the strategy objectives and then organise and advertise, not only in Europe but also internationally, local events by using appropriate communication channels.
- ✓ Organise a national cyber-security month, week or day in order to engage the public, and private- and public-sector partners through events and initiatives (i.e. campaigns, workshops, conferences) with different subject matter each time.[30]
- ✓ Enhance the content of well-known governmental web sites with information security related material e.g. presentations, webinars and lectures.
- ✓ Consider translating the material into other languages.

---

[27] *ENISA,* The new user's guide: How to raise information security awareness*, November 2010,* http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

[28] *See, for instance, the proposal for a regulation 'on electronic identification and trusted services for electronic transactions in the internal market'* http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

[29] *ENISA,* Raising awareness on information security across public and private organisations*, 2008.*

[30] *For further information on how to organise an information security month, see* European Month of Network and Information Security for All – A feasibility study, *ENISA, 2011,* http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2011/europeansecuritymonth

- ✓ Support and brand European or international information security initiatives like the Safer Internet.
- ✓ Participate in relevant European initiatives and campaigns like the Safer Internet Day, International Youth Day, ENISA's security month etc.

An example: The Finnish Strategy

National Information Security Strategy is to integrate information security firmly into the basic structures of the information society. This requires improvements in general information security awareness and skills, and better consideration of information security aspects in the purchase of systems and the procedures for making agreements. Increasing information security awareness and competence: the National Information Security Day project will be developed; awareness of information security will be improved, the level of awareness will be monitored and information security skills will be developed; a proactive plan for communications will be drawn up.

Source: Cyber Security Strategy of Finland

3.12 Foster R&D

Our lives depend on new IT tools and services. Before such tools and services become commercially widespread, it is important that research activities cover the cyber security requirements. A cyber security strategy should emphasise the importance of including – in the research and development lifecycle – concepts such as secure by design and privacy by design.

Typical objectives of this phase include the following.

- ✓ Identify the real causes of the vulnerabilities instead of repairing their impact.
- ✓ Bring together scientists from different disciplines to provide solutions to multidimensional and complex problems such as physical-cyber threats.
- ✓ Bring together the needs of industry and the findings of research, thus facilitating the transition from theory to practice.
- ✓ Find ways not only to maintain but also to increase the level of the public's trust in existing cyber infrastructure.

Typical tasks in this step comprise the following.

- ✓ Create a forum for industry and request R&D topics for consideration.
- ✓ Create an R&D agenda with topics that support the objectives of the cyber security strategy with a midterm horizon, of between four and seven years. For each topic the following should, at least, be described: the objective, the incentives and the challenges of the topic.
- ✓ Create a platform for bringing together high-level research and the private sector. This platform may take the form of a public–private partnership.

- ✓ Seek cooperation with similar European and international relevant activities i.e. the European Commission Research and Innovation programme (e.g. FP7/8).
- ✓ Create a coordination research plan in order to avoid overlaps between research activities undertaken by different institutions and programmes.
- ✓ Develop effective incentives to make cyber-security research ubiquitous. Both individuals and organisations might be the beneficiary of these incentives.

An example: The Estonian Strategy

It is important to stress that when it comes to cyber security, research and development cannot be separated from defence-related activities. Scientific research is important primarily because the implementation of protective measures for information systems is a rapidly advancing high-technology field. Efficient protection against malware is possible only if new versions of the threat are immediately identified and neutralised. The priority areas for development include intelligent protection software and the simulation of cyber-attacks to ensure cyber security and provide training. This line of research is also supported by the NATO Centre of Excellence of Cooperative Cyber Defence, based in Estonia.

Source: *Cyber Security Strategy*, Ministry of Defence, Estonia.

3.13 Strengthen training and educational programmes

Unfortunately, our universities and R&D institutions do not produce enough cyber-security experts to meet the increasing needs of this sector. Cyber security is usually not a separate academic topic but part of the computer science curriculum. Cyber security is also a continuously changing topic that requires constant training and education.

The objectives of a training and education program are to:

- ✓ enhance the operational capabilities of the existing information security workforce;
- ✓ encourage students to join and then prepare them to enter the cyber-security field;
- ✓ promote and encourage the relations between information security academic environments and the information security industry.

Typical tasks in this step include the following.

- ✓ Launch national information security training and educational programmes.
- ✓ Support the security accreditation and certification of skilled personnel in key working posts in every industrial sector.
- ✓ Create a catalogue of roles, and the relevant educational background needed, with information security responsibly.
- ✓ Add information security courses to university curricula – not only to the ones related with computer science but also to any other professional speciality tailored to the needs of that profession.
- ✓ Create a national register with accredited cyber-security experts with teaching skills.

An example: United Kingdom

The UK strategy states that 'As for business, some firms recognize the growing scale and impact of the risks. However, some sectors of the economy, particularly small and medium sized businesses, do not have access to the skills and knowledge to protect themselves online. We need to improve our understanding of the threat across the board and manage it more effectively. This can mean relying upon skills and knowledge, not often found in the same place.'

Source: The UK Cyber Security Strategy – Protecting and promoting the UK in a digital world, Cabinet Office, United Kingdom, London, 2011.

3.14 Establish an incident response capability

National/governmental CERTs play a key role in coordinating incident management with the relevant stakeholders at national level. In addition, they bear responsibility for cooperation with the national/governmental teams in other countries.[31]

In order to perform their tasks properly, it is important that the national cyber-security strategy empower CERTs with sufficient capabilities in the following categories.

- ✓ Mandate – this relates to the powers, roles and responsibilities that need to be allocated to the team by the respective government.
- ✓ Service portfolio – this covers the services that a team provides to its constituency or is using for its own internal functioning.
- ✓ Operational capabilities – these concern the technical and operational requirements a team must comply with.
- ✓ Cooperation capabilities – these encompass requirements regarding information-sharing with other teams that are not covered by the previous three categories e.g. policymakers, military, regulators, (critical information infrastructure) operators, law enforcement authorities.

The following tasks should be considered.

- ✓ Take steps to ensure that the CERTs can both carry out their mandate and adhere to national and EU data-protection legislation.
- ✓ Define procedures and best practices that require CERTs staff to handle data in compliance with EU rules and their Member State's laws. The risks to a CERT's reputation from a data breach or misuse of personal data are too significant for a CERT to risk non-compliance with data protection legislation.
- ✓ Establish working groups at international or regional meetings at which CERTs discuss best practices and the potential of instituting common data handling protocols.

[31] *ENISA's web page on baseline capabilities for national / governmental CERTs:* http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

- ✓ Establish thematic working groups on data protection to involve interested stakeholders, such as the banking industry, and improve the overall information exchange.
- ✓ Consider hiring or engaging a legal expert specialising in IT security issues in order to avoid uncertainty regarding handling of personal data.
- ✓ Create a national vulnerability database and constantly assess the potential impact on critical functions or potential disturbance of core operations.
- ✓ Initiate a national project on building an early warning system for CIIs. Such systems require the cooperation of a wide range of stakeholders, both private and public, and could potentially be the central capability for handling creeping, slow-burn and sudden crises.
- ✓ Create a vulnerability disclosure framework that deals with patch and vulnerability management (period, early warning, deployment requirements, etc.). Testbeds (clones/mirrors) should be considered in order to avoid major disturbances of systems after patching essential components of critical applications.

An example: The Finnish Strategy

Securing cyberspace largely relies on the exchange of information which, at the international level, is best achieved through co-operation networks. Such networks bolster the ability to take immediate actions in ensuring cyber security and combating cyber crime. The professional co-operation networks of the public and private sectors allow for the exchange of information on innovative IT solutions, best practice and other expert information. The exchange of expert information on cyber security requires close co-operation between the networks which deal with international data security, cyber defence and law enforcement. The most significant of these include the international network of national CERTs, the network of government CERTs (GovCERT), Interpol and Europol for co-operation in law enforcement, and organisations dealing with Critical Information Infrastructure Protection.

Source: The Cyber Security Strategy of Finland

3.15 Address cyber crime

The fight against cyber crime requires the collaboration of many actors and communities to be successful. In this respect, it is important to address and counter the rise of cyber crime and to prepare a concerted and coordinated response with relevant stakeholders.

Typical tasks that should be considered include the following:

- ✓ Adapt the required legislation and ratify existing international treaties.
- ✓ Create specialised national cyber crime units (law enforcement and judicial authorities).

- ✓ Ensure continuous and specialised training for police and judicial authority staff (e.g. on digital forensics).
- ✓ Develop knowledge and expertise on emerging cyber crime-related threats and vulnerabilities but also attack methods through information sharing at national and international level.
- ✓ Create a harmonised set of rules for police and judicial record-keeping and appropriate tools for statistical analysis of computer crime.
- ✓ Establish forums to foster cooperation between the various players (e.g. CERTs and intelligence communities).
- ✓ Encourage direct action by industry against computer-related crime.
- ✓ Establish cooperation with leading academic and R&D institutions on new digital forensic techniques.
- ✓ Establish cooperation between public and private sector stakeholders to quickly identify and respond to cyber crime related issues.

For more on this topic, please check the websites of both ENISA[32] and the European Commission[33] on cyber crime.

An example: The Czech Republic

The Czech Republic will improve legislative and procedural steps so that the cyber security field ultimately comprises prevention, detection, reaction and measures designed to identify and combat cyber crime.

Source: The Cyber Security Strategy of the Czech Republic

3.16 Engage in international cooperation

Cyber security threats and vulnerabilities are international in nature. Engaging in cooperation and information sharing with partners abroad is important to better understand and respond to a constantly changing threat environment.

The following points should be followed during the development of the strategy.

- ✓ Use the strategy as an instrument for fostering international cooperation. A strategy can indicate the Member State's stance towards international cooperation.
- ✓ Identify the countries you wish to cooperate with, explain why you want to engage with them and clarify the context of cooperation (e.g. cyber crime, operational) with each one.

[32] *http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cyber crime*

[33] *http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm*

- ✓ Assign to a national entity the task of promoting international cooperation. Assigning this task on a national level to a single organisation provides the benefit that all national efforts to cooperate internationally are consolidated.
- ✓ Promote international cooperation through information-sharing (for instance benchmarking, technological knowledge, and basic threat assessments), intelligence sharing, top level public–private partnerships (PPPs) (multinational), and potentially information sharing and analysis centres (ISACs).
- ✓ Join bilateral, multilateral or international treaties and conventions (e.g. International Code of Conduct for Information Security, Convention on Cyber crime) related to information security if they are compatible with the national regulatory framework and if this does not run counter to the interests of national security.
- ✓ Contribute to international efforts towards drafting standard operating procedures (SOPs) to be used for information sharing and response to real, major cross-country crises.
- ✓ Encourage participation in regional, European and international exercises as a means of supporting cooperation with strategic partners.

An example: The German Strategy

Given the global nature of information and communications technology, international coordination and appropriate networks focusing on foreign and security policy aspects are indispensable. This includes cooperation not only in the United Nations, but also in the EU, the Council of Europe, NATO, the G8, the OSCE and other multinational organizations. The aim is to ensure the coherence and capabilities of the international community to protect cyberspace.
Source: The Cyber Security Strategy of Germany

3.17 Establish a public–private partnership

A public–private partnership (PPP) establishes a common scope and objectives and uses defined roles and work methodology to achieve shared goals.[34] PPPs may focus on different aspects of security and resilience; these can be defined as the following:

- deterring (to deter attackers);
- protecting (uses research into new security threats);
- detecting (uses information-sharing to address new threats);
- responding (to deliver the capability to cope with the initial impact of an incident);
- recovering (to deliver the capability of repairing the final impact of an incident).

[34] *Cooperative Models for Effective Public Private Partnership - Good Practice Guide- ENISA, October 2011.*

PPPs addressing security and resilience have evolved in many countries as an efficient means of protecting their critical infrastructure. Building up a successful PPP requires taking into consideration different elements as well as the challenges and barriers such structures may face.

Typical elements to consider in setting up a successful PPP include the following.

- ✓ Assess the sectors in scope and the types of threat addressed; this will be a defining factor in shaping the membership and determining which external links are to be forged.
- ✓ Plan how to link the PPP with other organisations to share information and expertise and to avoid duplication.
- ✓ Assess the use of high-level strategic partnership at the CEO level in order to support senior understanding and awareness.
- ✓ Recruit real experts who are empowered from their organisations to act and change things.
- ✓ Seek legal advice to ensure that the legal framework used is suitable for the jurisdiction in which the PPP operates.
- ✓ Adopt information distribution policies such as the Traffic Light Protocol to give the source confidence that the information will be used only as agreed.
- ✓ Prepare together with a legal advisor a sample non-disclosure agreement (NDA) that describes the terms and conditions of the membership. Use this agreement and ask the parties involved to sign it.
- ✓ Make sure that all members of the partnership actively contribute in providing information, services and support that are of relevant value to the membership.
- ✓ Look for opportunities to create international links with other PPPs for cross-border sharing and collaboration.

An example: The Netherlands

ICT infrastructure, products and services are for the greater part supplied by private sectors. Continuity and certainty of supply are not only important for the business world in connection with their continuity. Society itself has an interest in this, e.g. to prevent social unrest due to disruptions. Mutual trust is essential for cooperation and sharing information with each other. Government and business communities must work together as equal partners. The relevant parties must derive benefit from participation in joint initiatives. A good cooperation model with clear tasks, responsibilities, powers and safeguards supports this.

Source: Cyber Security Strategy of the Netherlands

3.18 Balance security with privacy

Counter-terrorism measures and tools that tackle cyber crime often invade privacy in the most brutal ways and, at the same time, lack of personal online security leads to breaches of that same privacy. A cyber-security strategy should seek for the right balance between these two concepts. Moreover, the European Commission has provided the regulatory tools in order to support the Member States in facing this challenge. For this reason, every Member State should take seriously into account the right of citizens' privacy. Finally, the reader should bear in mind that privacy is a horizontal issue that cuts across most of the activities relevant to cyber strategy.

Typical tasks to consider include the following.

- ✓ Take into account national legal requirements for data protection when drafting cyber-security-relevant regulatory texts.
- ✓ Take the advice of the data protection authority(ies) on regulatory texts related to cyber security.
- ✓ Consider data protection law compliance measures when consulting the minimum security measures.
- ✓ Make data protection supervisory authority(ies) part of information security compliance audits to the most critical stakeholders.
- ✓ Support and brand, together with the national data protection authority(ies), the European Data Protection Day (January 28).
- ✓ Involve national data protection authority(ies) in national cyber exercises.

An example: The Czech Republic

In the Czech Republic strategy it is stated that an appropriate legislative framework for the purpose of ensuring cyber security will be defined. This framework will not impose any restrictions on rights to freedom of speech, will grant access to information for all population segments, and protect the privacy and confidentiality of information guaranteed by the national Constitution, taking into account the international commitments of the Czech Republic, in particular to EU and NATO.

Also, the Czech Republic aims to actively participate in the drafting of legal acts and standards, and other forms of cooperation in the field of cyber security in the framework of the EU and other international organisations.

Source: Cyber Security Strategy of the Czech Republic For The 2011 – 2015 period, Czech Republic, 2011.

4 Evaluate and adjust the national cyber-security strategy

Once the strategy has been developed and is being executed, the extent to which the objectives are achieved should be assessed. By assessing the achieved results of the activities it is possible to take any required corrective and preventative actions in order to align with or change the objectives of the strategy.

This chapter will cover the explicit requirements needed to evaluate and adjust the strategy. Evaluation is necessary to determine whether the objectives and the planned results have been effectively reached. The primary purpose of evaluation, in addition to gaining insights into the status of the existing initiatives, is to identify future objectives and adjust the strategy accordingly.

4.1 Evaluation approach

There are different methodologies to evaluate a strategy. In this chapter, we will not propose a specific one but rather focus on specific, practical actions necessary to perform an evaluation. This process should end with a report on the status of affairs and a list of actions that the national cyber-security strategy owner(s) should implement.

The following suggestions can be considered in defining the strategy evaluation report.

- ✓ Define the scope of the evaluation, the key objectives, the expected outcomes and the periodicity of it.
- ✓ Implement the 'Segregation of duties' principle: assign to an independent entity, a supervisor or a trusted third party (other than the national cyber council) the task of evaluating the effectiveness of a national cyber-security strategy and its activities (e.g. a national cyber security council).
- ✓ Empower the independent entity with the appropriate mandate, role and responsibilities to succeed in this operation.
- ✓ Encourage and offer incentives to stakeholders to be involved in the evaluation process.
- ✓ Evaluate not only the strategy but also the individual tasks of it.
- ✓ Follow both a quantitative and qualitative approach giving emphasis on both impact and results.
- ✓ Perform an internal/self-impact assessment for each activity of the strategy taking into consideration the opinion of the stakeholders.
- ✓ Perform an external impact assessment for each activity of the strategy taking into consideration the opinion of external and/or affected users/communities.
- ✓ Evaluate each activity against the action plan and key performance indicators (KPIs) agreed when the activity kicked off; evaluate KPIs through questionnaires (online) and polls within the stakeholder community.
- ✓ Create a data collection scheme for obtaining relevant data for the evaluation of the strategy and the action plan. Effectiveness of the strategy should be measured at all levels. The data collection process should become comprehensive.

- ✓ Identify lessons, good practices and bad practices from the internal and external impact assessment as well as the evaluation of each activity.
- ✓ Prepare an analytical evaluation report describing the achieved results and the expectations for the next evaluation.
- ✓ Carry out benchmarking studies in order to compare strategies between different Member States. The outcomes of a benchmarking study can be used to identify areas of improvement.

4.2 Key performance indicators

Both qualitative and quantitative measurements can be used to define KPIs. These KPIs might refer either to the strategy as a whole or to the activities of the strategy already described above. Below, we present a list of possible and indicative KPIs that could be considered for some of the key strategy components presented in Chapter 3.

- ✓ **Set the vision, scope, objectives and priorities**: By assessing the objectives of the strategy you will remain focused and therefore able to adjust and update the action plan. The action plan needs to be evaluated, to be followed up and, if necessary, to be updated. This is needed to cope with changes in the operational environment, making sure that the strategy and action plan are realistic and focused, and making sure that the strategy includes the right prioritised objectives. This way you make sure the strategy will remain dynamic and up to date. Typical KPIs include:
  - the number of tasks that have been completed on time according to the action plan;
  - the level of public trust in the usage and security of services targeted by the strategy (e.g. e-banking, e-government); this can be gauged by performing national surveys;
  - the existence of a well-established and functioning national cyber security community (working groups, PPPs, a national cyber security council, etc.);
  - reports from industry on improved resilience levels.
- ✓ **Follow a national risk assessment approach**: Each Member State should monitor the most significant emergencies as regards the cyber security its citizens could face through the national risk assessment. These assessments should be conducted at periodic intervals and should draw on expertise from a wide range of departments and agencies of both the government and the critical infrastructure owners. Typical KPIs for this phase include the following.
  - The success of a national risk assessment programme is measured by the number of incidents that occurred in a specific period and could not be addressed by the minimum security measures prepared. An absence of this type of incident conceptually mean that all threats have been identified and their impact has been mitigated. This KPI is the ratio of the incidents that have not been mitigated using existing measures and the total number of known incidents.

- Another metric might be the comparison between the calculated and the actual impact of the identified incidents using different evaluation units e.g. human lives or monetary values. This way deviation between these two metrics can be addressed.
- The number of emerging targets or critical assets identified after the completion of the national risk assessment.

✓ **Take stock of existing policies, regulations and capabilities**: The process of taking stock of existing policies, regulations and capabilities is usually a tricky exercise that reveals areas for improvement in the governance model of cyber security. Ideally, this process should be straightforward, with minimum cost and without gaps to fill. Typical KPIs could include:

- the level of complexity (i.e. number of overlaps, gaps, conflicting statements) of policy documents and internal procedures;
  the number of inventories and directories of all national cyber response capabilities (public and private);
- the number of policy documents adopted after the deployment of the strategy.

✓ **Develop a clear governance structure:** In order to evaluate the governance structure, the policy makers should organise national cyber exercises to test the command and control and the communications of the existing strategy governance structure. Typical KPIs include:

- the number of tasks executed and status of actions taken by designated entities within the strategy;
- the number of gaps (i.e. tasks/responsibilities/conflicts unassigned to specific roles) of the existing governance model;
- response time and coherency of the chain of command;
- the number of cooperation mechanisms, procedures and communication channels that did not work.

✓ **Identify and engage stakeholders:** A critical mass of stakeholders involved is vital for the successful implementation of the strategy. Typical KPIs include:

- the number of stakeholders involved; sectoral indexes have to be developed for both the private and the public sector and for each industry field;
- the number of entries in a national cyber-security directory;
- the number of existing working groups.

✓ **Establish trusted information sharing mechanisms:** At the end of the year, a network information security exchange (NSIE) is expected to publish a confidential report with minutes and results of its annual work. Typical KPIs include:

- a measure of the utilisation of information sharing platforms;
- the number of measures and actions taken as a result of the analysis done on the data collected;
- the number of parties involved;
- the number of new vulnerabilities, threats and incidents discussed;

- ✓ **Develop cyber-security contingency plans**: An NCP aims to develop a national response capability and promote overall coordination among the hierarchy of emergency response organizations and response or contingency plans. Typical KPIs include:
  - the number of activities of a national cyber contingency plan that have been completed on time;
  - the number of sectors and stakeholders involved in the development of the plan;
  - the number of national cyber exercises to test the plan;
  - the number of sectors and stakeholders involved in the development of the plan;
  - the level of preparedness to respond to a cyber crisis based on different scenarios (potential causes and different levels of impact);
  - the existence of crisis management facilities and situation rooms.
- ✓ **Organise cyber security exercises:** Exercises are an important tool to assess the preparedness of a community for natural disasters, technology failures and emergencies. For this reason, it is important to develop specific metrics to gauge the success of the exercises. Typical KPIs include:
  - the number of cyber security exercises conducted;
  - the status of actions implemented based on the findings/evaluation reports;
  - the number of sectors involved;
  - the number of people involved;
  - the level of involvement of the private sector;
  - the number of plans and procedures that have been tested.
- ✓ **Establish baseline security requirements:** Baseline security measures are the result of a consultation process among the national cyber-security partners. Moreover, it is expected that competent authorities will monitor on a regular basis the implementation of these measures. Typical KPIs include:
  - the number of incidents; individual indexes of this kind might be:
    - the number of incidents that failed to be addressed by the measures;
    - the number of incidents that are addressed by the measures.
  - the number of non-compliant organisations identified within a specific period of time;

5 Conclusions

The development of a national cyber-security strategy is a challenging effort that needs coordination among different national stakeholders of the public and the private sector. Although there are many – and considerably different - definitions, a cyber security strategy has proven to be an instrument that helps governments manage the efforts of all involved parties in order to tackle risks related to cyber at a national level.

This report has described a set of 20 concrete actions; these called upon policy makers to do the following.

1. Set the vision, scope, objectives and priorities.
2. Follow a national risk assessment approach.
3. Take stock of existing policies, regulations and capabilities.
4. Develop a clear governance structure.
5. Identify and engage stakeholders.
6. Establish trusted information-sharing mechanisms.
7. Develop cyber-security contingency plans.
8. Organise cyber-security exercises.
9. Establish baseline security requirements.
10. Establish incident-reporting mechanisms.
11. Make citizens aware.
12. Foster R&D.
13. Strengthen training and educational programmes.
14. Establish an incident response capability.
15. Address cyber crime.
16. Engage in international cooperation.
17. Establish a public–private partnership.
18. Balance security with privacy.
19. Evaluate.
20. Adjust the national cyber security strategy.

The structure of this guide was based on the Deming 'Plan-Do-Check-Act' (PDCA) model used to control and continuously improve strategies, policies, processes and products. Four phases, each corresponding to the model steps, have been described for the strategy lifecycle: development, execution, evaluation and adjustment.

In the future, ENISA will follow up this report with a second edition that will focus on the evaluation and adjustment phase. Thus, EU Member States will have a complete overview of the National Cyber Security Strategy development lifecycle.

Annex I – Glossary of Terms

Term	Definition
Action plan	The action plan outlines the activities for delivering the priorities and objectives as defined in the strategy.
Civil society	Civil society refers to the end users of (information) systems/infrastructures and civilians depending upon them.
Computer emergency response team (CERT)	Organisation formed to study internet security vulnerabilities, and to provide assistance to online sites that become victims of cracker or hacker attacks. Commonly, it offers a 24-hour emergency response service, shares information for improving cyber security, and coordinates responses to cyber-security threats.
Critical (information) infrastructure (CII)	The systems, services, networks and infrastructures that form a vital part of a nation's economy and society, providing essential goods and services. Their disruption or destruction would have a serious impact on vital societal functions.
Cyber security / information security	There is no universally accepted nor straightforward definition of cyber security. When comparing it to 'information security' some people regard it as overlapping, being the same thing. Or they may view information security as focused on protecting specific individual systems and the information within organisations, while cyber security is seen as being focused on protecting the infrastructure and networks of CIIs.
Developing a national cyber security strategy	Developing the national cyber security strategy means specifying the scope, determining priorities and defining the principles and objectives of cyber security on a national level.
Evaluating a national cyber security strategy	Evaluating the national cyber-security strategy means assessing the results of the activities using a set of objective performance metrics.
Executing a national cyber security strategy	Executing the national cyber-security strategy means specifying the action plan(s) and putting the strategy into practice through executing the activities.
Governance framework	The governance framework defines the roles, responsibilities and accountability of all stakeholders and provides a framework for dialogue and coordination of various activities undertaken in the lifecycle of the strategy.
Information sharing and analysis centre	An ISAC involves intelligence, CERT communities and critical infrastructures stakeholders in order to facilitate information-sharing. Within this structure the circulation of relevant information can be

(ISAC)	shared within a trustworthy environment.
Key performance indicator or metric	A key performance indicator (KPI) is a type of performance measurement. KPIs are commonly used by an organisation to evaluate its success or the success of a particular activity in which it is engaged. KPIs are metrics used to measure important business activities and processes of a strategic nature. The term 'metric' is generic. A metric is typically used to mean just about any sort of measurement applied to gauge a particular business process or activity.
Legal framework	A legal framework formally assigns tasks, roles/responsibilities and accountability to the different parties by enforcing legal requirements. In this way, expectations are managed and the division of tasks is formulated in the strategy. It is the outcome of the process of assigning tasks, roles/responsibilities and accountability. It can be used together with a governance framework.
Maintaining a national cyber security strategy	Maintaining the national cyber-security strategy means taking corrective and preventive actions based on the evaluation results in order to achieve the objectives of the strategy.
National cyber security centre (NCSC)	A national cyber security centre is commonly tasked with protecting the national (critical) information infrastructures. The NCSC may have responsibilities concentrating on, for example, developing and offering expertise and advice, supporting and implementing responses to threats or incidents, and strengthening crisis management.
National cyber security council	A national cyber security council commonly consists of representatives of the public and private sector. A council can advise both government and private parties on relevant developments in the area of cyber security, prioritise specific (emerging) IT threats, and ensure that basic values are incorporated in the execution of the strategy.
National cyber security strategy	A national cyber security strategy is a strategic framework for a nation's approach to cyber security. It is a tool to improve the security and resilience of national infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.
Network operating centers (NOC)	A network operations centre (NOC) commonly serves as a hub for coordinating the operational management of domestic incidents, as well as situational awareness. An NOC is a standing interagency organisation that operates on a 24/7 basis, fusing law enforcement, national intelligence, emergency response, and private-sector reporting. An NOC commonly facilitates national security information-sharing and operational coordination among (international) public and private sector

	partners.
Ownership	Ownership refers to creating commitment in executing the strategy and creating passion for the results of the strategy.
PDCA-model	The Deming 'Plan-Do-Check-Act' (PDCA)-model is commonly used to structure information security management systems.
Public–private partnership (PPP)	There is no common definition of what constitutes a PPP. However, it can be defined as an organised relationship between the public and private sector, which establishes common goals and objectives and uses defined roles and work methodology to achieve shared goals.
RACI	The RACI model ('responsible-accountable-consulted-informed') is a commonly used framework for clarifying roles and responsibilities. It describes the participation by various roles in completing tasks or deliverables for a project or business process.
Risk and crisis management	Risk management is the identification, assessment, and prioritisation of risks (the uncertainty on objectives, whether positive or negative) followed by coordinated and economic application of resources to minimise, monitor, and control the probability and/or impact of unfortunate events or to maximise the realisation of opportunities. Crisis management commonly represents a failure of risk management since it will never be possible to totally mitigate the chances of security breaches occurring.
Risk-based approach	Risk-based approach is an approach to intelligence analysis that has as its objective the calculation of the risk attributable to a threat source or acts threatened by a threat source. It provides a means of providing strategic intelligence for planning and policymaking.
Security baseline	A security baseline describes the measures that should be implemented to reach a specific minimum security level.
Security standard	A security standard is a set of security features to be provided by a system before it can be deemed to be suitable for use in a particular security processing mode, or in accordance with a generalized security policy.
Self-regulation	Self-regulation is the process whereby an organisation is asked, or volunteers, to monitor its own adherence to legal, ethical, or safety standards, rather than have an outside, independent agency such as a governmental entity monitor and enforce those standards.

Annex II – References

National cyber security strategies

Czech Republic
http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

Estonia
http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

Finland
http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-5405.pdf&title=Valtioneuvoston%20periaatep%C3%A4%C3%A4t%C3%B6s%20kansalliseksi%20tietoturvastrategiaksi%20%28su/ru/eng%20LVM62/2008%29

France
http://www.enisa.europa.eu/media/news-items/french-cyber security-strategy-2011

Germany
http://www.enisa.europa.eu/media/news-items/german-cyber security-strategy-2011-1

Lithuania
http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

Luxembourg
http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf

Netherlands
http://www.enisa.europa.eu/media/news-items/dutch-cyber security-strategy-2011

Slovakia
Not available online

United Kingdom
http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

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