Country Reports

09

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for enquiries on these reports, please use the following details:

Mr. Tim Mertens, Senior Expert in Co-ordination of activities with EU-bodies and Member States. Email: tim.mertens@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2008

Table of Contents

Foreword 4

Executive Summary 5

Introduction 7

Methodology 8

Results 10

Definition and Sources 601

Foreword

This report was prepared for and funded by ENISA. It represents the results of a research project that took place between July and December 2008. The aim of the project was to produce a series of country reports that provide an overview of the "state of the art" of network and information security (NIS) in each country regarding stakeholders, activities, events and current trends.

The research was conducted by a number of IDC project execution teams including a Central Operational Team from IDC CEMA's Prague office, and 16 Local Teams from IDC offices across Europe. The teams were led by a Project Manager and Project Manager Support Team from IDC CEMA's Consulting Group.

ENISA thanks IDC as well as the ENISA National Liaison Officers who reviewed and commented on the results of the research process.

Executive Summary

The main goal of the project was to provide an overview of the "state of the art" in network and information security (NIS) in each of the 30 countries defined by ENISA: the 27 European Union Member States and the 3 non-EU members of the European Economic Community.

In this report we explain the methodology used for the project, give an overview of the results of the research, and present the results for each of the 30 countries. Each country chapter contains the following sections: Country General Information, Country Highlights, Key Stakeholders Overview, Detailed Stakeholders Overview, Activities, Events, Current Trends.

The project was undertaken by IDC and funded by ENISA. The project was elaborated in three main stages:

1. Information and Data Gathering: information on each of the 30 countries was collected and input into a Country Data Collection Template. ENISA National Liaison Officers reviewed each Template and provided feedback;

2. Information and Data Review: the completed Data Collection Templates for all countries were reviewed internally by IDC and also by ENISA;

3. Report Production: the information from each completed Data Collection Template was used to produce each Country chapter. The other sections of this report were also written.

The categorization and mapping of stakeholders was one of the most important aims of the project. The results of this are shown in the Key Stakeholders Overview section of each Country chapter. In the Key Stakeholders diagram each organization is positioned horizontally according to its main field(s) of responsibility or activity, and vertically according to the type of organization it is. The fields of activity shown in the Key Stakeholders diagram were chosen to represent the most important areas in which national-level organizations have an impact on NIS: Policy Development, Policy Implementation, Privacy and Data Protection, Electronic Communications, CIP/CIIP (Critical Information Infrastructure Protection), and CERT (Computer Emergency Response Team).

The project has found that institutions and responsibilities vary substantially from country to country. However, the some general trends could be identified:

- **Governmental Organizations and Bodies:** generally the most important government actors defining the strategic policies for NIS issues are: the Ministry of Communications (often a department of a larger Ministry), the National Regulatory Agency for Electronic Communications, the National Office for Data Protection, the Ministry of Interior, the Ministry of Defense, and the Ministry or Department for Public Administration/eGovernment.

- **Public Network and Information Security Bodies:** their primary goal is to promote IT security at the national level, provide advice and recommendations, analyze the national security situation and define plans and other initiatives. Public NIS bodies typically they have very broad responsibilities, especially in the case of large organizations. Their main tasks concern information gathering for important IT security issues, consultancy (developing scientific and technical expertise), and specialized input to the main government policies in the area. Many of these bodies are responsible for approving, guaranteeing and certifying the security of national information systems. They also participate in the development of IT security applications and products for the public sector or for projects of public interest. These public NIS bodies are typically active in national and international networking activities for information sharing and risk management with their counterparts, or with other, less specialized, public bodies in their countries. Public NIS bodies exist in about one third of the country studies in this project.

- **CERTs:** There are over 100 selected CERTs active in the EU, but their geographical distribution is very uneven. Almost all countries have 1 or 2 public sector CERTs, responsible for governmental or national research/education networks. In most countries there is a CERT that acts as a national NIS point of contact, collaborating with CERTs from other countries at an international level as well as coordinating crisis response and other activities with other CERTs in the country. In most cases this role is fulfilled by the governmental CERT, which serves government and public sector agencies. Governmental or national CERTs also deal with CIIP issues, or collaborate with CIIP bodies.

Introduction

Main Goals of the Project

The main goal of the project was to provide an overview of the "state of the art" in network and information security (NIS) in each of the 30 member countries of ENISA: the 27 European Union Member States and the 3 non-EU members of the European Economic Community. This overview was to be presented in a series of Country Reports providing information on the stakeholder organizations that are the principal actors in NIS, summarizing the most important activities undertaken by these actors, listing the most relevant NIS events, and identifying key trends. A major output of the study was to be a categorization of the stakeholders and a mapping with respect to the principal activities that must be performed in the NIS field.

Outline of this Report

In this report we explain the methodology used for the project, give an overview of the results of the research, and present the results for each of the 30 countries. Each country chapter contains the following sections:

- Country General Information
- Country Highlights: including NIS Highlights giving an overview of which organizations are responsible for key elements of NIS.
- Key Stakeholders Overview: a diagram mapping the key stakeholders against areas of responsibility and showing their mutual relationships, and a table mapping the stakeholders against the ENISA focus points to which their activities are related.
- Detailed Stakeholders Overview: a table presenting information on NIS stakeholders.
- Activities: a table presenting information on significant NIS-related activities.
- Events: a table presenting information on conferences, workshops and media campaigns.
- Current Trends: focusing on the status of national electronic ID schemes, and major incidences of security breaches involving loss of data.

Methodology

The project was undertaken by several staff from IDC CEMA - a Project Manager, a Project Manager Support Team of two staff, and a Central Operational Team of four staff – and 16 local teams, each consisting of one or more National Correspondents from an IDC office.

The project to produce this report was elaborated in three main stages:

1. Information and Data Gathering: information on each of the 30 countries was collected and input into a Country Data Collection Template. ENISA National Liaison Officers reviewed each Template and provided feedback;

2. Information and Data Review: the completed Data Collection Templates for all countries were reviewed internally by IDC and also by ENISA;

3. Report Production: the information from each completed Data Collection Template was used to produce each Country chapter. The other sections of this report were also written.

A detailed description of each stage is provided below.

Stage 1: Information and Data Gathering

The key goals of the Information and Data Gathering stage of the project were:

- To collect accurate and up-to-date information and data on stakeholders, activities, events and trends in the field of NIS.
- To collect a consistent and comprehensive set of information and data for each country.
- To collect information and data of sufficient quantity and relevance in order to compile the Country Reports and achieve the overall goals of the project.

The major activities undertaken during this stage of the project were:

- **Research at National Level:** the National Correspondents, the majority of whom were based in-country, gathered information and data from various country-level sources including internal IDC information, printed and Web-based material, and direct contact with experts and stakeholder representatives.
- **Research at International Level:** members of the Central Operational Team gathered information and data from international sources including internal IDC sources (IDC studies and experts), and printed and Web-based sources including from the European Commission and ENISA.
- **ENISA NLO Review:** National Liaison Officers or, in some cases, ENISA Management Board Members were sent the completed Data Collection Template their respective countries and given the opportunity to review the information and provide feedback.

Stage 2: Information and Data Review

The key goals of the Information and Data review stage of the project were:

- To assess whether the completed Country Data Collection Template met the minimum requirements in terms of quantity and quality of information.
- To assess the relevance of information items and the comprehensibility of all information.
- To check for consistency between the completed Country Data Collection Templates.
- To request and receive any additional data and information from the National Correspondents that was necessary in order to complete each Country Data Collection Template.

The major activities undertaken during this stage of the project were:

- **Completeness Assessment:** a member of the Central Operation Team checked each Country Data Collection Template to ensure that it met the minimum requirements and was complete.
- **Relevance and Comprehensibility Assessment:** a member of the Central Operation Team checked each Country Data Collection Template to ensure that all items and information were relevant and that all information was comprehensible.
- **Consistency Assessment:** a member of the Central Operation Team compared each Country Data Collection Template to an Example Country Data Collection Template to ensure that items and information were consistent.
- **Final Review and Peer Review:** the Project Manager or member of the Project Manager Support Team reviewed each Country Template. A limited number of Country Templates were also Peer Reviewed by a member of the Project Advisory Board.

Stage 3: Report Production

The overall process for the completion of each Country chapter was:

1. Input of information and graphics into the Country General Information section.
2. Transfer of data and information from the completed Country Data Collection Template into the other sections of the Country chapter.
3. Review by the Project Manager or member of the Project Manager Support Team. A limited number of Country chapters were also Peer Reviewed by a member of the Project Advisory Board.
4. Internal review by ENISA
5. Review of selected Country chapters by ENISA National Liaison Officers

Results

Stakeholders and their Role in NIS

The categorization and mapping of stakeholders was one of the most important aims of the project. The results of this are shown in the Key Stakeholders Overview section of each Country chapter. In the Key Stakeholders diagram each organization is positioned horizontally according to its main field(s) of responsibility or activity, and vertically according to the type of organization it is.

The fields of activity shown in the Key Stakeholders diagram were chosen to represent the most important areas in which national-level organizations have an impact on NIS:

- Policy Development: the drafting of, or assistance in the process of drafting, governmental policies relating to NIS.
- Policy Implementation: the management of, or conducting of, activities carrying out policies relating to NIS.
- Privacy and Data Protection: ensuring that sensitive personal information held within computer systems or on computer devices, or transmitted across networks, is not accessed by or distributed to unauthorized individuals or agencies; ensuring that national laws transposing the European Directive on Protection of Personal Data are upheld; imposing obligations on public institutions, businesses and other organizations to protect personal data.
- Electronic Communications: upholding the regulatory framework on electronic communications that is addressed to public telecommunications operators; ensuring that national laws transposing the European Directive on Privacy and Electronic Communications are upheld.
- CIP/CIIP: Critical Infrastructure Protection / Critical Information Infrastructure Protection is the governance of ICT systems and networks that are critical for the management, control and communication of critical infrastructures: transportation, finance, electric power, water, emergency/rescue services, health services etc.
- CERT: Computer Emergency Response Team, also called Computer Security Incident Response Team (CSIRT), is a specialized organization or team with the task of monitoring, preventing, and detecting computer security incidents and circulating information about them.

The project has found that institutions and responsibilities vary substantially from country to country. However, some general trends could be identified that are presented in the following paragraphs.

Governmental Organizations and Bodies

Generally the most important government actors defining the strategic policies for NIS issues are:

- The Ministry of Communications (often a department of a larger Ministry), overseeing communication networks policies and sometimes having a role in Critical Information Infrastructures Protection.
- The National Regulatory Agency for Electronic Communications.
- The National Office for Data Protection.
- The Ministry of Interior overseeing national security, electronic identity, and cyber-crime policies and sometimes having a role in Critical Information Infrastructures Protection.
- The Ministry of Defense may share with the Ministry of Interior the definition of policies against cyber-terrorism and is normally a very important customer of specialized NIS products and services.
- The Ministry for Public Administration/eGovernment overseeing policies of NIS use within the government itself.

These government actors operate at the strategic policy level and consult with other national public bodies and, often, private organizations. They also represent their countries at an EU level. They are often supported by operative agencies (or sometimes internal departments) more focused on the actual implementation of security policies, monitoring of NIS threats and attacks, organizing and coordinating countermeasures, promoting awareness and education campaigns.

Public Network and Information Security Bodies

Public Network and Information Security bodies are typically created to implement National Programmes for IT security, or are born as the IT security arm of some Ministry (typically the Ministry of Interior or Ministry of Defense). Their primary goal is to promote IT security at the national level, provide advice and recommendations, analyze the national security situation and define plans and other initiatives (such as building relationships and cooperation between different stakeholders).

Public NIS bodies typically they have very broad responsibilities, especially in the case of large organizations such as BSI in Germany or the DCSSI in France. Their main tasks concern information gathering for important IT security issues, consultancy (developing scientific and technical expertise), and specialized input to the main government policies in the area. Many of these bodies are responsible for approving, guaranteeing and certifying the security of national information systems. They also participate in the development of IT security applications and products for the public sector or for projects of public interest.

These public NIS bodies are typically active in national and international networking activities for information sharing and risk management with their counterparts, or with other, less specialized, public bodies in their countries.

The bodies provide services to the users and manufacturers of information technology products, mainly other public agencies at the national, regional and local level but also sometimes certification for the private sector.

Examples of public NIS bodies are:

- Austria: Federal Chancellery of the Republic of Austria, Department of Security Policy
- Czech Republic: National Security Office
- Denmark: National IT and Telecom Agency
- Finland: Ministry of Transport and Communications
- France: Central Directorate for Information Systems Security (DCSSI)
- Germany: Federal Office for Information Security (BSI)
- Norway: Ministry of Transport and Communications
- Romania: National Registry Office for Classified Information (ORNISS)
- Slovakia: National Security Authority

Universities and Research Centres

Higher education and research institutions perform a critical role in the NIS market, by carrying out applied and long-term research in the field and by educating the necessary human resources.

In many European science and technical universities, IT security is a top priority research area. Security Labs are typically part of the Computer Science Department, but they can also be found in Engineering, Mathematics or other faculties. University research spans from theory to practice: from the theoretical foundations of cryptography to the development and analysis of cryptographic protocols and algorithms, systems security, and network security. Some universities study IT security issues not only from a technological point of view, but as a multidisciplinary field, with legal, regulatory and societal implications.

Through their networking and knowledge-sharing activities, universities and research centers perform an essential role for innovation development, technology transfer to EU enterprises for the creation of new products and services (thereby contributing to their competitiveness), and training and awareness raising among business users, especially SMEs. The best security labs generate spin-offs or start-ups who may progress to become dynamic, new-technology based enterprises.

CERTs

There are over 100 CERTs active in the EU, but their geographical distribution is very uneven. Almost all countries have 1 or 2 public sector CERTs, responsible for governmental or national research/education networks. But there are also a significant number of private CERTs in Germany and the UK, which are typically owned and organized by telecommunications operators, ISPs, banks, or industrial companies. These private CERTs primarily provide services to their owners, but may also participate in national or international forums.

In most countries there is a CERT that acts as a national NIS point of contact, collaborating with CERTs from other countries at an international level as well as co-ordinating crisis response and other activities with other CERTs in the country. In most cases this role is fulfilled by the governmental CERT, which serves government and public sector agencies. Governmental or national CERTs also deal with CIIP issues, or collaborate with CIIP bodies.

Country Report – Austria

Country General Information

Source: European Commission

Political system:	Federal republic
Capital city:	Vienna
Total area:	83 858 sq km
Population:	8.3 million
Official language:	German
Time zone:	CET (GMT + 1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Austria, we present a set of three indicators in the Country Highlights section.

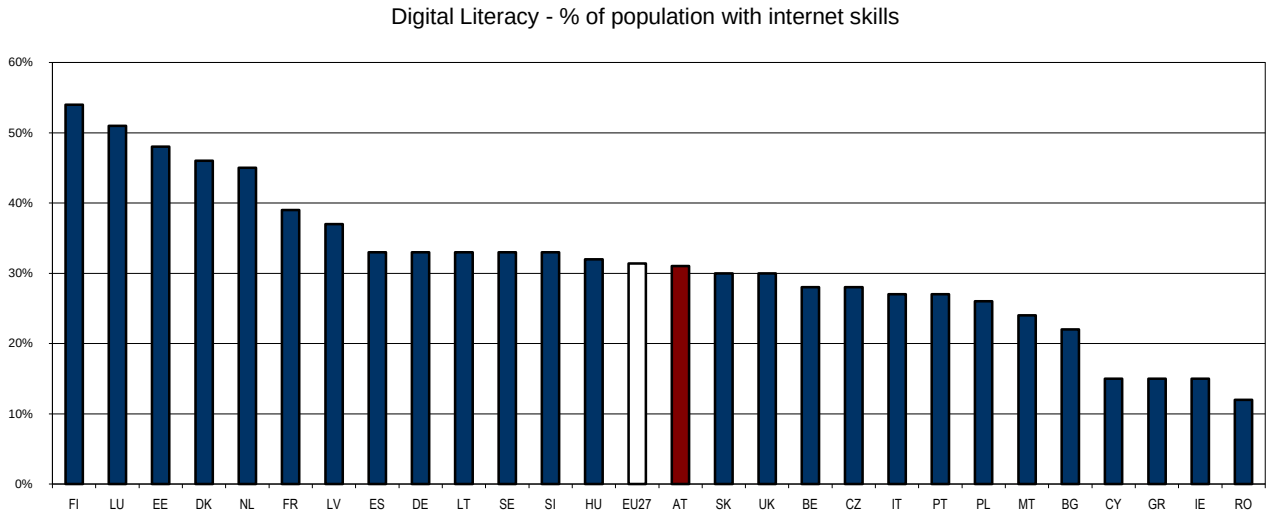
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Austria is fundamental to this NIS study.

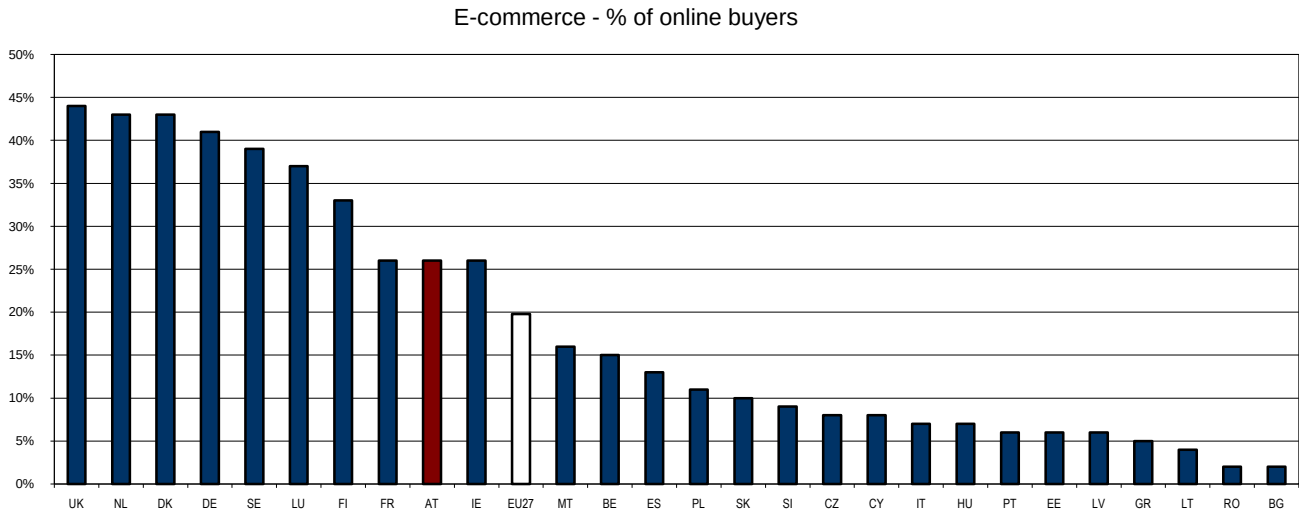
Information society – connectivity and ICT usage in households, enterprises, and government bodies – is very well developed in Austria, especially in the egovernment space.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

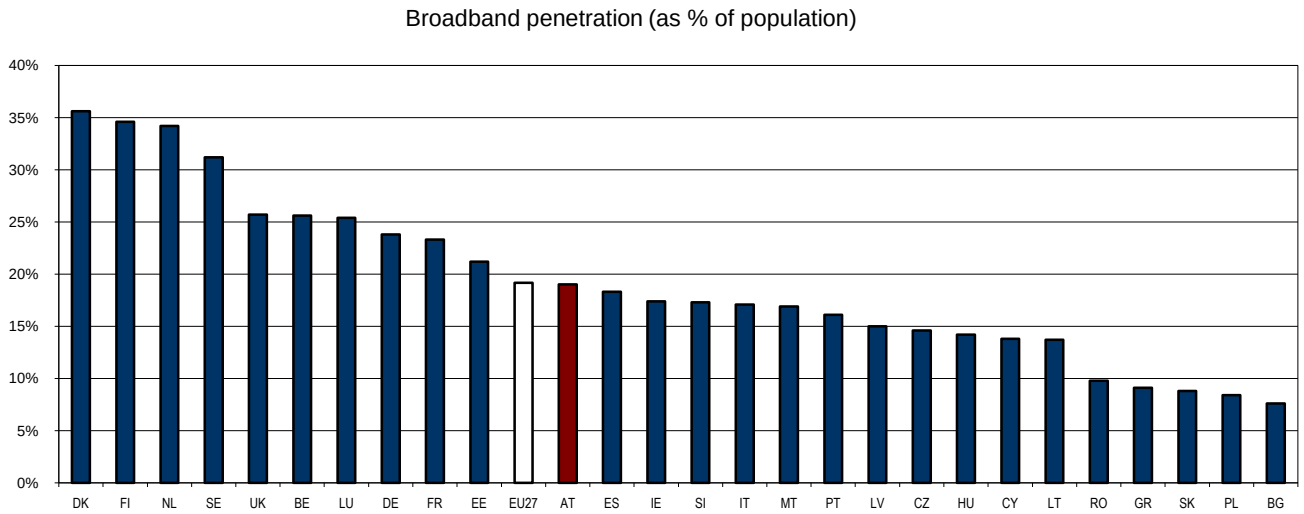
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Information Security Commission at the Federal Chancellery of the Republic of Austria is recognized among NIS stakeholders in Austria as the national security agency. The information security officers in the federal ministries are charged with the implementation of information security policy at the national level.

The Federal Chancellery (Dep. Media) is also responsible for coordinating the development of national information society strategy (including those aspects relating to information security) and all subjects related to E-Government ("Platform Digital Austria"). The Austrian data protection commission (*Datenschutzkommission*) is a governmental authority charged with data protection. The data protection commission is the Austrian supervisory authority for data protection, the equivalent of a national data protection commissioner.

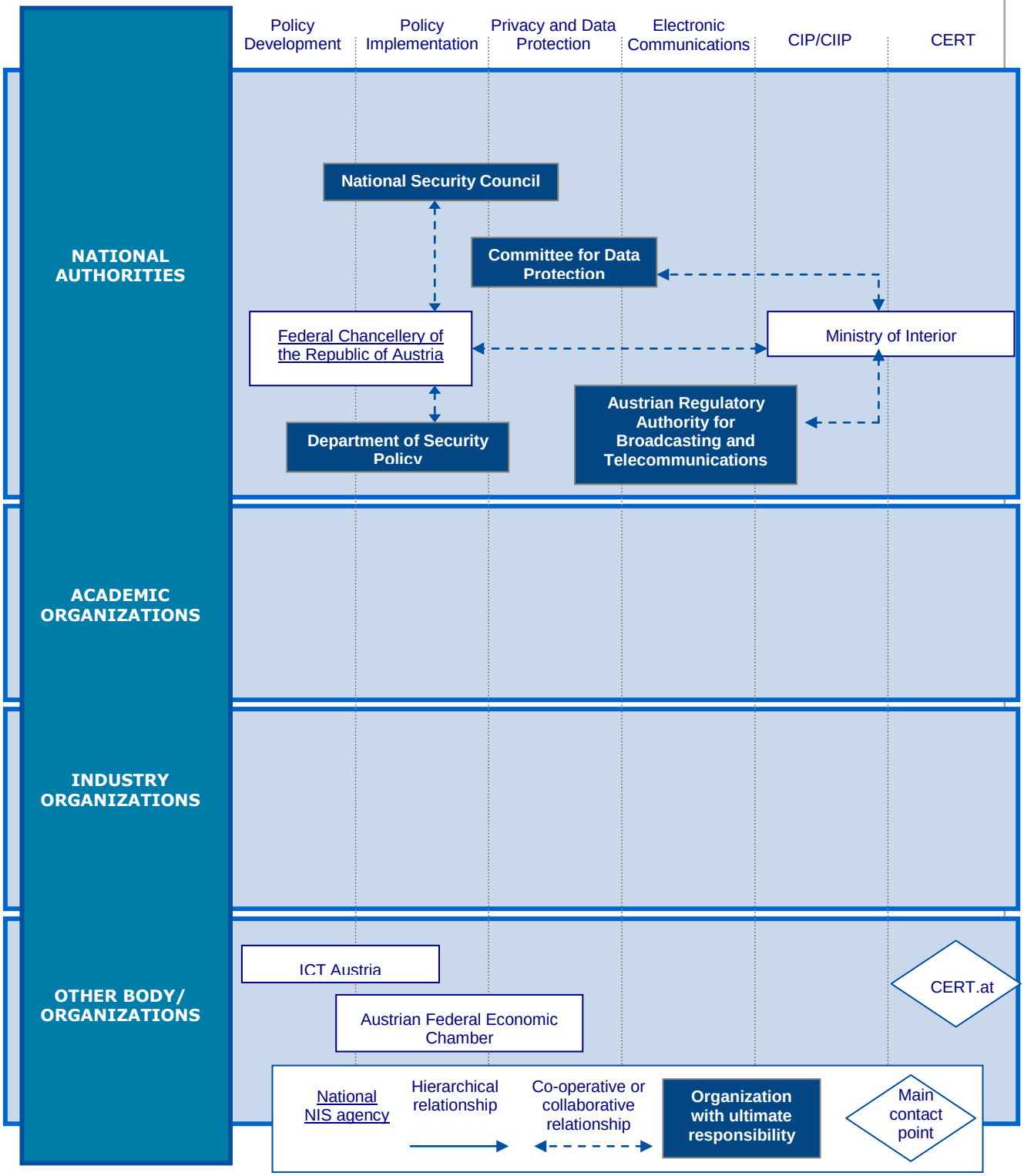
Austrian Regulatory Authority for Broadcasting and Telecommunications (*Rundfunk und Telekom Regulierungs-GmbH, or TKK*) in charge of competition regulation, frequency allocation procedures, the approval of general terms and conditions of business, as well as monitoring the fees charged by telecommunications companies. Another of the TKK's key duties is its role as the supervisory authority for electronic signatures.

CERT.at is the primary contact point for IT security in the national context. CERT.at coordinates other CERTs operating in the area of critical infrastructure or communication infrastructure. They also provide basic IT security information (warnings, alerts, advise) for SMEs.

The Federal Chancellery (Department of Security Policy), in consultation with Federal Ministry of the Interior (*Bundesministerium für Inneres*), handles coordination of all national critical infrastructure bodies and their infrastructures in relation to key elements of CIP/CIIP at the national level.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Austria. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	Awareness Raising (AR)	Emerging/Current Risks	Micro-enterprises	e-ID	Development of Security Technology and Standards	Implementation of Security Technology and Standards
Federal Chancellery of the Republic of Austria (Information Security Commission; NSA)		X		X			X	X
Federal Chancellery of the Republic of Austria (Platform Digital Austria; Dep. Media Affairs)			X				X	X
Committee for Data Protection (*Datenschutz-kommission*)							X	
Austrian Regulatory Authority for Broadcasting and Telecommunications (*Rundfunk und Telekom Regulierungs-GmbH*)		X				X		
CERT.at	X				X			
Federal Ministry of the Interior	X			X				

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Austria:

National Authorities in Network and Information Security	
Information Security Commission (*Informationssicherheitskommission*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.bka.gv.at	
Areas of Activity: The information security commission (National Security Authority) is responsible for the information security of all Federal ministries. It ensures the presence of unified national wide protection measures and coordinates all activities in the area of classified information with regard to the Federal administration. Moreover it focus on reporting new findings and experiences, also by suggesting improvements to the information security policy. Involved also at an international level in defining common policies for exchanging sensible information between countries.	
Intelligence Office of the Federal Ministry of Defence (*Abwehramt des Bundesministeriums für Landesverteidigung*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Emerging/Current Risks	
Relationships: None	
Weblink: http://www.bmlv.gv.at	
Areas of Activity: Conducting counter-intelligence within the military sphere.	
Platform "Digital Austria" (*Plattform Digitales Österreich*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience	

Relationships: Federal Chancellery, Dept. Media Affairs/Information Society; Center of secure IT (*A-SIT Zentrum für sichere Informationstechnologie* – Austria) saferInternet.at, Austrian Institute for Applied Telecommunications (*Österreichisches Institut für angewandte Telekommunikation*), and Austrian Regulatory Authority for Broadcasting and Telecommunications (*Rundfund und Telekom Regulierungs-GmbH*)
Weblink: http://www.digitales.oesterreich.gv.at
Areas of Activity: Federal Chancellery of the Republic of Austria – coordinates ICT and egovernment strategies.

Committee for Data Protection (*Datenschutzkommission*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Federal Chancellery of the Republic of Austria, Department of Corporate Safety Policy (*Bundeskanzleramt, Fachabteilung Sicherheitspolitik*); Federal Ministry of the Interior; and Federal Chancellery, Dept. Media Affairs/Information Society	
Weblink: http://www.dsk.gv.at	
Areas of Activity: The Austrian Data Protection Commission (*Datenschutzkommission*) is a governmental authority charged with data protection. The data protection commission is the Austrian supervisory authority for data protection – the equivalent of a national data protection commissioner.	

Federal Chancellery of the Republic of Austria, Department of Security Policy (*Bundeskanzleramt, Fachabteilung Sicherheitspolitik*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: cooperates with Ministry of Industry and Trade	
Weblink: http://www.bka.gv.at	
Areas of Activity: The Department of Security of the Federal Chancellery is responsible for coordinating the government security policy of the federal government. The Federal Chancellery represents the Republic of Austria *vis-à-vis* the Constitutional Court, the Administrative Court, and international law courts.	

Federal Ministry of the Interior (*Bundesministerium für Inneres*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: CERT, Emerging/Current Risks	
Relationships: Committee for Data Protection (*Datenschutzkommission*), saferInternet.at, and Austrian Institute for Applied Telecommunications (*Österreichisches Institut für angewandte Telekommunikation*)	
Weblink: http://www.bmi.gv.at	
Areas of Activity: Federal Ministry of the Interior	
Federal Chancellery, Dept. Media Affairs/Information Society	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: cooperates with Committee for Data Protection (*Datenschutzkommission*)	
Weblink: http://www.bka.gv.at/informationsgesellschaft	
Areas of Activity: Responsible for the coordination of the dissemination of information to the public with regard to NIS; the national point of contact at European Union level for public studies, like involvement in the European i2010 initiative; represents Austria at the United Nations World Summit on Information Society (WSIS).	
Austrian Regulatory Authority for Broadcasting and Telecommunications (*Rundfund und Telekom Regulierungs-GmbH*)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, e-ID	
Relationships: Committee for Data Protection (*Datenschutzkommission*), Center of Secure IT (*A-SIT Zentrum für sichere Informationstechnologie* – Austria), and Digital-Austria Platform (*Plattform Digitales Österreich*)	
Weblink: http://www.rtr.at	

Areas of Activity: RTR consists of two divisions (Broadcasting and Telecommunications) and provides operational support for the Austrian Communications Authority (KommAustria) and the Telekom-Control Commission (TKK). As experts in various fields such as law, technology, radio frequency management, business, and economics, RTR's employees prepare the decisions of the two authorities with the overall objective of securing Austria a high standing in terms of information society and ensuring sustainable competition on the country's communications markets. Regulatory body for telecommunications and supervisory body for electronic signatures.

Center of Secure IT (*A-SIT Zentrum für sichere Informationstechnologie* – Austria)	
Type of Organization: National Government	Ownership: Non-profit
ENISA Focus Points: Development of Security Technology and Standards and Implementation of Security Technology and Standards	
Relationships: Digital Austria Platform (*Plattform Digitales Österreich*) and the Austrian Regulatory Authority for Broadcasting and Telecommunications (*Rundfund und Telekom Regulierungs-GmbH*)	
Weblink: http://www.a-sit.at	
Areas of Activity: Conducts conformity assessments of secure signature creation devices	

Industry Organizations Active in Network and Information Security

Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*)	
Type of Organization: Other Industry Association	Ownership: Private
ENISA Focus Points: None	
Relationships: Austrian Federal Economic Chamber, IT and Consulting section (*Wirtschaftskammer Österreich, Bundessparte IT und Consulting*); and Austrian Federal Economic Chamber (Wirtschaftskammer Österreich)	
Weblink: http://www.ubit.at	
Areas of Activity: The Austrian Federal Economic Chamber (WKÖ) coordinates and represents the interests of the (whole) Austrian business community at both national and international level. Sector associations include: IT Security, Telecoms (650 enterprises), IT services (35,000 member companies). Activities in the area of NIS range from lobbying (e.g. on issues such as data retention) to awareness raising.	

Austrian Federal Economic Chamber, IT and Consulting section (*Wirtschaftskammer Österreich, Bundessparte IT und Consulting*)	
Type of Organization: Other Industry Association	Ownership: Public
ENISA Focus Points: AR	
Relationships: Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*); Austrian Federal Economic Chamber, IT and Consulting section (*Wirtschaftskammer Österreich, Bundessparte IT und Consulting*); and Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*)	
Weblink: http://www.it-safe.at	
Areas of Activity: Initiative run by the Austrian Federal Economic Chamber's Information and Consulting section. Target groups are both IT companies and SMEs in general. Service to members includes security checks and the "IT Sicherheitshandbuch" (web-based, dynamic) security manual, which addresses both companies and their staff.	
Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*)	
Type of Organization: Other Industry Association	Ownership: Public
ENISA Focus Points: AR and Micro-enterprises	
Relationships: Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*) and Austrian Federal Economic Chamber, IT and Consulting section (*Wirtschaftskammer Österreich, Bundessparte IT und Consulting*)	
Weblink: http://www.itsecurityexperts.at	
Areas of Activity: Group of accredited NIS experts (companies) providing NIS solutions. Their objective is to increase NIS among SMEs by raising awareness, exchanging experiences, and providing training for SMEs.	
ICT Austria	
Type of Organization: Other Industry Association	Ownership: Private
ENISA Focus Points: Development of Security Technology and Standards and Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.ictaustria.at	

Areas of Activity: ICT Austria represents enterprises of the Austrian ICT industry, including sectors such as telecoms and network infrastructure, content, software, hardware, and media. Issues dealt with include telecommunications, IT, Internet, broadband Internet, egovernment, elearning, ehealth, ebusiness, esecurity, digital divide, digital content, and management of digital rights.

Secure on the Net (*Sicher im Netz*) Microsoft Österreich	
Type of Organization: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.sicher-im-Internet.at	
Areas of Activity: Joint initiative by Microsoft Austria, Bank Austria Creditanstalt, eBay Austria, UPC, nic.at, Die Kinderfreunde, BM.I, and others with the intention of addressing end users, raising awareness, providing basic information on threats, and introducing main sollutions, including online security and anti-spam checks.	

Workgroup for Data Processing (*ADV Arbeitsgemeinschaft für Datenverarbeitung*)	
Type of Organization: IT Association	Ownership: Public
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.adv.at	
Areas of Activity: Independent group comprising 300 Austrian companies and public Institutions and around 450 professionals. The workgroup aims at helping the sharing of information by organizing congresses, seminars, presentations, and meetings at a national and international levels with similar groups abroad.	

Academic Organizations Active in Network and Information Security

Austrian Research Centers

Type of Organization: Research Centers	Ownership: Private
ENISA Focus Points: None	
Relationships: Vienna University of Technology, University Linz, University Klagenfurt	
Weblink: http://www.arcs.ac.at/	
Areas of Activity: Austrian Research Centers (ARC) is Austria's leading research and technology establishment and a key player on the European research landscape, where the exchange of knowledge with universities and companies is central to the successful development of industry. ARC conducts research to underpin the competitiveness of Austria in an international context. A total of around 1,200 employees located on 14 sites across Austria, with the main facilities in Seibersdorf, Lower Austria, and in Vienna, act as technology providers and innovation partners for society, industry, and commerce.	

Graz University of Technology

Type of Organization: Universities	Ownership: Private
ENISA Focus Points: None	
Relationships: Austrian Research Centers, Vienna University of Technology, University Linz, University Klagenfurt	
Weblink: http://www.tugraz.at	
Areas of Activity: Conducts research in the Information Security area	

University Klagenfurt

Type of Organization: Universities	Ownership: Private
ENISA Focus Points: None	
Relationships: Austrian Research Centers, Vienna University of Technology, University Linz, Graz University of Technology	
Weblink: http://www.uni-klu.ac.at	

Areas of Activity: Conducts research in the Information Security area
University Linz
Type of Organization: Universities — Ownership: Public
ENISA Focus Points: CERT, AR, Emerging Risks, Implementation of Security Technology and Standards Policy
Relationships: Austrian Research Centers, Vienna University of Technology, University Klagenfurt, Graz University of Technology
Weblink: http://www.uni-linz.ac.at
Areas of Activity: Conducts research in the Information Security area
Vienna University of Technology
Type of Organization: Other Academic — Ownership: Public
ENISA Focus Points: None
Relationships: Austrian Research Centers, Linz University, Klagenfurt University, and Graz University of Technology
Weblink: http://www.tuwien.ac.at
Areas of Activity: Conducts research in the area of information security

Other Bodies and Organizations Active in Network and Information Security

CERT AT.
Type of Organization: CERT — Ownership: private
ENISA Focus Points: CERT, Micro-enterprises
Relationships: part of CESNET
Weblink: http://www.cert.at

Areas of Activity: CERT.at is the Austrian national CERT, which started on a trial basis in march 2008. As the national CERT, CERT.at is the primary contact point for IT security in the national context. CERT.at will coordinate other CERTs operating in the area of critical infrastructure or communication infrastructure. It also provides basic IT security information (warnings, alerts, and advice) for SMEs. In the case of significant online attacks against Austrian infrastructure, CERT.at will coordinate a response through targeted operators and local security teams.

Initiative Information Security Austria – IISA	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: AR	
Relationships: co-operates with other CERTs	
Weblink: http://www.iisa.at	
Areas of Activity: It focuses on creating awareness of NIS-related issues in the private sector.	

Foundation for (*Stiftung*) Secure Information and Communication Technologies – SIC	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: None	
Relationships: None	
Weblink: http://jce.iaik.tugraz.at/	
Areas of Activity: The Institute for Applied Information Processing and Communication (IAIK) of the Graz University of Technology has established Stiftung Secure Information and Communication Technologies (SIC) to encourage independent scientific research and development, as well as teaching and knowledge transfer, in the fields of applied information processing and communication and information security.	

Secure Business Austria – organization promoting IT-security in Austria (*Verein zur Förderung der IT-Sicherheit in Österreich*)	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points:	
Relationships: None	

Weblink: http://securityresearch.at
Areas of Activity: Secure Business Austria (SBA) is the first Austrian competence centre focusing on organizational and technical aspects of IT Security. The main goal is to promote the collaboration of the industry sector and academic organizations in leading research programs centered around IT security.

saferInternet.at, Austrian Institute for Applied Telecommunications (*Österreichisches Institut für angewandte Telekommunikation*)	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: AR	
Relationships: Digital Austria Platform (*Plattform Digitales Österreich*), Federal Ministry of the Interior, Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*)	
Weblink: http://www.saferInternet.at	
Areas of Activity: It is part of the European Internet safety network, INSAFE, within the framework of the Safer Internet Programme, which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user as part of a coherent approach by the European Union.	

Consumer Organization (*Verein für Konsumenteninformation*)	
Type of Organization: Other Bodies and Organizations	Ownership: Public
ENISA Focus Points: None	
Relationships: None	
Weblink: http://www.konsument.at/konsument/k_overview.asp?nav=K%5FKontakt	
Areas of Activity: This is a consumer organization aimed to protect and educate consumers.	

L.S.Z. Consulting, Loisel.Spiel.Zach GmbH	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: None	
Relationships: None	
Weblink: http://www.lsz-consulting.at	

Areas of Activity: Private organizer of IT events.	
Business Circle Management Fortbildungs GmbH	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: None	
Relationships: None	
Weblink: http://www.businesscircle.at	
Areas of Activity: Private organizer of IT events.	
IIR - Institute for International Research	
Type of Organization: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: None	
Relationships: None	
Weblink: http://www.iir.at	
Areas of Activity: Private organizer of IT events.	
Certification & Information Security Services GmbH – CIS	
Type of Organization: CERTS	Ownership: Private
ENISA Focus Points: CERT, AR	
Relationships: None	
Weblink: http://www.cis-cert.com	
Areas of Activity: Private certification body also engaged in organization of events.	

Activities

Strategic Initiatives

Strategic Implementation and Platform of egovernment Solutions in Austria
Type of Activity: Governmental Policies
Responsible Organization(s): Digital Austria Platform (*Plattform Digitales Österreich*)
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards
Weblink: http://www.digitales.oesterreich.gv.at
Description: Development of the IT and egovernment strategy of the Austrian government

New Data Protection Law
Type of Activity: Governmental Policies
Responsible Organization(s): Committee for Data Protection (*Datenschutzkommission*)
ENISA Focus Points: Development of Security Technology and Standards
Weblink: http://www.dsk.gv.at
Description: The new data protection law is in draft status in Austria.

saferInternet.at
Type of Activity: Nongovernmental Initiative
Responsible Organization(s): Microsoft, Federal Chancellery of the Republic of Austria
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards
Weblink: http://saferInternet.at/
Description: SaferInternet was created by stakeholders to inform citizens about the hazards of the Internet and to provide information about esafety.

HELP
Type of Activity: Governmental Funding Program
Responsible Organization(s): Federal Chancellery of the Republic of Austria
ENISA Focus Points: AR, Emerging/Current Risks, e-ID
Weblink: n/a
Description: Help portal of the government providing basic IT security information to citizens.

E-card (Bürgerkarte)
Type of Activity: Governmental Policies
Responsible Organization(s): Federal Chancellery of the Republic of Austria, A-SIT
ENISA Focus Points: e-ID
Weblink: http://www.chipkarte.at
Description: The program targets to introduce e-ID in order to make egovernment services available to Austrian citizens.

Research Programmes

E-voting
Type of Activity: Technical Research Program
Responsible Organization(s): Federal Chancellery of the Republic of Austria, Center of secure IT (*A-SIT Zentrum für sichere Informationstechnologie* – Austria)
ENISA Focus Points: Resilience, e-ID, Development of Security Technology and Standards
Weblink: n/a
Description: eVoting initiative study to test evoting possibilities, ID management, and security solutions.

MECANOS (Smartcard Security)
Type of Activity: Technical Research Program
Responsible Organization(s): Vienna University of Technology
ENISA Focus Points: Development of Security Technology and Standards
Weblink: http://www.csirt.cz
Description: Research focused on identity management and verification in an online environment using smartcard technology
Managing Emerging Threats in ICT Infrastructures
Type of Activity: Technical Research Program
Responsible Organization(s): Vienna University of Technology
ENISA Focus Points: Development of Security Technology and Standards
Weblink: http://www.tuwien.ac.at/
Description: Research focused on countering emerging web threats
Defending Internet Users Against Web Attacks
Type of Activity: Technical Research Program
Responsible Organization(s): Vienna University of Technology
ENISA Focus Points: Development of Security Technology and Standards
Weblink:
Description: Research focused on the development of new security standards.
WOMBAT (Worldwide Observatory of Malicious Behaviors and Attack Threats)
Type of Activity: Technical Research Program

Responsible Organization(s): Vienna University of Technology
ENISA Focus Points: CERT, Emerging/Current Risks
Weblink:
Description: Founded by the European commission observing worldwide information security threats to develop viable countermeasures

Funding Program & Financial Initiatives

Development of Open Source Platform for eGovernment

Type of Activity: Governmental Funding Program
Responsible Organization(s): Digital Austria Platform (*Plattform Digitales Österreich*)
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards
Weblink: http://www.digitales.oesterreich.gv.at/
Description: Austria is trying to establish egovernment based on open source and is actively developing new technologies.

eGov-Bus

Type of Activity: Governmental Funding Program
Responsible Organization(s): Center of secure IT (A-*SIT Zentrum für sichere Informationstechnologie* – Austria)
ENISA Focus Points: e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards
Weblink: http://demo.a-sit.at/e_government/egov_bus/ , http://www.egov-bus.org

Description: Development of egovernment process management solutions and identity protection using e-ID card solutions.
FIT-IT Trust in IT Systems
Type of Activity: Governmental Funding Program
Responsible Organization(s): Austrian ministry for traffic, innovation, and technology (bmvit) & Austrian Research Promotion Agency (FFG)
ENISA Focus Points: CERT, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards
Weblink: http://www.fit-it.at/
Description: FIT-IT, short for "Research, Innovation, Technology – Information Technology," is an Austrian research programme that focuses on high-quality research in the area of information and communication technology. Currently, there are three program lines: embedded systems, semantic systems and services, and systems on chip.

Events

Conference and Workshops	
informationssicherheit – ocg IT-security	
Responsible Organization: Austrian Computer Society	Frequency: annual
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major = SMEs, Large Enterprises; Minor = Government Institutions, Security Professionals, Educational and Research Organizations, Consumers/Citizens	
Weblink: http://www.ocg.at/ia/security.html	
Description: All-day IT security information event and workshop.	
E-day	
Responsible Organization: IT security Experts	Frequency: annual

ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Target Groups: Major- Government Institutions, Large Enterprises, Security Professionals, SMEs	
Weblink: http://www.itsecurityexperts.at/index.php?option=com_content&task=view&id=18&Itemid=43	
Description: Event focusing on Web security	
IT Security Roadshow	
Responsible Organization: Austrian Federal Economic Chamber, IT and Consulting section (*Wirtschaftskammer Österreich, Bundessparte IT und Consulting*)	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Target Groups: Large Enterprises, Security Professionals, SMEs	
Weblink: http://www.it-safe.at/	
Description: Annual event taking place in all major cities promoting new IT security solutions and promoting awareness	
Day of the safer Internet	
Responsible Organization: saferInternet.at, Austrian Institute for Applied Telecommunications (*Österreichisches Institut für angewandte Telekommunikation*)	Frequency: annual
ENISA Focus Points: AR	
Target Groups: Consumers/Citizens	
Weblink: http://saferInternet.at/veranstaltungen/	
Description: Annual event targeted at citizens in order to promote safe Internet usage	
Information Security Symposium	
Responsible Organization: Certification & Information Security Services GmbH – CIS	Frequency: annual

ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major = Large Enterprises, SMEs; Minor = Government Institutions, Educational and Research Organizations, Security Professionals, Consumers/Citizens	
Weblink: http://www.cis-cert.com/index/index.php	
Description: Organized by the Chamber of Commerce, this event focuses on information security.	
WKO Infodays	
Responsible Organization: Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich*)	Frequency: annual
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major = Large Enterprises, SMEs; Minor = Government Institutions, Educational and Research Organizations, Security Professionals, Consumers/Citizens	
Weblink: http://portal.wko.at/wk/startseite_th.wk?SbId=249&DstId=0	
Description: Annual roadshow promoting NIS awareness and focusing on the enterprise segment, with stops in every major city	
Internet Summit Austria	
Responsible Organization: saferInternet.at, Austrian Institute for Applied Telecommunications (*Österreichisches Institut für angewandte Telekommunikation*)	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major = SMEs, Large Enterprises, Government Institutions; Minor = Security Professionals	
Weblink: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4263	
Description: Annual event focusing on hot topics regarding the Internet	

Media Campaigns	
Day of Data Protection	
Responsible Organization: Committee for Data Protection (*Datenschutzkommission*)	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Target Groups: Major- SMEs, Large Enterprises, Government Institutions, Consumers/Citizens	
Weblink: http://www.dsk.gv.at/site/6218/default.aspx	
Description: A day set by the EU to promote data protection and awareness in which Austria is actively participating	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Austria.

Country Report – Belgium

Country General Information

Source: European Commission

Political system:	Constitutional monarchy
Capital city:	Brussels
Total area:	30 158 sq.km
Population:	10.5 million
Official language:	Dutch, French, German
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Belgium, we present a set of three indicators in the Country Highlights section.

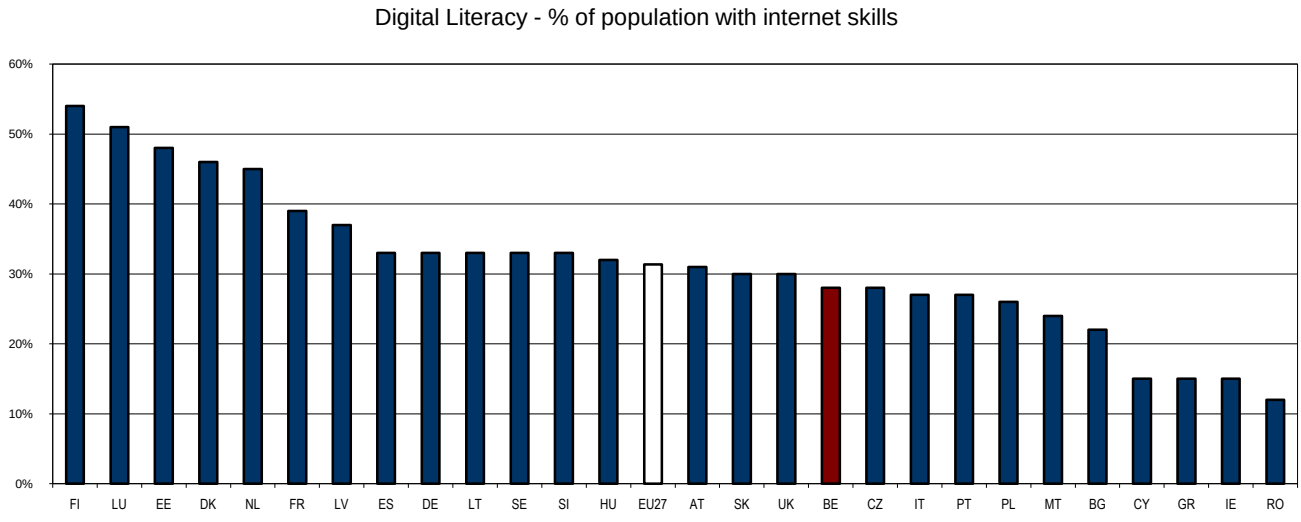
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Belgium is fundamental to this NIS study.

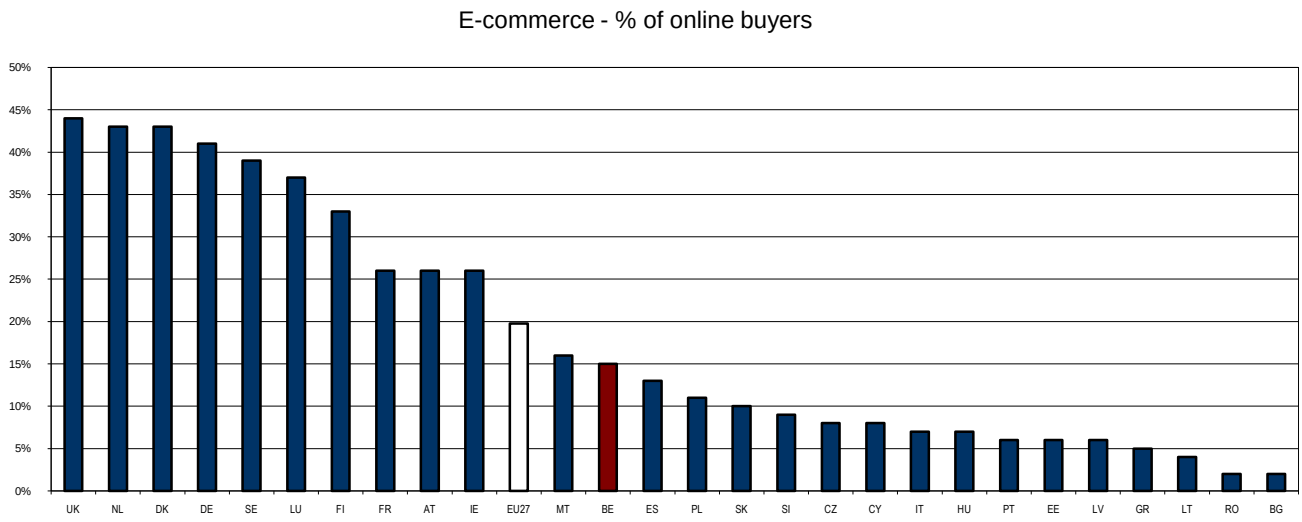
The development of the information society in Belgium is currently doing well, the situation may improve further with particularly strong progress in eGovernment, a rapid adoption of broadband by Internet users, and a business environment relatively favorable to ICT investment, which can rely particularly on a good eSkill base. Belgium has well developed online public services.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

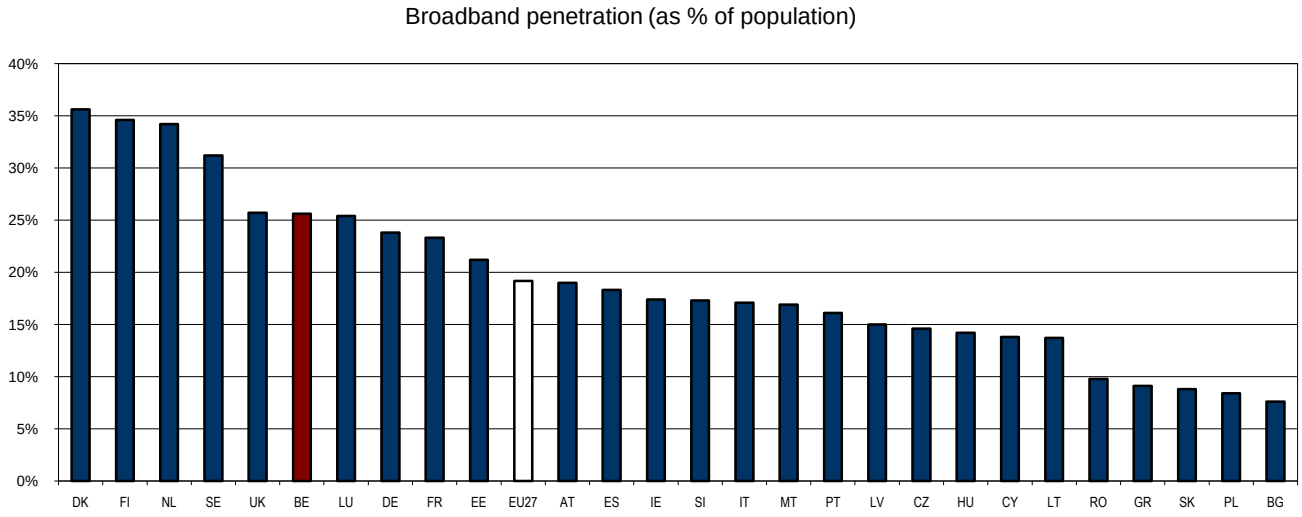
Digital Literacy Indicator



eCcommerce Indicator



Broadband Penetration Indicator



NIS Highlights

In Belgium there is no specific national security agency. The Ministerial Committee for Security and Intelligence has ultimate responsibility for the development of national information security policy, while the Federal Public Service Directorate-General Enforcement and Mediation is the main organization in charge of implementation of such policy.

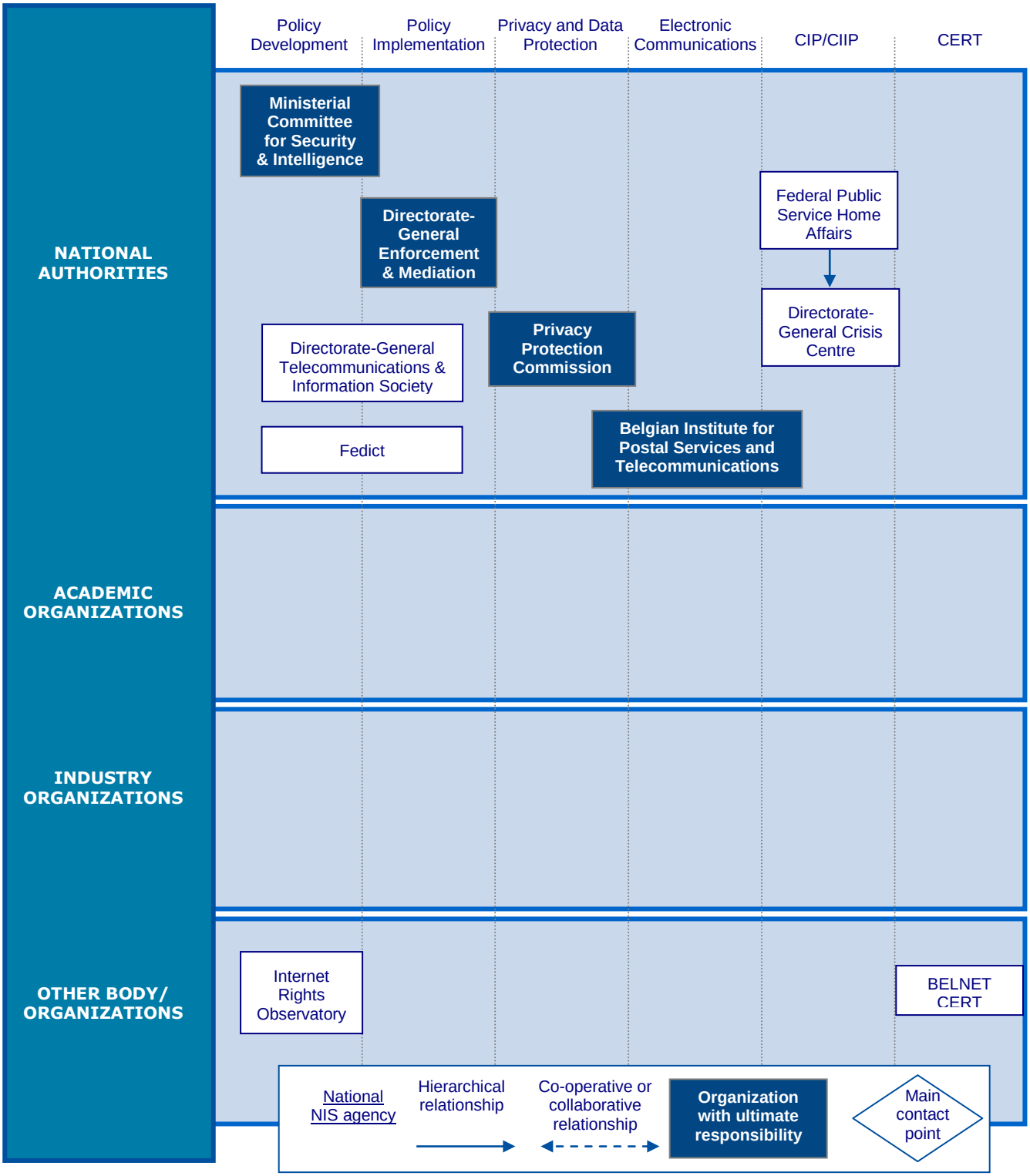
The Privacy Protection Commission ensures protection of personal data in Belgium.

The Belgian Institute for postal services and telecommunications breaches is responsible for implementing and ensuring compliance with electronic communications legislation.

A national CERT has yet to be established in Belgium, although the BELNET network runs a CERT for its constituents in the public and education sectors.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Belgium. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministerial Committee for Security and Intelligence							X	
Directorate-General Enforcement and Mediation			X	X		X		X
Directorate-General Telecommunications and Information Society							X	X
Federal Public Service Information and Communication Technology (Fedict)						X	X	X
Privacy Protection Commission								X
Belgian Institute for Postal Services and Telecommunications (BIPT)			X	X	X			X
Directorate-General Crisis Centre		X						
Internet Rights Observatory			X	X			X	
BELNET CERT	X		X					

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Belgium:

National Authorities in Network and Information Security	
Ministerial Committee for Intelligence and Security	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: N/A	
Areas of Activity: The Ministerial Committee for Intelligence and Security is chaired by the Prime Minister and comprises various government ministers. This Committee lays down the general intelligence and security policy for Belgium.	
Directorate-General Telecommunications and Information Society	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Part of Federal Public Service "Economy, SMEs, Self-Employed and Energy"	
Weblink: http://www.mineco.fgov.be	
Areas of Activity: The directorate is responsible for preparing policy in the area of electronic communications and co-ordinating ICT policy at a federal and inter-federal level.	
Directorate-General Enforcement and Mediation	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards Policy	
Relationships: Part of Federal Public Service Economy, SMEs, Self-Employed and Energy	
Weblink: http://www.economie.fgov.be/information_society/ecommerce/internet_watch/home_fr.htm	

Areas of Activity: The directorate is responsible for, among other tasks, implementation of rules on electronic commerce.
Federal Public Service Information and Communication Technology (Fedict)
Type of Organisation: National Government — Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards Policy
Relationships: cooperates with numerous federal public services bodies
Weblink: http://www.fedict.belgium.be/
Areas of Activity: Fedict is a horizontal unit that provides services to the other Federal Public Services and related authorities. Its three main tasks are: e-government development, e-society development, promotion of Belgium as a region of ICT knowledge.
Privacy Protection Commission
Type of Organisation: National Government — Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy
Relationships: co-operates with Ministry of Industry and Trade
Weblink: http://www.privacy.fgov.be
Areas of Activity: The commission provides advice on and fixing of rules and procedures for electronic systems containing, handling or transporting personal data.
Belgian Institute for Postal Services and Telecommunications
Type of Organisation: National Government — Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises, Implementation of Security Technology and Standards Policy
Relationships: None
Weblink: http://www.bipt.be/

Areas of Activity: The Belgian Institute for Postal Services and Telecommunications (BIPT) is responsible for ensuring implementation of the regulatory framework for electronic communications. It is also responsible for security and QoS of public electronic communications networks. The institute runs a virus alerting service for the general public and SMEs.	
Federal Public Service Home Affairs	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.ibz.be	
Areas of Activity: The Federal Public Service Home Affairs office is responsible for critical infrastructure protection and preparedness.	
Directorate-General Crisis Centre	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience	
Relationships: Part of Federal Public Service Home Affairs	
Weblink: http://crisis.ibz.be/	
Areas of Activity: The centre coordinates the management of crises at a national level as well providing support at a regional and local level.	
Federal Computer Crime Unit (FCCU)	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: Part of the Federal Judicial Police	
Weblink: http://www.fccu.be	

Areas of Activity: The Federal Computer Crime Unit (FCCU) deals with cyber-crime and illegal content on the internet. The unit conducts awareness-raising campaigns with regards to NIS directed at private companies. The unit runs a website where anonymously illegal content on the internet can be reported.

Crossroads Bank for Social Security	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: collaborates with Fedict	
Weblink: http://www.ksz-bcss.fgov.be	
Areas of Activity: The Crossroads Banks for Social Security (CBSS) was created to improve service delivery related to social security. The mission of the CBSS is to be the motor of e-government in the social sector ie: to stimulate and to support the actors in the Belgian social sector to grant more effective and efficient services; to promote information security and privacy protection by the actors in the Belgian social sector; to deliver integrated statistical information to politicians and researchers in order to support social policy. The Crossroads Bank for Social Security was asked by the Belgian federal government to elaborate an E-government plan for the federal public services. This plan, that is now being executed and permanently updated by Fedict, contained among others the creation of an electronic identity card, a company register, a messaging engine between the federal public services and an integrated portal environment.	

Industry Organisations Active in Network and Information Security

Agoria	
Type of Organisation: Other Industry Associations	Ownership: Private
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: co-operates with the National Authorities	
Weblink: http://www.agoria.be/	
Areas of Activity: Agoria is Belgium's largest employers' organisation and trade association. The companies represented are active in the technology industry.	

Brussels-European Chapter of the International System Security Association (ISSA)	
Type of Organisation: Other Industry Associations	Ownership: Private
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.issa-be.org/	
Areas of Activity: The mission of the ISSA is to enhance the knowledge and skills of its, encourage exchange of information security techniques, approaches, and problem solving, be the global voice of the information security professional, and promote best practices in information security.	

LSEC	
Type of Organisation: Other Industry Associations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.lsec.be/	
Areas of Activity: LSEC is an information security cluster, whose membership includes over 600 IT security-specialized companies, and more than 500 individual IT security professionals. LSEC is supported by the Flemish institute for sciences and development (IWT). L-SEC's main objective is to create IT security awareness in the industry at large. This is achieved through the organization of major IT security events in Belgium. Other LSEC activities include start-up projects and an incubation facility, and participation in a number of research programs such as ADAPID (Advanced Applications for electronic Identity Cards) and SEC SOA (Secure Service Oriented Architectures).	

Belgian Computer Security Club (BELCIV / CLUSIB)	
Type of Organisation: Other Industry Associations	Ownership: Private
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.belcliv.be	

Areas of Activity:

The main objective of BELCLIV / CLUSIB is to take any initiative aimed at fostering the security of information systems and networks. More precisely, BECLIV / CLUSIB aims at: introducing and spreading methods and technical recommendations concerning the security of information systems and networks; presenting summaries about the state of the art and the technologies in this field; promoting the exchange of experience and ideas among its members; providing on-going training for its members, e.g. conferences, training seminars and publications.

Other Bodies and Organisations Active in Network and Information Security

Internet Rights Observatory

Type of Organisation: Other Bodies and Organizations	Ownership: PPP
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy	
Relationships: supported by the Federal Public Service Economy, SMEs, Self-Employed and Energy	
Weblink: http://www.internet-observatory.be	

Areas of Activity:

The Internet Rights Observatory is a body composed of representatives from government ministries, universities and research centres, information society service providers, and Internet users. The tasks of the observatory are to: submit opinions on the economic problems brought about by the use of new information and communication technologies; organise consultation among the economic actors concerned; inform the public on these areas. The observatory's Website josted and financed by Federal Public Service Economy, SMEs, Self-Employed and Energy.

SpamSquad

Type of Organisation: Other Bodies and Organizations	Ownership: Private
ENISA Focus Points: Emerging/Current Risks	
Relationships: supported by the Federal Public Service Economy, SMEs, Self-Employed and Energy	
Weblink: http://www.spamsquad.be/fr/home.html	

Areas of Activity:

SpamSquad is an informal group, comprised of academics, representatives of public authorities, and professionals. The group focuses on developing methods to measure spam, and possible solutions to prevent spam. The group runs a portal, which is financed by Federal Public Service Economy, SMEs, Self-Employed and Energy.

BELNET CERT	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT, AR, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://cert.belnet.be	
Areas of Activity: BELNET CERT is the Computer Emergency Response Team for the BELNET community, consisting of all Belgian universities, public libraries, most Belgian high schools and most of the Belgian public administration.	

Activities

Strategic Initiatives

Ecops.be
Type of Activity: Governmental Policies
Responsible Organisation(s): Federal Computer Crime Unit, and Federal Public Service Economy, SMEs, Self-employed and Energy
ENISA Focus Points: Emerging/Current Risks
Weblink: http://www.ecops.be
Description: eCops is an online reporting service to which the Internet user can report crimes committed on or through the Internet.

Safer Internet Belgium
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): Child Focus, and Research Centre of the Consumers Organisation (CRIOC)
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: http://www.saferinternet.be/

Description:

Safer Internet Belgium is part of the European internet safety network INSAFE within the framework of the Safer Internet Programme, which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user.

Towards a Belgian Strategy in Information Security

Type of Activity: Non-governmental Initiative

Responsible Organisation(s): ISACA, ISSA, LSEC, Solvay Business School

ENISA Focus Points: AR

Weblink: http://www.lsec.be/upload_directories/documents/TowardsaBelgianStrategyonInformationSecurity_BISI_080908.pdf

Description:

The result of an initiative by private associations and academic institutions, "Towards a Belgian Strategy in Information Security" is a White Paper aiming to promote the establishment of a more cooperative IT security framework in Belgium.

Action Innocence Belgique

Type of Activity: Non-governmental Initiative

Responsible Organisation(s):

ENISA Focus Points: Awareness raising, Emerging and Current Risks

Weblink: http://www.actioninnocence.org/belgique/index.asp?antenne_news=25&navig=15

Description:

Action Innocence is an NGO which contributes to preserving the dignity and integrity of children on the Internet. Headquartered in Switzerland but locally active in all French-speaking countries in Europe (Belgium, France, Switzerland, Monaco). The organisation's resources come from dues paid by its members, donations, as well as funds raised through special events.
The mission of AiG is to become an independent, French-language reference organisation committed to fighting acts of sexual abuse involving children on the Internet.
The goal of the organisation is to develop the following types of action:

- Prevention and information, intended for parents, children, teenagers, and professionals who work in the school system (the target audience)
- Information and intervention, specifically aimed at government bodies and political authorities

Co-operation with computer professionals with a view to "cleaning up" content that may be accessed via the Internet and developing suitable IT tools.

AiG thus wants to ensure that children and teenagers are able to access information that correspond to their development "in accordance with the age and maturity" (Convention on the Rights of the Child) of each young person, while enabling him/her to take part in the creation of a healthier, more responsible environment. This goal fits into the context of the various aspects of the Rights of the Child.

Events

Conference and Workshops	
Global Security Week	
Responsible Organisation: LSEC	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major- Security Professionals, Educational and Research Organizations, Large Enterprises, Government Institutions; Minor- SMEs, Consumers/Citizens	
Weblink: http://www.lsec.be/index.php/whats_happening/news/global_security_week_by_lsec_september_8_12th	
Description: This event promotes awareness on protection against cyber-crime with some basic awareness activities and afternoon seminars.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

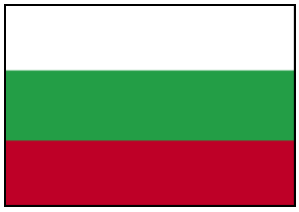
In the preceding 12 months, one security breach was reported in Belgium:

1. In June 2008 Belgacom, the largest Belgian ISP, admitted that 2,000 of its ADSL accounts were compromised earlier this year. The company discovered details of its subscribers posted on a webpage by hackers who weren't happy with download limits on broadband Internet connections.

   http://www.theregister.co.uk/2008/06/11/security_breach_at_belgacom/

Country Report – Bulgaria

Country General Information



Political system:	Republic
Capital city:	Sofia
Total area:	111 000 sq.km
Population:	7.7 million
Official language:	Bulgarian
Time zone:	EET (GMT+2)
Currency:	Lev (BGN)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Bulgaria, we present a set of three indicators in the Country Highlights section.

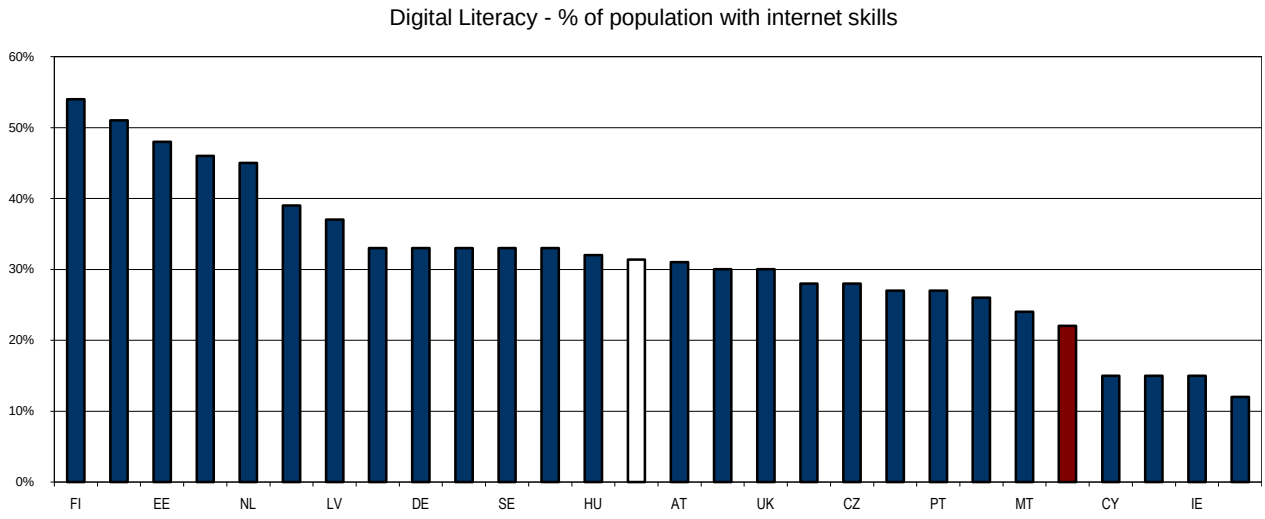
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Bulgaria is fundamental to this NIS study.

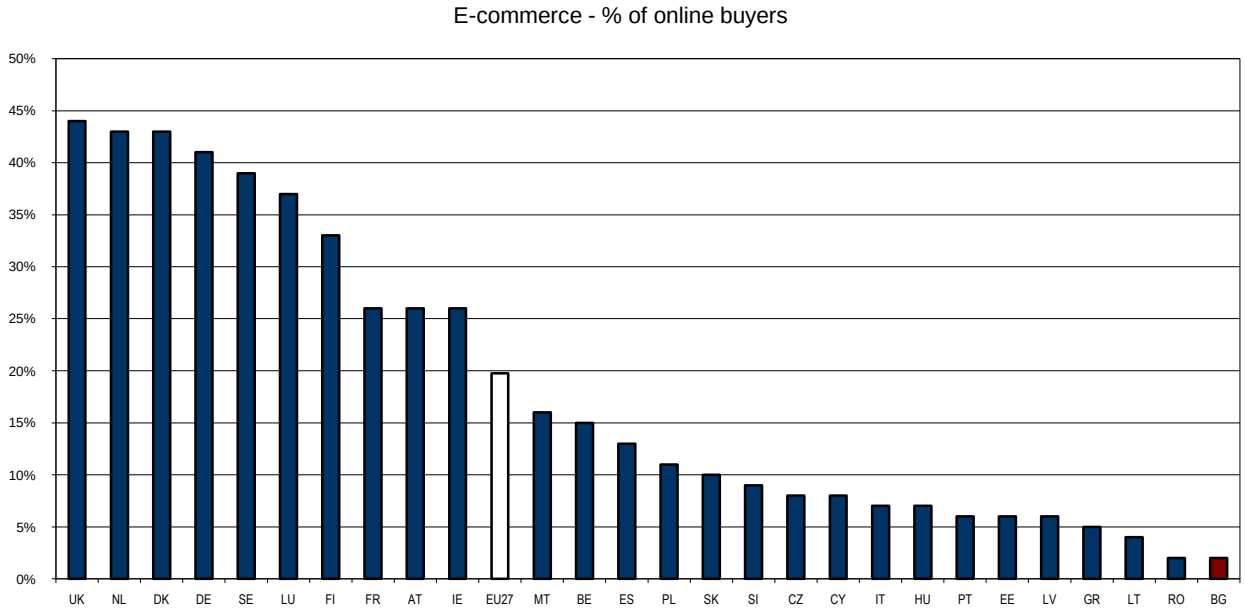
Based on the data below it is clear that the information society in Bulgaria is at a relatively early stage of development. However, there are some strengths and signs, such as the adoption of broadband by Internet users, that Bulgaria is leapfrogging outdated technologies to catch up with its new partners in the EU. eGovernment is high in the list of priorities of the government.

The shown indicators – Digital Literacy, E-commerce Buyers, and Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

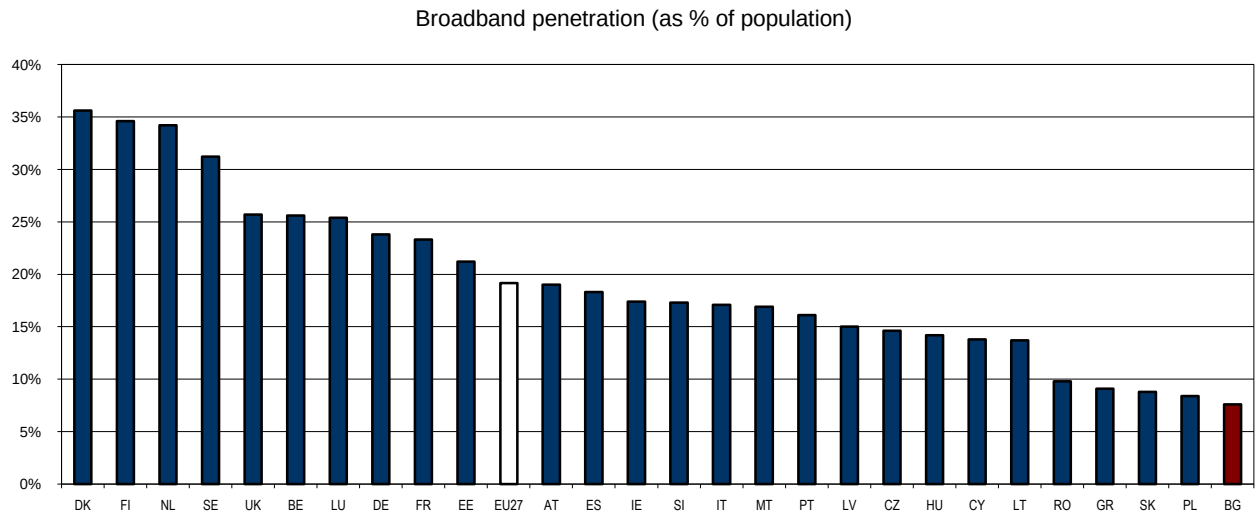
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Bulgarian State Agency for Information Technology and Communications (SAITC), an independent government body, has responsibilities in relation to information security stemming from the Electronic Governance Act. Further the agency is responsible for development and implementation of the national policy for IT and communication security. The agency keeps registers of standards, lists of accredited entities and certified information systems and supervises the adherence to the requirements for information security and interoperability.

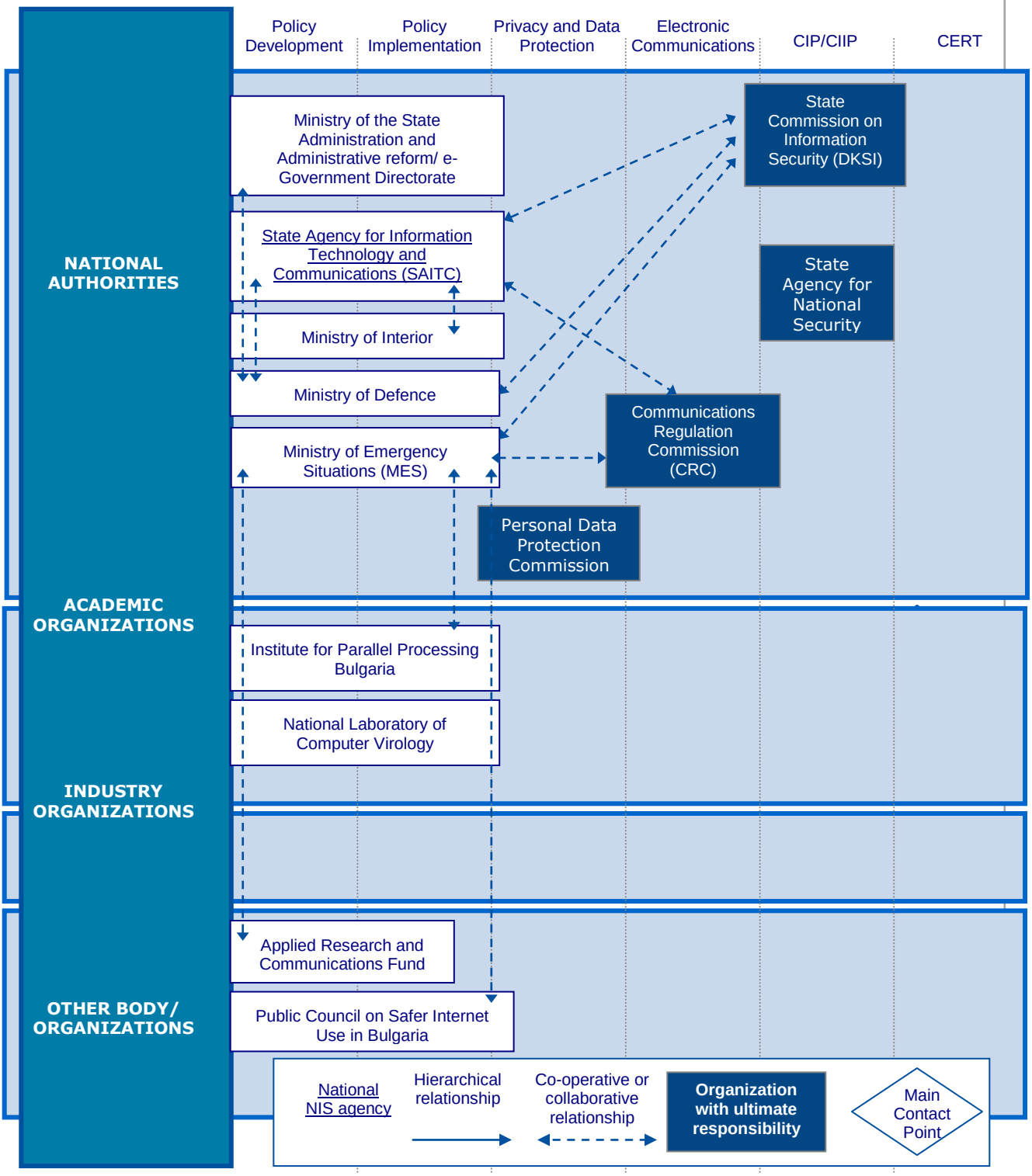
Personal Data Protection Commission is responsible for implementing and ensuring compliance with privacy and data protection legislation in Bulgaria.

The Communications Regulation Commission (CRC) is charged with regulation and control of electronic communications and postal services in Bulgaria.

Currently there is no CERT recognized as the national point of contact for IT security in Bulgaria although this is currently under development by the State Agency for Information Technology and Communications. The Ministry of Emergency Situations (MES) is also responsible for CIP in general and SAITC will have obligations related to critical information infrastructure protection, but the regulatory framework is not yet fully in place.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Bulgaria. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Bulgarian State Agency for Information Technology and Communications (SAITC)		X	X	X		X	X	X
Personal Data Protection Commission		X	X	X		X	X	
Communications Regulation Commission (CRC)		X	X	X		X	X	X
Ministry of Emergency Situations (MES)	X	X		X				X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Bulgaria:

National Authorities in Network and Information Security	
State Commission on Information Security (DKSI)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Ministry of Defence, Ministry of Interior, Ministry of Foreign Affairs, State Agency "National Security"	
Weblink: http://www.dksi.bg	
Areas of Activity: The commission conducts the classified information protection policy of the Republic of Bulgaria. It is responsible for the fulfilment of obligations on classified information protection, arising from international treaties to which the Republic of Bulgaria is a party.	
State Agency for Information Technology and Communications (SAITC)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging Risks/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Ministry of Defence, Ministry of Interior, CRC	
Weblink: http://www.daits.government.bg	
Areas of Activity: The State Agency keeps registers of standards on information security and interoperability, lists of accredited entities and certified information systems. The organization focuses on electronic communication, postal services, accessibility of ICT and other projects.	
Communications Regulation Commission (CRC)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: SAITC	

Weblink: http://www.crc.bg	
Areas of Activity: The commission is responsible for regulation and control in the field of telecommunications and postal services. The Communications Regulation Commission (CRC) implements the state sector policy in the field of telecommunications and postal services. CRC is a specialized independent state authority, entrusted with the functions of regulation and control over the carrying out of the electronic communications.	
Ministry of the State Administration and Administrative reform/ e-Government Directorate	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging Risks/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: SAITC	
Weblink: http://www.mdaar.government.bg/	
Areas of Activity: The ministry draws up strategic guidelines for the establishment and development of the e-government and its components and carries out guidance and control of the fulfilment of the plans for the realization of the strategic guidelines.	
Ministry of Interior	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging Risks/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: State Agency for National Security, DKSI	
Weblink: http://www.mvr.bg	
Areas of Activity: The ministry is responsible for protection of information and communication systems related to national security, as well as R&D in the area of security of computer systems.	
Ministry of Defence	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging Risks/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	

Relationships: Ministry of Interior, DKSI
Weblink: http://www.mod.bg
Areas of Activity: The ministry is responsible for strategic guidance to the armed forces related to information security, and for the availability of CERT for defence purposes.

State Agency for National Security	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging Risks/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Ministry of Interior, DKSI, Ministry of defence, DAITS	
Weblink: N/A	
Areas of Activity: The agency prevents destructive actions toward communications and information systems and provides help to institutions and business in case of security incidents.	

Industry Organisations Active in Network and Information Security

Bulgarian Association of Information Technology (BAIT)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: SAITC, CRC	
Weblink: http://www.bait.bg	
Areas of Activity: This is a non-governmental organisation whose main goal is to defend the interests of its members and help the development of the sector as a whole; lobbying to the state and legislative organs, participating in the activities of various Bulgarian and international institutions and organizations devoted to IT development; participating in the legislative processes related to IT, organizing exhibitions; public discussions and round-tables; and, using well-targeted media policies.	

Bulgarian Association of Software Developers (BASD)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.newhorizons.bg/	
Areas of Activity: BASD is a non-profit organization that actively supports the professional development of the Bulgarian developers by various activities, aiming to improve their knowledge and skills in the area of software design and development.	

Association for Information Security (ISECA)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: FMI at Climent Ohridski University, BARDA	
Weblink: http://www.iseca.org	
Areas of Activity: ISECA is a non-profit organization, aimed at building of awareness of the IS risks and protection necessity and at boosting the development of professional attitude and high standards in IT area.	

Information Systems Audit and Control Association – Sofia Chapter (ISACA Sofia Chapter)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.isaca-sofia.org	
Areas of Activity: The organisation's prime focus is to expand its members' knowledge in the IT governance and control field by providing training, resource sharing, advocacy, professional networking and other benefits. The Sofia Chapter is part of ISACA worldwide. The organization certifies in a number of IT professional skills (CISA, CISM, CGEIT) and CobiT.	

Telecommunications Association	
Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: State Agency for Information Technology and Communications, the Commission on Regulation of Communications, Sofia University "St Kliment Ohridski", Technical University of Sofia	
Weblink: http://www.astel-bg.com/	
Areas of Activity: The Telecommunications Association focus on co-operation in elaborating of the new legal framework, consulting the national policy and regulatory authorities in telecommunications market regulations, participation in EU fostered programs, promoting an improved information environment for telecommunications players, and enhancement of qualification and professional training of its members' staff.	

Academic Organisations Active in Network and Information Security

Sofia University "St. Kliment Ohridski", Faculty of Mathematics and Informatics (FMI)	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: BAIT, BARDA, ISECA	
Weblink: http://www.fmi.uni-sofia.bg	
Areas of Activity: The university conducts teaching, training and research and development in Information Technologies. The course "Information security in computer systems and networks" is a Master program and is 3 semesters long. The university cooperates with IT companies in the organization of different events and trainings in the IT security field.	

Technical University of Sofia	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: BAIT, BARDA, FMI	

Weblink: http://www.tu-sofia.bg	
Areas of Activity: The largest higher engineering school in Bulgaria. The Faculty of computer systems provides bachelor and master programs, which include courses in IT security. For example the course "Security Code Writing" is part of the bachelor program "Computer systems".	
Rakovski Defence and Staff College	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Ministry of Education	
Weblink: http://rdsc.md.government.bg	
Areas of Activity: National institution for higher education, qualification, and scientific research on issues of national security and Defence. The Academy is the main educational institution concerning issues of international and national security, civil-military cooperation, military art, and interoperability with NATO armed forces.	
Technical University of Varna	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.tu-varna.bg/	
Areas of Activity: The department of Computer Science and Engineering provides courses in IT security. The faculty is partnering with Cisco Systems and Microsoft.	
Institute for Parallel Processing Bulgaria	
Type of Organisation: Other Academic	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: SAITC	
Weblink: http://www.bas.bg/clpp/index.html	

Areas of Activity: The institute is responsible for information security of the academic network. The institute is one of the leading scientific institutions in the area of Mathematical Sciences of the Bulgarian Academy of Sciences. The organization carries out fundamental and applied research mainly in the fields of Computer Science and Communication Technologies.

National Laboratory of Computer Virology	
Type of Organisation: Other Academic	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID Development of Security Technology and Standards Policy	
Relationships: FMI at Climent Ohridski University, SAITC	
Weblink: http://www.nlcv.bas.bg	
Areas of Activity: The lab houses antivirus laboratories, which has CERT functions and consultancy role in the development of national security policies and plans.	

Academy of the Ministry of internal affairs	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Ministry of Interior	
Weblink: http://www.academy.mvr.bg/default.htm	
Areas of Activity: The academy is educating professionals for the National Police and the other national security offices; the IT systems protection is part of the bachelor degree program "National security protection".	

Other Bodies and Organisations Active in Network and Information Security

New Horizons Bulgaria	
Type of Organisation: Technical & Professional Certification Providers	Ownership: private
ENISA Focus Points: Micro-enterprises, Implementation of Security Technology and Standards Policy	

Relationships: None	
Weblink: http://www.newhorizons.bg/	
Areas of Activity: The organization provides large spectrum of technical and business training courses including technical and certification vendor partner programs and program for Certified Penetration Testing Specialist (CPTS).	
Applied Research and Communications Fund	
Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy	
Relationships: co-operates with other CERTs	
Weblink: http://www.arcfund.net	
Areas of Activity: The fund conducts applied research and analysis that assists the development and implementation of public policies. The organization was established to promote innovation in the European economy and facilitate the transfer of new and advanced technologies and know-how, and to support cross-border networking and capacity building of businesses, public agencies or private organizations, by using the advances in information and communication technologies.	
Public Council on Safer Internet Use in Bulgaria	
Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: Ministry of Education and Science, State Agency for Child Protection, Ministry of Interior, Sofia Municipality Internet Society-Bulgaria, Bulgarian Association for Information Technologies (BAIT), Bulgarian Telecommunications Company, Cisco Systems-Bulgaria, Foundation Law and Internet, Association for Consumers Protection Partners-Bulgaria Foundation, Bulgarian Federation for Electronic Sport Gender Education, Research and Technologies Foundation, Applied Research and Communications Fund, Center for the Study of Democracy	
Weblink: http://www.web112.net/en/	

Areas of Activity:

The council supports the national Safer Internet Hotline in Bulgaria that enables local Internet users to report incidences of harmful and illegal content disseminated over the Internet. At the initial stage of its implementation the hotline will be primarily concerned with issues of child pornography on the Internet but, as the service gains experience and public recognition, the scope of activity will be extended to cover also other forms of harmful content and conduct, as well as other interactive technologies (incl. mobile, online games, chat channels, etc.)

Activities

Strategic Initiatives

Implementation of e-signature in the state administration

Type of Activity: Governmental Policies

Responsible Organisation(s): Ministry of Sate Administration and administrative reform, CRC

ENISA Focus Points: AR, e-ID, Implementation of Security Technology and Standards

Weblink:

Description:

The activity is part of the e-Government strategy and is targeted to authentication of the sources of information in state administration.

Creation of CERT

Type of Activity: Governmental Policies

Responsible Organisation(s): State Agency for Information Technology and Communications

ENISA Focus Points: CERT

Weblink:

Description:

The "Ordinance on the general requirements on interoperability and information security" and its annexes formulate the policy and the specific requirements for network and information security in the administrative information systems. A series of measures for network and information security management will be realised both on at central level and on the level of the administrative bodies. In this document are presented those activities, which are ongoing.

Certification of all the administrative IS for security and interoperability compliance from SAITC
Type of Activity: Governmental Policies
Responsible Organisation(s): State Agency for Information Technology and Communications, Ministry of State administration and Administrative reform
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards
Weblink: N/A
Description: The IT systems within state administrative bodies will be audited for compliance with security regulations on general requirements for Information Security. The certification will be accredited by SAITC assessors, who will be registered in official registry and monitored by SAITC.
Certification of administrative bodies for compliance with ISO 27001:2005*
Type of Activity: Governmental Policies
Responsible Organisation(s): SAITC - project sponsor, Bureau Veritas - auditor
ENISA Focus Points: Resilience, Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: N/A
Description: Description: The activity is a component the government NIS policy and focuses on the readiness of the administration bodies to comply with requirements imposed by the Electronic Governance Act. The procedure covers: assets management, risk assessment and treatment, access control, communications and operations management, protection against malicious code, monitoring and incident management, physical and environmental security, human resources security.
Creation of the registry of Information objects and e-services
Type of Activity: Governmental Policies
Responsible Organisation(s): Ministry of State Administration and administrative reform, SAITC
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards
Weblink: N/A

Description: The creation of registries is part of the National Administrative data model, which is an element of creating a Unified environment for secure exchange of electronic documents (ESOD).
Creation of PKI-based integrated system for exchange of e-documents in state administration
Type of Activity: Governmental Policies
Responsible Organisation(s): Ministry of State Administration and administrative reform, SAITC
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: N/A
Description: The initiative is aimed at securing exchange of information between Bulgarian administrative bodies.
Creation of "In safe" Internet Center
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): ARC Foundation
ENISA Focus Points: AR, Implementation of Security Technology and Standards
Weblink: N/A
Description: Creation of a national center for building awareness of the safety for children while using the Internet.
Series of Round tables for Internet Safety, under the Safer Internet Plus Programme
Type of Activity: Governmental Policies
Responsible Organisation(s): SAITC, ARC Foundation
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: N/A

Description: This is a series of round tables on different aspects of safety including a round table on Public-Private Partnerships in the Area of Safer Internet Use, and a Round table on "Computer Games and Children's Safety in Internet".
Introduction of Biometric Passports
Type of Activity: Governmental Policies
Responsible Organisation(s): Ministry of Interior
ENISA Focus Points: e-ID, Implementation of Security Technology and Standards
Weblink: N/A
Description: Description: As a member of the EU, Bulgaria is obliged to introduce biometric passports for Bulgarian citizens. The project has been delayed several times during the last 2 years and most likely will be launched in Q1 2009.

Events

Conference and Workshops	
Children's Safety in Internet Day	
Responsible Organisation: SAITC, ARC Found	Frequency: annual
ENISA Focus Points: AR	
Target Groups: Major- Consumers/Citizens	
Weblink: N/A	
Description: The aim of the event is building awareness of the risks for children in Internet and protection measures, promotion of the availability of national hot line for harmful content, and protection measures. The day was followed by film shows on the subject in schools.	
Computer security	
Responsible Organisation: National Laboratory of Computer Virology	Frequency: annual
ENISA Focus Points: AR	

Target Groups: Major- Government Institutions, Educational and Research Organizations, Security Professionals; Minor- Large Enterprises	
Weblink: N/A	
Description: The events are targeted to professionals in the field of information security and are focused on the changing threat environment and innovations in IT security technologies including new scientific researches and projects.	
Internet: technologies and problems	
Responsible Organisation: National Laboratory of Computer Virology	Frequency: annual
ENISA Focus Points: AR	
Target Groups: Major- Government Institutions, Educational and Research Organizations, Security Professionals; Minor- Large Enterprises	
Weblink: N/A	
Description: The events are targeted to professionals in the field of information security and are focused on the impact of the Internet on different aspects of life and business.	

Media Campaigns

Safety for children on the Internet	
Responsible Organisation: Microsoft, Az-deteto.com	Frequency: annual
ENISA Focus Points: AR	
Target Groups: Major- Consumers/Citizens; Minor- Educational and Research Organizations	
Weblink: N/A	
Description: The initiative includes initiatives in schools, lessons for parents and teachers. An on-line game is available on the site Az-deteto.com and the children were able to propose rules for safety in the Internet. A notebook was delivered as prize to the child, who provided the best proposal. The event is supported by: SAITC, Public Council on Safer Internet Use in Bulgaria, the Ministry of education, The State Agency for Child protection. More than ten media are media partners.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Bulgaria.

Country Report – Cyprus

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Nicosia
Total area:	9 000 sq.km
Population:	0.8 million
Official language:	Greek, English
Time zone:	EET (GMT+2)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Cyprus, we present a set of three indicators in the Country Highlights section.

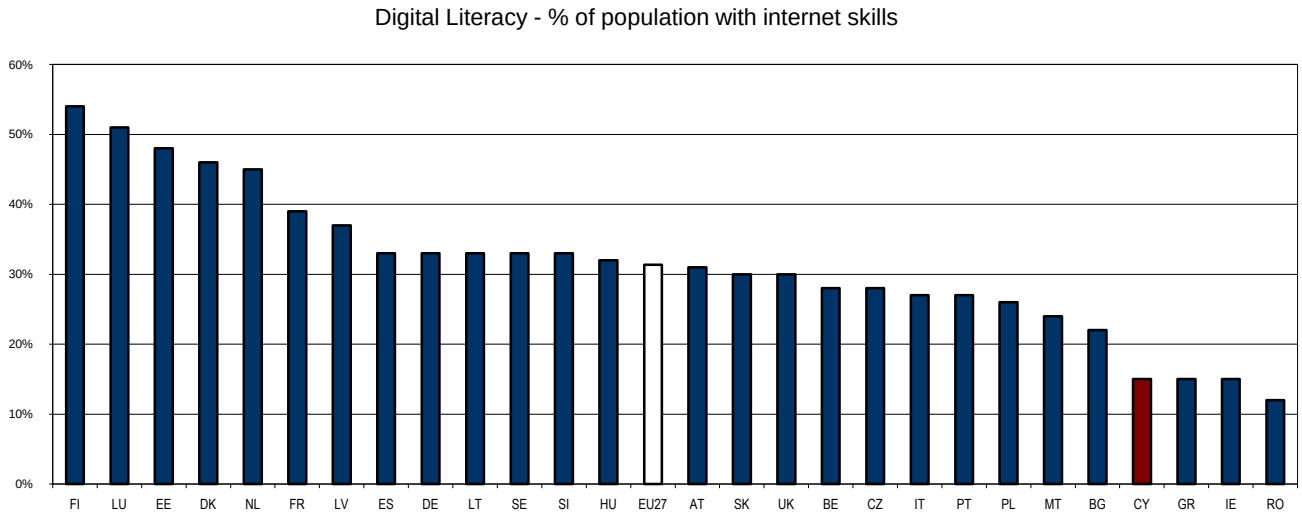
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Cyprus is fundamental to this NIS study.

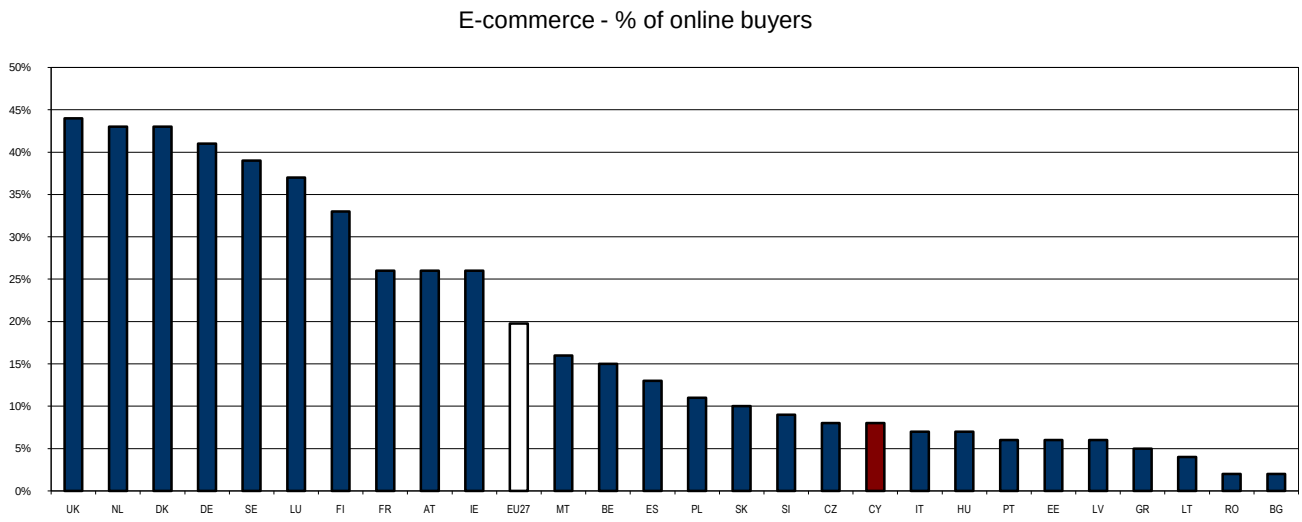
Efforts in developing e-Government services and a business environment relatively favorable to ICT investment, in particular with a good e-Skill base, are laying the foundations for further development.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

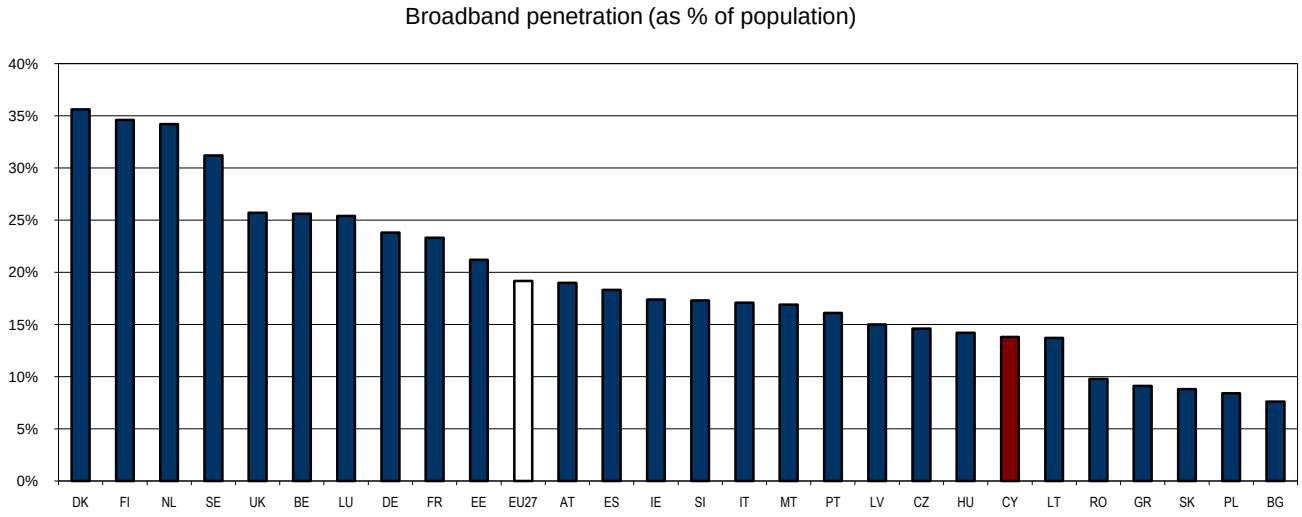
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Office of the Commissioner of Electronic Communications and Postal Regulation is recognized among NIS stakeholders in Cyprus as the national security agency. The office is charged with electronic Communications Regulation in conjunction with administration of network and information security issues.

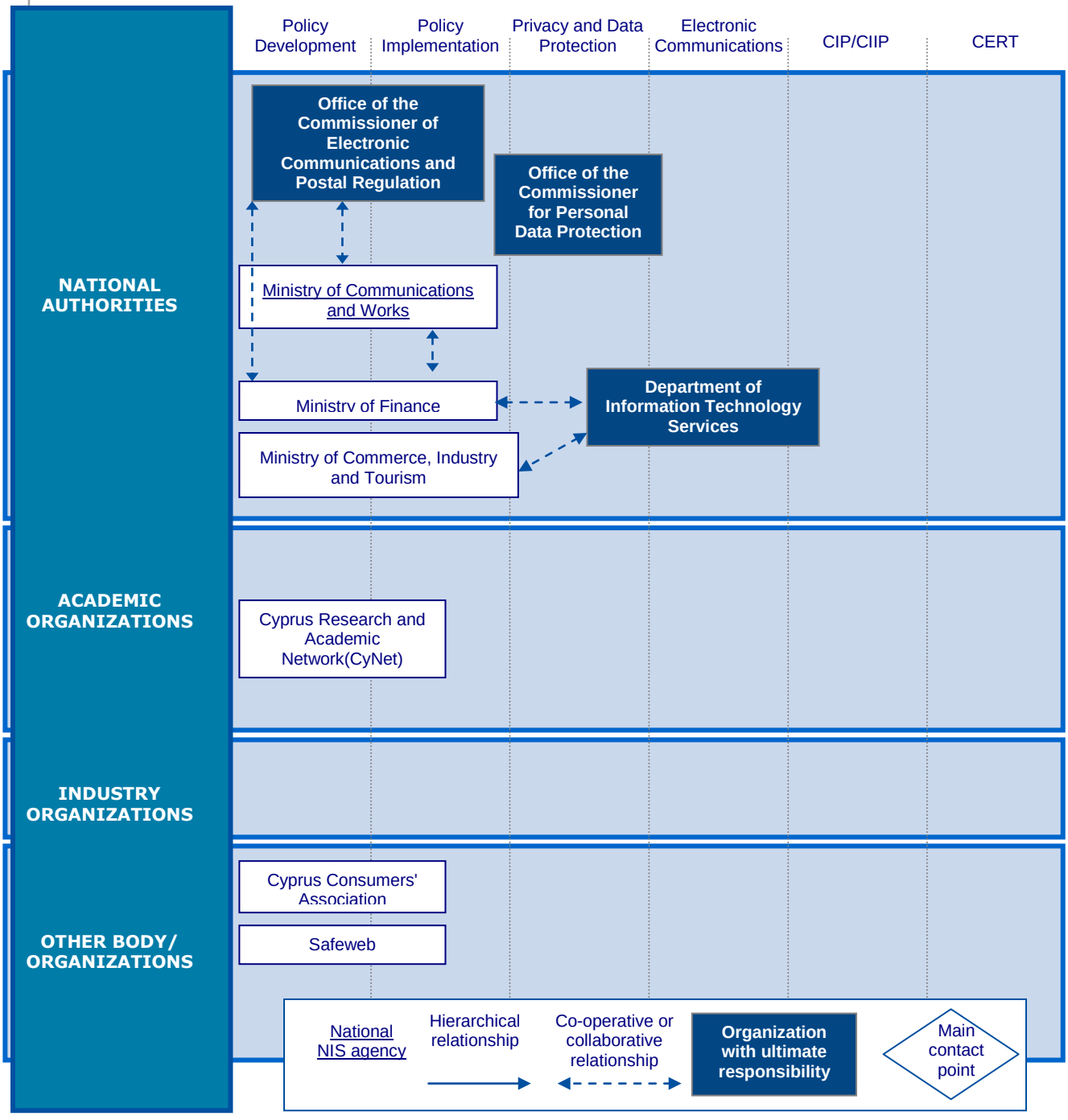
The Ministry of Communications and Works and the Office of the Commissioner of Electronic Communications and Postal Regulation are responsible for information security policy development and implementation at the national level. The bodies are responsible for representation of the government of Cyprus in international and regional telecommunications organizations in the field of electronic communications as well as responsible for managing and implementing the obligations of the Republic emanating from the Conventions or other legal instruments of such organizations on technical, regulatory, management and other related issues.

The Office of the Commissioner for Personal Data Protection is charged with the protection of personal information relating to an individual against its unauthorized and illegal collection, recording and further use and it also grants the individual certain rights, i.e. the right of information, the right of access and gives him the possibility to submit to the Office complaints relating to the application of the Law. The office is also responsible for CIP/CIIP activities at the national level in Cyprus.

Office of the Commissioner of Electronic Communications and Postal Regulation and the Ministry of Communications and Works are responsible for development and implementation of legislation pertaining to electronic communications in Cyprus.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Cyprus. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Office of the Commissioner of Electronic Communications and Postal Regulation		X	X	X	X	X	X	X
Ministry of Communications and Works		X	X	X	X	X	X	X
Office of the Commissioner for Personal Data Protection		X	X	X	X	X	X	X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Cyprus:

National Authorities in Network and Information Security	
Office of the Commissioner of Electronic Communications and Postal Regulation	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Cooperate with Ministry of Finance	
Weblink: http://www.ocecpr.org.cy	
Areas of Activity: The office is responsible for electronic communications regulation, including administration of network and information security issues. Representation of Cyprus in the ENISA Management Board, and acting as the liaison office is also a responsibility of the office.	
Ministry of Communications and Works	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Cooperate with Ministry of Finance	
Weblink: http://www.mcw.gov.cy	
Areas of Activity: The Ministry is charged with developing and implementing electronic communications policies. In general, the mission of the Ministry is the provision of efficient and effective services in telecommunications, postal services, road safety with a sufficient road network, modernized buildings, up to-date airports and ports with efficient services, and the promotion of our culture and heritage.	
Ministry of Finance , Department of Information Technology Services	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: cooperates with the Ministry of Communications and Office of the Commissioner of Electronic Communications and Postal Regulation	

Weblink: http://www.mof.gov.cy/dits
Areas of Activity: The department is responsible for information security policy in Cyprus, as well as administration of e-government issues.

Ministry of Commerce, Industry and Tourism	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, Micro-enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.mcit.gov.cy	
Areas of Activity: The ministry is responsible for administration of e-commerce issues in Cyprus.	

Office of the Commissioner for Personal Data Protection	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, AR, Micro-enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.dataprotection.gov.cy	
Areas of Activity: The office is charged with personal information and data protection.	

Industry Organisations Active in Network and Information Security

Cyprus Information Technology Enterprises Association (CITEA)	
Type of Organisation: IT Association	Ownership: PPP
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Micro-enterprises	
Relationships: co-operates with the National Authorities	
Weblink: http://www.citea.net/	

Areas of Activity: Cypriot ICT industry association. The goal of the association is to play an important role in the development of information technologies in the Cyprus economy and evangelize information society issues.	
Cyprus Computer Society	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Micro-enterprises	
Relationships: None	
Weblink: http://www.ccs.org.cy	
Areas of Activity: The objectives of the association include promotion of computer science and information technology areas and their related subjects within the Cyprus economy, society, businesses and organizations of the public and private sectors, education of and raising awareness on IT related issues, organization of events (i.e. seminars, lectures, conferences etc), and cooperation with the government, the general and IT industries for the effective introduction and use of IT in all aspects of economic and social activity in Cyprus Computer Society. The organization represents computer scientists and IT professionals within the Cyprus IT industry, and to promotes their requirements, rights and goals within their working environments.	
ERMIS	
Type of Organisation: Other Industry Association	Ownership: Private
ENISA Focus Points: Emerging/Current Risks, e-ID, Micro-enterprises	
Relationships: None	
Weblink: http://www.ermis.org/	
Areas of Activity: The mission of ERMIS is to contribute to the technological upgrading of the country's productive base and encourage and support local and regional development. The main objectives of the organization include development the necessary infrastructure and appropriate services to support, nurture and transform innovative ideas into successful business ventures, upgrade of existing production units through the utilisation of new technologies developed at the incubator, and training human resources.	
DIOGENES	
Type of Organisation: Other Industry Association	Ownership: PPP
ENISA Focus Points: e-ID, Micro-enterprises	

Relationships: Private entity wholly owned by the University of Cyprus and the Ministry of Commerce
Weblink: http://www.diogenes.com.cy
Areas of Activity: DIOGENES business incubator provides a nurturing, instructive and supportive environment for entrepreneurs during the critical stages of starting up a new business. The goal of incubators is to increase the chance that a start-up will succeed, and shorten the time and reduce the cost of establishing and growing its business.

Academic Organisations Active in Network and Information Security

University of Cyprus -Department of Computer Science	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, e-ID	
Relationships: Information Security Office at the University of Cyprus	
Weblink: http://www.cs.ucy.ac.cy	
Areas of Activity: The department undertakes research and organizes courses and seminars related to information security, protection, cryptography and other NIS areas.	
University of Cyprus - Information Security Office	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: CERT, AR	
Relationships: N/A	
Weblink: http://www.ucy.ac.cy/security	
Areas of Activity: The mission of the Information Security Office is to provide proactive security analysis, development, education, and guidance related to University's information asset and information technology environment. The entity focuses on network security, operating system security and application security.	
Cyprus Research and Academic Network(CyNet)	
Type of Organisation: Research Centers	Ownership: Public

ENISA Focus Points: Resilience
Relationships: University of Cyprus, Research Promotion Foundation, Planning Bureau
Weblink: http://www.cynet.ac.cy
Areas of Activity: The University of Cyprus in collaboration with the Research Promotion Foundation and the Planning Bureau, in their effort to enhance the research activities in Cyprus, have created the Cyprus Research and Academic Network (CyNet) whose aim is the creation of a network infrastructure and the provision of advanced Internet services to the research and academic community of Cyprus.

Other Bodies and Organisations Active in Network and Information Security

Cyprus Consumers' Association

Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: CERT, AR	
Relationships: N/A	
Weblink: http://www.cyprusconsumers.org.cy/	
Areas of Activity: This is a consumer organisation whose aim is to protect and educate consumers in various areas including information technology.	

Safeweb

Type of Organisation: CERT	Ownership: Non-profit
ENISA Focus Points: CERT, AR, Emerging/Current Risks	
Relationships: University Of Cyprus (UCY), Department of Computer Science, High Performance Systems Laboratory (HPCL), FORTH-ICS	
Weblink: http://www.safeweb.org.cy/contact.php?lang=en	

Areas of Activity:

SafeWeb is the hotline of Cyprus. As such, it aims to participate in the efforts to provide citizens and the global community a safer Internet, where illegal and offensive content distribution is minimized. In doing so, it provides concerned users the means to anonymously report related incidents. Its primary objective is to create a contact point where incidents concerning child pornography, racism, fraud and consumer protection in general are reported.

Activities

Strategic Initiatives
Privacy Security of communications and self-privacy of users and subscribers
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): CYBERETHICS
ENISA Focus Points: AR, Emerging/Current Risks, e-ID
Weblink: N/A
Description: Presentation to universities concerning the safe and proper use of the Internet.
Privacy Security of Communications and Self-privacy of Users and Subscribers
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): CYBERETHICS
ENISA Focus Points: AR, Emerging/Current Risks, e-ID
Weblink: N/A
Description: Presentation to schools concerning the safe and proper use of the Internet.
Dangers of the Internet and How to Protect Your Children
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): CYBERETHICS
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: N/A

Description: Providing parents with information on dangers of the Internet and ways to protect the children.
Secondary Legislation on Electronic Communications Networks Integrity and Resilience
Type of Activity: Governmental Policies
Responsible Organisation(s): OCECPR
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy
Weblink: N/A
Description: Update legislation with new proposals, aligned with EU regulations.
Development of National CSIRTs
Type of Activity: Governmental Policies
Responsible Organisation(s): OCECPR/MCW
ENISA Focus Points: CERT, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy
Weblink: N/A
Description: Development of National CSIRTs.
Raising awareness on Information Security issues
Type of Activity: Governmental Policies
Responsible Organisation(s): OCECPR and other public and private stakeholders
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Micro-enterprises, Implementation of Security Technology and Standards Policy
Weblink: N/A
Description: Campaign to increase awareness among citizens and enterprises on new security risks and issues.

Funding Programmes & Financial Initiatives

"Strengthening Consumer Protection in Cyprus: Preparing to Meet the European Challenge"

Type of Activity: Non-Gov Funding Programmes & Financial Initiatives

Responsible Organisation(s): CCS

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: N/A

Description:

The purpose of the program is to strengthen and develop consumer protection in Cyprus and to increase public awareness and sensitivity, and promote active citizenship on consumer related issues.

Raising Awareness on Consumer Protection and Rights

Type of Activity: Non-Gov Funding Programmes & Financial Initiatives

Responsible Organisation(s): CCS

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: N/A

Description:

To raise the level of awareness of Greek Cypriot and Turkish Cypriot consumers and to give Greek Cypriot and Turkish Cypriot consumers the means to protect their own interests.

Events

Conference and Workshops

ICT Forum

Responsible Organisation: CITEA	Frequency: annual

ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Micro-enterprises, Implementation of Security Technology and Standards Policy

Target Groups: Major- Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions Minor- Consumers/Citizens

Weblink: http://www.ictcyprus.com/
Description: The goal of the conference is to bring together top-level executives from leading companies as they reveal opportunities and challenges raised by the emergence of next-generation ICT services and solutions.

Standard For Information Security Management Systems	
Responsible Organisation: CITEA	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards Policy	
Target Groups: Major- Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions Minor- Consumers/Citizens, Security Professionals	
Weblink: http://www.ictcyprus.com/	
Description: This seminar is meant for participants from IT companies or other companies interested in IT security (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations).	

CYPRUS INFOSEC	
Responsible Organisation: CCS	Frequency: Every Two Years
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Target Groups: Major- Security Professionals, SMEs, Large Enterprises, Government Institutions Minor- Consumers/Citizens, Educational and Research Organizations	
Weblink: http://www.cyprusinfosec.org/	
Description: This event attempts to promote and raise awareness amongst business leaders and IT professionals in the most recent developments in the field of information security. To expose the business, professional and academic communities as well as policymakers to the experiences of internationally renowned professionals in the field of information security.	

SHPCS 2008	
Responsible Organisation: n/a	Frequency: n/a

ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy
Target Groups: Major- Security Professionals, SMEs, Large Enterprises, Government Institutions Minor- Consumers/Citizens, Educational and Research Organizations
Weblink: http://www.diiga.univpm.it/~spalazzi/nicosia/
Description: This workshop addresses relationships between security and high performance systems in three directions: how to add security properties (authentication, confidentiality, integrity, non-repudiation, access control) to high performance computing systems; how to use high performance computing systems to solve security problems; and, investigates the tradeoffs between maintaining high performance and achieving security in computing systems and solutions to balance the two objectives.

Media Campaigns

In Radio Interviews

Responsible Organisation: CYBERETHICS	Frequency: n/a
ENISA Focus Points: CERT, AR	
Target Groups: Major- Security Professionals, Educational and Research Organizations, Consumers/Citizens; Minor- Security Professionals, SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.cyberethics.info/cyethics2/pageSingleModule.php?pageID=31&instance_ID=53&newsid=40	
Description: This campaign features a phone in Greek speaking radio program to discuss the dangers of the Internet and what the role of Awareness Node.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

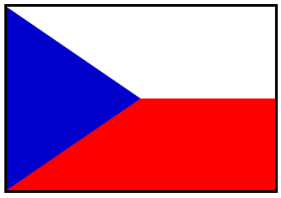
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Cyprus.

Country Report –Czech Republic

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Prague
Total area:	79 000 sq.km
Population:	10.3 million
Official language:	Czech
Time zone:	CET (GMT+1)
Currency:	Czech koruna (CZK)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Czech Republic, we present a set of three indicators in the Country Highlights section.

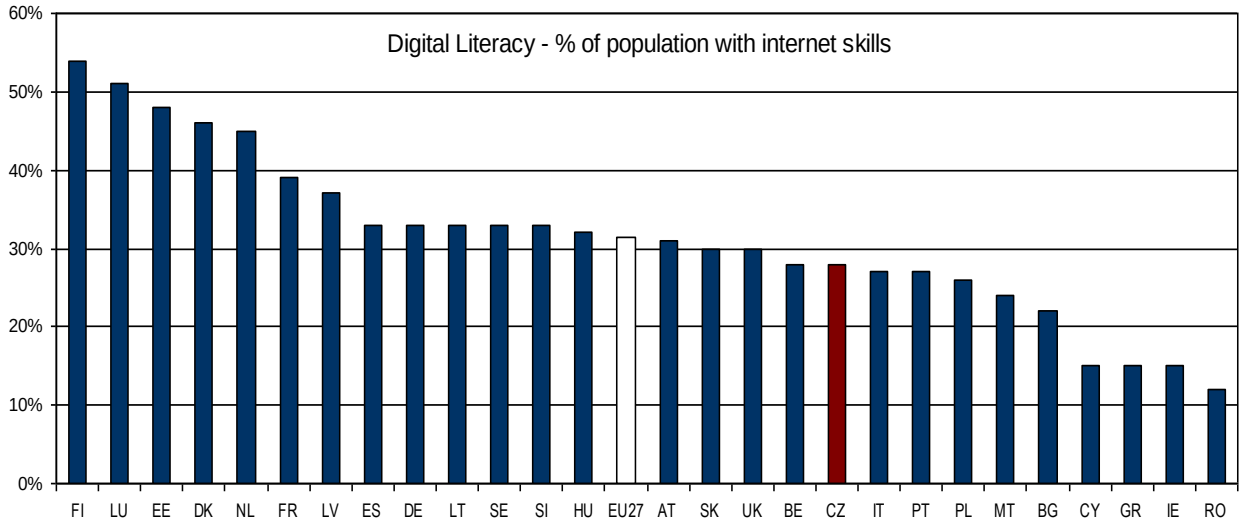
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Czech Republic is fundamental to this NIS study.

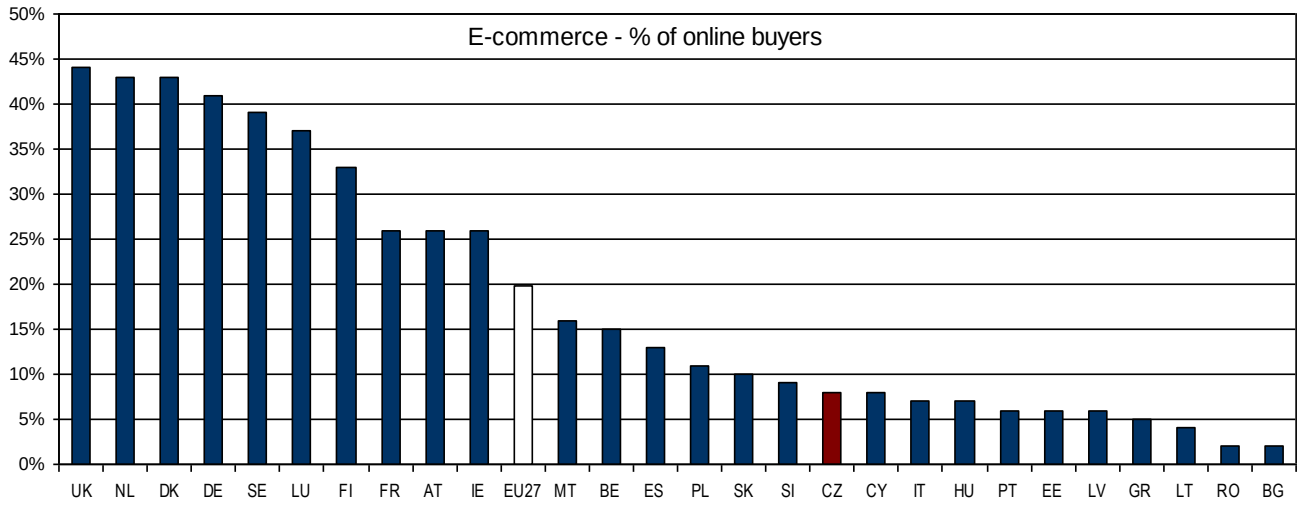
The development of the information society in the Czech Republic is currently doing well, the situation may improve further with particularly strong progress in eGovernment, a rapid adoption of broadband by Internet users, and a business environment relatively favorable to ICT investment, which can rely particularly on a good eSkill base.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

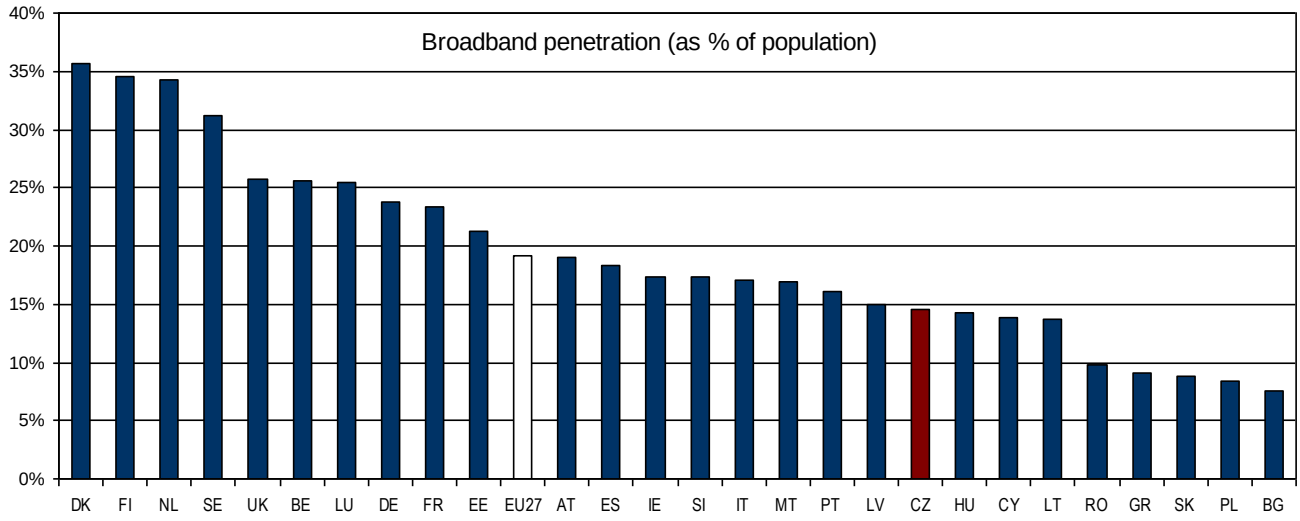
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The National Security Authority, an independent government body, is recognized among NIS stakeholders in the Czech Republic as the national security agency related to classified information. The Government Council for Information Society as an advisory body of the Czech Government comprises representatives from various ministries and from the public administration, academic and business sectors as well as independent experts. The Council is responsible for co-ordinating the development and implementation of national information society strategy, including those aspects relating to information security.

Taking responsibility for the implementation of national information security policy is the Ministry of the Interior and the Ministry of Industry and Trade. The Ministry of the Interior plays a central role in implementation of the key e-government, e-signature, security for public administration information systems and government infrastructure development projects. The Ministry of Industry and Trade oversees the implementation of electronic communications legislation.

The Czech Republic is committed to data protection and ensuring compliance in this regard. The Office for Personal Data Protection is an independent oversight body responsible for this task. The Office is also charged with maintaining a register of databases; investigating complaints; imposing fines for violations; conducting audits and providing consultations on data protection; and commenting on legislative proposals.

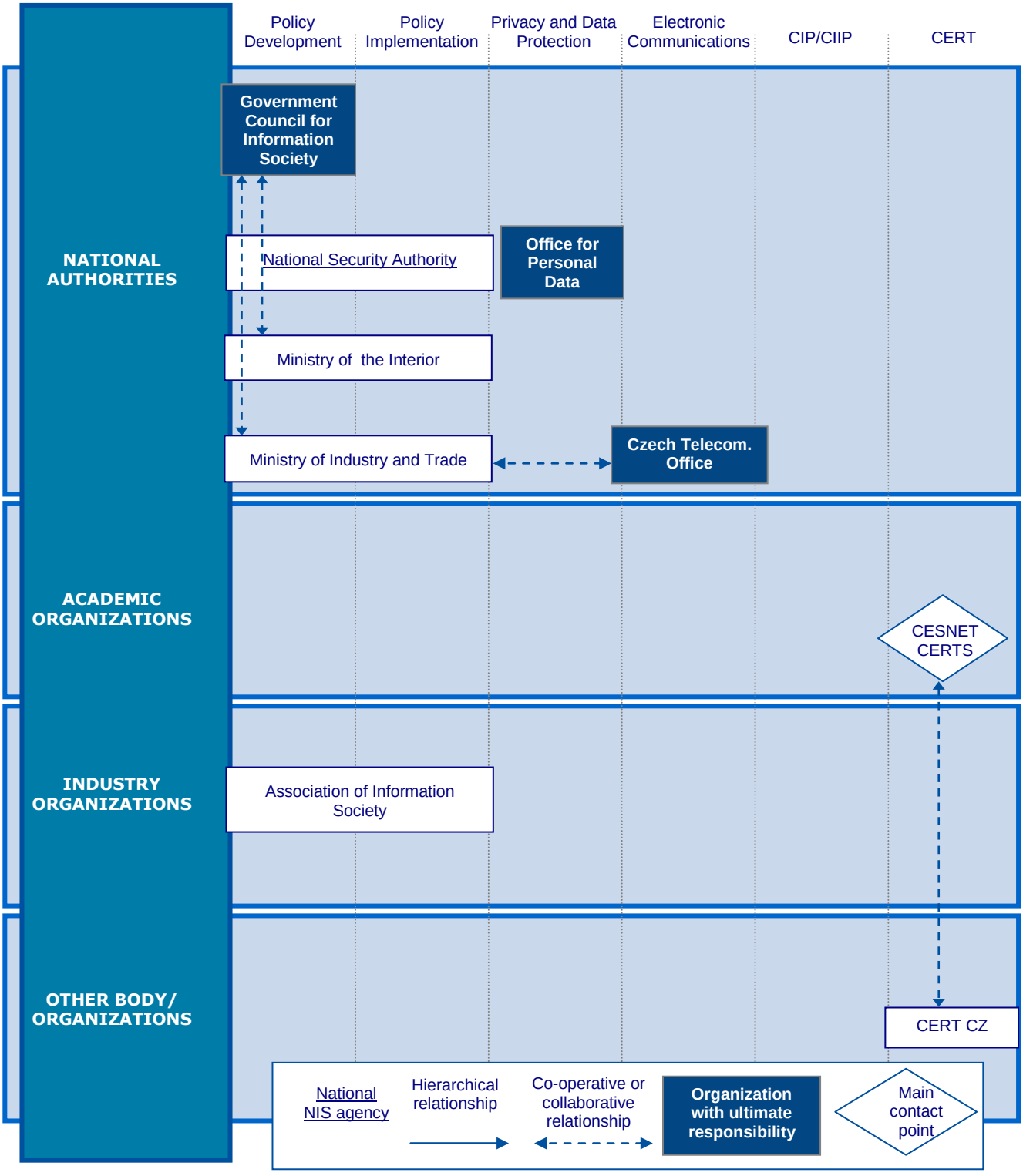
Additionally the Czech Republic has security response teams in place to handle security breaches and other incidents. CSIRT.CZ (Computer Security Incident Response Team) is the model security team, which coordinates security incident solving in the computer networks of the Czech Republic. The CSIRT.CZ team was founded in September 2007. Currently it consists of the CESNET-CERTS Computer Security Incident Response Team members. In addition to solving computer security incidents, they will educate and train new CSIRT.CZ members who will eventually take over.

There are a number of projects currently underway in the country, many of which are e-government projects, which are tied to the security of public information and especially to. filling of approved National Strategy for Information Security of the Czech Republic which creates a platform for building a credible and democratic information society based on a legal foundation and takes care to secure information in all areas of peoples' activities and enables information to be used and shared freely and securely. The priority areas for this strategy are: information security management and risk management, information security knowledge, national and international cooperation in information security, usage of best practices in information security, human rights and freedoms protection and the competitiveness of the Czech economy.

The country hosts a number of conferences on NIS: events are organized by stakeholders in the public sector and industry organizations, as well as the business and academic communities.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Czech Republic. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of the Interior	X		X	X		X	X	X
Government Council for Information Society		X	X	X		X	X	
Ministry of Industry and Trade		X			X		X	X
Office for Personal Data Protection						X		X
Czech Telecommunication Office		X					X	X
National Security Authority (classified information)							X	X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in the Czech Republic:

National Authorities in Network and Information Security	
Ministry of the Interior	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, e-ID, Development and Implementation of Security Technology and Standards Policy	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.mvcr.cz/egovernment.aspx	
Areas of Activity: The Ministry of the Interior is responsible for management and coordination of e-government initiatives; development of government information systems; electronic signature; secure communication infrastructure for public administration; computer crime; emergency management of critical infrastructure.	
Government Council for Information Society	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging Risks / Current Risks, e-ID, Development of Security Technology and Standards Policy	
Relationships: advisory body of the Czech Government	
Weblink: http://www.mvcr.cz/egovernment-rada-vlady-pro-informacni-spolecnost.aspx	
Areas of Activity: The Government Council for Information Society is a public sector advisory body responsible for development and implementation of national information society strategy. The council serves as coordinator in place of the abolished Ministry of Informatics, and ensures the government has an adequate knowledge base to help address concerns and make decisions regarding information society development. The council consists of members from the ministries of the interior, finance, industry and trade, as well as additional experts in from other public administrative bodies. The academic and business communities are also represented on the council.	

National Security Authority	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: independent body which co-operates with all national government bodies	
Weblink: http://www.nbu.cz/	
Areas of Activity: The National Security Authority provides support in domain of information security and information systems certification, crypto – security and crypto - certification, personal security, R&D, and administrative security for the Czech Republic. The office operates the National Center of Communication Security and National Center for Information System Security.	

Ministry of Industry and Trade	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: co-operates with Ministry of the Interior, Czech Telecommunication Office	
Weblink: http://www.mpo.cz/en/e-comm-and-post/default.html	
Areas of Activity: The Ministry of Industry and Trade oversees telecommunication and postal markets and digitalization. Agencies under the ministry's control include CzechInvest, the business and investment development concern, and the Technological Testing Institute for Telecommunications and Postal Services.	

Czech Telecommunication Office	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: co-operates with Ministry of Industry and Trade and Ministry of the Interior	
Weblink: http://www.ctu.cz/	

Areas of Activity: The Czech Telecommunication Office exercises state administration in the area of electronic communications and postal services, including market regulation and the determination of business conditions to substitute for the missing effects of economic competition. The office is also charged with creating and ensuring an open, competitive market and that market players are fully protected until a properly functioning competitive market is developed. The office provides protective services to the audio and television broadcasting areas, and parts of the information society.

Office for Personal Data Protection	
Type of Organisation: Independent body	Ownership: Public
ENISA Focus Points: None	
Relationships: independent body which co-operates with all national government bodies and citizens	
Weblink: http://www.uoou.cz	
Areas of Activity: The Office for Personal Data Protection supervises the observance of legally mandated responsibilities in the processing of personal data, maintains a register of instances of permitted personal data processing, deals with notifications and grievances from citizens concerning infringements of the law, provides consultations in the area of personal data protection. The Office acts on Act No. 101 of April 4, 2000 on the Protection of Personal Data and on Amendments to Some Related Acts. The purpose of this act is to protect citizens' right to privacy, which while guaranteed by the Charter of Fundamental Rights and Freedoms, is coming increasingly under threat in contemporary society due to advancements in information technologies.	

Industry Organisations Active in Network and Information Security

Association of Information Society (SPIS)	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Emerging Risks	
Relationships: co-operates with the National Authorities	
Weblink: http://www.spis.cz	

Areas of Activity: The Association for Information Society (SPIS) is a professional organization of enterprises operating in the (ICT) sector. Its chief objective is to create an information society based on knowledge and innovation. The association promotes information technology as vital for creating an efficient public administration system, as a necessary prerequisite for the full integration of the Czech Republic into European structures, and for further development and growth of the Czech Economy.

Czech Association of IT Managers (CACIO)	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.cacio.cz	
Areas of Activity: CACIO is an IT industry association and attempts to unite IT managers throughout the Czech Republic. The association was established in June 1998 and currently has 101 CIOs as members. The association aims to create a professional platform for CIOs so that they are able to contribute to IT management at an organizational level as well as to the overall Czech economy. Goals of the association include: information sharing, presentation of expert opinions, and support/develop professional/expert opinions concerning IT legislation. Members participate at NIS connected conferences, and organize workshops and seminars.	

ISACA Czech Republic Chapter (ISACA CRC)	
Type of Organisation: Chapter of International Association	Ownership: Private
ENISA Focus Points: AR, Emerging risk	
Relationships: IT Governance Institute	
Weblink: http://www.isaca.cz/	
Areas of Activity: ISACA Czech Republic is a chapter of international Association ISACA. The chapter was established in 1997 and currently has about 170 members (IT and Security Professionals) both from public and private sector. Goals of the association include: information governance, control, security and audit professionals , organizing workshops and seminars.	

Association of Mobile Network Operators	
Type of Organisation: Association	Ownership: Private

ENISA Focus Points: AR, Emerging risk, Resilience
Relationships: Association co-operates with Association of Public Telecommunication Networks Operators; Czech Association of Competitive Communications; Czech Association of Telecommunications
Weblink: http://www.apms.cz/
Areas of Activity: The subject of activity of the association includes creation of optimum conditions for development of public mobile telecommunication networks and provision of public mobile telecommunication services in the Czech Republic. The association protects common interest of its members as well as individual interests of its members, unless this is contrary to the common interest. With regard to the fact that the optimum conditions of development of entrepreneurial activities of the association members are based on open competition, the main aim of the Association is to support and protect fair open market of electronic communications in the Czech Republic based on rules that respect protection of economic competition.

Czech Society for Quality	
Type of Organisation: Association	Ownership: Private
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.csq.cz/cs/	
Areas of Activity: The Czech Society for Quality is an unincorporated association joining together the wide spectrum of people and organisations acting in various areas of management systems and at the same time it provides, not only its members, with top education in the area of management systems and quality management tools (information security - ISO/IEC 27001). At the present time its membership consists of more than 1800 individual members and more than 155 collective members.	

Academic Organisations Active in Network and Information Security

CESNET	
Type of Organisation: Other Academic	Ownership: Private
ENISA Focus Points: CERT, AR, Emerging Risks, Implementation of Security Technology and Standards Policy	
Relationships: none	

Weblink: http://www.ces.net/
Areas of Activity: CESNET is an association of legal entities held by all universities of the Czech Republic and the Czech Academy of Sciences. Its main goals are to facilitate operation and development of the Czech NREN (National Research and Education Network), conduct research and development of advanced network technologies and applications, and to broaden public knowledge about advanced networking topics.

Other Bodies and Organisations Active in Network and Information Security

CESNET-CERTS	
Type of Organisation: CERT	Ownership: private
ENISA Focus Points: CERT	
Relationships: part of CESNET	
Weblink: http://www.cesnet.cz/csirt/index_en.html	
Areas of Activity: CESNET-CERTS is the official name of the CESNET Computer Security Incident Response Team since January 2004. The team consists of employees of CESNET Association. One of the main objectives is to provide a single, trusted point of contact for the CESNET2 network, to coordinate the handling of security incidents, which originated in the CESNET2 network, as well as preventing such incidents. The activities include also helping the CESNET2 members and customers to improve their computer and network security.	

CERTCZ	
Type of Organisation: CERT	Ownership: PPP
ENISA Focus Points: CERT	
Relationships: co-operates with other CERTs	
Weblink: http://www.certcz.org/	
Areas of Activity: CERT CZ provides strategic coordination and organization support in case of security incidents. CERT CZ is focused on educating the public about information security, coordinating responses to and solving incidents as they arise, and maintaining a high level of quality and efficiency when reacting to said incidents.	

Data Security Management Magazine	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR, Emerging Risks	
Relationships: none	
Weblink: http://www.dsm.tate.cz/	
Areas of Activity: DSM (Data Security Management) magazine was established in the second half of 1997 as a result of the efforts of Tate International, s.r.o. to create a professional-level periodical magazine, which would bring high quality and up-to date information on information security development. DSM addresses the issue of information security in rather a wide context. This is explicitly suggested by the official subtitle of the magazine, where DSM declares it is a "magazine on information systems security, administration and risk management".	

Technologies and Prosperity Magazine	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR, Emerging Risks, Resilience	
Relationships: None	
Weblink: http://www.tapmag.cz/	
Areas of Activity: T&P (Technologies and Prosperity)Magazine on electronic communications, informatics and business, meant for professionals, middle and senior management of corporate users and suppliers and service providers, public and state administration. Particular issues of the T&P is published bilingually, according to their focus and target groups: in Czech and English, in Slovak and English or monolingually: in Czech, in Slovak, in English.	

eTAPMAG Bulletin	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR, Emerging Risks, Resilience	
Relationships: None	
Weblink: http://www.tapmag.cz/	

Areas of Activity: eTAPMAG is an electronic bulletin. It is distributed free of charge based on an electronic application to T&P readers and professional ICT community. This bulletin is in Czech language only.	
Security World Magazine	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR, Emerging Risks, Resilience	
Relationships: None	
Weblink: http://www.securityworld.cz/	
Areas of Activity: Magazine on security issue for IT and Security Professionals	
Computerworld Magazine	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR, Emerging Risks, Resilience	
Relationships: None	
Weblink: http://www.computerworld.cz/	
Areas of Activity: Magazine on security, hardware, software, Internet, communication, information technologies, testing and emergence for IT and Security Professionals	
Business World Magazine	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR, Emerging Risks, Resilience	
Relationships: None	
Weblink: http://www.businessworld.cz/	
Areas of Activity: Magazine on IT strategy for managers	

Activities

Strategic Initiatives

Czech Safer Internet Combined Node (CZESICON)

Type of Activity: Non-governmental Initiative

Responsible Organisation(s): CZI Company. CZI provides e-Business, information system, and application hosting services to medium and large enterprises across numerous sectors to local clients in the Czech Republic, as well as others throughout Europe. The vendor also provides services to government bodies.

ENISA Focus Points: AR

Weblink: http://www.saferinternet.cz

Description:

The project started on January 1, 2007 under the coordination of CZI. CZESICON includes the awareness node/helpline and the internet hotline modules: The Safer internet awareness node/helpline is provides children with first aid in the form of psychological and social assistance helping them to work, learn, chat, browse, and feel comfortable on the Internet. The CZESICON project will share the information and experiences with other national Safer Internet projects throughout Europe by exchanging the best practices, and contributing to European approach. The project adapted as necessary for the Czech national linguistic and cultural preferences and will actively co-operate with INSAFE network at the European level.

Research Programmes

Cyber Threats and Implications for the Czech Republic

Type of Activity: Technical Research Programme

Responsible Organisation(s):

Ministry of the Interior, CESNET, Ness Technologies

ENISA Focus Points: CERT

Weblink: http://www.csirt.cz

Description: The project deals with the issue of cyber threats related to informatics and computer technology. The results of the project will include the development of technological solutions for CSIRT infrastructure in the Czech Republic.

R&D projects in the sector of e-Communications and Postal Services
Type of Activity: Technical Research Programme
Responsible Organisation(s): Ministry of Industry and trade
ENISA Focus Points: None
Weblink: http://www.mpo.cz/zprava37678.html
Description: The goals of these projects are: to ensure the optimal development of network infrastructure and related e— communication services for the total improvement in the area of the information society; to develop the universal and protected communication environment; to support the new technology and their application within the network communication infrastructure, particularly within the access networks etc.

Events

Conference and Workshops	
Internet in Public Administration and Self-government	
Responsible Organisation: TRIADA	Frequency: Annual
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Government Institutions, Educational and Research Organizations, Security Professionals; Minor – SME	
Weblink: http://www.isss.cz/	
Description: the biggest Czech national ICT conference for public administration, of which part is the international LORIS (Local and Regional Information Society) Conference.	
CESNET conference	
Responsible Organisation: CESNET	Frequency: Biennial
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Security Professionals, Educational and Research Organizations; Minor- SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.ces.net/events/2008/conference/	

Description: conference focusing on advances in high-speed communication technologies, Grids, related middleware and their sophisticated applications. Security is one of three major topics.	
Quality & Security	
Responsible Organisation: Technologies and Prosperity	Frequency: Annual
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Government Institutions, Large Enterprises, Security Professionals; Minor- SMEs, Educational and Research Organizations	
Weblink: http://www.itsbratislava.sk/quality/index.php#aktualni	
Description: conference focusing on information security.	
Present and Future of Crisis Management	
Responsible Organisation: T-Soft	Frequency: Annual
ENISA Focus Points: Resilience, Emerging Risks	
Target Groups: Major- Large Enterprises, Educational and Research Organizations, Security Professionals; Minor- SMEs, Government Institutions	
Weblink: http://www.emergency.cz/konference/index.php?q=en/2008/index	
Description: conference on emergency management, mission-critical systems, and security.	
Information Security Summit	
Responsible Organisation: Tate International	Frequency: Annual
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Large Enterprises, Government Institutions; Minor- SMEs	
Weblink: http://www.dsm.tate.cz/	
Description: conference focussed on information security.	
Security and Protection of Information	
Responsible Organisation: University of Defence	Frequency: Biennial
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Large Enterprises, Government Institutions, Educational and Research Organizations, Security Professionals; Minor- SMEs	

Weblink: http://www.unob.cz/spi/	
Description: conference focusing on information security.	
CNZ	
Responsible Organisation: CNZ	Frequency: Annual
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Government Institutions; Minor- SMEs, Large Enterprises, Educational and Research Organizations, Security Professionals	
Weblink: http://www.cnz.cz	
Description: conference on e-archiving with a focus on information security aspects.	
TELEINFORMATIKA	
Responsible Organisation: Technologies and Prosperity Magazine	Frequency: Annual
ENISA Focus Points: Resilience, Emerging Risks	
Target Groups: Major - state and public administration, service providers, technology suppliers, Security Professionals, Minor – Educational Organizations	
Weblink: http://www.teleinformatika.cz/	
Description: information society, security, corporate informatics and communications, mobile communications and navigation, trends in fixed network, digitalization and media, e-Health, ICT and Property, innovation and high-tech, law, regulation in communication.	
eConference - international conference on Internet, Competitiveness and Organisational Security	
Responsible Organisation: University of Tomas Bata in Zlin	Frequency: Annual
ENISA Focus Points: Resilience, Emerging Risks	
Target Groups: Major- Government Institutions, Educational and Research Organizations, Security Professionals; Minor – SME	
Weblink: http://e-konference.utb.cz	
Description: security of information systems, crisis management, competitive intelligence, organisational security, cyber terrorism, cyber criminality, strategic decision-making, municipal security.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the last 12 months 3 security breaches were reported in the Czech Republic:

1) In October 2007, Panasonic reported an employee of the company got access to a database housing all Panasonic employee social security numbers, addresses and salary information and subsequently sent the data to a third party.

   http://www.denik.cz/ekonomika/panasonic-unik-dat-20071030.html

2) In December 2007, CSOB reported a loss of limited clients' data during one day in November 2007. The reported incident did not include information about cash-flow data, and passwords, nor codes were compromised. Total IT systems were not hacked, and banking card security and electronic banking operations were not threatened.

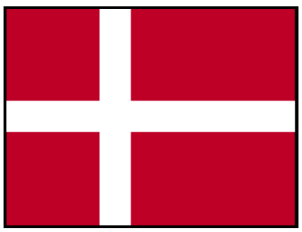
   http://ekonomika.ihned.cz/c1-22587250-csob-zjistila-unik-dat-banka-podala-trestni-oznameni; http://www.bankovnipoplatky.com/o-bankach/unik-dat-v-csob-3206/

2. In May 2008, Česká Spořitelna reported that data for approximately 300 bank clients from the year 2004 were found on Internet (bank account numbers, mailing addresses, account balances).

   http://www.novinky.cz/clanek/139585-banky-chystaji-trestni-oznameni-kvuli-uniku-osobnich-dat-klientu.html

Country Report – Denmark

Country General Information



Source: European Commission

Political system:	Constitutional monarchy
Capital city:	Copenhagen
Total area:	43 094 sq.km
Population:	5.4 million
Official language:	Danish
Time zone:	CET (GMT+1)
Currency:	Danish krone (DKK)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Denmark, we present a set of three indicators in the Country Highlights section.

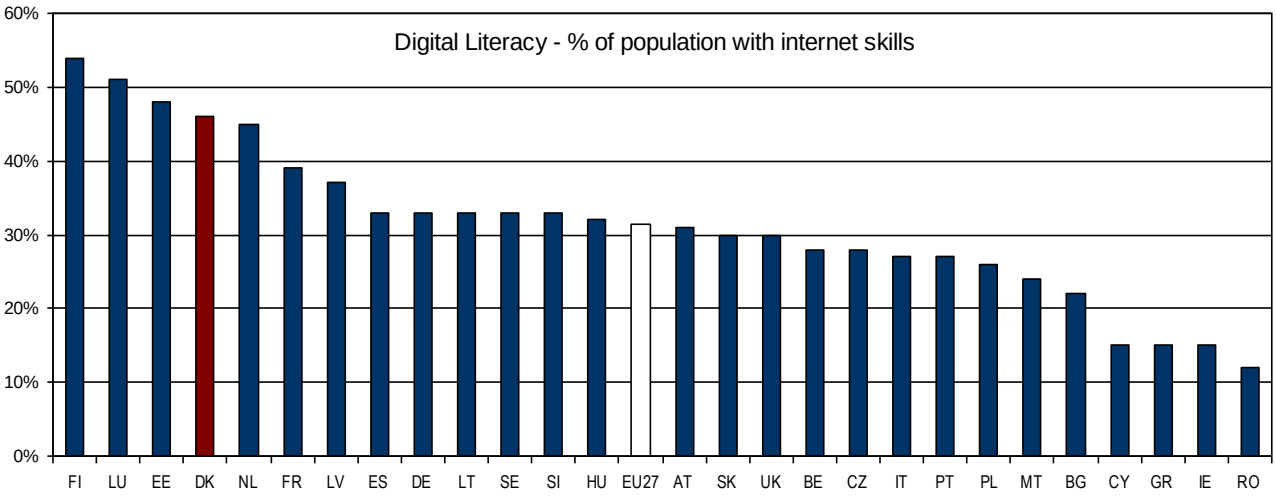
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Denmark is fundamental to this NIS study.

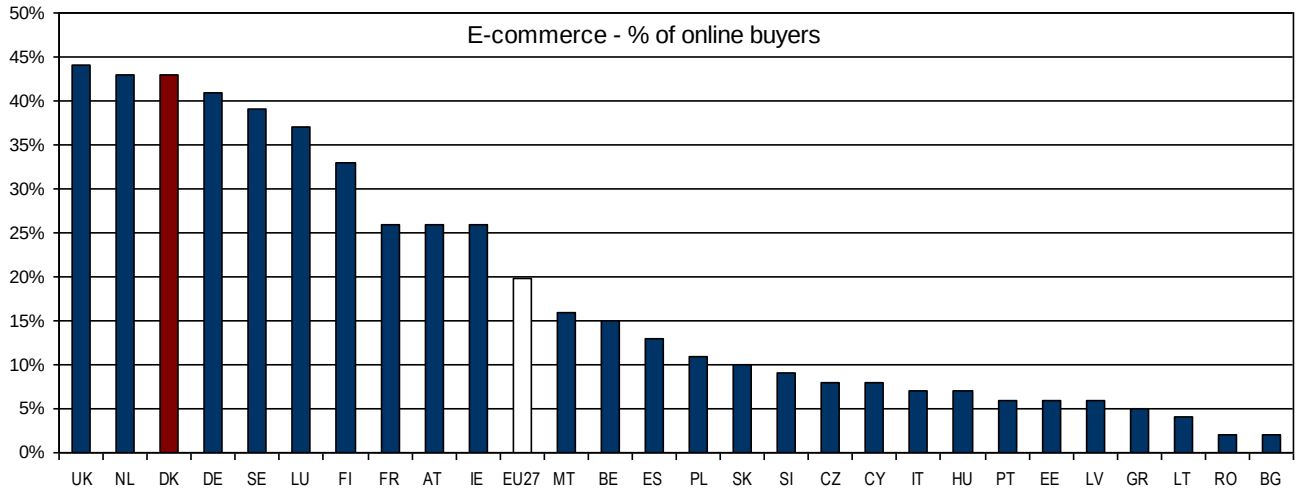
Information society is highly developed in Denmark with strong eSkills among the population, high use of ecommerce, and the highest rate of adoption of broadband access.

The shown indicators – Digital Literacy, E-commerce Buyers, and Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

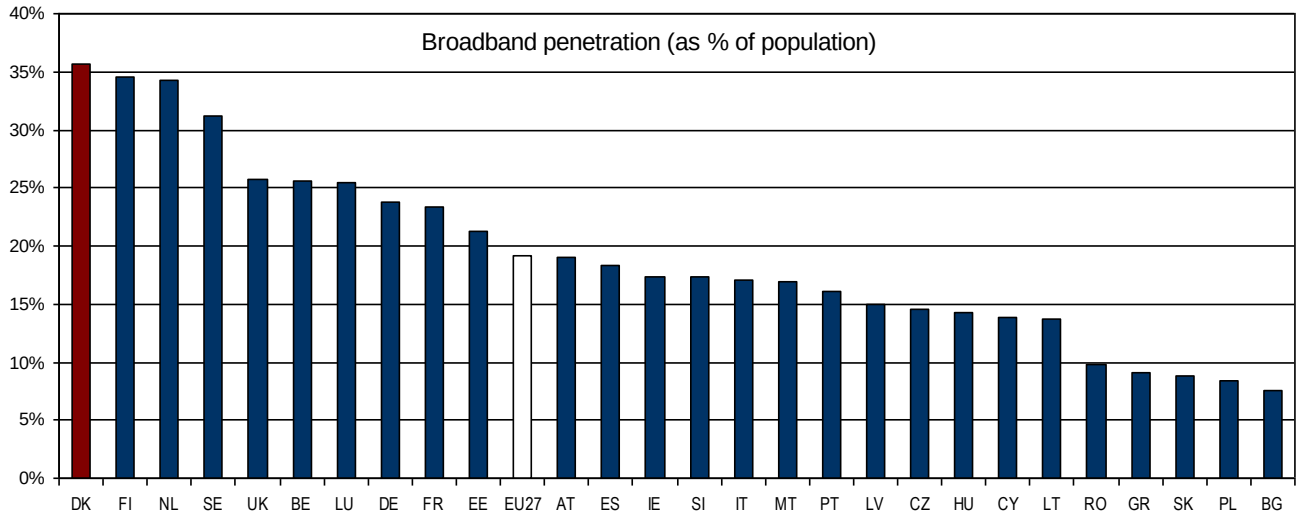
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

In Denmark, the Ministry of Science, Technology and Innovation is appointed by the government as a single organization with a wide range of competencies in all aspects of network and information security at the national level. The ministry is responsible for coordinating the development and implementation of national information security strategy. The National IT and Telecom Agency, which reports to the Ministry, is regarded as the national NIS agency, and is also responsible for ensuring compliance with the Electronic Communications law.

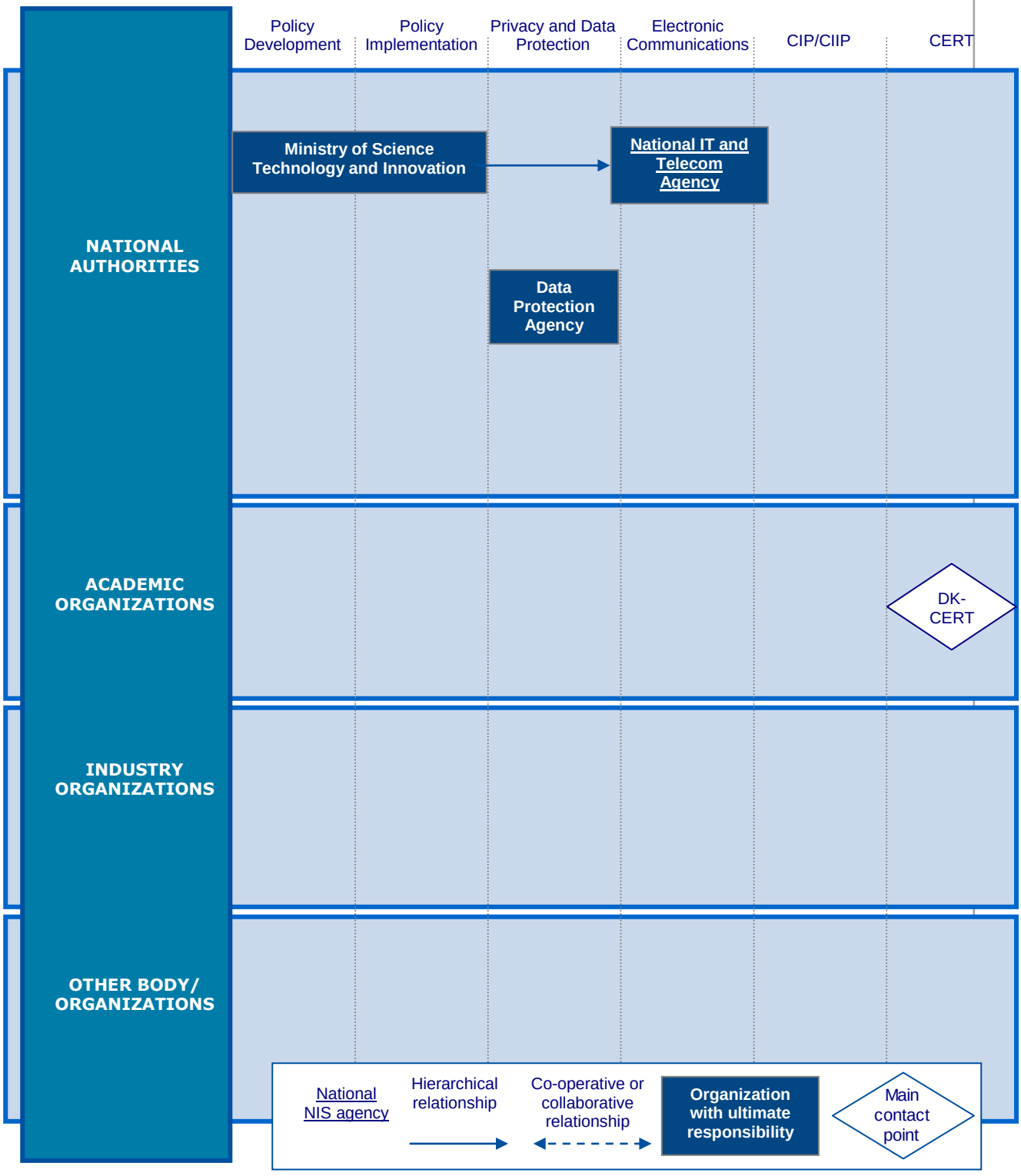
Denmark is committed to data protection and ensuring compliance in this regard. The Data Protection Agency is the state authority, which oversees the personal data laws.

Additionally Denmark has industry security response teams in place to handle security breaches and other incidents. DK-CERT is a sector-CERT for two governmental networks, Forskningsnettet and Sektornettet. On a broader level, DK-CERT's purpose is to prevent, identify and correct security issues related to the Internet in Denmark. It is currently under consideration whether or not to establish a GOV-CERT.

There are a number of projects currently underway in the country, which are tied to the security of public information. The country hosts a number of conferences on NIS. Stakeholders in the public sector, industry organizations, as well as the business and academic, communities organize regularly NIS-related events.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Denmark. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA focus points							
Name of the Key Stakeholder	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Science Technology and Innovation		X	X	X	X		X	X
Danish Data Protection Agency							X	X
National IT and Telecom Agency		X	X	X	X		X	X
Danish Security Intelligence Service		X	X	X				
Council for Greater IT Security			X	X				
Council for IT and Personal Data Security			X	X				
DK-CERT	X							

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Denmark:

National Authorities in Network and Information Security	
Ministry of Science Technology and Innovation	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Awareness Raising, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards, Emerging and Current Risks, Micro-enterprises	
Relationships: None	
Weblink: http://www.vtu.dk	
Areas of Activity: Within the framework of Information and Communication Technology of the Danish society, the Ministry works to secure the following: progressive and sustainable development in society, securing growth and innovation in business life, implementing service improvements and secure quality, and finally, to create efficiency benefits within the public service sector using information and communication technology.	
Danish Ministry of Justice	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: cooperates with other ministries	
Weblink: http://www.justitsministeriet.dk/	
Areas of Activity: The Ministry of Justice is responsible for the overall justice system, including the police, the prosecution, the courts of law, and the prisons and probation service. In addition, the Ministry is responsible for underlying agencies in the fields of family affairs, civil affairs and data protection.	
Danish Data Protection Agency	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: None	

Weblink: http://www.datatilsynet.dk/
Areas of Activity: The Danish Data Protection Agency is the state authority which oversees the personal data laws.

National IT and Telecom Agency	
Type of Organisation: Public Network and Information Security Bodies	Ownership: Public
ENISA Focus Points: Awareness Raising, Development and Implementation of Security Technology and Standards Policy, Emerging and Current Risks, Micro-enterprises	
Relationships: Reporting to the Ministry of Science, Technology and Innovation. Subordinate to the IT Security Panel, an 18-member body chaired by the Minister for Science, Technology and Innovation.	
Weblink: http://www.itst.dk	
Areas of Activity: The National IT and Telecom Agency handles tasks within the area of information and communication technology (ICT) in relation to citizens and businesses and the public sector. The Agency is in charge of developing tools, templates, seminars and workshops to support implementation and maintenance of the Danish IT security standard DS 484. The Agency also acts as a secretariat to the Government IT Security Forum (SISF), appointed for the purpose of promoting knowledge sharing and exchange of experience among IT security managers in the government sector. Within the agency, the IT Security Division's task is to enhance confidence as much as possible by defining standards for IT security, disseminating information about IT security issues, providing guidance on secure solutions, and contributing to the protection of telecommunications.	

Danish Board of Technology	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: Founded and controlled by the Danish Ministry of Science, Technology and Innovation	
Weblink: http://www.tekno.dk/	
Areas of Activity: The Danish Board of Technology is established to spread out the knowledge of technology, and the related opportunities and consequences for people, society and environment. The Danish Board of Technology should promote the public debate about technology, assess the technology and advise the Parliament and the government in technological questions.	

Danish Security and Intelligence Service (PET)	
Type of Organisation: National Security Actor	Ownership: Public
ENISA Focus Points: Awareness Raising, Resilience, Emerging and Current Risks,	
Relationships: PET reports to the Ministry of Justice, co-operates with various other ministries and national authorities including the Danish Defence Intelligence Service and the Danish Emergency Management Agency	
Weblink: http://www.pet.dk	
Areas of Activity: PET is the national security and intelligence service of Denmark. In the area of IT security, PET approves the civil authorities' electronic information systems and networks, which provide, process, communicate, and store classified information. With the increase in information stored and communicated electronically, PET has established a specialised IT security section handling these issues. In this connection, PET co-operates closely with national as well as international authorities, including foreign intelligence services. The Service also participates in national and international forums on IT security.	

Media Council for Children and Young People	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: Founded by the Danish Ministry of Culture	
Weblink: http://andk.medieraadet.dk/	
Areas of Activity: The purpose of the organisation is to create awareness and inform about secure usage of the internet and other new technologies for children, parents and teachers.	

Danish Emergency Management Agency (DEMA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging and Current Risks	
Relationships: DEMA reports directly to the Ministry of Defence	
Weblink: http://www.brs.dk/uk/	

Areas of Activity:
DEMA is responsible for relief work as to secure the resilience of the Danish society against the consequences of catastrophes and accidents.

Industry Organisations Active in Network and Information Security

ITEk	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: Awareness Raising, Implementation of Security Technology and Standards	
Relationships: Part of the Danish Industry Association (DI)	
Weblink: http://itek.di.dk/	
Areas of Activity: DI ITEK is the Danish ICT and electronics federation for IT, telecommunications, electronics and communication enterprises.	

Academic Organisations Active in Network and Information Security

IT University	
Type of Organisation: Academic Organization	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www1.itu.dk/sw5211.asp	
Areas of Activity: The IT University of Copenhagen (ITU) is a teaching and research-based tertiary institution concerned with information technology (IT) and the opportunities it offers. The University was established in 1999. It is funded to undertake both theoretical research and applied research into the interaction and growing importance of information technology to society.	

Other Bodies and Organisations Active in Network and Information Security	
DK-CERT	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT	
Relationships: DK-CERT is part of Uni-C (Danish IT Centre for Education and Research)	
Weblink: http://www.cert.dk	
Areas of Activity: DK-CERT's supervises the IT-security in Denmark. On a broader level, DK-CERT's purpose is to prevent, identify and correct security issues related to the internet in Denmark	
Council for Greater IT Security	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: none	
Weblink: http://www.rfsits.dk/	
Areas of Activity: More than 20 organisations and IT security experts established the Council in 2008. The purpose of the Council is to discuss and raise awareness about holistic IT security and privacy challenges that affect the world of today and the world of tomorrow. The council hence deals with technological as well as socio-economic challenges posed to the current society in the transition to the next generation of digital service-society.	
Dansk IT	
Type of Organisation: Philanthropic, Educational and Professional Associations	Ownership: Private
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: co-operates with the National Authorities	
Weblink: http://www.dansk-it.dk	

Areas of Activity: DANSK IT is Denmark's largest organisation for IT professionals, which seeks to expand the usage IT for the benefit of society. DANSK IT manages the Council for IT and Personal Data Security.

Danish Consumer Council	
Type of Organisation: Other Organization	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: Partly founded by the government	
Weblink: http://www.fbr.dk	
Areas of Activity: The Danish Consumer Council takes care of the interest of consumers in matters of conflict with the business environment. The Consumer Council is involved in a wide range of consumer issues: food quality, environmental protection, health services, financial and legal services and issues connected with media, telecommunications, universal services, etc.	

Innovationlab	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Private
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: Partly founded by the government	
Weblink: http://www.innovationlab.dk	
Areas of Activity: Innovationlab is an international knowledge centre for new technology.	

Activities

Strategic Initiatives

Free IT security check
Type of Activity: Strategic initiative – government policy
Responsible Organisation(s): Ministry of Science, Technology and Innovation
ENISA Focus Points: Awareness raising, Development of Security Technology and Standards Policy

Weblink: N/A
Description: The Ministry of Science, Technology and Innovation is now offering a free service for all Danish citizens to have a security check of their PCs via the internet.
Joint Nordic Initiative re safe IT for children and teenagers
Type of Activity: Strategic initiative – government policy
Responsible Organisation(s): Ministry of Justice
ENISA Focus Points: Awareness raising, Emerging and Current risks
Weblink: N/A
Description: A joint Nordic initiative to exchange technologies and findings related to improving IT security for children and teenagers.
IT security committee
Type of Activity: Strategic initiative – government policy
Responsible Organisation(s): Ministry of Science, Technology and Innovation
ENISA Focus Points: Awareness raising, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: N/A
Description: The Ministry of Science, Technology and Innovation has established a committee for improving IT security and to manage the interactions with the many different stakeholders in Denmark.
New legislation concerning emergency planning in the IT and telecommunications sector
Type of Activity: Strategic initiative – government policy
Responsible Organisation(s): Ministry of Science, Technology and Innovation
ENISA Focus Points: Resilience, Implementation of Security Technology and Standards
Weblink: http://www.itst.dk/it-sikkerhed/lovstof/lovgivning-om-beredskab/bekendtgorelse-om-teleberedskab/?searchterm=teleberedskab

Description: During crisis, war, disasters or any other extraordinary situations in peacetime, electronic communications must be ensured by a number of initiatives.
Digital signature
Type of Activity: Strategic initiative – government policy
Responsible Organisation(s): Ministry of Science, Technology and Innovation
ENISA Focus Points: e-ID
Weblink: http://www.itst.dk/nyheder/nyhedsarkiv/2008/pressemeddelelse-ny-generation-digital-signatur-2013-mobil-og-brugbar-til-netbankerne/?searchterm=None
Description: A new generation of the Digital Signature, which is safer and more mobile and user-friendly than the previous version.

Events

Conference and Workshops	
Netsafe Now!	
Responsible Organisation: IT-borger	Frequency: annual
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Target Groups: Consumers / Citizens, SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.netsikkernu.dk	
Description: Netsafe Now! (Netsikker Nu!) is an annual campaign that promotes safe internet-surfing. The purpose of the campaign is to broaden the general knowledge of it-security for the citizens.	
Secure Internet Day	
Responsible Organisation: The Media Council for Children and Young People	Frequency: annual
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Target Groups: Consumers / Citizens	

Weblink: N/A

Description:

The secure internet day is a global event to promote secure internet usage.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Denmark.

Country Report – Estonia

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Tallin
Total area:	45 000 sq.km
Population:	1.3 million
Official language:	Estonian
Time zone:	EET (GMT+2)
Currency:	Estonian kroon (EEK)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Estonia, we present a set of three indicators in the Country Highlights section.

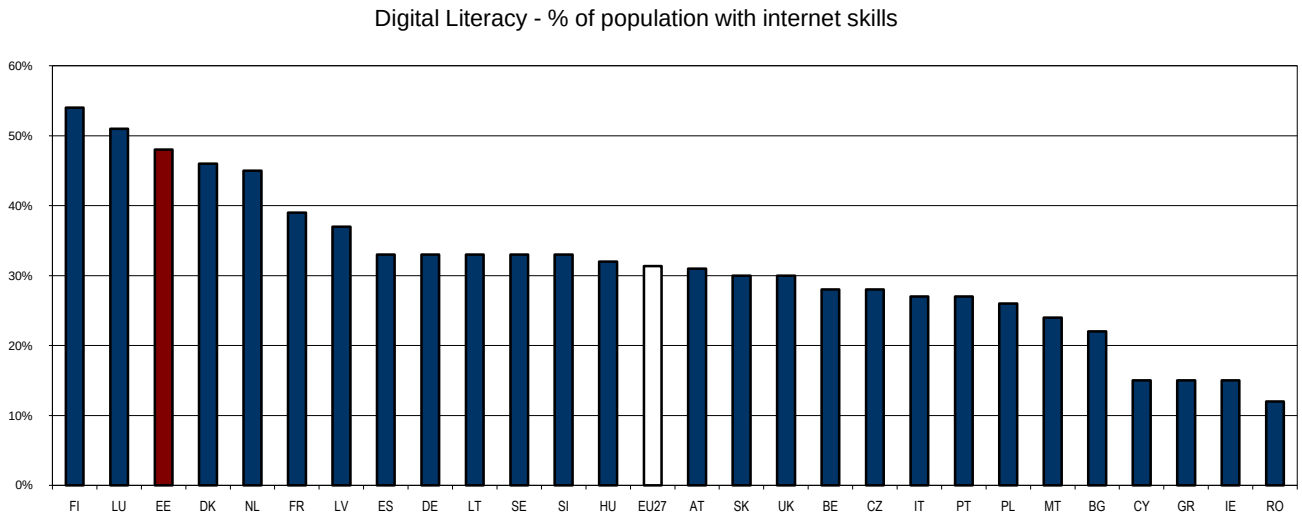
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Estonia is fundamental to this NIS study.

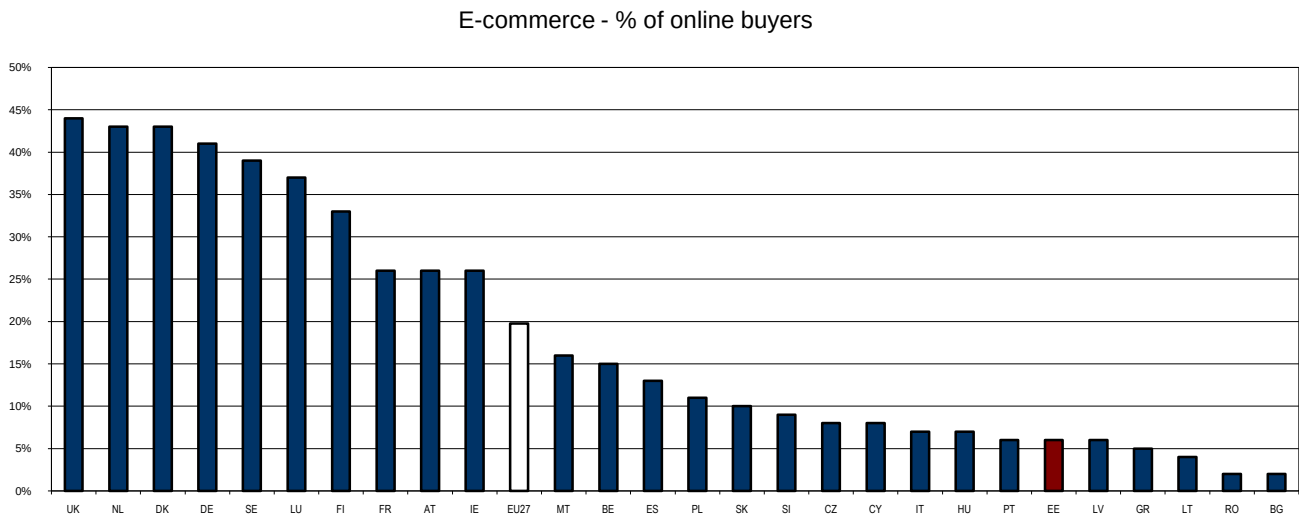
The development of the information society in Estonia is currently doing well, the situation may improve further with particularly strong progress in eGovernment, a rapid adoption of broadband by Internet users, and a business environment relatively favorable to ICT investment, which can rely particularly on a good eSkill base.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

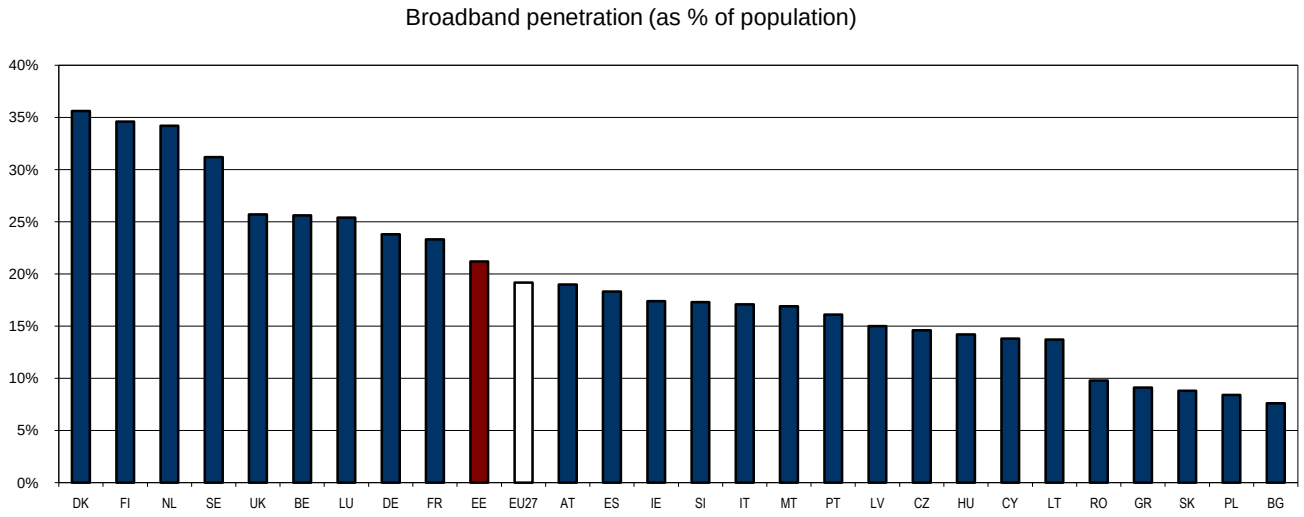
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Estonia does not have a single body that is recognized among NIS stakeholders in Estonia as the national security agency.

The Ministry of Economic Affairs and Communications is responsible for both the development and implementation of national information security policy in Estonia.

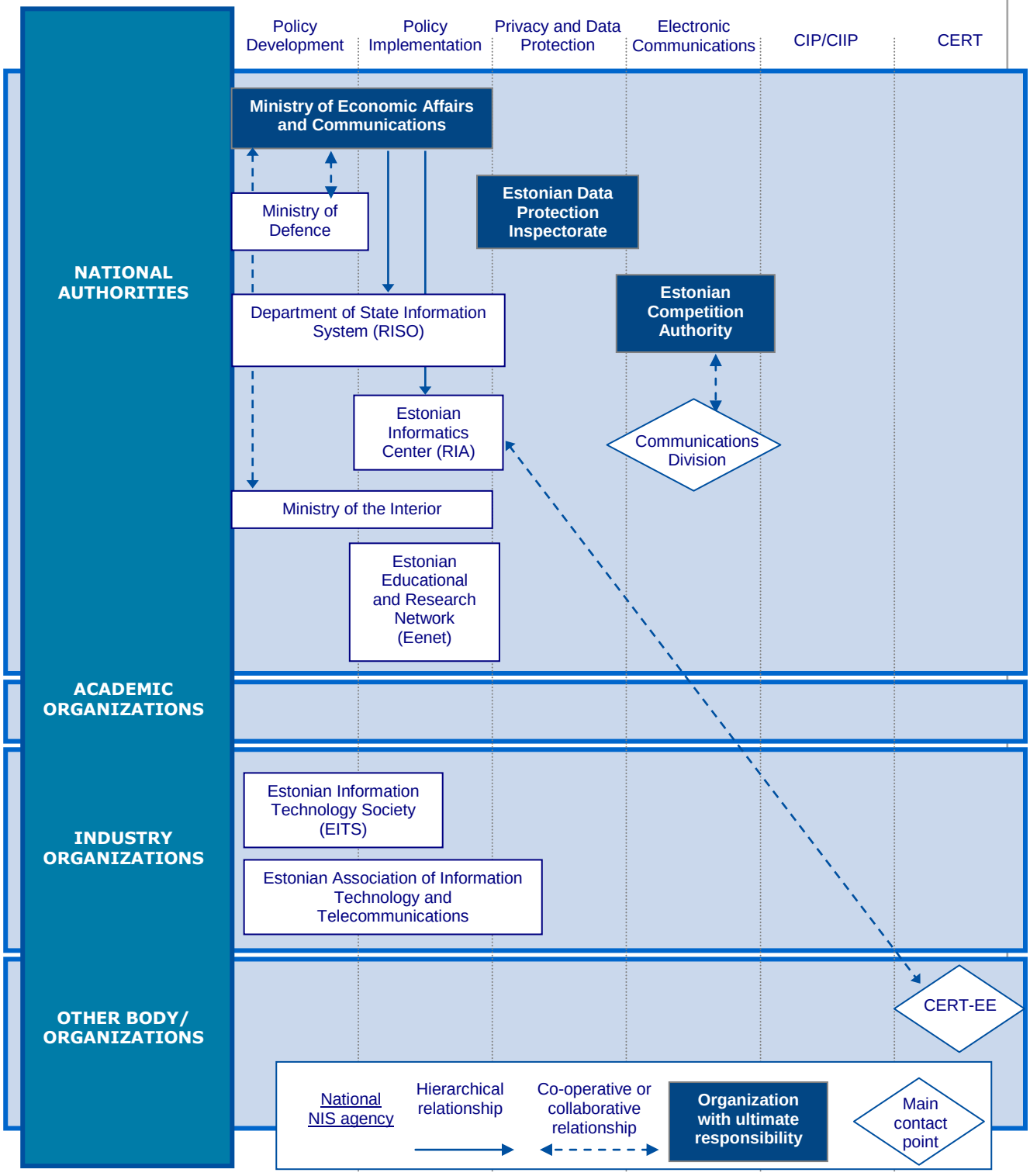
The Estonian Data Protection Inspectorate is charged with data protection in Estonia. The main task of the Data Protection Inspectorate is the implementation of the independent supervision over the legality of processing personal data and keeping databases, as well as organizing data protection activities. The issue of precepts to the chief and authorized personnel dealing with databases, and the administrative penalization for violating the order of keeping and processing of personal data, also falls within the competence of the Data Protection Inspectorate.

Estonia has security response teams in place to handle security breaches and other incidents. CERT-EE is responsible for the management of security incidents in .ee computer networks, and is a national contact point for international cooperation in the field of IT security.

In Estonia, there is no single central authority responsible for CIIP. Several ministries and their respective subunits are directly involved. However, the main tasks of CIIP are assigned to the Ministry of Economic Affairs and Communications, which plays a leading role with regard to information security, since two central agencies for the national IT policy are subordinated to it: The Department of State Information System (RISO), which is the central body for overall ICT coordination; and the Estonian Informatics Centre (RIA), which constitutes the implementing body under the Ministry. Other important public agencies that are dealing with CIIP are located within the Ministry of the Internal Affairs and the Ministry of Defense. These two ministries are responsible for internal security and crisis management.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Estonia. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Name of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Economic Affairs and Communications							X	X
Estonian Data Protection Inspectorate		X		X				X
Estonian Competition Authority		X						
Computer Emergency Response Team of Estonia (CERT-EE)	X							

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Estonia:

National Authorities in Network and Information Security	
Ministry of Economic Affairs and Communications (MEAC)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: The Department of State Information System (RISO) and the Estonian Informatics Centre (RIA) are subordinate to the Ministry of Economic Affairs.	
Weblink: http://www.mkm.ee/	
Areas of Activity: Implementing Estonian Information Policy and Information Society Strategy focusing on elaboration of ID card applications, proceeding also from the list of egovernment services defined in the eEurope+ Action Plan; improving skills and access for disadvantaged social groups to electronically provided services; elaboration and introduction of systems for digital document management and archival processing; etc.	
The Department of State Information System (RISO)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: The Department of State Information System is a subdivision of the Ministry of Economic Affairs and Communications.	
Weblink: http://www.riso.ee/	
Areas of Activity: Coordination of state IT-policy actions and development plans in the field of state administrative information systems, with a key focus on state IT budgets, IT legislation, coordination of IT projects, IT audits, standardisation, IT procurement procedures, and international cooperation in the field of state IS.	
Estonian Informatics Centre (RIA)	
Type of Organization: National Government	Ownership: Public

ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy
Relationships: The Estonian Informatics Centre is a subdivision of the Ministry of Economic affairs and Communications. It is responsible for running CERT-EE.
Weblink: http://www.ria.ee/
Areas of Activity: General coordination of state information policy and public sector IT development, which includes responsibility for the coordination and implementation of the development of state registers, computer networks and data communication, standardization, IT public procurement, monitoring the Estonian IT situation, etc.

Ministry of Defence of the Republic of Estonia	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: Cooperates with MEAC on information security policy in two domains – crisis management and cybercrime and education and training.	
Weblink: http://www.mod.gov.ee/	
Areas of Activity: The Ministry of Defence is a government agency that performs the duties pursuant to laws and follows the guidelines given by the Government of the Republic. The ministry focuses on national defense courses for schools and executives relating to IT security.	

Estonian National Security Authority (NSA)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Part of the Ministry of Defence of the Republic of Estonia (Security Department)	
Weblink: http://www.mod.gov.ee/?op=body&id=522	

Areas of Activity: The receipt and protection of classified information of foreign states in the Republic of Estonia. The institution was established in 1995 in order to assure the protection of classified information of a foreign state made available to Estonia. This function was initially fulfilled by the Coordination Director's Office of the State Chancellery. Regulation no. 231 of the Government of the Republic was adopted in 2001, according to which respective authority was transferred to the Ministry of Defence, having elected the Security Department of the Ministry of Defence to represent the National Security Authority under the Statutes of the Ministry. The Department reports to the Minister of Defence and to the Security Committee of the Government of the Republic.

Ministry of the Interior	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Cooperates with MEAC on information security policy in two domains – crisis management and cyber-crime.	
Weblink: http://www.siseministeerium.ee/?lang=en	
Areas of Activity: The ministry is an agent in the domain of crisis management and cyber-crime in the following areas: preparation of the state crisis management plan; coordination of the work of the state and local crisis committees; and coordination of the international cyber-crime related initiatives.	

Office of the National Security Coordinator – State Chancellery	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.riigikantselei.ee/?id=670	
Areas of Activity: The Office of the National Security Coordinator advises the Prime Minister on issues related to national security and manages the operations of the National Security Committee of the Government of the Republic of Estonia.	

Estonian Data Protection Inspectorate	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Implementation of Security Technology and Standards Policy	

Relationships: None
Weblink: http://www.dp.gov.ee/
Areas of Activity: The main task of the Data Protection Inspectorate is the implementation of the independent supervision over the legality of processing personal data and keeping databases, as well as organizing data protection activities. The issue of precepts to authorized personnel dealing with databases and the administrative penalization for violating the order of keeping and processing personal data also falls within the competence of the inspectorate.

Estonian Competition Authority	
Type of Organization: Other Public Bodies	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.konkurentsiamet.ee/	
Areas of Activity: The Communications Division of the Estonian Competition Authority manages and regulates the market for electronic communications in Estonia. It is responsible for the management of limited communication resources (e.g., radio frequencies) as well as for the regulation of the electronic communications market in Estonia. In this function, the National Communication Board oversees the companies operating in the field of electronic communications and ensures compliance with security requirements.	

Estonian Educational and Research Network (EEnet)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: EENet is a non-profit state agency administered by the Estonian Ministry of Education and Research	
Weblink: http://www.eenet.ee/	

Areas of Activity:

EENet is a governmental non-profit organization that was established in August 1993 by the Ministry of Education with the task of managing, coordinating, and developing the computer network of science, education, and culture. Since 1997, EENet has been operating as a state agency administered by the Estonian Ministry of Education and Research. The mission of EENet is to provide a high-quality national network infrastructure for Estonia's research, educational, and cultural communities. Its services include a permanent Internet connection as well as Web hosting, email, ftp, DNS, and consultations in the event of security problems.

Industry Organizations Active in Network and Information Security

Estonian Information Technology Society (EITS)

Type of Organization: Other Bodies and Organizations	Ownership: Non-profit

ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards

Relationships: Cooperates with the National Authorities

Weblink: http://www.eits.ee/

Areas of Activity:

The objectives of EITS include: the formation of good communications and information exchange practices between IT companies and users; the extensive promotion of the ideas of the information society to the general public; improvement of the qualifications and professional level of IT specialists and organising the vocational certification system in the information technology sector; and representation of society members in domestic and international organizations.

Estonian Association of Information Technology and Telecommunications (ITL)

Type of Organization: Other Bodies and Organizations	Ownership: Non-Profit

ENISA Focus Points: Development of Security Technology and Standards

Relationships: None

Weblink: http://www.itl.ee/

Areas of Activity:

The primary objective of the association is to unite Estonian IT and telecommunications companies, to promote their cooperation in Estonia's development towards the information society, to represent and protect the interests of its member companies, and to express their common positions. Main activities of the association include popularization of information and communication technology (ICT), promotion of vocational education, and amendment of legislation.

Cybernetica AS	
Type of Organization: Other	Ownership: Private
ENISA Focus Points: Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: None	
Weblink: http://www.cyber.ee/	
Areas of Activity: Cybernetica is a private research and development company, original equipment manufacturer and solutions provider in the field of Information and Communication Technologies (ICT). Cybernetica is also involved in component-based development of security-critical distributed systems with complex protocols and infrastructure. Areas of implementation include communications security products and specialized solutions and digital signature technology.	

Academic Organizations Active in Network and Information Security

Faculty of Information Technology – Tallinn University of Technology	
Type of Organization: Academic/University	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.ttu.ee/?id=1865	
Areas of Activity: Information and communications technology programs provide for specialists who develop the resources for the information society in Estonia. Knowledge and skills of those specialists establish a sound foundation to the high-tech and science-based industry. The Faculty trains specialists in the main fields of information and communications technology, including informatics, computer and systems engineering, and electronics and telecommunications. NIS-related courses include Computer Network Attacks and Defence Mechanisms, Network Applications, Computer Networks, and Introduction to Data Security.	

Estonian IT College	
Type of Organization: Other Academic	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.itcollege.ee/?url=overview	

Areas of Activity:

To satisfy the demand for high-level IT professionals, a solution was proposed by the government (represented by the Ministry of Education) that the largest Estonian universities – Tallinn Technical University and Tartu University – and the Estonian ICT industry create an Estonian Information Technology College. The College is a private institution, established and financed by the Estonian Information Technology Foundation (EITF). It works very closely with both universities as well as with IT and telecoms industries. The EITF will have a further role in supporting IT research and development activities of the academic universities and the private sector. NIS-related courses include Network Applications, Network Administration, Software Protection, and Data Security and Cryptology.

Other Bodies and Organizations Active in Network and Information Security

Certification Centre (AS Sertifitseerimiskeskus) (SK)

Type of Organization: Other	Ownership: Private

ENISA Focus Points: e-ID, Implementation of Security Technology and Standards

Relationships: Cooperates with the Citizenship and Migration Board, a government agency within the Ministry of Internal Affairs, in issuing e-ID cards.

Weblink: http://www.sk.ee/

Areas of Activity:

SK was established in 2001 by Hansapank, SEB, Elion, and EMT. The goal of SK is to be the leading provider of certification products and services in Estonia. Its main service is provision of different certificates to individuals and organizations. Currently, the largest project handled by SK involves issuing authentication and digital signature certificates for Estonian ID cards. The core function of SK is to ensure the reliability and integrity of the electronic infrastructure behind the Estonian ID Card project. SK provides certificates for the card and also the services necessary for utilizing the certificates and giving legally binding digital signatures. SK also functions as a competence center for the ID card and assists with the creation of electronic applications for the card.

Look@World Foundation

Type of Organization: Other	Ownership: Private

ENISA Focus Points: AR

Relationships: Cooperates with the Ministry of Economic Affairs and Communications on Infosecurity 2009.

Weblink: http://www.vaatamaailma.ee/

Areas of Activity: The Look@World Foundation was created in 2001 by ten major Estonian companies. The foundation maintains the Internet sources www.arvutikaitse.ee and www.infosecurity.ee.	
Computer Emergency Response Team of Estonia (CERT-EE)	
Type of Organization: CERT	Ownership: Public
ENISA Focus Points: CERT, AR	
Relationships: CERT-EE is a department within the Estonian Informatics Centre	
Weblink: http://www.cert.ee/	
Areas of Activity: CERT-EE is responsible for the management of security incidents in .ee computer networks. Its task is to assist Estonian internet users in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats. CERT-EE deals with security incidents that occur in Estonian networks, whether started there or abroad. CERT-EE is also a national contact point for international cooperation in the field of IT security.	
Estonian IT Foundation	
Type of Organization: Other	Ownership: PPP
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.eitsa.ee/?url=eitf	
Areas of Activity: As a non-profit organization founded by the Estonian Republic, Tartu University, Tallinn Technical University, Eesti Telekom, and the Association of Estonian Information Technology and Telecommunications Companies, the five-member Council of the EITF is made up of the representatives of the aforementioned founders. EITF's aims are to assist in preparation of highly qualified IT specialists and to support information and communication technology-related development in Estonia. For these purposes, the Foundation established and manages the Estonian IT College and administers the National Support Program for ICT in Higher Education "Tiger University".	

Activities

Strategic Initiatives
eGovernment
Type of Activity: Governmental Policies
Responsible Organization(s): Ministry of Economic Affairs and Communications
ENISA Focus Points: AR, e-ID, Implementation of Security Technology and Standards
Weblink: None
Description: eGovernment plays a crucial role in cutting transaction costs for public sector online services in Estonia. eGovernment legislation in Estonia emerged around the same time as in many other Central and Eastern European countries; the general institutional framework was more fundamental in the success of egovernment than were specific initiatives. In addition to online services, some resources are also dedicated to efforts aimed at encouraging edemocracy and eparticipation.
e-Citizen
Type of Activity: Governmental Policies
Responsible Organization(s): Ministry of Economic Affairs and Communications
ENISA Focus Points: AR
Weblink: None
Description: The e-Citizen project is a nation-wide project that focuses on developing cooperation between Estonian citizens and the public sector via the Internet. In the course of the project, the e-Citizen environment is created, which enables the citizen to conveniently obtain information about state services and citizens' rights and obligations. It enables people to participate more actively in public life at the national, regional, and local levels and to communicate with all national information systems.
Infosecurity 2009 (Arvutikaitse 2009)
Type of Activity: Non-governmental Initiative
Responsible Organization(s): Look@World Foundation, Ministry of Economic Affairs and Communications
ENISA Focus Points: AR, e-ID

Weblink: None

Description:

In May 2006, the major partners of the Look@World consortium signed a cooperation agreement with the Estonian Ministry of Economic Affairs and Communications to launch this nationwide initiative. The signatories pledged investments of up to EEK 60 million for 2006–2008. The initiative aims to ensure that Estonia will have the world's most secure information society by 2009. Activities foreseen by the agreement include: development of the electronic use of the ID card; integration of e-ID and PKI in service provision; investment in AS Sertifitseerimiskeskus (certification center); development and launch of new e-ID card-based services; and launch and develop the Internet portal Arvutikaitse.ee.

National information Security Policy

Type of Activity: Governmental Policies

Responsible Organization(s): Estonian Ministry of Economic Affairs and Communications

ENISA Focus Points: Development of Information Security Technology and Standards, Implementation of Information Security Technology and Standards

Weblink: None

Description:

The Estonian Ministry of Economic Affairs and Communications (MEAC) has prepared a nation-wide information security policy that specifies and coordinates the security-related initiatives. The main goal of the Estonian information security policy is a secure, security-aware, internationally cooperating Estonian information society. Specific goals include elimination of non-acceptable risks, defense of basic human rights, information security awareness and training, participation in international esecurity initiatives, as well as competitiveness of the economy. The policy comprises five domains: 1) MEAC is coordinating the domain of esecurity cooperation. The domain covers initiatives such as coordination of the Estonian ICT environment risk analysis, establishment and operation of the Estonian CERT, participation in the activities of the European Network and Information Security Agency, and coordination of the cross-border initiatives. 2) The Ministry of Internal Affairs together with the Ministry of Defence serves the domain of crisis management and cyber-crime. It includes preparation of the state crisis management plan, coordination of work by state and local crisis committees, and coordination of the international cyber-crime initiatives. 3) The Ministry of Education and Research, the Ministry of Defence, the MEAC, and the State Chancellery are responsible for the domain of education and training. The initiatives include public relations activities, training, awareness Web sites, cooperation with schools, and satisfaction research. 4) Secure egovernment based on appropriate legislation, standards, and procedures, such as security requirements for databases, services, and state procurement. The domain of regulations is coordinated by the MEAC together with the Ministry of Internal Affairs. 5) Coordination of security-related tasks within applications, such as distributing the ID card solutions and using the Trans European Services for Telematics between Administrations network, is performed in the application domain. The domain is assigned to the Ministry of Internal Affairs and the Ministry of Defense.

Estonia's Cyber Security Strategy for 2008–2013
Type of Activity: Governmental Policies
Responsible Organization(s): Cyber Security Strategy Committee, Ministry of Defense
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Information Security Technology and Standards, Implementation of Information Security Technology and Standards
Weblink: None
Description: The Cyber Security Strategy Committee – led by the Ministry of Defence in cooperation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs, and the Ministry of Foreign Affairs – submitted "Estonia's Cyber Security Strategy for 2008–2013" to the Government of the Republic. This strategy was adopted by the government in May 2008. In order to pursue the strategy, an implementation plan will be developed, which will relate to the specific development plans of the relevant government agencies. The implementation plan includes: * The implementation plan for 2008–2010 will be submitted to the government for approval within three months of the adoption of the strategy. It will be developed on the basis of proposals from different state agencies and work groups, which have been set up for development of the strategy. Attention will be given to the concrete actions and funds needed to achieve the objectives of the strategy in its various fields of competence. Implementation plans will be developed for two periods: 2008–2010 and 2011–2013. * The responsibility for developing the "Implementation Plan for Cyber Security Strategy 2008–2010" lies with the Cyber Security Strategy Committee. * The implementation and overall efficiency of the strategy in meeting its stated objectives will be assessed by the Cyber Security Council of the Security Committee of the Government of the Republic. This effort will bring together representatives and experts from different ministries and other actors involved in bolstering national cyber security. The council will monitor the success of the strategy by submitting annual reports to the government, which will detail the progress of implementation and the realization of the objectives. The implementation plan will also define the membership, meeting procedures, and tasks of the council.
m-Estonia
Type of Activity: Government Policies
Responsible Organization(s): N/A
ENISA Focus Points: Implementation of Information Security Technology and Standards
Weblink: None

Description:

Am SMS-based communication program, the goal of m-Estonia is to establish a direct electronic communication channel between government offices and citizens. The first project involved notifying students about their high school test results. To have their results sent to their mobile phones, students log in to the state portal, activate the corresponding service, and enter a mobile phone number where the result can be sent. Authentication is done via ID card, mobile ID or Internet banking passwords. In 2007 there were 24,586 examinees taking 56,118 exams, of which 15,538 requested the SMS notification service, and a total of 37,910 SMS notifications were completed. SMS notification is provided by the National Examinations and Qualifications Centre in cooperation with EMT and Mobi solutions.

ePassport

Type of Activity: Governmental Policies

Responsible Organization(s): Estonian Citizenship and Migration Board

ENISA Focus Points: Implementation of Information Security Technology and Standards

Weblink: None

Description:

In order to comply with the EU regulation 2252/2004/EC on standards for security features and biometrics in passports and travel documents issued by member states, the systems of the Estonian Citizenship and Migration Board (CMB) have undergone considerable changes that have been implemented step-by-step. The first biometric passports were delivered in May 2008. Initially, only the user's face is inserted electronically in the passport and a fingerprint is added later. Changes in the organization of work and supporting systems of the CMB will occur at both customer service and document issuance levels.

eProcurement (etender portal)

Type of Activity: Governmental Policies

Responsible Organization(s): Public Procurement Office

ENISA Focus Points: Implementation of Information Security Technology and Standards

Weblink: None

Description:

Established in 2001 and maintained by the Public Procurement Office, the Public Procurement State Register is an etenders portal where all public procurement notices are published electronically. The register is using CPV standards in the catalogue, and all the information in the register is publicly accessible over the Internet for free. In 2003, the number of public tenders advertised via the Public Procurement State Register was 4,859, representing a value of EUR 663 Million. Until recently, Estonia has had no eprocurement experience beyond etendering. But the new Public Procurement Act, which came into force in May 2007, includes legal provisions enabling the further development of eprocurement (e-auctions, dynamic purchasing systems, ecatalogues, etc.) to foster opportunities for advancing a fully electronic procurement tendering process. Furthermore, the Estonian government program set 2010 as the date when the submission of tenders should only be made electronically.

Mobile-ID (mobile digital signature)

Type of Activity: Governmental Policies

Responsible Organization(s): EMT

ENISA Focus Points: Implementation of Information Security Technology and Standards

Weblink: None

Description:

The new mobile-ID service (wireless PKI) was launched in May 2007 by mobile operator EMT, in cooperation with several banks and the Certification Authority AS Sertifitseerimiskeskus. This service allows access to Internet banking services without entering ebanking codes. Secure authentication with the mobile-ID will make use of an authentication PIN via the user's mobile phone. The digital signature aspect of the mobile-ID has the same legal value as that of the e-ID card. When using the mobile-ID, no separate e-ID card or card reader is needed, as the phone itself performs both functions. The mobile-ID is designed to be user-friendly and convenient; the computer no longer needs to be equipped with a card reader or have special additional software installed. One of the objectives of the Computer Protection 2009 initiative is to get at least 200,000 users for the mobile-ID authentication and digital signing by 2009.

Document Exchange Centre

Type of Activity: Governmental Policies

Responsible Organization(s): Estonian Informatics Centre and the State Chancellery

ENISA Focus Points: Implementation of Information Security Technology and Standards

Weblink: None

Description: The Document Exchange Centre (DEC) is an information system providing a common central document exchange service for various document managements systems (DMS) as well as other information systems dealing with documents. The objectives of the DEC include: interfacing dispersed information systems through the secure data exchange layer X-Road; short-term preservation of documents; long-term preservation and backup of documents; and, in the future, provision of services that will support the processing of documents.
SMS Texting Scheme (service provided over X-Road)
Type of Activity: Governmental Policies
Responsible Organization(s): Government of Estonia
ENISA Focus Points: AR, Implementation of Information Security Technology and Standards
Weblink: None
Description: The SMS project is the second project aiming to establish a direct electronic communication channel between government offices and citizens. The first project established "an official email forwarding address" for every resident of Estonia. As the next step, people will have an opportunity to choose a preferred medium for communicating with the government. The expectation is that people will want timely information about tax payment deadlines, expiration of passports or driver's licenses, etc. The services will be unified on governmental service bus infrastructure called X-Road, and every office will be able to integrate the SMS interface with existing information systems or to use the online interface of government portal.
e-ID Card
Type of Activity: Governmental Policies
Responsible Organization(s): Ministry of Economic Affairs and Communications
ENISA Focus Points: e-ID, Implementation of Information Security Technology and Standards
Weblink: None
Description: The e-ID card is valid everywhere in Estonia. According to law, no other document can be required for the purposes of personal identification in lieu of this electronic card. The e-ID card can be used for Internet-based services provided by the state as well as several private enterprises. The e-ID card can also be used for issuing digital signatures. The card provides citizens with a personal @eesti.ee email address that constitutes an easy and convenient way for state institutions, companies, and other interested parties to communicate with citizens.
X-Road

Type of Activity: Governmental Policies
Responsible Organization(s): Ministry of Economic Affairs and Communications
ENISA Focus Points: Implementation of Information Security Technology and Standards
Weblink: None
Description: X-Road is the modernization program intended to change national databases into a common public, service-rendering resource, which would enable agencies and individuals to search data from national databases over the Internet, provided they are legally entitled to do so. At the same time, the system will ensure sufficient security for the treatment of inquiries made to databases and responses received. After the successful start-up, the X-Road environment was expanded to send all kinds of XML-format electronic documents securely over the Internet. At the same time, the X-Road began to develop as a "skeleton" for all egovernment services.

Events

Conference and Workshops	
Baltic Dynamics 2008: Innovation-Key From Slowdown to Growth	
Responsible Organization: Tartu Science Park; Tehnopol-Tallinn Technology Park	Frequency: N/A
ENISA Focus Points: Resilience, AR	
Target Groups: Major – Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.spidera.eu/baltic-dynamics-2008-tartuestonia	
Description: Baltic Dynamics is an annual international conference organized in rotation by Estonia, Latvia, and Lithuania, focusing on topics related to innovation and economic competitiveness. Baltic Dynamics 2007 took place in Riga, Latvia, while next year's event will most likely be held in Lithuania.	
eGovernance – New Horizons?	
Responsible Organization: eGovernance Academy	Frequency: N/A
ENISA Focus Points: AR	
Target Groups: Major – Government Institutions, Large Enterprises, Security Professionals; Minor – SMEs, Educational and Research Organizations	

Weblink: http://www.ega.ee/en/node/296

Description: Event in 2007 was titled e-Estonia 2007: Information Society for Everybody.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

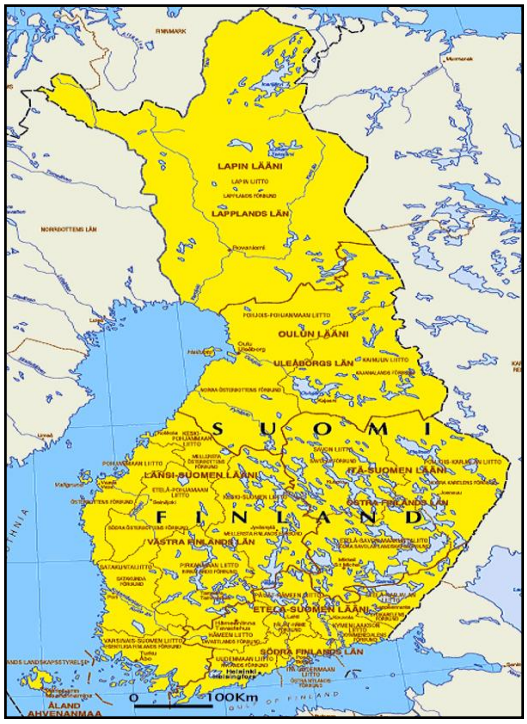
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Estonia.

Country Report – Finland

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Helsinki
Total area:	338 000 sq.km
Population:	5.3 million
Official language:	Finnish, Swedish
Time zone:	EET (GMT+2)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Finland, we present a set of three indicators in the Country Highlights section.

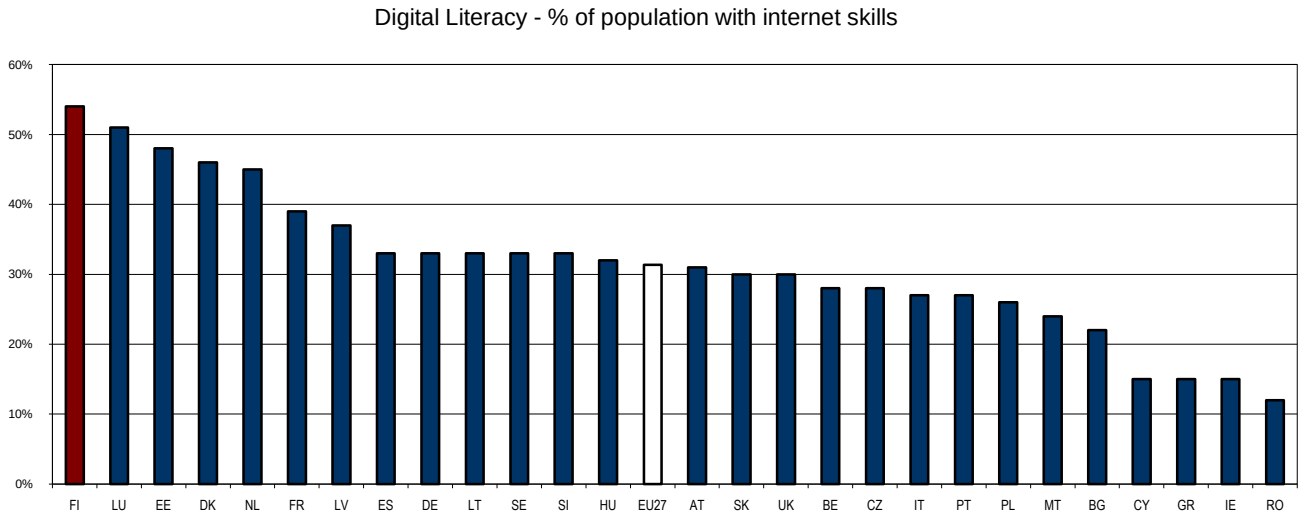
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Finland is fundamental to this NIS study.

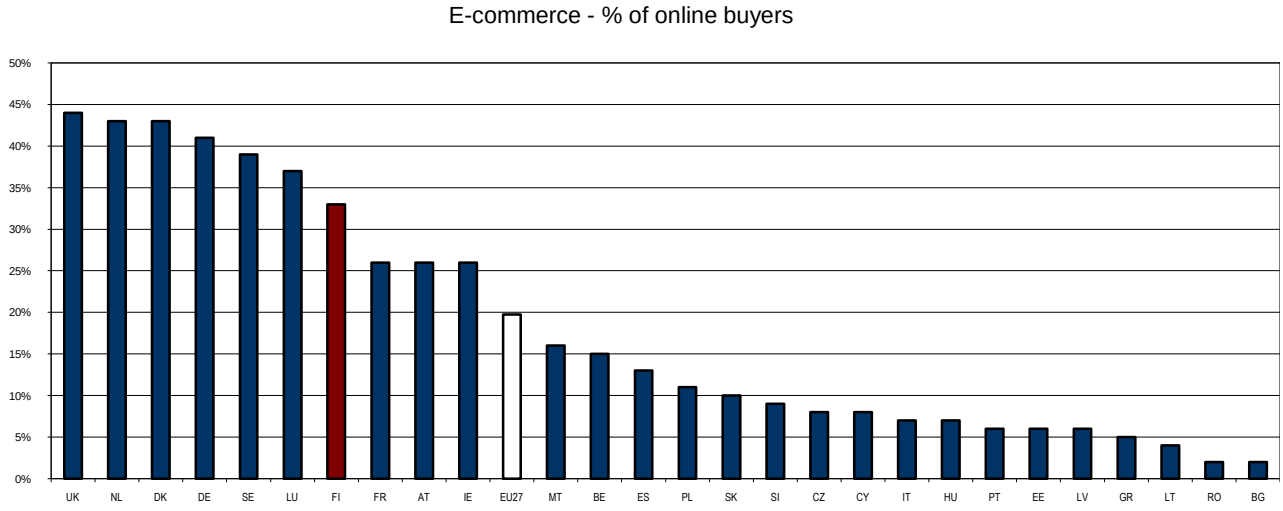
ICT in Finland is performing strongly and the country is a leader in information society developments in all respects. It also has one of the most competitive and dynamic ICT sectors in the EU. However, there are signs that a sizeable group of companies are not using e-Business tools at a level matching the overall development in Finland. Skill levels are high both in the workforce and throughout the population. Finland is very active in fighting against the spread of any kind of malware, and despite the increasing number of broadband customers it managed to reduce considerably the number of such incidents during the last two years.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

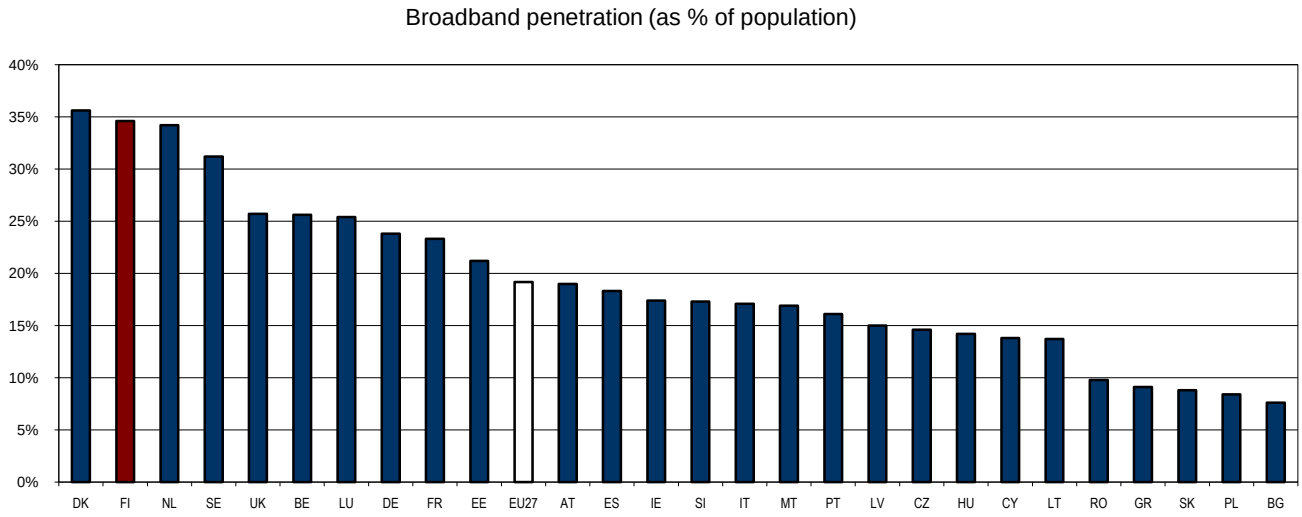
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Ministry of Transport and Communications is responsible for the legislation on communications networks, issues of privacy protection and data security and promoting access to communications services, which give it responsibility for development and implementation of national information security policy at the national level. The Ministry of Transport and Communications is responsible for legislation and strategy development concerning information security in communications services.

Finnish Communications Regulatory Authority (FICORA) is a general administrative authority under the Ministry of Transport and Communications for issues concerning electronic communications and information society services in Finland. FICORA is the national security authority in Finland.

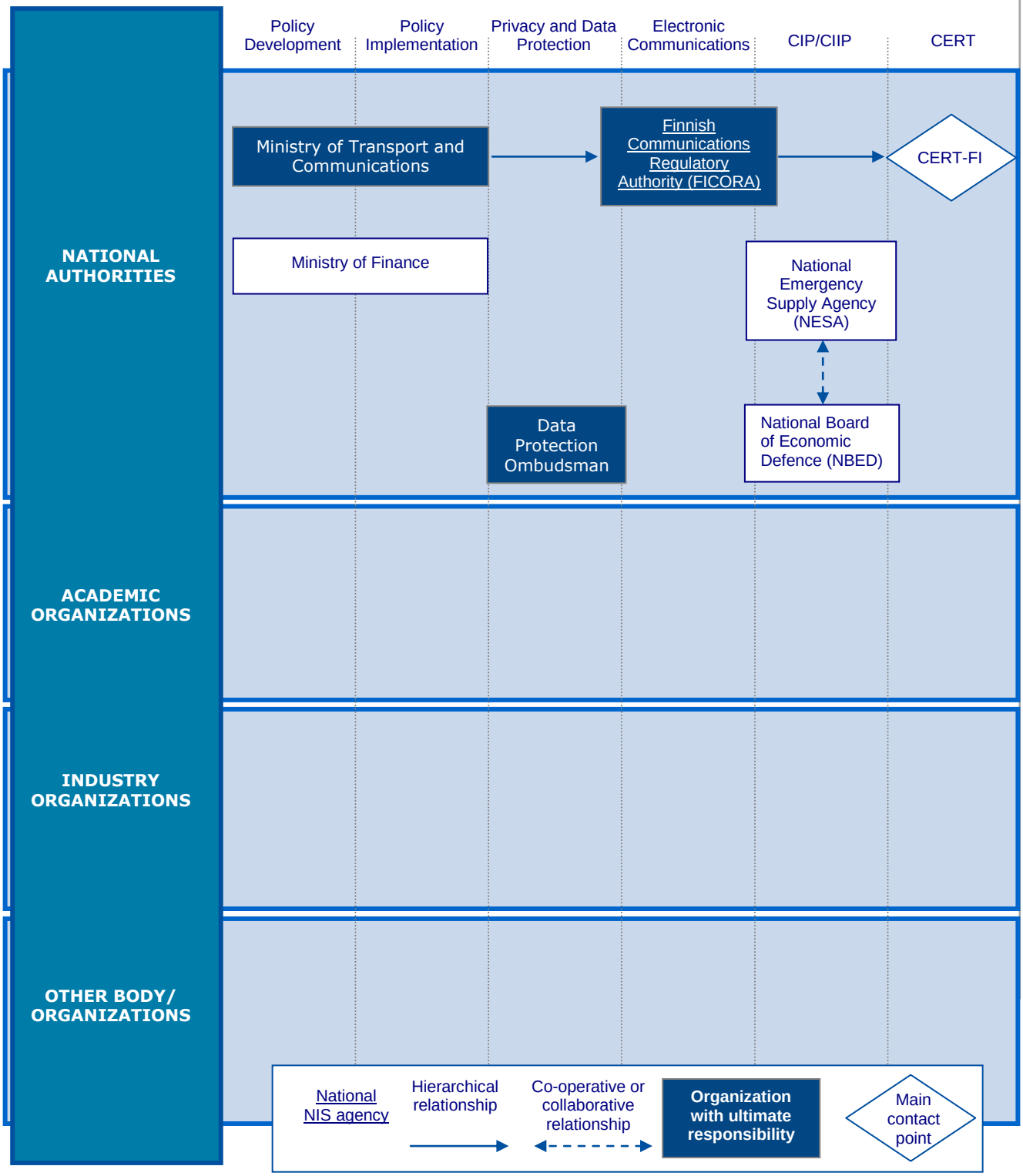
CERT-FI is the Finnish national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. CERT-FI is a part of FICORA.

The Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice. It guides and controls the processing of personal data and provides related consultation.

The Ministry of Finance steers the development of the Government Information Security.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Finland. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Transport and Communications		X	X	X		X	X	X
Ministry of Finance				X			X	
Data Protection Ombudsman			X	X				
Finnish Communications Regulatory Authority (FICORA)		X	X	X		X	X	X
CERT-FI	X	X	X	X				
National Emergency Supply Agency (NESA		X		X				
National Board of Economic Defence (NBED)		X		X				

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Finland:

National Authorities in Network and Information Security	
Ministry of Transport and Communications Finland	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID	
Relationships: None	
Weblink: http://www.lvm.fi/	
Areas of Activity: The Ministry is responsible for legislation and strategy development concerning information security in communications services and the co-ordination of the National Information Security Strategy.	
The Group on Information Security Issues	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID	
Relationships: part of Ministry of Transport and Communications	
Weblink: N/A	
Areas of Activity: The aim of the Group is to promote and follow the development of information security and to take initiatives to improve information security.	
Finnish Communications Regulatory Authority (FICORA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy	
Relationships: under the Ministry of Transport and Communications, co-operates with other national authorities on an ad-hoc basis	
Weblink: http://www.ficora.fi	

Areas of Activity: FICORA is the national security agency/authority in Finland. FICORA is a governmental agency under the Ministry of Transport and Communications. FICORA maintains an overview of the functionality of electronic communications networks and information security and reports of eventual information security threats. FICORA also aims to increase the awareness of information security in homes and companies, and arranges the Information Security Day. FICORA is the national information security authority.

CERT-FI	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks	
Relationships: A special unit at FICORA	
Weblink: http://www.cert.fi	
Areas of Activity: CERT-FI is the Finnish national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security.	

Ministry of Finance	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.ministryoffinance.fi	
Areas of Activity: The Ministry of Finance has the overall responsibility for The Finnish Government Information Security Development Program.	

The Security and Defence Committee	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Development Security Technology and Standards Policy	
Relationships: co-operates with numerous ministries	

Weblink: http://www.defmin.fi	
Areas of Activity: A co-operation body between the various ministries concerning the issue of total defence concept and actions to secure vital functions of society, including anti-cyber war issues.	
Finnish Defence Forces (FDF)	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks	
Relationships: co-operates with various other authorities	
Weblink: http://www.mil.fi/english/	
Areas of Activity: The FDF implements all the information security actions within its own structure in accordance with the MoD's guidance. It participates in cross-sectoral work with other security-related authorities.	
Data Protection Ombudsman	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: Ministry of Justice	
Weblink: http://www.tietosuoja.fi/	
Areas of Activity: The ombudsman is an independent authority operating in connection with the Ministry of Justice. The Data Protection Ombudsman guides and controls the processing of personal data and provides related consultation.	
National Emergency Supply Agency, NESA	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks	
Relationships: NESA is a body working under the auspices of the Ministry of Trade and Industry	
Weblink: http://www.nesa.fi	

Areas of Activity: The Agency plans with actors in the ICT industry to reduce vulnerabilities and create preparedness for exceptional circumstances. The Agency finances ICT backup systems of national importance.

National Board of Economic Defence, NBED	
Type of Organisation: National Security Actors	Ownership: PPP
ENISA Focus Points: Resilience, Emerging/Current Risks	
Relationships: NESA provides the Secretariate for the NBED	
Weblink: http://www.nesa.fi/organisation/national-board-of-economic-defence	
Areas of Activity: The National Board of Economic Defence (NBED) is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyse threats against the country's security of supply and to plan measures to control these threats. NBED makes plans and formulates guidelines, which public authorities implement when disturbances occur. NBED also promotes companies' contingency planning. NBED does not have the power of public authorities, but its assembled expertise constitutes an important resource of national security.	

Industry Organisations Active in Network and Information Security

Finnish Federation for Communications and Teleinformatics, FiCom	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.ficom.fi	
Areas of Activity: Finnish Federation for Communications and Teleinformatics, FiCom is a co-operation organisation for the ICT (information and communications technology) industry in Finland and looks after its interests. FiCom's members are companies and other entities that operate in the communications and teleinformatics sector in Finland. FiCom's task is to promote business opportunities for its members and to enhance their competitiveness.	

Confederation of Finnish Industries, EK	
Type of Organisation: Other	Ownership: Non-profit

ENISA Focus Points: AR
Relationships: None
Weblink: http://www.ek.fi
Areas of Activity: EK promotes the interests of its member companies in Finland, the European Union and internationally. EK's mission is to improve the competitiveness of the companies in Finland.

Academic Organisations Active in Network and Information Security

VTT Technical Research Centre of Finland	
Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: co-operates with numerous ministries	
Weblink: http://www.vtt.fi/	
Areas of Activity: VTT Technical Research Centre of Finland is an impartial expert organisation. With its know-how VTT produces research, development, testing and information services to public sector and companies as well as international organisations.	

Helsinki University of Technology	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.tkk.fi	
Areas of Activity: The Department of Communications and Networking at HUT is by far the largest unit of research and higher education in communications and networking in Finland (and probably around Europe).	

Helsinki Institute for Information Technology	
Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.hiit.fi/	
Areas of Activity: HIIT is a joint research institution of Helsinki University of Technology TKK and the University of Helsinki (UH). Key competences: Internet architecture and technologies, mobile and human-centric computing, user-created media, analysis of large sets of data, and probabilistic modelling of complex phenomena.	

University of Helsinki / Department of Computer Science	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.cs.helsinki.fi/index.en.html	
Areas of Activity: The Department of Computer Science at the University of Helsinki is known for its quality research and teaching among other in the Information Security area.	

University of Jyväskylä	
Type of Organisation: Universities	Ownership: Private
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.jyu.fi/it/en	
Areas of Activity: The Faculty of Information Technology is the largest and oldest in Finland in its branch. The major subjects of the Faculty are Information Systems Science and Computer Science, which actively conduct research in the area of Information security.	

Lappeenranta University of Technology	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.lut.fi/en/technologymanagement/it/research/comlab/pages/default.aspx	
Areas of Activity: The LUT Communications Software Laboratory's goal is to perform high quality research in its focus areas and to educate future experts for the industry and academia.	

Oulu University Secure Programming Group	
Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.ee.oulu.fi/research/ouspg	
Areas of Activity: The purpose of the OUSPG is to study, evaluate and develop methods of implementing and testing application and system software in order to prevent, discover and eliminate implementation level security vulnerabilities in a pro-active fashion. The focus is on implementation level security issues and software security testing.	

Turku Centre for Computer Science	
Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.tucs.fi/research/labs	
Areas of Activity: TUCS coordinates research and education in the field of Information Technology. These activities are carried out in the TUCS Master's and Graduate Schools and in the centre's own research laboratories. At the departments participating in TUCS there are presently about 35 professors, 65 Ph.D. level researchers, 100 doctoral students and 2000 Master's students.	

University of Tampere / Department of Computer Sciences	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.cs.uta.fi/en/index.php	
Areas of Activity: The research unit of the University of Tampere, called Finnish Internet Security Consortium (FISC) has an internal website (http://www.cs.uta.fi/fisc) which is not publicly accessible. The objective of the Finnish Information Security Consortium (*FISC*) is to enhance research, education and co-operation around information security.	

Other Bodies and Organisations Active in Network and Information Security

The Government Information Security Management Board VAHTI	
Type of Organisation: National government	Ownership: public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Ministry of Finance	
Weblink: http://www.vm.fi/vahti	
Areas of Activity: The Board, set by Ministry of Finance, assists the Ministry of Finance in steering, developing and coordinating the Finnish Government Information Security Development Program.	

Tekes, the Finnish Funding Agency for Technology and Innovation	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards	
Relationships: None	
Weblink: http://www.tekes.fi/eng/	

Areas of Activity: Tekes, the Finnish Funding Agency for Technology and Innovation is the main government financing and expert organisation for research and technological development in Finland. Tekes funds innovative research and development projects in companies, universities and research institutes.	
Children On-Line (at Save the Children Finland)	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.pelastakaalapset.fi	
Areas of Activity: Save the Children Finland fights for children's rights in order to immediately and permanently improve children's lives in Finland and all over the world. Save the Children Finland engages in Internet safety work with the objective of improving children's safety and well-being as well as children's rights in the domain of modern information and communications technology.	
Mannerheim League of Child Welfare / Children online	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: Save the Children Finland, the Finnish Communications Regulatory Authority (Ficora)	
Weblink: http://www.mll.fi/	
Areas of Activity: The Mannerheim League is an NGO, which promotes the wellbeing of children, increases respect for childhood, and sees that children's views are taken into account in public decision-making.	
Finnish Information Security Association (FISA)	
Type of Organisation: IT Associations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.tietoturva.fi	

Areas of Activity:

FISA is the largest information security association in Finland. It is a non-profit association, which objective is to advance information security professionalism, awareness and best practices. Activities include member meetings, discussion groups, company visits, conferences, CISSP-certification and participation of various information security programmes.

Activities

Strategic Initiatives

Finnish Internet Awareness (FIA) project

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s): Save the Children Finland, The Mannerheim League for Child Welfare (MLL) and the Finnish Communications Regulatory Authority (Ficora)

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.mll.fi/in_english/projects/fia/

Description:

The primary objectives are:

- to arrange Safer Internet Day activities and campaigns
- to create a training model for web content providers, particularly for moderators, together with the industry, about internet safety
- maintain a Hotline for internet users to report about illegal content on net anonymously
- to create a helpline for children, where they can raise their concerns and get support on troubles regarding their experiences in the internet.

Funding Programmes & Financial Initiatives

TrustInet Project

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s):

Tekes, Helsinki Institute for Information Technology HIIT, Helsinki University of Technology, University of Helsinki

ENISA Focus Points: AR

Weblink: http://trustinet.org

Description:

The Finnish National Technology Agency (Tekes) has granted funding of 1.8 million Euro for 3 years 2006-2008 to establish an excellence group "Trustworthy Internet" at the Helsinki Institute for Information Technology (HIIT), the Telecommunications and Multimedia Laboratory (TML) at the Helsinki University of Technology, and the Computer Science Department (TKTL) at the University of Helsinki. The project is one of the four strategic research projects of the national GIGA research program for which TEKES has granted 100% funding.

The main objective of the project is to study the trust provisioning in the Internet. As changing the current Internet infrastructure is difficult, the project will explore the use of overlay networks to build and manage trust relationships between service providers and customers over networks. The project will proceed along research lines of overlay access, application integration, identity management, trust and session management, overlay scalability, and measurements.

Internet Bus

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s):

Tampere City

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.tampere.fi/kirjasto/nettinysse/

Description:

The Internet bus Netti-Nysse is one example of a new, approachable, non-formal way to help people to learn and see the possibilities and then make their own choices concerning their role in the information society.

VerkkoTikas

Type of Activity: Non-Gov Funding Programmes & Financial Initiatives

Responsible Organisation(s):

Finnish National Board of Education

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.tikas.fi

Description:

Tikas is an innovative ICT training model designed for student groups with special needs. Tikas aims to assist educational establishments, associations and other organisations in providing ICT tuition for learners with special needs of all different ages. Tikas gives comprehensive support to students who are learning basic ICT skills.

Events

Conference and Workshops

eCitizen 2.0 preparation seminar

Responsible Organisation: Baltic Institute of Finland and the Union of the Baltic Cities, Commission on Information Society.	Frequency: biennial
ENISA Focus Points: AR, e-ID, Implementation of Security Technology and Standards	
Target Groups: Major- Educational and Research Organizations, Consumers/Citizens	
Weblink: http://www.baltic.org/events/current_events/	
Description: The seminar was held as part of the "Baltic and Mediterranean – Shared Future in Action, A Euro-Mediterranean Gathering".	

Civilian Response Team (CRT) Induction Training Course

Responsible Organisation: Ministry of the Interior	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Government Organizations, Consumers/Citizens; Minor- Educational and Research Organizations	
Weblink: http://www.cmcfinland.fi/pelastus/cmc/home.nsf/en/centre	
Description: The event aims at developing common and shared training in crisis management by combining civilian and military expertise. CRT in crisis management, safety and security, fact-finding and assessment, mission build-up and support of existing crisis management activities. The intended participants include all those involved in a potential crisis organization.	

International Congress on Nursing Informatics

Responsible Organisation: University of Kuopio	Frequency: annual
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards	
Target Groups: Major- Consumers/Citizens, Educational and Research Organizations, Government Organizations; Minor- SMEs, Large Enterprises	

Weblink: http://www.ni2009.org/
Description: The theme and topics of the Congress are consistent with the central theme of Nursing Informatics – Connecting Health and Humans in support of nursing informatics practice, management education and research. The intended audience is nurses, nurse informaticians, nursing and informatics educators, nurse managers and executives, nurse and informatics researchers as well as other health care and IT professionals. The over-all idea is to present current research and to share knowledge.

Media Campaigns

Information Security Day	
Responsible Organisation: Ficora	Frequency: n/a
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Educational and Research Organizations, SMEs, Consumers/Citizens	
Weblink: http://www.tietoturvakoulu.fi/	
Description: The project is a joint project between companies, authorities and education to raise awareness on Internet usage. The intended participants are primary school students, teachers, parents and SME:s. The goal is to teach Internet users how to steer clear of Internet-based threats. The Safer Internet Day actions aim to provide information for schoolchildren and their teachers as well as parents. The target group will be offered information of the possibilities and threats on the Internet and how to avoid problems. The most appropriate media will be used to do this: mostly the Internet, but also magazines targeted to children and the television. The key messages are: follow the rules, safeguard yourself and protect your computer. An Safer Internet Day conference is also held for the stakeholders and other decision makers.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the

evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

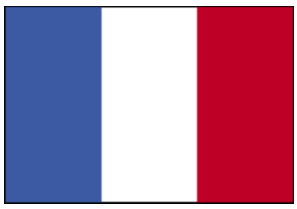
In the preceding 12 months, one security breach was reported in Finland

1. In June 2008 the European Court of Human Rights recently ordered the Finnish government to pay out €34,000 when it failed to protect a citizen's personal data, by not adequately securing and protecting her confidential medical record. €14,000 of that went to the woman who brought the case: an HIV-positive nurse who worked in a public hospital between 1989 and 1994 on a series of contracts that were not renewed. She suspected this was because her medical notes had been accessed inappropriately and asked the hospital for details of who had seen them and when. The hospital was unable to supply the data because it kept only a limited audit trail; but the court ruled the nurse did not have to prove there had been a "wilful" release. It decided that the hospital's failure to establish a system to ensure that her records could not be accessed was enough for her to win her case. More significantly, the court made a link between the breach and the European Convention on Human Rights, ruling that failure to ensure the confidentiality of medical records was a breach of article 8, which guarantees every European citizen "the right to respect for his private and family life, his home and his correspondence."

   http://www.microsoft.com/uk/nhs/content/articles/untitled_0008.aspx

Country Report – France

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Paris
Total area:	550 000 sq.km
Population:	60.9 million
Official language:	French
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in France, we present a set of three indicators in the Country Highlights section.

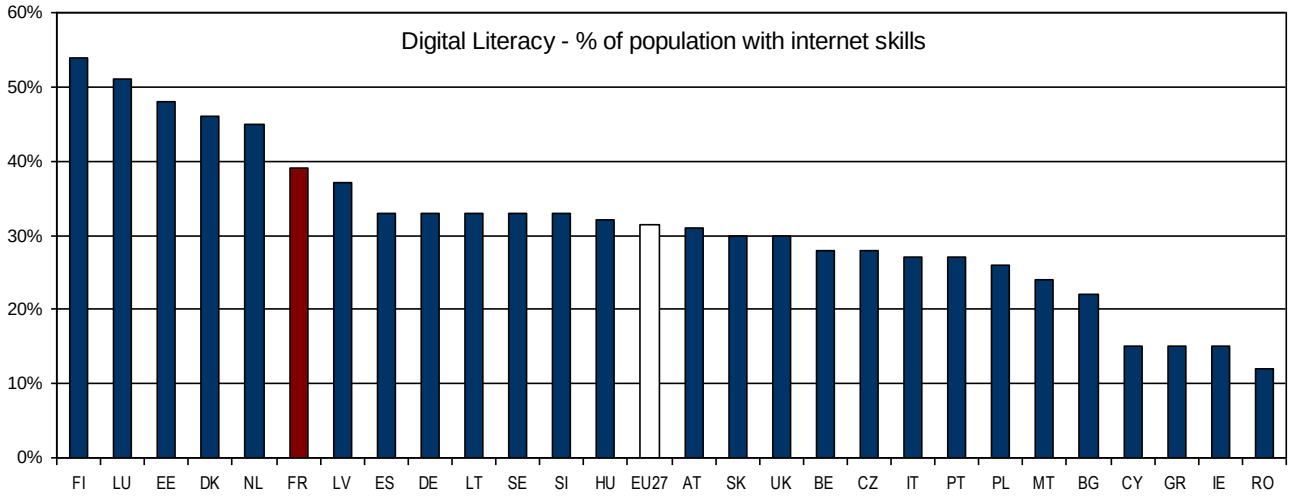
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in France is fundamental to this NIS study.

For all information society benchmarking indicators France is above the EU average values, with a relatively high digital literacy rate and e-commerce activity. France is also among the leading countries in terms of eGovernment initiatives.

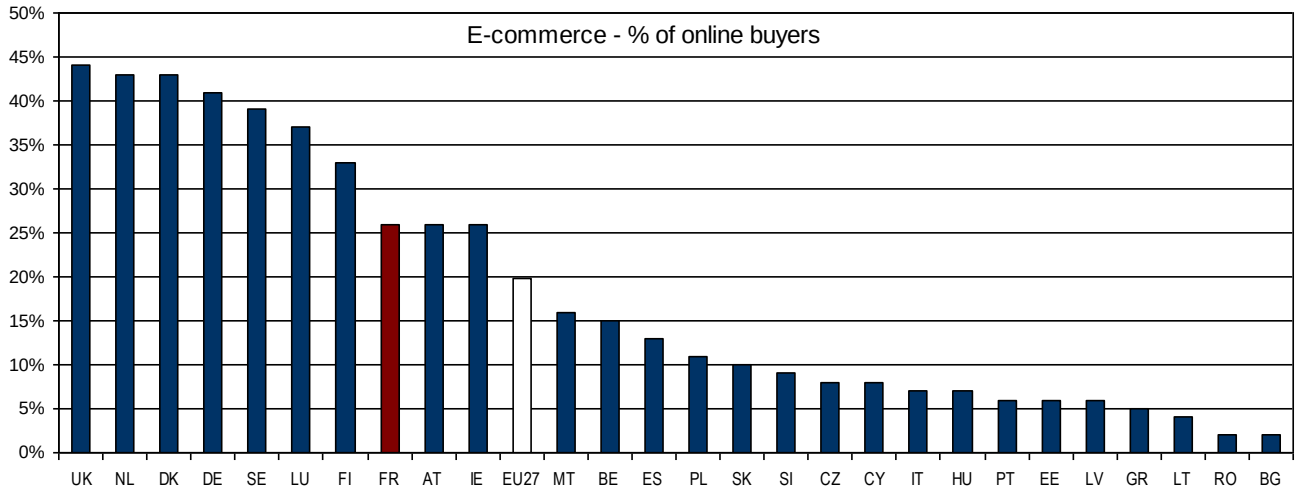
The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

Digital Literacy Indicator

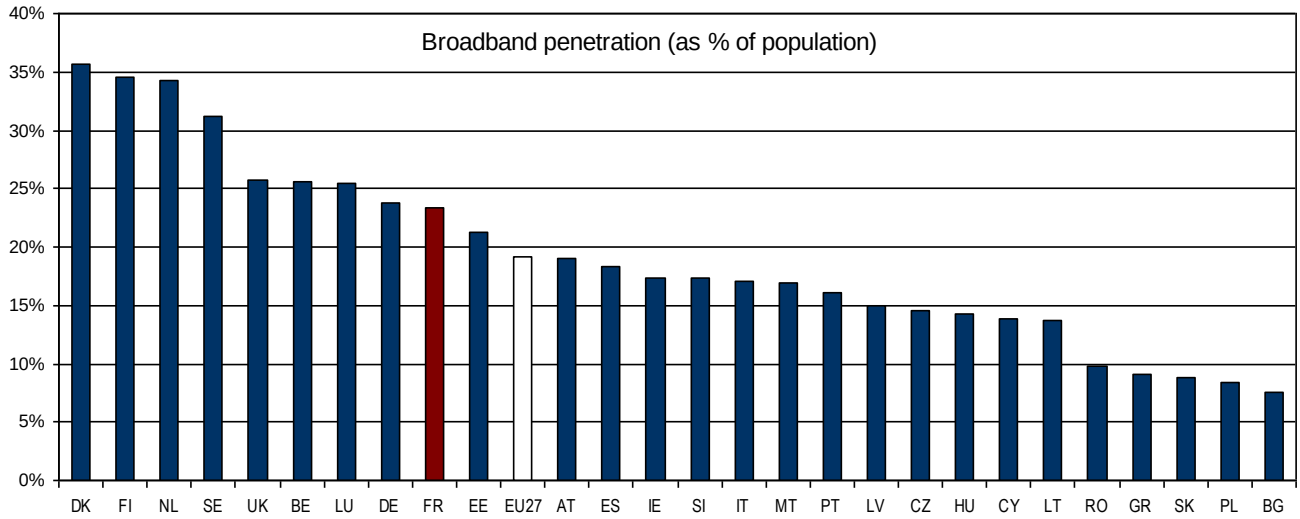


Source: IDC and Eurostat, 2008

eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Central Directorate for Information Systems Security (DCSSI), a part of the General Secretariat for National Defence, is recognized among NIS stakeholders in France as the national security agency as well as the body responsible for coordinating the development and implementation of national information security policy. One of the four main tasks of the DCSSI is to develop scientific and technical expertise in information system security,

for the benefit of public bodies and services. DCSSI contributes to government policy in the area of information systems security. The organization also acts as a national regulatory authority by issuing approvals, guarantees and certificates for national information systems, cryptological processes and products used by public bodies and services, and by controlling the information technology security evaluation centers (CESTI).

The French Data Protection Authority (CNIL) is responsible for ensuring compliance with data protection laws.

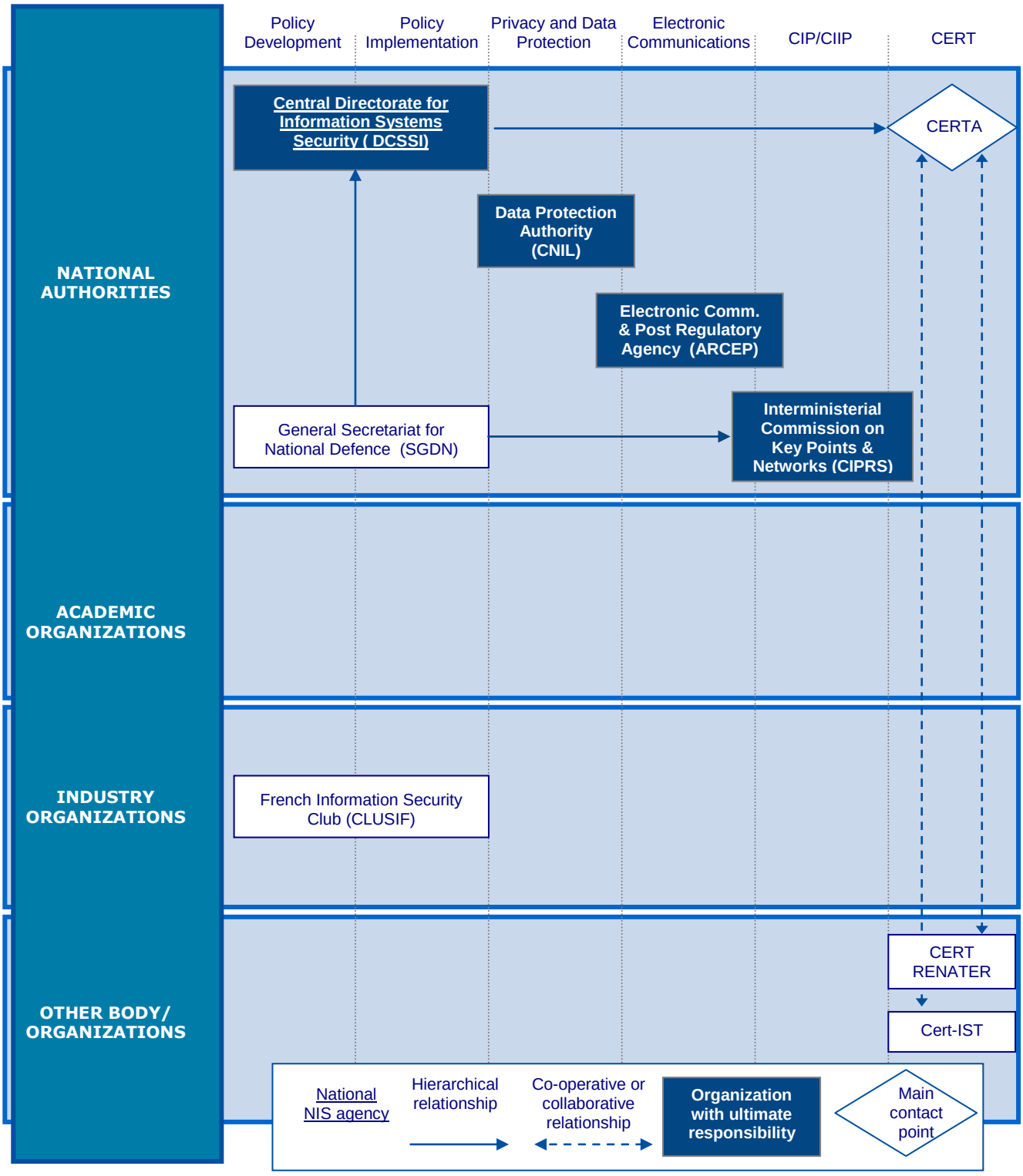
To handle security breaches and other incidents France has several security response teams in place:

- CERT-A for governmental organizations
- Cert-IST serving the industrial, services and tertiary sectors
- CERT-RENATER for members of the National Telecommunications Network for Technology, Teaching and Research (RENATER).

France has several research projects currently underway in the field of information security and has in place the information resources (such as information security portal) that contribute to technical development and knowledge sharing. The country hosts a number of conferences on NIS organized by stakeholders in the public sector, industry organizations, as well as the business and academic communities.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in France. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Name of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Central Directorate for Information Systems Security (DCSSI) & CFSSI			X	X			X	X
General Secretariat for National Defense (SGDN)		X					X	X
Data Protection Authority (CNIL)			X					
Electronic Communication and Post Regulatory Agency (ARCEP)			X	X				
Interministerial Commission on Key Points & Networks (CIPRS)		X						
CERTA	X		X	X				
French Information Security Club (CLUSIF)			X	X				

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in France:

National Authorities in Network and Information Security	
Secrétariat Général de la Défense nationale (SGDN) – General Secretariat for National Defense	
Type of Organization: National Government; attached to Prime Minister's Office	Ownership: Public
ENISA Focus Points: Resilience, Implementation of Security Technology and Standards Policy, Development of Security Technology and Standards Policy	
Relationships: Reports to the Prime Minister; works closely with President of the Republic's Office	
Weblink: http://www.sgdn.gouv.fr	
Areas of Activity: The secretariat is primarily responsible for the implementation of the security aspects of the information society development policy decided upon by the government, and for the development of security policy. This means that SGDN has a very wide mission, from public IT security to nuclear security and economic warfare tasks. As part of the ADELE (electronic administration development program), it runs a plan for strengthening the security of information systems, in order to protect the main governmental networks, both centrally and locally, as well as those used for managing vital infrastructures.	
Direction centrale de la sécurité des systèmes d'information (DCSSI) – Central Directorate for Information Systems Security	
Type of Organization: Public NIS Body	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: A department of the General Secretariat for National Defense (SGDN)	
Weblink: http://www.ssi.gouv.fr/fr/dcssi/index.html	

Areas of Activity:

DCSSI is a division of SGDN. The duties of DCSSI include: to contribute to government policy in the area of information systems security; to act as the national regulatory authority for information systems security (by issuing approvals, guarantees, and certificates for national information systems, cryptographic processes and products used by public bodies and services, and by controlling the information technology security evaluation centers); to evaluate threats and develop threat prevention capacity; to assist public services in respect to information systems security; and to develop scientific expertise and technical standards in information systems security. DCSSI also provides training and increases awareness about information systems security through the Information Systems Security Training Centre (CFSSI).

In the area of CIP/CIIP, SGDN carries out risk analysis and planning of terrorist threat prevention and intervention measures and monitors their application. It also runs the Interministerial Commission on Key Points and Networks (CIPRS), undertaking inspections of major installations.

Centre de formation à la Sécurité des Systèmes d'Information (CFSSI) – Center of Information Systems Security Education and Training	
Type of Organization: Public NIS Body	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging/Current Risks	
Relationships: Part of the Central Directorate for Information Systems Security (DCSSI)	
Weblink: http://www.formation.ssi.gouv.fr	

Areas of Activity:

The center offers training for various IT security actors in the public sector (officials, designers and end users) and hosts an exchange network in education on information systems security with universities, engineering schools, and training centers. Objectives also include increasing awareness on information systems security and training experts capable of designing, evaluating, and making recommendations in information systems security. The center has a remit to develop partnerships with higher education and further training centers. The activity and education provided are controlled and monitored by an improvement committee chaired by the general secretary for national defense and composed of civil servants and military staff.

Commission Nationale de l'Informatique et des Libertés (CNIL) – French Data Protection Authority	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: Independent	
Weblink: http://www.cnil.fr	

Areas of Activity: CNIL's overall responsibility is to ensure that the development of information technology remains at the service of citizens and does not breach human rights, privacy, or personal or public liberties. It authorizes the implementation of sensitive files, such as the ones including biometric data. It puts forward statutory and regulatory measures to adjust liberties and privacy protection to IT and technical changes. CNIL holds specific competence to access on behalf of citizens' state security, defense and public security files, including those of the security and investigation branches of the police force. The authority supervises compliance with the law by inspecting IT systems and applications.

Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) – French Telecommunications and Posts Regulator	
Type of Organization: Other Public Body	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging/Current Risks	
Relationships: Independent	
Weblink: http://www.arcep.fr	
Areas of Activity: ARCEP is the National Regulation Agency for Telecoms, driven by Telecom Paquet's EU Framework. ARCEP was created by an act of parliament in 2005, when the Telecommunications Regulator (ART) was also made responsible for regulating postal activities. In the telecommunications sector, ARCEP is responsible for applying the legal framework resulting from transposition of the European directives on electronic communications.	

Direction Générale de la Modernisation de l'Etat (DGME) – Directorate for the Modernization of State Administration	
Type of Organization: Other Public Body	Ownership: Public
ENISA Focus Points: Emerging/Current Risks	
Relationships: Part of the Ministry of Budget, Public Accounts, and Public Service	
Weblink: http://www.modernisation.gouv.fr/	
Areas of Activity: As part of its overall duties focused on modernization of public administration, the DGME advises ministries on implementing egovernment.	

L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) – Central Office for the Fight against Crime Related to Information Technology and Communication	
Type of Organization: National Security Actor	Ownership: Public

ENISA Focus Points: Awareness Raising, Emerging/Current Risks	
Relationships: Part of the National Police	
Weblink: http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organization/dcpj/cyber-criminalite	
Areas of Activity: The office was established in May 2000 and has operational and technical competence in the area of cyber-crime. The main task of the office is to facilitate and coordinate police activities against cyber-crime at the national level. The remit of the OCLCTIC includes carrying out investigations, and assisting the police, the gendarmerie, and the Directorate General for Competition, Consumption and Fraud Prevention in their judicial activities. OCLCTIC supports local and regional police with IT expertise, IT data collection, and other IT crime-related needs. The OCLCTIC is the international contact point in the area of cyber-crime.	
Delegation aux usages de l'internet (DUI) – Internet Usage Delegation	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: Part of the Ministry of Higher Education and Research	
Weblink: http://www.delegation.internet.gouv.fr/mission/index.htm	
Areas of Activity: The DUI was founded in July 2003 at the Inter-ministerial Committee for the Information Society (CISI). The overall remit of the DUI is to bridge the digital gap in France. The DUI's priorities include: creation of public access points to the Internet; promotion of alternative access technologies; Internet safety for the public (especially the protection of minors); ICT training and support.	
Direction du développement des médias (DDM) – Directorate for Media Development	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Emerging/Current Risks	
Relationships: Under the authority of the Prime Minister and the political and administrative supervision of the Ministry of Culture and Communication	
Weblink: http://www.ddm.gouv.fr/	
Areas of Activity: The DDM is responsible for implementing public policy in the realm of the media and the information society. The DDM set up the Signal Spam initiative.	

Industry Organizations Active in Network and Information Security

Club de la Sécurité de l'Information Français (CLUSIF) – French Information Security Club

Type of Organization: IT Association	Ownership: Non-Profit
ENISA Focus Points: Awareness Raising, Emerging/Current Risks	
Relationships: n/a	
Weblink: http://www.clusif.asso.fr/	

Areas of Activity:

CLUSIF, created in 1984, is a non-profit organization allowing professionals dealing with information security (including IT security) to meet, work, exchange opinions, and progress together. CLUSIF contributes to information security education, improvements, and awareness via publications resulting from the activity of its work groups, market studies, and public conferences. Most of the documents resulting from these activities are made publicly available. CLUSIF also regularly initiates public studies on cyber-crime and security policies. An important contribution of CLUSIF to the management of information-related security is a comprehensive risk management methodology, called MEHARI, which is built around a set of modules, tools, and questionnaires.

Alliance TiCS

Type of Organization: IT Association	Ownership: Non-Profit
ENISA Focus Points: n/a	
Relationships: formed by the unions SFIB (Information Technology) and GITEP TICS (Telecommunications)	
Weblink: http://www.alliance-tics.org/index.htm	

Areas of Activity:

Professional Union Alliance TICS is a professional union created in 2003 by the merger of two unions – SFIB (Technologies of Information) and GITEP TICS (Telecommunications). Through its member unions, Alliance TICS represents sixty companies, or economic backing of EUR 27 billion with a workforce of 70,000 employees. The activities of the union are centered around information/document processing, office automation, mail processing, fixed/mobile/private networks, support and services, and areas relating to SMEs. The mission of the union includes: ensuring the representation of its members; identification and promotion of the interests of professions represented and creating conditions conducive to the development of these industries; bringing together the positions of its members by taking advantage of complementary trades; and promoting the themes in France that underlie the development of the market and the overall image of France as an ICT leader.

Observatoire de la Sécurité des Systèmes d'Information et des Réseaux (OSSIR) – Observatory of Information Systems and Network Security	
Type of Organization: IT Association	Ownership: Non-Profit
ENISA Focus Points: Awareness Raising, Emerging Risks / Current Risks	
Relationships: Originally created inside the Military Academy for Telecommunications, OSSIR is unofficially very close to the defense and military sectors. Widely opened to the IT security community, OSSIR gathers many experienced users in the public sector.	
Weblink: http://www.ossir.org/	
Areas of Activity: OSSIR was formed in 1996 by users interested in the security of information systems and networks. The association organises an annual conference called Information Systems Security Day (JSSI).	

Other Bodies and Organizations Active in Network and Information Security

CERT-A	
Type of Organization: CERT	Ownership: Public
ENISA Focus Points: CERT	
Relationships: Part of the DCSSI	
Weblink: http://www.certa.ssi.gouv.fr	
Areas of Activity: CERT-A was founded in February 2000 and is attached to the Central Directorate for Information Systems Security (DCSSI). It is responsible for helping government organizations set up protection and resolve computer incidents or attacks. The objectives of the CERT-A are to detect vulnerabilities and solve incidents related to information systems security and to help set up means to safeguard against future incidents.	

CERT RENATER	
Type of Organization: CERT	Ownership: Private
ENISA Focus Points: CERT	
Relationships: Coordinates with other French and international CERTs	
Weblink: http://www.renater.fr/spip.php?rubrique19/CERT_Renater.htm&lang=fr	

Areas of Activity: CERT RENATER was founded in 1995 and serves the members of the National Telecommunications Network for Technology, Teaching, and Research (RENATER) in matters of information security, particularly in the areas of security protection and threat detection and resolution.

Computer Emergency Response Team - Industrie, Services et Tertiaire (Cert-IST) – Computer Emergency Response Team - Industry, Services, and Tertiary	
Type of Organization: CERT	Ownership: Private
ENISA Focus Points: CERT	
Relationships: Coordinates with other French and international CERTs	
Weblink: http://www.cert-ist.com/	
Areas of Activity: Cert-IST was created by a consortium of French companies in 1998. The association has four partner members – CNES, France Telecom, Sanofi Aventis, and the Alcatel-Lucent group – that have access to all Cert-IST services, and adherent members that have partial access to services. The offer of Cert-IST includes security advisories and alerts, security bulletins, a vulnerability database, and an incident handling service.	

Activities

Strategic Initiatives

Portail de la sécurité informatique – Computer Security Portal
Type of Activity: Governmental Policy
Responsible Organization(s): DCSSI
ENISA Focus Points: Awareness Raising, Emerging/Current Risks, Micro enterprises
Weblink: http://www.securite-informatique.gouv.fr/
Description: Set up in 2008, the purpose of this information portal is to offer practical information and advice to private individuals, professionals, and SMEs. The information includes: a glossary of computer security jargon; a set-up guide for the recommendations provided on the portal; modules on the subjects of passwords; the importance of security policy; etc. The portal also offers news and alerts about emerging security threats.

Internet sans craintes – Internet without Fear
Type of Activity: Governmental Policy

Responsible Organization(s): DUI
ENISA Focus Points: Awareness Raising, Emerging/Current Risks
Weblink: http://www.internetsanscrainte.fr
Description: Internet without Fear is supported by DUI and coordinated by Tralalère, which is in charge of the communications component and awareness program. e-Enfance is in charge of the telephone hotline. Specific aims are: to educate young people about the risks and uses of the Internet; to inform their parents and teachers so they can better protect them; and to give teachers practical tools for creating workshops with young people in their charge. The main outcomes of the program have been: the www.internetsanscrainte.fr Website; a series of animated cartoons called "Vinz and Lou on the Internet"; a telephone hotline for children and parents; and communication tools for the educational community, such as postcards, posters, cd-roms, brochures, and comic books.
Le Référentiel Général de Sécurité (RGS) – The General Security Repository
Type of Activity: Governmental Policy
Responsible Organization(s): DCSSI and DGME
ENISA Focus Points: Awareness Raising, Emerging/Current Risks
Weblink: http://www.synergies-publiques.fr/rubrique.php?id_rubrique=159
Description: The RGS was created in 2005 and is a security framework for information systems and networks involved in the electronic exchange of information among administrative authorities and between these authorities and their users.
Signal Spam
Type of Activity: Public-Private Initiative
Responsible Organization(s): DDM
ENISA Focus Points: Awareness Raising, Emerging/Current Risks
Weblink: https://www.signal-spam.fr/
Description: Signal Spam was set up in 2005 by DDM as an association comprising most of the main French organizations involved in the fight against spam, including public authorities, industry associations and private companies. Signal Spam is engaged in the following activities: the design, implementation, and operation of a computerized system for tracking spam; the production of reports on spam; informing the public about how to combat spam; and the formation of recommendations for public authorities.
Protège ton ordi

Type of Activity: Public-Private Initiative
Responsible Organization(s): DUI, Microsoft
ENISA Focus Points: Awareness Raising
Weblink: http://www.protegetonordi.com/
Description: The Web site is the result of a public-private partnership between Microsoft and the public authorities, aimed at raising the awareness of internet threats, alerting about possible damages to personal IT equipment, and targeting deceptions aimed particularly at young users. Topics like viruses or phishing threats are presented with humor to reach a young audience as well as adults.
e-enfance
Type of Activity: Non-Profit Initiative
Responsible Organization(s): n/a
ENISA Focus Points: Awareness Raising
Weblink: http://www.e-enfance.org
Description: e-enfance is a French non-profit organization funded by private donors. It aims at informing parents and children about responsible Internet use, via PCs, mobile phones, and gaming consoles. The e-enfance mission focuses on making adults more aware of their "cyberparent" role.
Action Innocence
Type of Activity: Non-Profit Initiative
Responsible Organization(s): Non-Governmental Organization (NGO)
ENISA Focus Points: Awareness raising, Emerging/Current Risks
Weblink: http://www.actioninnocence.org/

Description: Action Innocence is an NGO that contributes to preserving the dignity of children on the Internet. Headquartered in Switzerland, but locally active in all French-speaking countries in Europe (Belgium, France, Switzerland, Monaco), the organization's resources come from dues paid by its members, donations, and funds raised through special events. The Association cooperates with the Canton of Geneva Department of Justice, Police, and Safety, as well as the Canton's Department of Public Education.

The mission of AiG is to become an independent, French-language reference organization committed to fighting acts of sexual abuse involving children on the Internet.
The goal of the organization is to develop the following types of action:

- Prevention and information intended for parents, children, teenagers, and professionals who work in the school system (the target audience)
- Information and intervention specifically aimed at government bodies and political authorities
- Cooperation with computer professionals with a view to "cleaning up" content that may be accessed via the Internet and developing suitable IT tools.

AiG wants to thus ensure that children and teenagers are able to access information that correspond to their development "in accordance with the age and maturity" of each young person, while enabling him/her to take part in the creation of a healthier, more responsible environment. This goal fits into the context of the various aspects of the Rights of the Child convention.

Research Programmes

Research on the Politics of Information Security and Cybercrime

Type of Activity: Social and Other Research Program

Responsible Organization(s): CLUSIF

ENISA Focus Points: Awareness raising, Emerging/Current Risks

Weblink: https://www.clusif.asso.fr/fr/production/sinistralite/

Description:

CLUSIF contributes to information security education, improvements, and awareness via publications resulting from the activity of its work groups, market studies, and public conferences and meetings. Most of the documents resulting from these actions are offered to the public on this site, including some technical studies translated into English. CLUSIF also regularly initiates public studies on cyber-crime and security policies.

Events

Conference and Workshops	
Infosecurity France	
Responsible Organization: REED EXPOSITION	Frequency: Annual
ENISA Focus Points: Awareness raising, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises	
Weblink: http://www.infosecurity.com.fr/	
Description: conferences and exhibition around the topics of intrustion, phishing, trojan horses, VoIP security, and business continuity.	
La journée de la Sécurité des Systèmes d'Information – Seminar on Information System Security	
Responsible Organization: OSSIR	Frequency: Annual
ENISA Focus Points: Awareness raising, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises	
Weblink: http://www.ossir.org/jssi/index.shtml/	
Description: This event organized by OSSIR brings together experts and professions from all aspects of network and information security – technical, legislative, etc.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in France.

Country Report – Germany

Country General Information

Source: European Commission

Political system:	Federal Republic
Capital city:	Berlin
Total area:	356 854 sq.km
Population:	82.5 million
Official language:	German
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Germany, we present a set of three indicators in the Country Highlights section.

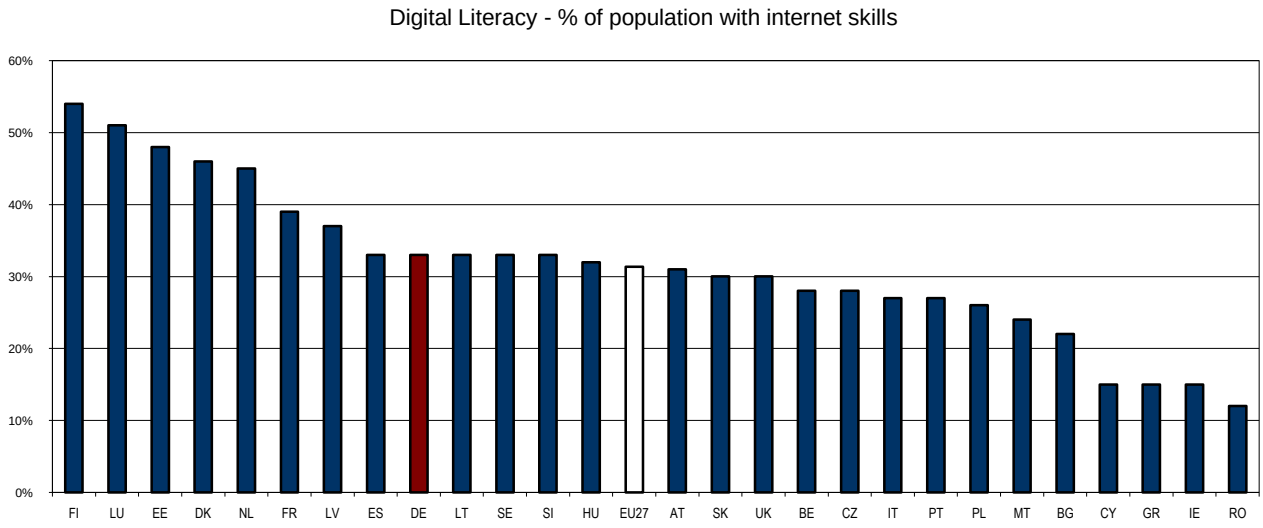
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Germany is fundamental to this NIS study.

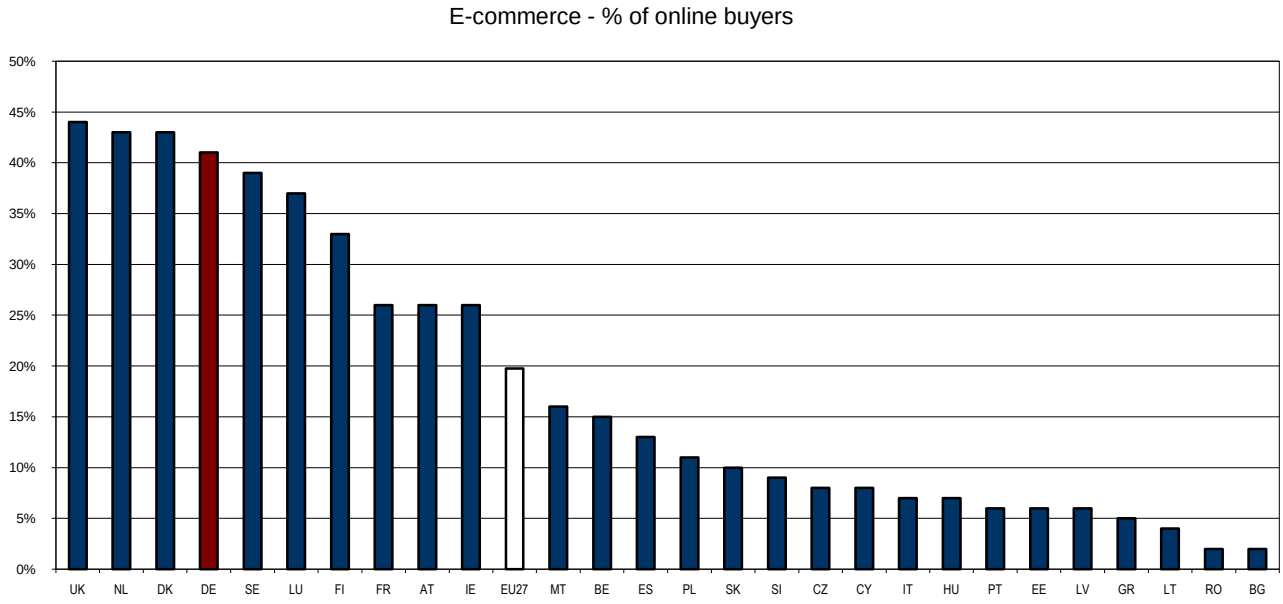
Information society – connectivity and ICT usage in households, enterprises, and government bodies – is very well developed in Germany, which ranks particularly high in the use of eCommerce.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

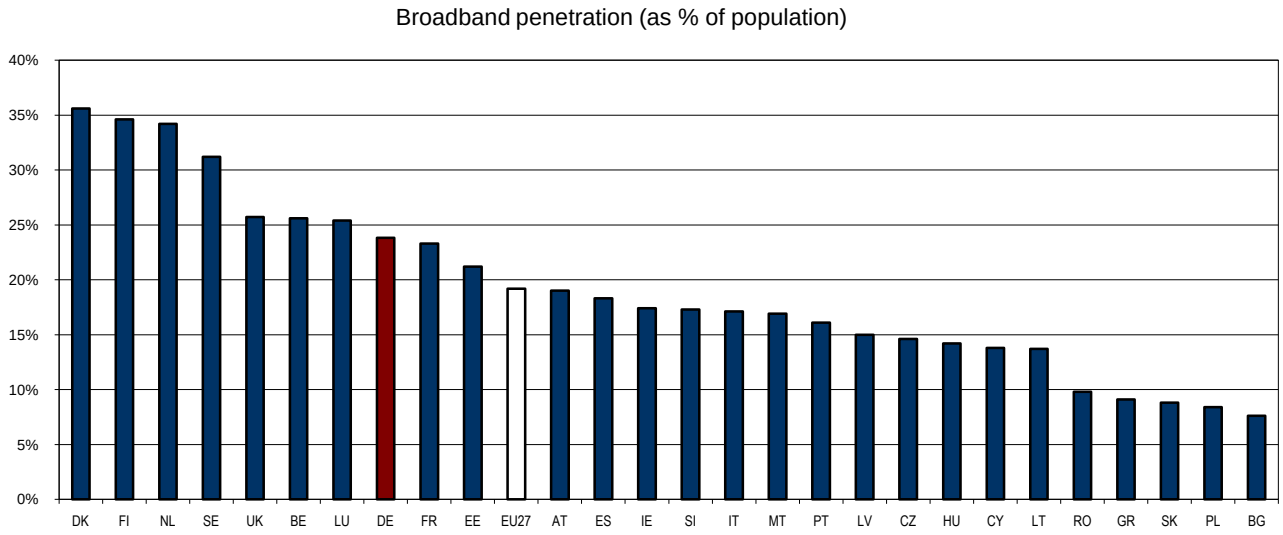
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Federal Office for Information Security (BSI) is the central IT security service provider for the German government. It advises users and manufacturers of IT products.

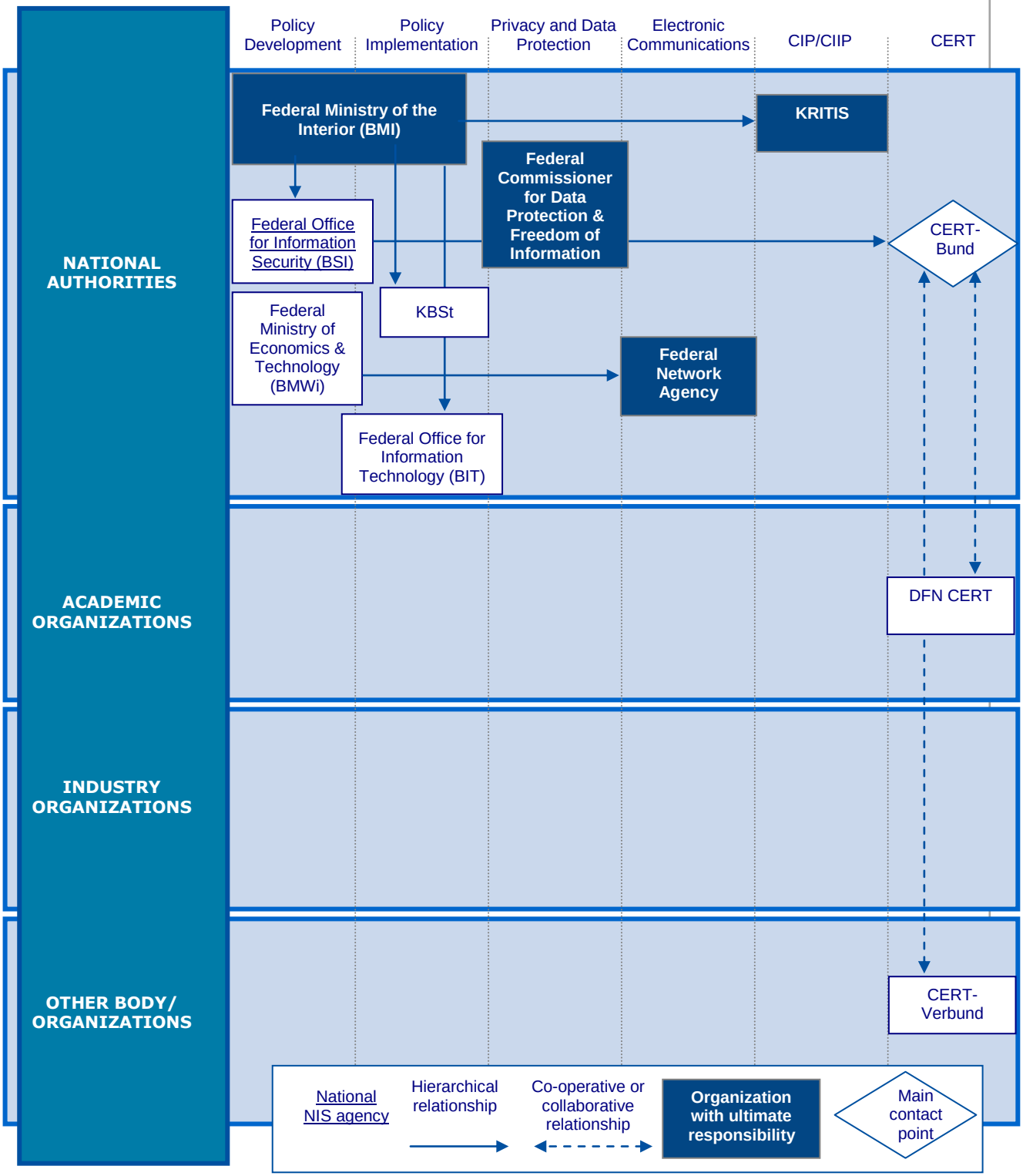
Also responsible for the implementation of national information security policy is the Ministry of the Interior (BMI). The most important responsibility of the BMI is guaranteeing Germany's internal security. The BMI is also responsible for the comprehensive use of information technology to modernize the public administration, and the security of information technology.

The Federal Commissioner for Data Protection and Freedom of Information is charged with ensuring compliance with privacy and data protection legislation. The Federal Ministry of Economics and Technology (BMWi) is the agency ensuring compliance with electronic communications legislation.

The BMI task force KRITIS is responsible for CIP/CIIP at the national level. It includes members of the BMI, the BSI, the Federal Office of Civil Protection and Disaster Assistance (BBK), the State Disaster Protection Organization (THW), and the Federal Criminal Police Office (BKA).

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Germany. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Federal Ministry of the Interior (BMI)		X	X	X		X	X	X
Federal Office for Information Security (BSI)	X	X	X	X		X	X	X
Federal Government Coordination and Advisory Agency for IT in the Federal Administration (KBSt)							X	X
Federal Office for Information Technology (BIT)								X
Federal Commissioner for Data Protection and Freedom of Information								X
Federal Ministry of Economics and Technology (BMWi)		X					X	X
Federal Network Agency		X		X				X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Germany:

National Authorities in Network and Information Security	
Bundesministerium des Inneren (BMI) – Federal Ministry of the Interior	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Federal Office for Information Security (BSI), KBSt, Federal Office for Information Technology (BIT), KRITIS	
Weblink: http://www.bmi.bund.de/	
Areas of Activity: BMI's most important responsibility is guaranteeing Germany's internal security. The Ministry is also responsible for the comprehensive use of information technology to modernize the public administration, and the security of information technology. Areas of responsibility include information security policy, protection of critical information, infrastructure, egovernment, travel documents, and biometrics. The BMI task force KRITIS includes members of the following organizations: BMI, BSI, BBK, THW, and BKA.	
Bundesamt für Sicherheit in der Informationstechnik (BSI) – Federal Office for Information Security	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, eID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Reports to the BMI	
Weblink: http://www.bsi.bund.de/	

Areas of Activity: The Federal Office for Information Security (BSI) is the central IT security service provider for the German federal government. BSI investigates security risks associated with the use of IT and develops preventive security measures. This work includes IT security testing and assessment of IT systems, including their development, in cooperation with industry. The BSI advises manufacturers, distributors, and users of information technology. It also analyzes IT development and trends. The BSI is organized into four departments, each of which comprises two divisions: Department Z: Administration Department 1: Security of Applications, Critical Infrastructure and Internet. Comprises Division 11: Security of Applications and Division 12: Security of Critical Infrastructure and Internet. The Federal Computer Emergency Response Team (CERT-Bund), which acts as a central contact point for solving computer and network security problems for federal institutions, is part of Division 12. Department 2: Cryptography and Counter-Eavesdropping. Comprises Division 21: Cryptographic Technology and Division 22: Counter-Eavesdropping. Department 3: Certification, Approval and Conformity Testing, New Technologies. Comprises Division 31: New Technologies and Conformity Products and Division 32: Certification, Approval and Conformity Assessments.

Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) – Federal Government Coordination and Advisory Agency for IT in the Federal Administration	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: Part of BMI; cooperates with BIT	
Weblink: http://www.kbst.bund.de	
Areas of Activity: Located within the Federal Ministry of the Interior, the KBSt is an interministerial agency of the federal government intended to ensure the federal administration optimizes its use of information technology for specific fields and in organizational, economic, and technical terms. The KBSt advises federal authorities on their IT strategies and publishes recommendations on IT strategy and methodological guidelines for implementing such strategies. The KBSt also deals with issues of software architecture and its standardization and with the definition of interfaces. To perform its mission, the KBSt develops framework rules for the use of IT within the federal administration.	

Bundesstelle für Informationstechnik (BIT) - Federal Office for Information Technology	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: A service center within the Central Administrative Office (BVA), which reports to the BMI. Cooperates with the KBSt	

Weblink: http://www.bit.bund.de/	
Areas of Activity: Provides Central IT services to the federal administration.	
Bundesministerium für Wirtschaft und Technologie (BMWi) – Federal Ministry of Economics and Technology	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.bmwi.de/	
Areas of Activity: The Ministry is responsible for developing economic policy, including ICT policy, telecommunications security policy, and contingency planning for telecommunications networks and services.	
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen – Federal Network Agency for Gas, Telecommunications, Post, and Railway	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: Reports to the BMWi	
Weblink: http://www.bundesnetzagentur.de	
Areas of Activity: The Federal Network Agency is a separate federal authority within the Federal Ministry of Economics and Technology. The agency provides, through liberalization and deregulation, for the further development of the electricity, gas, telecommunications, postal, and railway markets. The agency is responsible for ensuring compliance with the Telecommunications Act.	
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – Federal Commissioner for Data Protection and Freedom of Information	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: Associated with the BMI but not constrained by functional directives	
Weblink: http://www.bfdi.bund.de/	
Areas of Activity: Supervisory authority on data protection.	

Bundeskriminalamt (BKA) – Federal Criminal Police Office	
Type of Organization: National Security Actor	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy	
Relationships: Subordinate to the BMI	
Weblink: http://www.bka.de/	
Areas of Activity: The Federal Criminal Police Office is the main national criminal police agency.	

Industry Organizations Active in Network and Information Security

Bundesverband Informationswirtschaft,Telekommunikation und neue Medien (BITKOM) – German Association for Information Technology, Telecommunications, and New Media	
Type of Organization: Industry Association	Ownership: Private
ENISA Focus Points: AR, Emerging Risks	
Relationships: None	
Weblink: http://www.bitkom.org	
Areas of Activity: BITKOM is the voice of IT, telecommunications, and new media in Germany. The organization represents more than 1,000 businesses, 850 of which are members, and focuses on egovernment, ehealth, reducing bureaucracy, policies for medium-sized enterprises, IT security, knowledge management, software development and sustainability, as well as advanced radio and media regulation. BITKOM has a seat on the executive board of the European Information, Communications, and Consumer Electronics Technology Industry Associations (EICTA).	

Verband der deutschen Internetwirtschaft (eco) – Association of the German Internet Industry	
Type of Organization: Industry Association	Ownership: Private
ENISA Focus Points: AR, Emerging Risks	
Relationships: None	
Weblink: http://www.eco.de	

Areas of Activity: eco, the association of German Internet enterprises, counts all of the country's approximately 150 major Internet service providers (ISPs) as members. eco runs the largest German data exchange, the Deutscher Commercial Internet Exchange (De-CIX), which covers approximately 80% of national and 35% of international network traffic. eco is a founding member of the European Internet Service Providers Association (EuroISPA).

Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) – Association of Telecommunications and Value-Added Service Providers	
Type of Organization: Industry Association	Ownership: Non-Profit
ENISA Focus Points: AR, Emerging Risks	
Relationships: Maintains contact with the BMWi and the Federal Network Agency	
Weblink: http://www.vatm.de	
Areas of Activity: VATM represents more than 50 telecommunications and multimedia companies active in the German market. The majority of VATM's members are subsidiaries of, or affiliated with, European and overseas service providers. VATM supports a working group on safety and data protection.	

IT Security Made in Germany (ITSMIG)	
Type of Organization: Industry Association	Ownership: PPP
ENISA Focus Points: Development of Security Technology and Standards	
Relationships: Managed by SIT; supported by the BMWi and the BMI	
Weblink: http://www.itsmig.de/content/pages/home.htm	
Description: ITSMIG is an association of German IT security companies that aims to foster cooperation between German IT security solutions suppliers and partners in foreign countries. It is a network of manufacturers, systems integrators, service providers, research institutes, and public services. Organization and management lies with the Fraunhofer Institute for Secure Information Technology (SIT). This international partner network enables German IT security companies to use instruments of external trade promotion and consolidates the export control of the federal government. The association links this network of German companies to the federal authorities, improving the use of existing public services in developing markets in target regions, i.e., the Arab states, Southeast Asia, and Eastern Europe. The network encompasses a considerable number of German enterprises in crypto-economy, trusted services (PKI), secure service provision, biometry, and systems integration.	

Academic Organizations Active in Network and Information Security	
DFN CERT	
Type of Organization: Other Academic	Ownership: Non-profit
ENISA Focus Points: AR, Emerging Risks, Implementation of Security Technology and Standards, CERT	
Relationships: Cooperates with CERT-Verbund	
Weblink: http://www.cert.dfn.de/	
Areas of Activity: CERT for the members of Germany's National Research and Education Network (DFN).	
Fraunhofer-Institut für Sichere Informationstechnologie (SIT) – Fraunhofer Institute for Secure Information Technology	
Type of Organization: Research Centers	Ownership: Private
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: Part of the Fraunhofer-Gesellschaft	
Weblink: http://www.sit.fraunhofer.de/	
Areas of Activity: The SIT is the leading German research and development center for IT security. Its main areas of research include: security modelling and validation, secure mobile systems, secure processes and infrastructure, and transaction and document security.	
Horst Görtz Institut für IT-Sicherheit (HGI) – Horst Görtz Institute for IT-Security	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: Institute at the Ruhr-University Bochum	
Weblink: http://www.hgi.rub.de	
Areas of Activity: The HGI is one of Europe's largest university-based institutions for interdisciplinary research in the field of IT security. The HGI actively participates in international research in theoretical and applied cryptography; embedded security; mobile and fixed network security; trusted computing; secure operating systems and platforms; and legal and economic aspects of security.	

Institut für Sicherheit im E-Business (ISEB) – Institute for eBusiness Security	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: Institute at the Ruhr-University Bochum	
Weblink: http://www.iseb.ruhr-uni-bochum.de/profil/index-en.shtml	
Areas of Activity: The ISEB researches the business and economic implications of security in ebusiness, as well as information security in companies and public institutions. The main focus is economical analyses and organizational design tasks in the context of information security. Examples include information risk and security management, or questions of information security and confidence in online trading.	

Institut für IT-Sicherheit und Sicherheitsrecht (ISL) – Institute of IT-Security and Security Law	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: Department of the University of Passau	
Weblink: http://www.isl.uni-passau.de/	
Areas of Activity: The Institute of IT-Security and Security Law (ISL) is characterized by its interdisciplinary focus on computer science, law, and economics.	

Institut für Internet-Sicherheit if(is) – Institute for Internet-Security	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: Independent scientific facility of the Gelsenkirchen University of Applied Sciences	
Weblink: http://www.internet-sicherheit.de/	
Areas of Activity: The institute conducts research and development in the area of internet security, and is also a creative service provider with a focus on internet security. One of the institute's overall tasks is to improve the statutory internet security framework in Germany.	

Lehrstuhl Management der Informationssicherheit – Chair for IT-security Management of the University of Regensburg	
Type of Organization: Universities	Ownership: Public

ENISA Focus Points: Emerging/Current Risks, Development of Security Technology and Standards
Relationships: University of Regensburg
Weblink: http://www-sec.uni-regensburg.de
Areas of Activity: Conducts research into testlab IT security; secure business processes; secure communications infrastructures; network and Internet security; mobile security and distributed systems; data protection, privacy and multilateral security; identity management and public key infrastructures (PKI); and digital rights management (DRM).

Other Bodies and Organizations Active in Network and Information Security

Gesellschaft für Informatik (GI) – Network for IT	
Type of Organization: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.gi-ev.de	
Areas of Activity: GI is a non-profit organization with approximately 25,000 worldwide, most of whom teach, research, or otherwise work in the field of informatics, while others are involved in related business and political areas. The main purpose of this network of professionals is to promote the impact informatics has had on the economy, business, and society.	

CERT Verbund - CERT Network	
Type of Organization: Other Organizations	Ownership: Non-profit
ENISA Focus Points: CERT, AR	
Relationships: Promotes cooperation among CERTs	
Weblink: http://www.cert-verbund.de/	
Areas of Activity: The CERT Network is an alliance of German CERTs.	

Initiative D21 – D21 Initiative	
Type of Organization: Other Bodies and Organizations	Ownership: PPP
ENISA Focus Points: AR, Emerging/Current Risks	

Relationships: None	
Weblink: http://www.initiatived21.de	
Areas of Activity: The D21 Initiative is Germany's largest public/private partnership with more than 200 currently involving representatives of enterprises, associations, parties, political institutions, and other organizations. The goal of the D21 Initiative is to improve the general conditions necessary to move successfully into an information and knowledge-based society. The D21 Initiative pursues these objectives through some 40 practical projects.	
TeleTrusT Deutschland – TeleTrusT Germany	
Type of Organization: Other Bodies and Organizations	Ownership: Non-Profit
ENISA Focus Points: AR, Emerging/Current Risks, e-ID	
Relationships: None	
Weblink: http://www.teletrust.de	
Areas of Activity: Non-profit organization for the promotion of trustworthiness of information and communications technology. TeleTrusT aims to achieve acceptance of the digital signature as an instrument conferring legal validity on electronic transactions; support research into methods of safeguarding electronic data interchange (EDI) and the application of its results; and develop standards in this field; collaborate with institutes and organizations in other countries to coordinate objectives and standards within the European Union. TeleTrusT supports the incorporation of authenticity standards in planned or existing IT applications in public organizations and associations. Special attention is being paid to security services and their management as a means for secure IT in medicine and public health administration, electronic communications in legal matters, and tele-cooperation via EDI.	
CAST	
Type of Organization: Other Bodies and Organizations	Ownership: Non-profit
ENISA Focus Points: AR	
Relationships: Supported by the Media Authority of Northrhine-Westfalia (LfM)	
Weblink: http://www.cast-forum.de/home.html	
Areas of Activity: The CAST forum includes over 200 members from the scientific world, industry, and the public sector. CAST offers a number of services in the field of modern information technology security, with a focus on the Internet. This includes education opportunities, consulting, evaluation of security concepts and technologies, as well as the exchange of and access to research and developments in the field.	

Activities

Strategic Initiatives
Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) – National Plan for the Protection of Information Infrastucture
Type of Activity: Government Policies
Responsible Organization(s): BMI
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy
Weblink: http://www.bmi.bund.de/nn_163950/Internet/Content/Themen/Informationsgesellschaft/Sicherheit/NPSI.html
Description: The NPSI lays important foundations for secure and reliable egovernment for administrations and users alike. The main goals of the plan are the development of security standards, incident prevention, and the strengthening of IT security expertise.
Umsetzungsplan KRITIS – CIP Implementation Plan
Type of Activity: Government Policies
Responsible Organization(s): BSI, BMI and about 30 critical infrastructure operators or related business associations
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: http://www.bsi.bund.de/english/topics/kritis/veroeff_upkritis.htm
Description: The CIP Implementation Plan was drawn up to substantiate the goals of "Prevention, Preparedness, and Sustainability" set out in the National Plan for Information Infrastructure Protection in the shape of specific measures and recommendations for critical infrastructures. Four working groups with chairpersons from the private sector are supporting the adoption of the recommendations given in the CIP Implementation Plan: WG 1 Emergency and crisis exercises WG 2 Crisis response and management WG 3 Maintaining critical infrastructure services WG 4 National and international cooperation
IT-Grundschutz Catalogs
Type of Activity: Government Policies

Responsible Organization(s): BSI
ENISA Focus Points: AR, Implementation of Security Technology and Standards
Weblink: http://www.bsi.bund.de/english/gshb/index.htm
Description: The IT-Grundschutz Catalogs of the BSI describe a simple method for identifying necessary IT security measures and their implementation. With ISO 27001 certification on the basis of IT-Grundschutz, companies can check their IT security management and concrete IT security measures, and have these certified by an independent body.
BSI Standard 100-1 – Information Security Management Systems (ISMS)
Type of Activity: Government Policies
Responsible Organization(s): BSI
ENISA Focus Points: CERT, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: http://www.bsi.bund.de/english/publications/bsi_standards/standard_1001_e.pdf
Description: BSI Standard 100-1 defines the general requirements for an ISMS. It is completely compatible with ISO Standard 27001 and moreover takes the recommendations in ISO Standards 13335 and 17799 into consideration. It provides readers with easily understood and systematic instructions, regardless of which methods they wish to use to implement the requirements. BSI presents the content of these ISO Standards in its own BSI Standard in order to describe some issues in greater detail and therefore facilitate a more didactic presentation of the contents. In addition, the organization was arranged to be compatible with the IT-Grundschutz approach. The common headings in the two documents make orientation easier for the reader.
BSI Standard 100-2 – IT-Grundschutz Methodology
Type of Activity: Government Policies
Responsible Organization(s): BSI
ENISA Focus Points: CERT, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: http://www.bsi.bund.de/english/publications/bsi_standards/standard_1002_e.pdf

Description: The IT-Grundschutz Methodology progressively describes (step by step) how IT security management can be set up and operated in practice. The tasks of IT security management and setting up an IT security organisation are important subjects in this context. The IT-Grundschutz Methodology provides a detailed description of how to produce a practical IT security concept, how to select appropriate IT security measures and what is important when implementing the IT security concept. The question as to how to maintain and improve IT security in ongoing operation is also answered. Thus, IT-Grundschutz interprets the very general requirements of the ISO Standards 13335, 17799 and 27001 mentioned above and helps the users to implement them in practice with many notes, background expertise and examples.
BSI Standard 100-3 – Risk Analysis based on IT-Grundschutz
Type of Activity: Government Policies
Responsible Organization(s): BSI
ENISA Focus Points: CERT, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: http://www.bsi.bund.de/english/publications/bsi_standards/standard_1003_e.pdf
Description: The IT-Grundschutz Catalogues of the BSI contain standard security measures required in the organisational, personnel, infrastructure and technical areas that are generally appropriate for normal security requirements and to protect typical IT environments. To cover these issues, the BSI has worked out a method of analysing risks that is based on IT-Grundschutz. This approach can be used when companies or public authorities are already working successfully with the IT-Grundschutz Manual and would like to add an additional security analysis to the IT-Grundschutz analysis as seamlessly as possible.
BSI Standard 100-4 – Emergency Management
Type of Activity: Government Policies
Responsible Organization(s): BSI
ENISA Focus Points: CERT, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: http://www.bsi.bund.de/literat/bsi_standard/bsi-standard_100-4_v090.pdf
Description: BSI Standard 100-4 is an emergency management standard comparable to FEMA NFPA 1600 (US), or BS25999-1 Business Continuity Management (UK).
handysektor
Type of Activity: Non-government Initiative
Responsible Organization(s): The State Media Authority of Rhineland-Palatinate (LfM); Research Association for Media Education (mpfs)

ENISA Focus Points: AR
Weblink: http://www.handysektor.de/
Description: Handysektor is a Website that provides information to teenagers, parents, and teachers about security issues related to online access via mobile devices.
A4M – Academia for the Masses
Type of Activity: Non-governmental Initiative
Responsible Organization(s): Horst Görtz Institute for IT Security, Dublin City University, University of Oviedo, SODERCAN
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises
Weblink: http://www.security4business.eu/
Description: This knowledge distribution initiative, partly financed by the EU, involves the development of an elearning platform for small companies in the field of IT security.
Deutschland sicher im Netz (DsiN) – Germany Secure in the Web
Type of Activity: Government Policies
Responsible Organization(s): under the auspices of the BMI
ENISA Focus Points: AR, Micro-enterprises
Weblink: https://www.sicher-im-netz.de/Default.aspx
Description: This initiative aims to raise awareness of IT security in small and medium-sized enterprises, e.g., drawing attention to the necessity for a secure ecommerce system.
Anti Spam Task Force (ASTF)
Type of Activity: Non-government Initiative
Responsible Organization(s): eco, Federation of German Consumer Organizations, Center for Protection against Unfair Competition, Federal Network Agency
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: http://www.eco.de/initiativen/1463.htm
Description: Through its Anti-Spam Task force the Internet industry is seeking to provide ISPs with information on measures to combat spam and to suggest concepts for reducing the nuisance to users from unsolicited emails without affecting transmission of legitimate emails.

ehealthcard (eGK)
Type of Activity: Government Policies
Responsible Organization(s): Federal Ministry of Health
ENISA Focus Points: e-ID
Weblink: http://www.bmg.bund.de/nn_1210508/DE/Gesundheit/Gesundheitskarte-Focuspage/gesundheitskarte__node.html
Description: The eHealth card project started in 2005. The plan is to deliver the card to all 72 million customers of the health insurance companies in Germany, which give access to state health care. The release is planned in different steps in which the functionalities of the eGK should be tested. Release 0: lab test; Release 1: offline in test regions; Release 2: online, basic functionalities; Release 3: additional functionalities (e.g. patient record, pharmaceutical documentation). Since 2006, the eGK has been tested in seven regions as part of Release 1. The rollout for Release 2 is due to take place during 2009, while Release 3 is planned for 2010.

Bürger-CERT – Citizen-CERT
Type of Activity: Government Policies
Responsible Organization(s): BSI
ENISA Focus Points: AR
Weblink: http://www.buerger-cert.de/ , http://www.bsi-fuer-buerger.de
Description: On the Bürger-CERT platform, members of the public and responsible staff in small companies can receive information regarding viruses, worms, and other computer security risks.

Research Programs

CarmentiS Project
Type of Activity: Technical Research Programs
Responsible Organization(s): CERT Network; BSI
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: http://www.cert-verbund.de/carmentis/index.html
Description: Implementation of the technical and organizational infrastructure for a national early warning information system, identifying current and emerging risks.

German Advisory Format (DAF)
Type of Activity: Social & Other Research Programs
Responsible Organization(s): CERT-Network
ENISA Focus Points: CERT
Weblink: http://www.cert-verbund.de/daf/daf_description.html#eispp_v2.0
Description: DAF is an initiative of the German CERT-Network and a core component of an infrastructure for the generation of security advisories. DAF is tailored to the needs of German CERTs. Its security advisories goals are: improving the quality of advisories; quality assurance; developing of a model for system description; establishing a common rating scheme; and releasing resources for better analysis capabilities. DAF is based on the EISPP advisory format.
SIRIOS Project
Type of Activity: Technical Research Program
Responsible Organization(s): CERT-Bund
ENISA Focus Points: CERT
Weblink: http://www.sirios.org/
Description: The main goal of the SIRIOS project is the development of an open-source incident handling and vulnerability management system that fulfils the needs of computer emergency response teams.
Arbeitsgruppe Identitätsschutz im Internet (a-i3) – Workgroup for Identity Protection on the Internet
Type of Activity: Social & Other Research Programs
Responsible Organization(s): Ruhr University of Bochum
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: https://www.a-i3.org/
Description: ai3 is a multidisciplinary organization that conducts research aimed at enhancing security solutions for Internet users.

Funding Programs & Financial Initiatives

Klicksafe.de

Type of Activity: Government Funding Programs

Responsible Organization(s): State Media Authority of Rhineland-Palatinate (LMK), Media Authority of Northrhine-Westfalia (LfM), European Center for Media Competence

ENISA Focus Points: AR

Weblink: http://www.klicksafe.de

Description: The German awareness node Klicksafe.de is part of the European Internet safety network INSAFE within the framework of the Safer Internet Program, which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight illegal content and content unwanted by the end user, as part of a coherent approach by the European Union.

Events

Conferences and Workshops

Common Criteria Workshops

Responsible Organization: BSI	Frequency: Monthly

ENISA Focus Points: Micro-enterprises, Implementation of Security Technology and Standards

Target Groups: Major – security professionals; Minor – SMEs, large enterprises, government organizations, educational and research organizations

Weblink: http://www.bsi.bund.de/zertifiz/aktuell/ccworkshop.htm

Description: A monthly workshop on common criteria for the examination and evaluation of IT security.

IT-Grundschutz-Tag

Responsible Organization: BSI	Frequency: Every two Months

ENISA Focus Points: Micro-enterprises, Implementation of Security Technology and Standards

Target Groups: Major – government institutions, large enterprises, security professionals; Minor – SMEs, educational and research organizations

Weblink: http://www.bsi.bund.de/veranst/index.htm	
Description: Workshop on management tools for information security.	
IT Incident Management and IT Forensics 2008	
Responsible Organization: German Informatics Society (GI)	Frequency: Annual
ENISA Focus Points: Emerging/Current Risks	
Target Groups: Government institutions, large enterprises, security professionals, educational and research organizations	
Weblink: http://www.gi-ev.de	
Description: The special interest group, Security Intrusion Detection and Response (SIDAR), of the GI organizes an annual conference providing a platform for experts from throughout the world, to discuss the state of the art in the areas of IT security incident management and IT forensics (IMF). IMF promotes the collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies. The IMF conference will be held for the fourth time in 2008. The concept has matured from a purely academic event to an academic track section complemented by practical workshops.	
DFN-Workshop	
Responsible Organization(s): DFN, DFN-CERT	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major – educational and research organizations; Minor – SMEs	
Weblink: http://www.dfn-cert.de/veranstaltungen/workshop.html	
Description: Workshop with extensive focus on network security, emerging risks, RFID-security, data protection, security of web-based applications, intrusion detection and prevention, and identity management.	
Deutscher Anti-Spam-Kongress (German Anti Spam Summit)	
Responsible Organization(s): eco, Contact Network of Spam Authorities (CNSA), the London Action Plan (LAP), Hessen-IT and ENISA	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major – large enterprises, SMEs; Minor – consumers, government organizations, education and research organizations	
Weblink: http://www.eco.de/antispamsummit2008	

Description: This two-day international conference is held in English and has a different theme each year, with recent events focusing on phishing, lottery spam, and other advance fee frauds committed via e-mail. Speakers represent law enforcement agencies, industry, watchdog organizations, and universities.
Deutscher IT-Sicherheitskongress (German IT Security Congress)
Responsible Organization(s): BITCOM, BSI — Frequency: Biennial
ENISA Focus Points: CERT, AR, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards
Target Groups: Major – SMEs, large enterprises, security professionals
Weblink: http://www.bsi.bund.de/veranst/IT-SiKongress/index.htm
Description: German IT-security conference. Topics include: Internet security; CERT; Next Generation Networks; secure communication; mobile security; e-ID; secure platforms; embedded systems security; and management of IT-security.
Systems – IT Security Forum
Responsible Organization: Messe München GmbH — Frequency: tbd
ENISA Focus Points: AR, Emerging/Current Risks
Target Groups: SMEs, large enterprises, security professionals
Weblink: http://www.systems.de/
Description: The event consists of 200 presentations divided into two forums. In the "Blue Forum", technical experts (including CIOs, IT security directors, computing center directors, and administrators) are offered detailed knowledge, discuss new developments, and explore new trends for IT experts. The "Red Forum" provides managers with fundamentals, new ideas, and assistance with basic planning. Business decision-makers also find information about how and why they should make IT security investments. There will be no “Systems” in the future, the “Systems 2008” was the last one, however the Security Forum will continue, but at this point of time it hasn’t been decided yet in which form and with which frequency.
ISEB-Workshop
Responsible Organization: Institute for E-Business Security (ISEB), supported financially by Horst Görtz Institute for IT-Security — Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards

Target Groups: Major – SMEs, large enterprises, security professionals; Minor – educational and research organizations
Weblink: http://www.iseb.ruhr-uni-bochum.de/workshop/index.shtml
Description: The ISEB Workshop has a different theme each year, with recent events focusing on: information security in the healthcare sector; information security in banking and insurance; IT security and consulting; IT security in practice.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the last 12 months 5 security breaches were reported in Germany:

1. In June 2008, residential rolls on half a million people became freely accessible on the Internet. The rolls, which list names, dates of birth, marital status, and religious affiliation, are normally protected by passwords. HSH, the company that supplied the software and maintained the databases, admitted that a non-secret password had applied to rolls kept by 15 local authorities. The password was in software documentation on the web. After the error was discovered, new, secret passwords were adopted.

   http://www.earthtimes.org/articles/show/214379,germany-accidentally-reveals-residential-rolls-on-internet.html

2. In July 2008, the scientific journal of the Chaos Computer Club (CCC), Die Datenschleuder, reported that market research firm TNS Infratest/Emnid lost 41,000 private data records of survey participants. This made it possible for participants to read master data records and consumer profiles without bypassing even the most basic security measures. Access to the comprehensive survey results could be gained by simply changing the customer ID number in the browser's address bar. Names, addresses, birth records, email addresses, and phone numbers were made available by the slip-up. Other sensitive was also available, including: monthly income; education; bank account information; health insurance data; credit card use; household electronic devices; and ages of children.

   http://www.ccc.de/updates/2008/umfragetief?language=en

3. In August 2008, Best Western hotels confirmed three separate attempts were made via a single log-on ID to access the same data from a single hotel, the Best Western Hotel am Schloss Kopenick in Berlin. The hotel's antivirus software detected a Trojan horse virus, and Best Western immediately terminated the account and disconnected the affected PC from the network, according to the statement. News of the breach first surfaced in Scotland's *Glasgow Sunday Herald*, which claimed that an Indian hacker devised a method for breaking into Best Western's online booking system and then sold this information to Russian mafia operatives. According to *The Herald*, the attack revealed personal data on approximately 8 million customers who stayed at one of the chain's 1,312 European hotels since 2007, including home addresses, telephone numbers, credit card data, and employment details.

   http://www.crn.com/security/210201135

4. In September 2008, a call center whistleblower, Detlef Tiegel, handed a CD containing the banking details of some 17,000 German citizens over to the authorities. The information in question was obtained by an unidentified company that had employed Tiegel. The initial 17,000 records were only a fraction of the roughly 1.5 million records Tiegel claimed he could produce. German officials took Tiegel's claims seriously enough to open their own investigation, and were dismayed when they were able to purchase 6 million records of personally identifiable information (PII) for €850 ($1,220).

   http://whistlersear.wordpress.com/2008/09/09/good-for-germanywhistleblowers-get-results/

5. In October 2008, T-Mobile confirmed that an error in their system exposed the confidential data of 30 million customers. The data breach, which included bank account information, was accessible online. T-Mobile quietly introduced a new

security system that immediately closed the security hole and assured customers that no theft of the exposed data had occurred.

http://www.boygeniusreport.com/2008/10/13/t-mobile-germany-exposes-confidential-data-for-30-million-customers/

Country Report – Greece

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Athens
Total area:	131 957 sq.km
Population:	11.1 million
Official language:	Greek
Time zone:	EET (GMT+2)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Greece, we present a set of three indicators in the Country Highlights section.

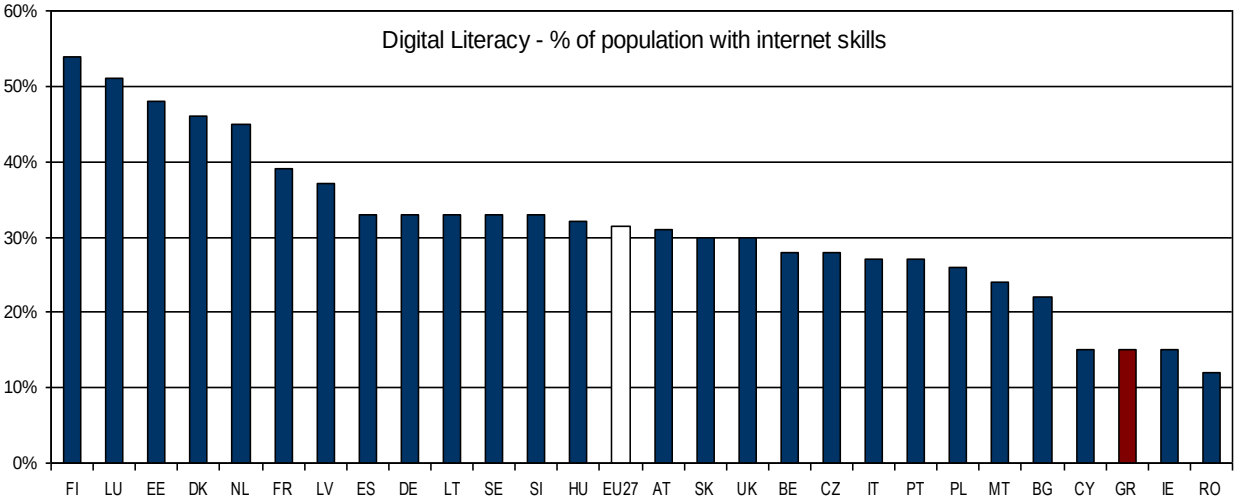
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Greece is fundamental to this NIS study.

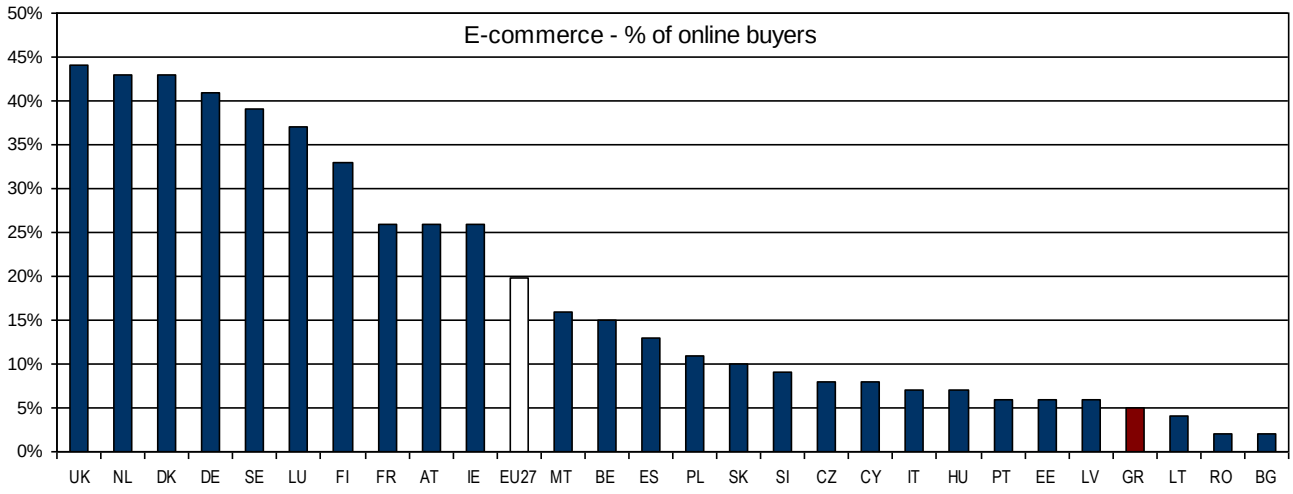
The availability of online services in Greece keeps increasing both in public and private sectors. The level of digital literacy and ICT skills experienced a steady improvement over the past decade.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

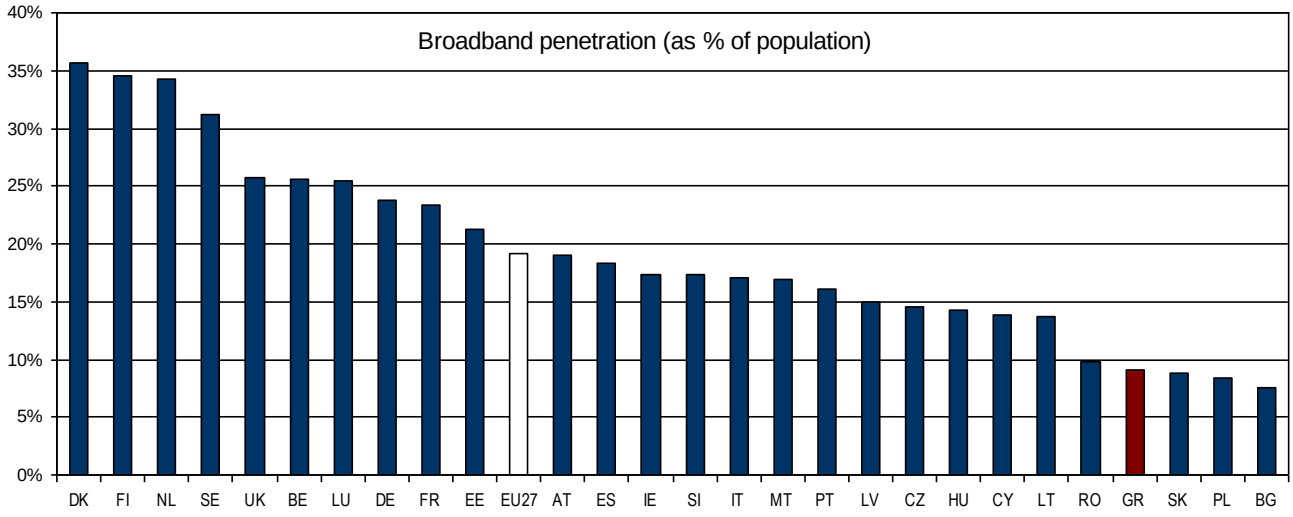
Digital Literacy Indicator



eCommerce Indicator



Broadband penetration Indicator



NIS Highlights

Greece does not have a single institution recognized among NIS stakeholders as the national security agency; there are various organizations sharing the responsibilities and competencies concerning the classified information.

The Ministry of Transport and Communications is responsible for coordinating the development and implementation of national information society strategy, including those

aspects relating to information security. The Ministry of Interior, Ministry of Economy and Finance, and the Ministry of Development are also taking responsibility for the development and implementation of national information security policy.

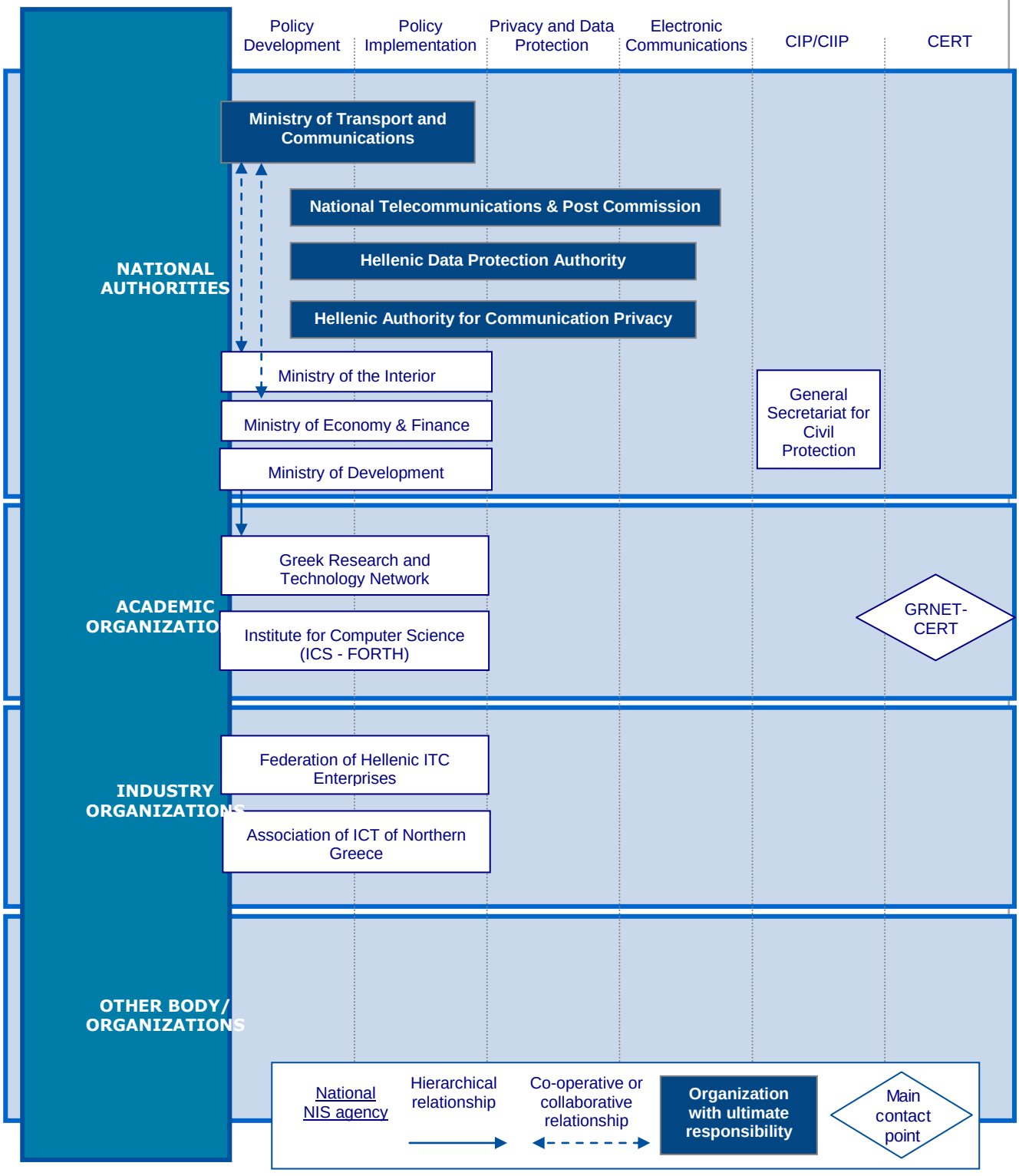
Greece is committed to data protection and ensuring compliance in this regard. National Telecommunications & Post Commission (EETT), Hellenic Authority for Communication Privacy (ADAE) and Hellenic Data Protection Authority are the bodies responsible for this task. They cover various tasks in the data and privacy protection. In addition, the National Telecommunications & Post Commission oversees the implementation of electronic communications legislation.

Greece has security response teams in place to handle security breaches and other incidents. GRNET-CERT is the Greek Research and Technology Network (GRNET) Computer Emergency Response Team. GRNET provides network services to all educational and research institutions. GRNET-CERT responds to security incidents that involve its constituency and cooperates with respective incident response teams. GRNET-CERT is a member of the Terena TF-CSIRT (Task Force of Computer Security Incident Response Teams) and an accredited member of Trusted Introducer, the trusted network for CSIRTs or CERTs in Europe.

The country hosts a number of security related events every year that are organized by the industry stakeholders and research centers. There are several projects currently underway in the country related to Internet security and various research programs aiming at developing security standards.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Greece. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Transport and Communications		X	X	X	X	X	X	X
Ministry of the Interior		X	X	X	X	X	X	X
Ministry of Economy and Finance		X	X	X	X	X	X	X
Ministry of Development		X	X	X	X	X	X	X
National Telecommunications & Post Commission		X	X	X	X	X	X	X
Hellenic Authority for Communication Privacy		X	X	X	X	X	X	X
Hellenic Data Protection Authority		X	X	X	X	X	X	X
Federation of Hellenic ICT Enterprises		X	X	X	X	X	X	X
Association of ICT of Northern Greece		X	X	X	X	X	X	X
GRNET-CERT,	X							
General Secretariat for Civil Protection								X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Greece:

National Authorities in Network and Information Security	
Ministry of Transport and Communications	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Develop Policy with GSPA and GSIS	
Weblink: http://www.yme.gov.gr	
Areas of Activity: Planning and implementing national policy and creating the appropriate institutional framework at European and international levels for the development of top quality telecom and postal services under conditions of healthy competition.	
Ministry of the Interior, Public Administration and Decentralisation, General Secretariat for Public Administration and Electronic Governance	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Develop Policy with Ministry of Transport and Communication and GSPA	
Weblink: http://www.gspa.gr	
Areas of Activity: The main responsibilities of the ministry include: development of the national framework, monitoring and providing guidance on the structure and operations of all public organizations that are responsible for citizens' supports; building and monitoring the business plan of "Information Society" project regarding research, projects and actions referring to Electronic government and value added services to the citizens	
Ministry of Economy and Finance, General Secretariat for Information Systems	
Type of Organisation: National Government	Ownership: Public

ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Relationships: Develop Policy with Ministry of Transport and Communication and GSPA
Weblink: http://www.e-oikonomia.gr
Areas of Activity: The main responsibilities of the ministry include: development of new electronic systems for economic purposes for the citizens; building a new IT Data centre for providing data information; and supporting internet citizens, enterprises and public authorities.

Ministry of Development, General Secretariat for Research and Technology	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.gsrt.gr	
Areas of Activity: The organization supports R&D activities, establishes institutes and research organizations around IT and new technologies, encourages cooperation between different organizations and promotes advanced technologies.	

National Telecommunications & Post Commission (EETT)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.eett.gr	
Areas of Activity: EETT is the National Regulatory Authority, which supervises and regulates the telecommunications as well as the postal services market. EETT's institutional purpose is to promote the development of the two sectors, to ensure the proper operations of the relevant market in the context of sound competition, and to provide for the protection of the interests of the end-users.	

Hellenic Authority for Communication Privacy (ADAE)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, Resilience, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.adae.gr	
Areas of Activity: The Hellenic Authority for the Information and Communication Security and Privacy (ADAE) has been established to protect the secrecy of mailing, the free correspondence or communication in any possible way as well as the security of networks and information. The concept of privacy encompasses the control of observing and regulating the terms and processes of waiving of privacy protection rights as foreseen by the law.	

Hellenic Data Protection Authority	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.dpa.gr	
Areas of Activity: Principal scope of the activities of the Authority is to protect the personal data of the citizens and to prevent the illegal elaboration of them.	

Industry Organisations Active in Network and Information Security

Federation of Hellenic Information Technology & Communications Enterprises (SEPE)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.sepe.gr	

Areas of Activity: The main activities of the associations include: to cooperate with National Bodies for building up National Strategy on Digital Technology, to plan and support projects for the needs of SMBs to increase their competitiveness in Greek market, to support the research for development in all areas of IT and Communication, and to encourage the cooperation between IT Universities and other bodies of the segment.

Association of Information Technology Companies of Northern Greece (SEPVE)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID	
Relationships: None	
Weblink: http://www.sepve.org.gr/	
Areas of Activity: The main activities of the associations include (in Northern Greece): to cooperate with National Bodies for building up National Strategy on Digital Technology, to plan and support projects for the needs of SMBs to increase their competitiveness in Greek market, to support the research for development in all areas of IT and Communication, and to encourage the cooperation between IT Universities and other bodies of the segment.	

Academic Organisations Active in Network and Information Security

Institute for Computer Science (ICS)	
Type of Organisation: University	Ownership: Non-profit
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID,	
Relationships: Part of Foundation For Research and Technology - Hellas (FORTH)	
Weblink: http://www.ics.forth.gr	
Areas of Activity: Research and development areas encompassing new perspectives, emerging fields of research and technological challenges.	

Greek Research and Technology Network (GRNET)	
Type of Organisation: Research Centre	Ownership: Public-Private Partnership
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID,	

Relationships: Part of Ministry of Development, cooperates with General Secretariat for Research and Technology
Weblink: http://www.grnet.gr
Areas of Activity: The objective of GRNET S.A. concerns the provision of advanced Internet services to academic and research institutions and organizations of similar activities, along with the wider promotion of innovative Internet applications with the participation of relevant national and communal projects.

Other Bodies and Organisations Active in Network and Information Security

SafeNetHome

Type of Organisation: CIIP Body	Ownership: Non-profit
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks, e-ID, Implementation of Security Technology and Standards	
Relationships: In cooperation with GSPA and Ministry of Finance and Research Universities and organizations	
Weblink: http://www.saferinternet.gr	
Areas of Activity: Scope of Safer Internet is to inform all Greek citizens for the methods and regulations that exist and can help to protect themselves and their children from unsafe and incorrect usage of internet, mobiles and information technologies.	

Safeline

Type of Organisation: CIIP Body	Ownership: Non-profit
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks, e-ID, Implementation of Security Technology and Standards	
Relationships: In collaboration with Safenet, FORTH and FORTHnet	
Weblink: http://www.safeline.gr	
Areas of Activity: SafeLine is a hotline accepting reports concerning websites or newsgroups on the Internet that contain images of child abuse, racist and xenophobic content that violates the Greek law, and other illegal content.	

General Consumers' Federation of Greece (INKA)	
Type of Organisation: Other organization	Ownership: Non-profit
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID	
Relationships: None	
Weblink: http://www.inka.gr	
Areas of Activity: The main activities of the federation include informing and educating consumers and propose regulations and laws for consumer's rights and protections.	

Consumers' Protection Center (KEPKA)	
Type of Organisation: Other organization	Ownership: Non-profit
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks	
Relationships: None	
Weblink: http://www.kepka.org	
Areas of Activity: Tasks: Informing citizens about their rights and how they can claim them; organization of events and meetings to educate consumers on their rights and issues they are facing; representing consumers at national and international bodies and offices for education and complaints.	

Association for the Quality of Life (E.K.PI.ZO)	
Type of Organisation: Other organization	Ownership: Non-profit
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks	
Relationships: None	
Weblink: www.ekpizo.gr	
Areas of Activity: EKPOIZO is acting in the following dimensions: Inform and educate consumers, propose regulations and laws for consumers' rights and protections, put pressure for the implementation of current legislation.	

Activities

Strategic Initiatives
Safer Internet Plus
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): SaferINternet
ENISA Focus Points: CERT, Awareness Raising, Micro- enterprises
Weblink: N/A
Description: The programme has four main actions: Fighting against illegal content, tackling unwanted and harmful content, promoting a safer environment, and awareness raising.
SafeNet Home Plus
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): SaferINternet
ENISA Focus Points: CERT, Awareness Raising, Micro- enterprises
Weblink: N/A
Description: The goal of the program is to inform parents about the ways they can protect themselves as well as their children from the dangers resulting from the new interactive technologies, such as the Internet and the mobile phones.
Information Security Programme
Type of Activity: Government funding program
Responsible Organisation(s): FORTH
ENISA Focus Points: CERT, Resilience, Awareness Raising, Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: N/A

Description: Program aims at addressing security issues in modern information systems, while storing, processing, communicating, and sharing information. Security relates to both technological aspects of information systems, as well as to social, economic, and law issues. The main research areas addressed by the programme are: Network security, computer systems security, authentication of high volumes of data in non-trusted distributed environments, and cryptographic algorithms and digital signatures.
Privacy Security of Communications and Self-privacy of Users and Subscribers
Type of Activity: Non-governmental initiative
Responsible Organisation(s): ADAE
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, e-ID, Implementation of Security Technology and Standards
Weblink: N/A
Description: Series of roadshows in Universities with two main topics: IT Development in Communication Security and Self-Privacy at e-Communication.
School Visits
Type of Activity: Non-governmental initiative
Responsible Organisation(s): Safeline - Safenet - FORTHnet
ENISA Focus Points: CERT, Awareness Raising, Emerging and Current Risks
Weblink: N/A
Description: Aim to raise the hotline visibility to the younger ages. Through conversation, pupils are encouraged to report any illegal content they spot and learn where they can be informed for the safer use of the internet.
Ambient Intelligence Programme
Type of Activity: Governmental Funding Program
Responsible Organisation(s): ICS
ENISA Focus Points: Micro- enterprises, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: N/A

Description:

To improve the quality of life of all citizens of the emerging Information Society through the creation and provision of safe, efficient and user-friendly technologies, which support and cater to the needs of each and every individual user in a seamless, unobtrusive and invisible way.

Research Programmes

Network Coding for Robust Architectures in Volatile Environments

Type of Activity: Technical Research Program

Responsible Organisation(s): Centre for Research and Technology - Hellas

ENISA Focus Points: CERT, e-ID, Development of Security Technology and Standards Policy

Weblink: N/A

Description:

The program aims at developing solutions for architecting and controlling wireless networks in performance-challenged and resource-constrained environments. Positive ramifications in security will be used to fortify confidentiality, secrecy and resilience to data corruption and other threats.

Unobtrusive Authentication Using Activity Related and Soft Biometrics

Type of Activity: Technical Research Program

Responsible Organisation(s): Centre for Research and Technology - Hellas

ENISA Focus Points: e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards

Weblink: N/A

Description:

Program aims at developing a novel activity related and soft biometrics technologies for substantially improving security, trust and dependability of "always on" networks and service infrastructures. The goal is to integrate biometric technologies in Ambient Intelligence security infrastructures in order to support continuous authentication and monitoring. Emphasis will be on the unobtrusiveness of the approach and the universal usage of such a system.

Mobile Peer-to-Peer Security Infrastructure

Type of Activity: Technical Research Program

Responsible Organisation(s): ATHENS TECHNOLOGY CENTER

ENISA Focus Points: CERT, Emerging and Current risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: N/A
Description: The project will address issues related to security, privacy, trust and access control in mobile peer-to-peer (p2p) systems by proposing relevant framework architecture. The framework will include support for policy-based security management for mobile systems.

Ad-hoc PAN and Wireless Sensor Secure Network
Type of Activity: Technical Research Program
Responsible Organisation(s): EAV
ENISA Focus Points: CERT, Resilience, Emerging and Current risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: N/A
Description: Project focused on security and resilience across ad-hoc PANs and wireless sensor networks to implement and validate a scalable, secure, trusted networking protocol stack, able to offer self-configuration and secure roaming of data and services over multiple administrative domains and across insecure infrastructures of heterogeneous ad-hoc and wireless tiny sensory networks.

Events

Conference and Workshops	
Information Security Matrix Forum	
Responsible Organisation: Hellenic American Union	Frequency:
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, e-ID, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.securitymatrix.net/	
Description: An international forum, bringing together the most respected names & leading specialists in information security. The forum is designed for information security managers, directors and staff, analysts, engineers, network and system administrators, CIOs, and anyone involved in information security in their organization.	

Athens International Forum on Security	
Responsible Organisation: Hellenic American Union	Frequency: annual
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://conferences.hau.gr/?i=aifs2008	
Description: AIFS aims to provide a fresh, in-depth look into information security technologies, policies, techniques, and best practices, and to help all parties involved, from front-line IT personnel to policy makers, gain valuable insights into key information security issues.	

Pan-Hellenic Conference on Informatics	
Responsible Organisation: PCI	Frequency: annual
ENISA Focus Points: Resilience, Emerging and Current Risks, e-ID, Development of Security Technology and Standards Policy	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.icsd.aegean.gr/pci2008/index.html	
Description: The PCI 2008 Conference will run in parallel sessions, with invited talks, research and case study tracks to cover topics in the areas of informatics, computer science, computer engineering, telecommunications, and information systems.	

International Wireless Communications and Mobile Computing Conference	
Responsible Organisation: National Telecommunications & Post Commission (EETT)	Frequency: annual
ENISA Focus Points: CERT, Emerging and Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://dropzone.tamu.edu/%7Exizhang/IWCMC2008/IWCMC08.html	

Description: "Next Generation Techniques of Wireless Communications and Mobile Computing/Networking". The conference aims to promote further research interests and activities on computer, network and wireless security, and to increase the synergy between academic and industrial researchers working in this area.

Workshop in Information Security Theory & Practices	
Responsible Organisation: National Telecommunications & Post Commission (EETT)	Frequency: annual
ENISA Focus Points: CERT, Emerging and Current Risks, e-ID, Development of Security Technology and Standards Policy	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://wistp2007.xlim.fr/index.php?id=55	
Description: The goal of the workshop is to bring together researchers and practitioners in related areas and to encourage interchange and cooperation between the research community and the industrial/consumer community.	

Summer School on Network & Information Security	
Responsible Organisation: ENISA - Institute of Computer Science of the Foundation for Research and Technology – Hellas	Frequency: annual
ENISA Focus Points: Resilience, Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.nis-summer-school.eu/	
Description: Summer School themes and topics to be decided at a yearly basis. For 2008, the theme was Security and it covered topics as: Emerging and future threats, security of network technologies and protocols, security in next generation networks, wireless access network security, legal/policy issues related to network security, etc.	

Exposec	
Responsible Organisation: Information Society	Frequency: annual

ENISA Focus Points: CERT, Resilience, Awareness Raising, Emerging and Current Risks, Micro-enterprises, e-ID, Implementation of Security Technology and Standards
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions
Weblink: http://www.infosoc.gr/infosoc/el-GR/grafeiotypou/events/agenda_opis/exposec_01-04-2008.htm
Description: The topic of the event is home & corporate security.

Conference on IT Systems & Solutions at Helexpo	
Responsible Organisation: Federation of Hellenic Information Technology & Communications Enterprises (SEPE) - The Association of Information Technology Companies of Northern Greece (SEPVE)	Frequency: annual
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, Micro-enterprises, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: www.helexpo.gr/infosystem/2008/sinedrio08.htm	
Description: The conference focuses on synergies for IT technologies & communication.	

Media Campaigns

SaferInternet	
Responsible Organisation: SaferInternet	Frequency:
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.saferinternet.gr/	

Description:

TV awareness campaign with the broadcasting of five TV spots and two cards.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Greece.

Country Report – Hungary

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Budapest
Total area:	93 000 sq.km
Population:	10.1 million
Official language:	Hungarian
Time zone:	CET (GMT+1)
Currency:	Forint (HUF)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Hungary, we present a set of three indicators in the Country Highlights section.

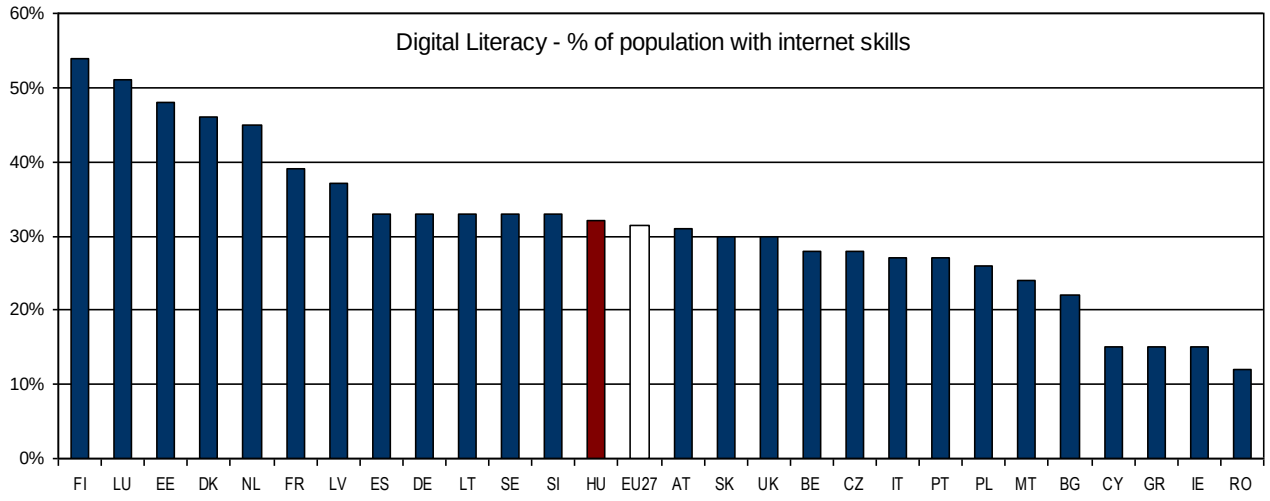
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Hungary is fundamental to this NIS study.

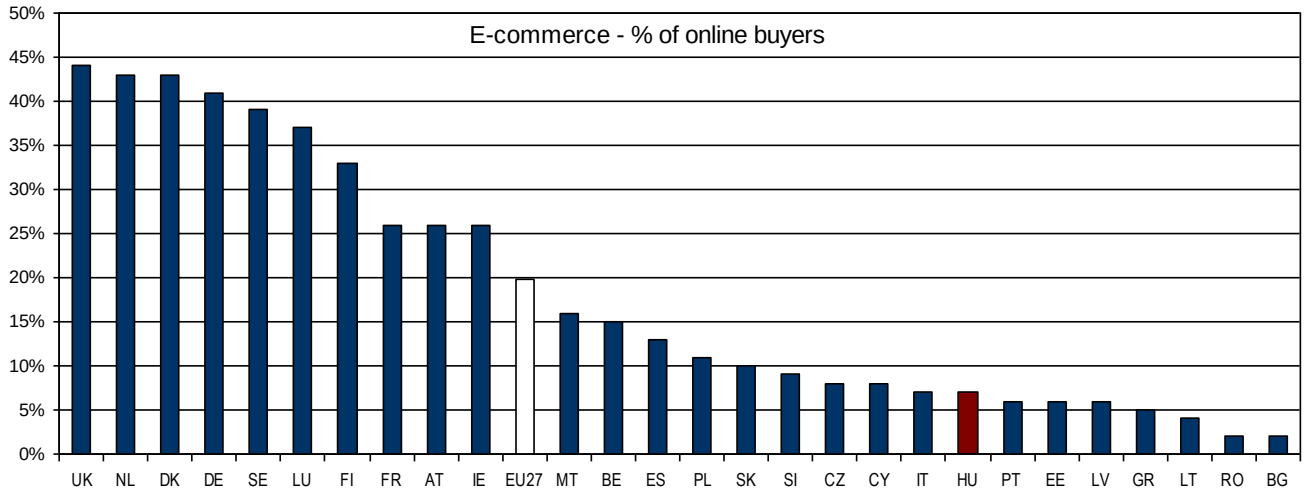
Hungary does all the necessary efforts and raise program in order to develop e-Government services, increase the number of Internet users and improve the skills in digital technologies. ICT, e-government and digital literacy indicators are catching up on the EU average fast.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

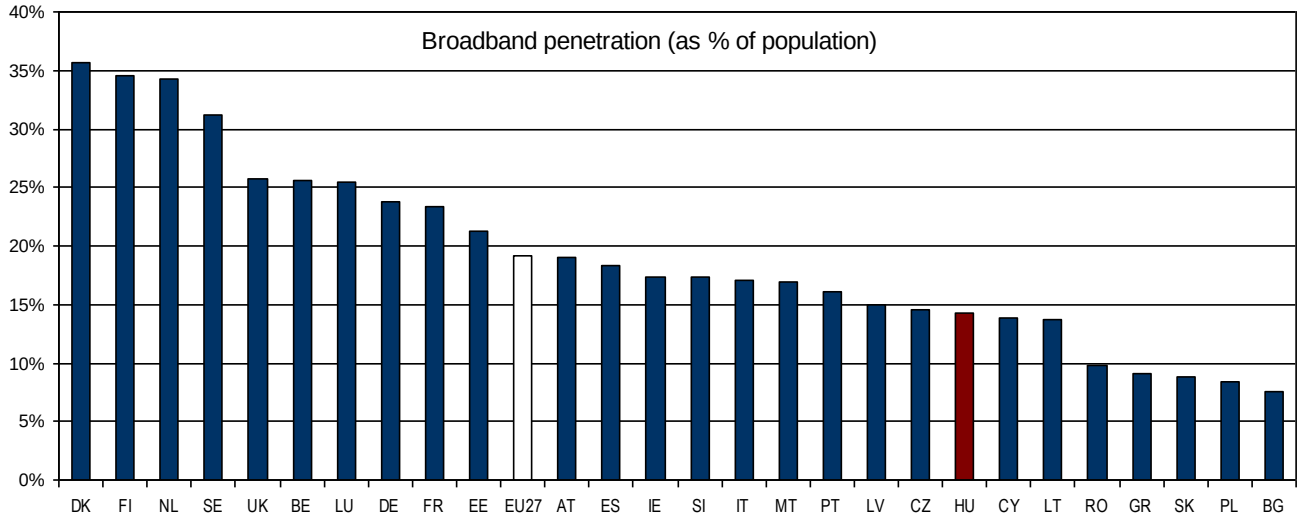
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Hungary does not have one single institution recognized among NIS stakeholders as the national security agency; there are various organizations sharing the responsibilities. The National Board for Communications and Information Technology is an advisory board of

the government advising it on information technology strategic topics and taking the responsibility for the development of national information society strategy, including those aspects relating to information security.

The Electronic Government, subordinated directly to the Prime's Minister Office, oversees the implementation of information society and technology policy among governmental organizations and education institutions. The National Communication Authority is responsible for the implementation of electronic communications legislation.

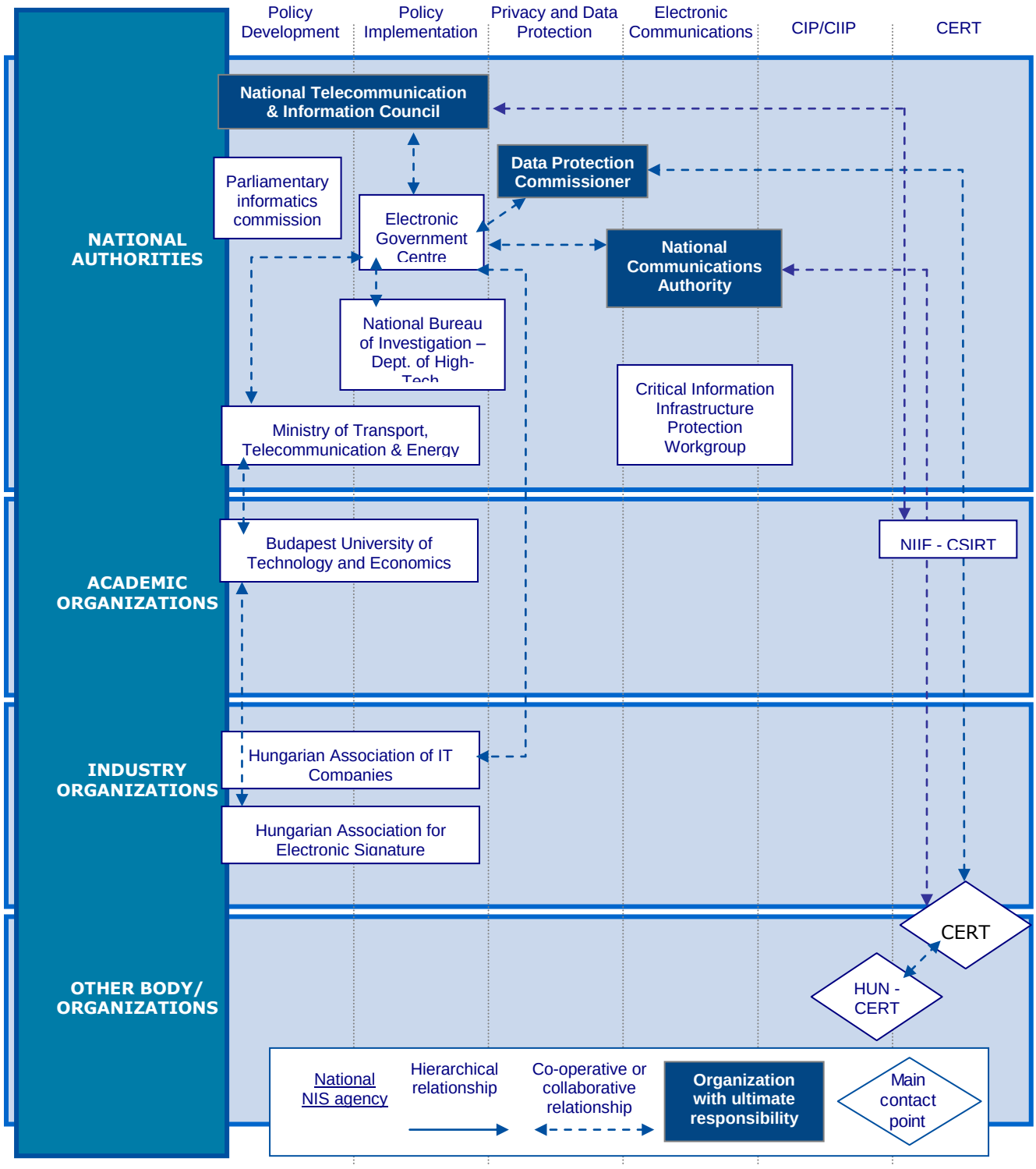
Hungary is committed to data protection and ensuring compliance in this regard. The Data Protection Commissioner of Hungary is an independent oversight body responsible for this task. The organization is also charged with maintaining a register of databases, investigating complaints, imposing fines for violations, conducting audits, providing consultations on data protection, and commenting on legislative proposals.

Additionally, Hungary has security response teams in place to handle security breaches and other incidents. The CERT is the incident management center of the Hungarian government; its task is to support the IT security of the Hungarian government and the business sector. It also serves as a knowledge center for private citizens and security professionals.

The country hosts a number of conferences on NIS. Events are organized by stakeholders in the public sector, industry organizations, and the business and academic communities.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Hungary. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholder activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Name of Key Stakeholders	CERT	Resilience	Awareness Raising (AR)	Emerging/Current Risks	Micro-enterprises	e-ID	Development of Security Technology and Standards	Implementation of Security Technology and Standards
National Telecommunication And Information Council			X			X	X	X
Electronic Government Centre		X					X	
Data Protection Commissioner of Hungary			X				X	
National Communications Authority Hungary		X						
CERT-Hungary	X							
Critical Information Infrastructure Protection Workgroup			X			X	X	X
National Bureau of Investigation			X	X				
Ministry of Transport, Telecommunication and Energy			X				X	
Hungarian Association of IT Companies			X			X		

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Hungary:

National Authorities in Network and Information Security

Electronic Government Centre (MEH EKK)

Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy	
Relationships: Part of Prime Minister's Office; cooperates with Data Protection Commissioner of Hungary; National Communications Authority Hungary; Ministry of Transport, Telecommunications and Energy; NHIT; National Telecommunications and Information Council; National Association for Consumer Protection in Hungary (NACPH-OFE); and Hungarian Association of IT Companies (IVSZ)	
Weblink: http://www.ekk.gov.hu/	
Areas of Activity: The organization's main focus is the implementation of egovernment and the supervision of IT development on the local and national government level to comply with regulations of the egovernment framework.	

Data Protection Commissioner of Hungary

Type of Organization: Other Public Bodies	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy	
Relationships: Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK); National Communications Authority Hungary; CERT-Hungary; Ministry of Transport, Telecommunications, and Energy; NHIT; National Telecommunications and Information Council, and National Association for Consumer Protection in Hungary (NACPH-OFE).	
Weblink: http://abiweb.obh.hu/abi/	
Areas of Activity: The organization is responsible for the oversight of data handling legality on all levels, as well as access to public information. The Data Protection Commissioner is independent from the government, other state organizations, and the private sector. The commissioner may make recommendations for new regulations and for the amendment of legislation pertaining to data control, and may express his opinion on drafts covering the same subject. The commissioner informs the public about citizens' right to information and the risks of breaching said rights by means of the commissioner's own publications, and with the help of the press, radio, and television. The commissioner supports teaching in this field and related scientific research.	

National Communications Authority Hungary	
Type of Organization: Other Public Bodies	Ownership: Public
ENISA Focus Points: Resilience	
Relationships: Cooperates with Data Protection Commissioner of Hungary; Prime Minister's Office; Electronic Government Centre (MEH EKK); CERT-Hungary; Ministry of Transport, Telecommunications, and Energy; NHIT; National Telecommunications and Information Council; National Association for Consumer Protection in Hungary (NACPH-OFE); and Hungarian Association of IT Companies (IVSZ)	
Weblink: http://www.nhh.hu	
Areas of Activity: The organization is a regulatory authority of the Hungarian telecommunications market. The authority is responsible for encouraging and supporting the smooth and successful operation and development of the electronic communications, postal, and IT markets. The authority protects the interests of both service providers and users. Its duties are to establish and maintain fair and efficient competition and to supervise legal compliance on the behalf of service providers. The authority participates in the activities of international organizations connected with electronic communications, post, and informatics and establishes and maintains relations with regulatory authorities and organizations in and outside Europe.	

National Bureau of Investigation	
Type of Organization: National Security Actor	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK); and dedicated division within the National Police	
Weblink: http://www.police.hu	
Areas of Activity: The Department of High-Technology Crime functions as a cyber-crime unit.	

Ministry of Transport, Telecommunications, and Energy	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy	
Relationships: Cooperates with Data Protection Commissioner of Hungary; National Communications Authority Hungary; NHIT; National Telecommunications And Information Council; National Association for Consumer Protection in Hungary (NACPH-OFE); CERT-Hungary; Ministry of Transport, Telecommunications, and Energy; and Barátságos Internet	

Weblink: http://www.khem.gov.hu
Areas of Activity: Ministry of Transport, Telecommunications, and Energy is a government body imposing regulations on the ICT market. The ministry focuses on the development of domestic and international market environments and on the regulation and support policies regarding info-communication infrastructure and domestic econtent.

Parliamentary Informatics Commission	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK)	
Weblink: www.parlament.hu	
Areas of Activity: Special commission of the parliament focused on information policy development.	

National Board for Communications and Information Technology (NHIT)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK); Ministry of Transport, Telecommunications, and Energy; National Communications Authority Hungary; NIIF-CSIRT; and Hungarian Association of IT Companies (IVSZ)	
Weblink: http://www.nhit.hu/	
Areas of Activity: The National Board for Communications and Information Technology (NHIT) is a government body with the task of formulating opinions and making recommendations; it was established by the government to cooperate on tasks relating to info-communication (information technology, telecommunications, media) on the basis of applicable law.	

MSZT – Hungarian Standards Institutions	
Type of Organization: Other Public Bodies	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK); Ministry of Transport, Telecommunications and Energy; and National Communications Authority Hungary	

Weblink: http://www.mszt.hu/
Areas of Activity: Hungarian standard certification body.

National Association for Consumer Protection in Hungary (NACPH-OFE)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK); Ministry of Transport, Telecommunications, and Energy; and National Communications Authority Hungary	
Weblink: http://www.ofe.hu/	
Areas of Activity: Organization for protection of consumer rights.	

Industry Organizations Active in Network and Information Security

Hungarian Association of IT Companies (IVSZ)	
Type of Organization: IT Association	Ownership: Private
ENISA Focus Points: Resilience, AR, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Cooperates with National Communications Authority Hungary; Prime Minister's Office; Electronic Government Centre (MEH EKK); Internethotline; NHIT; and National Telecommunications and Information Council	
Weblink: www.ivsz.hu	
Areas of Activity: The Hungarian Association of IT Companies represents the most influential IT vendors in the Hungarian market and is a strong lobbying force.	

eSec.hu	
Type of Organization: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Implementation of Security Technology and Standards	

Relationships: Co-operates with CERT – Hungary	
Weblink: www.esec.hu	
Areas of Activity: eSec is a group of Hungarian IT security firms promoting new technology and expertise, as well as providing lobby activities. The organization addresses the key components that are necessary to significantly increase government and corporate security measures.	
Inforum	
Type of Organization: IT Association	Ownership: Private
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.inforum.org.hu/	
Areas of Activity: The association focuses on developing Hungarian Internet content and combating the negative aspects such as spam and viruses. It also acts as a lobby organization for increasing Internet penetration.	
Association of Hungarian Content Providers	
Type of Organization: IT Association	Ownership: Private
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.mte.hu	
Areas of Activity: Industry association created by content providers in order to establish safe content on the Internet and raise awareness about online security.	
Hungarian IT Security Centre	
Type of Organization: IT Association	Ownership: Private
ENISA Focus Points: Emerging and Current Risks, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.itsecu.hu/	

Areas of Activity: Industry association created to audit security solutions and develop new security processes.	
Hungarian Association for Electronic Signature	
Type of Organization: Other Industry Association	Ownership: Private
ENISA Focus Points: AR, e-ID	
Relationships: Cooperation with Budapest University of Technology and Economics; Laboratory of Informatics; Virus Competency Centre	
Weblink: http://www.melasz.hu	
Areas of Activity: Organization focused on promoting signature legislation.	
MATISZ – Hungarian Association of Content Industry	
Type of Organization: Other Industry Association	Ownership: Private
ENISA Focus Points: AR	
Relationships: Cooperation with Barátságos Internet	
Weblink: http://www.matisz.hu/	
Areas of Activity: Association of Hungarian content providers.	
Biztonságos Internet	
Type of Organization: IT Association	Ownership: PPP
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: Part of CERT-Hungary; cooperation with HUN-CERT; SZTAKI; and MATISZ	
Weblink: http://www.biztonsagosinternet.hu/	
Areas of Activity: Knowledge base and awareness-raising Web site promoting safe Internet use.	
Barátságos Internet	
Type of Organization: IT Association	Ownership: PPP

ENISA Focus Points: AR
Relationships: Cooperation with MATISZ; Ministry of Transport and Communication
Weblink: http://www.baratsagosinternet.hu
Areas of Activity: Knowledge base and awareness-raising Web site promoting safe Internet use.

Academic Organizations Active in Network and Information Security

Budapest University of Technology and Economics (BME)

Type of Organization: Other Academic	Ownership: Public
ENISA Focus Points: AR, Emerging Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Cooperates with Ministry of Transport, Telecommunications, and Energy and MELASZ, Hungarian Association for Electronic Signature	
Weblink: http://www.ik.bme.hu/szakmaimuhely/itsec_eng.php	
Areas of Activity: Experts at IT security in the BME Centre of Information Technology (CIT) founded a dedicated IT Security (ITSEC) team in September 2003. Most of the experts have also been involved in MBE CIT's IT security projects during their university studies. The members of the ITSEC group focus on security solutions for the corporate and public sectors, and are involved in the creation of Hungarian and international technological and legal regulatory standards.	

NIIF-CSIRT

Type of Organization: Research Centre (CSIRT)	Ownership: PPP
ENISA Focus Points: CERT, Emerging Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Cooperates with National Telecommunications And Information Council	
Weblink: http://csirt.iif.hu/	

Areas of Activity:
NIIF-CSIRT is the Computer Security Incidents Response Team of NIIF/HUNGARNET, the Internet provider of universities, higher education institutes, some secondary schools, academic research organizations, and non-profit institutions in Hungary. NIIF-CSIRT assists in all cases of computer security incidents in which NIIF/HUNGARNET members are involved, either as a victim or as a suspect. NIIF-CSIRT will disseminate important security related information to NIIF/HUNGARNET members, on a structural basis (e.g., distributing security advisories) as well as on an incidental basis.

Other Bodies and Organizations Active in Network and Information Security

CERT – Hungary

Type of Organization: CERT	Ownership: Public
ENISA Focus Points: CERT	
Relationships: Cooperates with HUN-Cert; National Communications Authority Hungary; Ministry of Transport, Telecommunications, and Energy; NHIT; National Telecommunications And Information Council; eSec.hu; and Internethotline	
Weblink: http://www.cert-hungary.hu/	
Areas of Activity: CERT-Hungary is the network information security centre of the Hungarian government. It is operated in the Theodore Puskas Government Foundation under the supervision of the Prime Minister's Office. It is responsible for incident management, international representation of Hungary (ENISA, IWWN, EGC), think-tank for the government in information security policy making (National Information Security Strategy, MIBA framework for information security certification), co-operation (e-Sec.hu, CIIP working group, Financial ISAC), and awareness raising (biztonsagosinternet.hu).	

HUN-CERT

Type of Organization: CERT	Ownership: PPP
ENISA Focus Points: CERT	
Relationships: Cooperates with NHIT and National Telecommunications And Information Council	
Weblink: http://www.cert.hu/	
Areas of Activity: Certification body of Hungarian ISPs; workgroup of the Hungarian National Academy of Sciences.	

ISACA

Type of Organization: Certification Provider	Ownership: PPP
ENISA Focus Points: Emerging/Current Risks	
Relationships: None	
Weblink: www.isaca.hu	
Areas of Activity: ISACA focuses on the certification of various security professionals. The organization deals with information governance, control, security, and audits of professionals. The institution's IS auditing and IS control standards are followed worldwide. ISACA provides two certification programs: Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).	

Critical Information Infrastructure Protection Workgroup (KIIV)

Type of Organization: Other (expert group)	Ownership: N/A
ENISA Focus Points: Development of Security Technology and Standards Policy and Implementation of Security Technology and Standards	
Relationships: CERT-Hungary; MOL; National Security Agency; National Communications Authority; HUN-CERT; and Hungarian Controlling Agency for Electricity Market	
Weblink: www.kiiv.hu	
Areas of Activity: Specialized in critical infrastructure protection for Hungary.	

Activities

Strategic Initiatives

Regulation of Electronic Document Archiving at Public Services

Type of Activity: Government Policy
Responsible Organization(s): NHIT and National Telecommunication and Information Council
ENISA Focus Points: Development of Security Technology and Standards Policy and Implementation of Security Technology and Standards
Weblink: None

Description: The project was aimed at developing a universal regulation for archiving data within public services with special focus on data protection and security.
MIBA – Hungarian IT Security Recommendations
Type of Activity: Government Policy
Responsible Organization(s): Prime Minister's Office and Electronic Government Centre (MEH EKK)
ENISA Focus Points: Development of Security Technology and Standards Policy and Implementation of Security Technology and Standards
Weblink: None
Description: Recommendation for the security audit of egovernment systems.
Biztonságos Internet
Type of Activity: Funding Program
Responsible Organization(s): HUN-CERT; CERT-Hungary SZTAKI; and MATISZ
ENISA Focus Points: AR and Emerging/Current Risks
Weblink: http://www.biztonsagosinternet.hu/
Description: Knowledge base and awareness-raising website promoting safe Internet use.
Barátságos Internet
Type of Activity: Funding Program
Responsible Organization(s): MATISZ and Ministry of Transport and Communication
ENISA Focus Points: AR
Weblink: http://www.baratsagosinternet.hu
Description: Awareness-raising portal targeted at home users.
Incident Management Workgroup (IKMCS)
Type of Activity: Non-governmental Initiative

Responsible Organization(s): CERT-Hungary; National Bureau of Investigation (Department of High Technology); Hungarian Banking Association; Hungarian Financial Supervisory Authority
ENISA Focus Points: Development of Security Technology and Standards Policy
Weblink: None
Description: Workgroup cooperating on improving the security of ebanking.
Critical Information Infrastructure Protection Workgroup (KIIV)
Type of Activity: Non-governmental Initiative
Responsible Organization(s): CERT-Hungary; MOL; National Security Agency; National Communications Authority; HUN-CERT; Hungarian Controlling Agency for Electricity Market
ENISA Focus Points: Development of Security Technology and Standards Policy and Implementation of Security Technology and Standards
Weblink: None
Description: Workgroup specialized in critical infrastructure protection for Hungary.
www.bigyoo.hu
Type of Activity: Non-governmental Initiative
Responsible Organization(s): MTE
ENISA Focus Points: AR
Weblink: http://www.bigyoo.hu/
Description: T-Com, in cooperation with MTE, launched this portal to provide children with a collection of safe Web sites as well as information about their rights on the Internet.
Internethotline
Type of Activity: Non-governmental Funding Program
Responsible Organization(s): MTE; Inforum; and MATISZ
ENISA Focus Points: AR, Emerging/Current Risks

Weblink: None
Description: This portal is part of the EU's Safer Internet Program and provides citizens with the means of reporting malicious or illegal pages on the Internet.

Research Programmes

Electronic Communication Based on eSignature Between Partners
Type of Activity: Non-governmental funding program
Responsible Organization(s): MELASZ
ENISA Focus Points: e-ID
Weblink: None
Description: Developing procedures to make esignature verification easier and more understandable.

SecureFilter
Type of Activity: Non-governmental Funding Program
Responsible Organization(s): NIIF-CSIRT
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: None
Description: The SecureFilter is a specially tailored and hardened Debian-based Linux system developed for firewall purposes.

Authentication and Authorization Infrastructure
Type of Activity: Non-governmental funding program
Responsible Organization(s): HUN-CERT; SZTAKI; and NIIF-CSIRT
ENISA Focus Points: Development of Security Technology and Standards Policy and Implementation of Security Technology and Standards
Weblink: None

Description: Primary users of AAI are research and higher education institutions, however, it is possible for commercial providers to join the federation, offering their services to the academic scope. Shibboleth technology can be used to build up an intranet single sign-on solution, while access to particular resources and services can be granted to arbitrary portions of national or international academic networks.

Events

Conference and Workshops

Day of Information Security	
Responsible Organization: IVSZ, Budapest University of Technology and Economics, Laboratory of Informatics	Frequency: Annual
ENISA Focus Points: Resilience, AR, Emerging and Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions	
Weblink: www.itbn.hu	
Description: Annual event for IT security under the patronage of Budapest University of Technology, focusing on current security trends, threats, and solutions.	

Networkshop 2008	
Responsible Organization: NIIF-CSIRT	Frequency: Annual
ENISA Focus Points: e-ID, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions	
Weblink: https://nws.niif.hu/ncd2008/	
Description: Annual event organized at the College of Dunaújváros, focusing on computing solutions, networking, and IT security.	

Kriminalexpo – Itsec	
Responsible Organization: National Bureau of Investigation (Department of High Technology)	Frequency: Annual
ENISA Focus Points: Awareness raising, Implementation of Security Technology and Standards	

Target Groups: Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions
Weblink: http://www.kriminalexpo.hu
Description: Annual conference organized by the Hungarian Ministry of Police about current and upcoming security threats and solutions.

CERT-Hungary Workshop	
Responsible Organization: CERT-Hungary, National Bureau of Investigation (Department of High Technology), Hungarian Banking Association, Hungarian Financial Supervisory Authority, Prime Minister's Office, Electronic Government Centre (MEH EKK)	Frequency: Annual
ENISA Focus Points: CERT, Awareness raising, Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.neti.hu/pta/hu/node/116	
Description: Annual conference organized by the Hungarian Ministry of Police about current and upcoming security threats and solutions.	

Media Campaigns

Day of the Safer Internet	
Responsible Organization: Internethotline.hu, MATISZ	Frequency: Biannual
ENISA Focus Points: AR	
Target Groups: Citizens, Consumers, SMEs	
Weblink: http://www.saferinternet.org	
Description: Workshop held twice a year in order to facilitate cooperation among key players in Hungarian public infrastructures.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

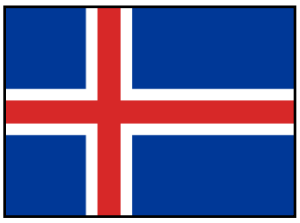
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Hungary.

Country Report – Iceland

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Reykjavík
Total area:	103 000 sq.km
Population:	0.3 million
Official language:	Icelandic
Time zone:	GMT
Currency:	Icelandic króna (ISK)

Source: Eurostat

NIS Highlights

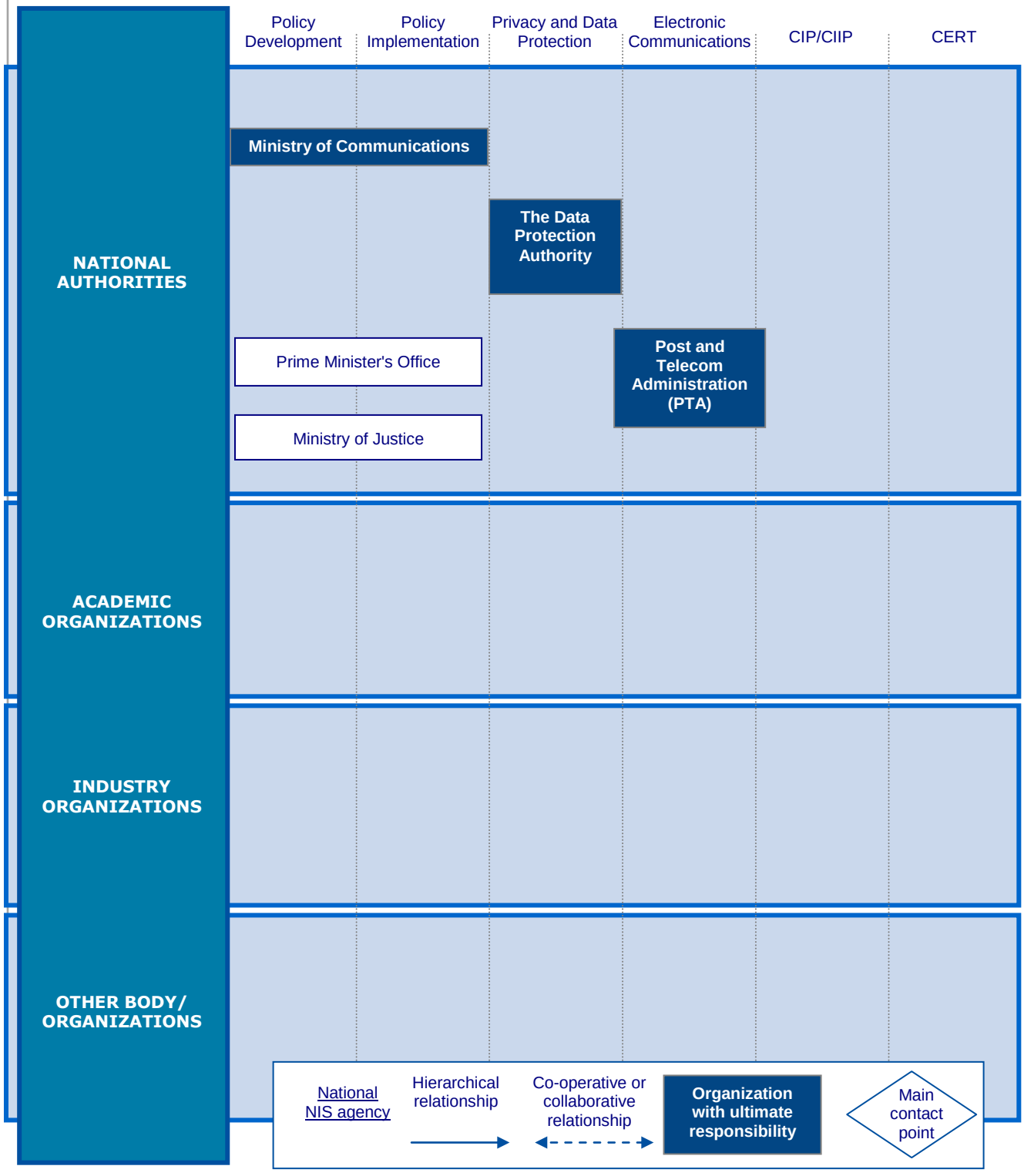
The Ministry of Communications is responsibility for the preparation of drafts of legislative proposals for parliamentary purposes, drafting of regulations, issue of work permits and professional licenses, publication of reports and information dissemination. Recognized as the stakeholder responsible for national information security policy at the national level, the ministry is thus charged with both development and implementation of said policy.

The Icelandic Data Protection Authority exercises surveillance over processing of data to which the act applies. With proper identification the staff of the DPA is admitted to any and all premises where personal data is being processed without a court order.

Post- and Telecom Administration (PTA) is responsible for electronic communications in Iceland. It is further charged with ensuring an economic, safe and accessible service, to ensure effective competition and to implement the policy of the public authorities, ensuring evolution of the information society, informing consumers, ensuring clear and transparent rules of the game on the market, and ensuring effective measures and first class staff.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Iceland. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Communications							X	X
The Data Protection Authority			X	X				X
Post and Telecom Administration (PTA)								X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Iceland:

National Authorities in Network and Information Security

Ministry of Communications

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.samgonguraduneyti.is	
Areas of Activity: The Ministry of Communications is divided into five departments: The Minister's department, the department of Transportation and Planning, the department of Telecommunications, Maritime Affairs and Transport Safety, the department of Administration and Legal Affairs the department of Municipal affairs and Equalization Fund. The work of the Ministry of Communications thus covers i.a. the preparation of drafts of legislative proposals for parliamentary purposes, drafting of regulations, issue of work permits and professional licences, publication of reports and information dissemination. International co-operation is also an important feature of Ministry operations.	

Ministry of Justice

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: part of Ministry of Interior	
Weblink: http://www.domsmalaraduneyti.is	
Areas of Activity: The purpose of the Ministry of Justice is to uphold law and order and ensure that civil rights are respected.	

Prime Minister's Office

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	

Weblink: http://www.forsaetisraduneyti.is	
Areas of Activity: The Office serves as secretariat to the Prime Minister and assists the Minister in his role as head of government by providing political, operational and administrative services.	
Post and Telecom Administration (PTA)	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: PFA is an independent body under the ultimate direction of the Minister of Communications	
Weblink: http://www.pfs.is	
Areas of Activity: The primary objectives of PTA are to ensure an economic, safe and accessible service, to ensure effective competition and to implement the policy of the public authorities, ensure evolution of the information society, inform the consumers, ensure clear and transparent rules of the game on the market, and ensure effective measures and first class staff.	
The Data Protection Authority	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.personuvernd.is	
Areas of Activity: The Icelandic Data Protection Authority exercises surveillance over processing of data to which the act applies. With proper identification the staff of the DPA is admitted to any and all premises where personal data is being processed without a court order.	
The Icelandic Centre for Research (Rannís)	
Type of Organisation: National Governmental	Ownership: Public
ENISA Focus Points: AR	
Relationships: Rannís reports to the Ministry of education, Science & Culture	

Weblink: http://www.rannis.is/english/about-rannis/
Areas of Activity: The purpose of Rannís is to provide professional assistance in the preparation and implementation of science and technology policy in Iceland.

Academic Organisations Active in Network and Information Security

The Laboratory for Dependable, Secure Systems

Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: CERT, Resilience, Development of Security Technology and Standards Policy	
Relationships: School of Computer Science, Reykjavík University, Iceland.	
Weblink: http://ldss.ru.is/	
Areas of Activity: The LDSS conducts research and education to advance the state of the art in the security and dependability of computer systems. Topics include secure software construction, security policy specification and enforcement, as well as scalable, readily available distributed systems. The LDSS aims to be a centre of technical expertise that benefits the wider community. To support this goal, the LDSS is structured to work in partnership with industry and government, for instance, to identify practical, motivating security vulnerabilities and attacks.	

Other Bodies and Organisations Active in Network and Information Security

The Icelandic Computer Society (ISIP)

Type of Organisation: Philanthropic, Educational and Professional Associations	Ownership: Public
ENISA Focus Points: AR	
Relationships: co-operates with other CERTs	
Weblink: http://www.sky.is	
Areas of Activity: The main function of the ISIP is to organise conferences and lectures, co-operating in international work with other societies, publishing a bi-monthly magazine on domestic topics and running a committee dedicated to translating computing terms into Icelandic.	

Activities

Strategic Initiatives
SAFT (Society, Family and Technology)
Type of Activity: Social & Other Research Programmes
Responsible Organisation(s): Home and School (National Parents' Association)
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: http://www.saft.is
Description: The purpose of SAFT is to empower children and parents to enjoy the internet and new media in a safe and positive way. The focus of SAFT is awareness work on net-ethics, computer game rating, source criticism, uses of mobile phones and personal protection on the internet.

Events

There are no significant security-related events held in Iceland.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

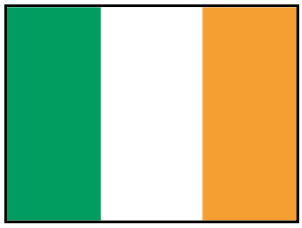
Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing

concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Iceland.

Country Report – Ireland

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Dublin
Total area:	70 000 sq.km
Population:	4.2 million
Official language:	English, Irish
Time zone:	GMT
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Ireland, we present a set of three indicators in the Country Highlights section.

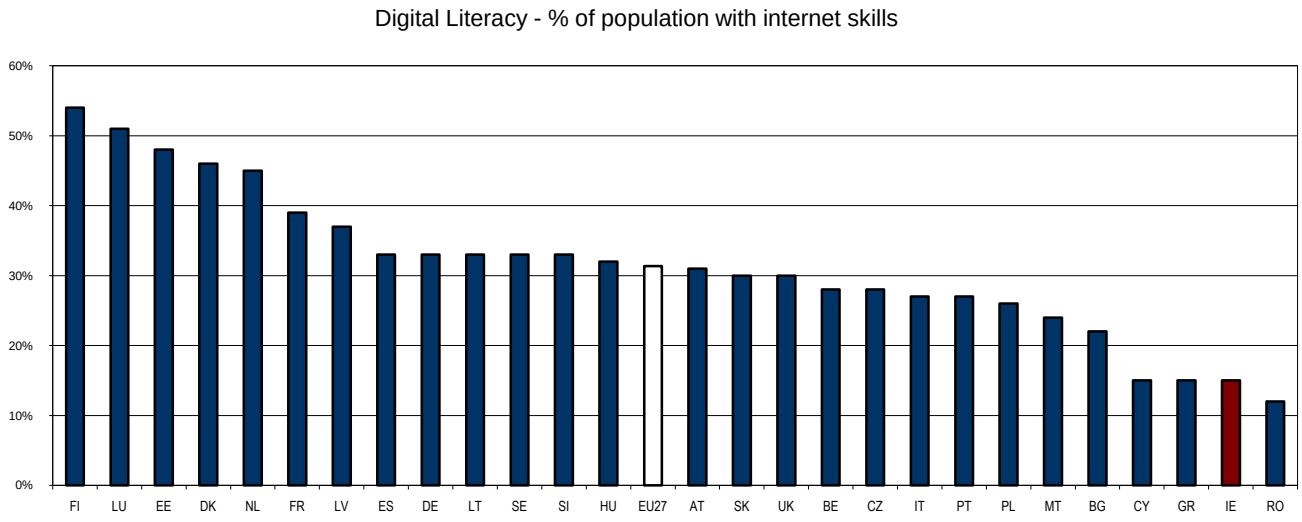
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Ireland is fundamental to this NIS study.

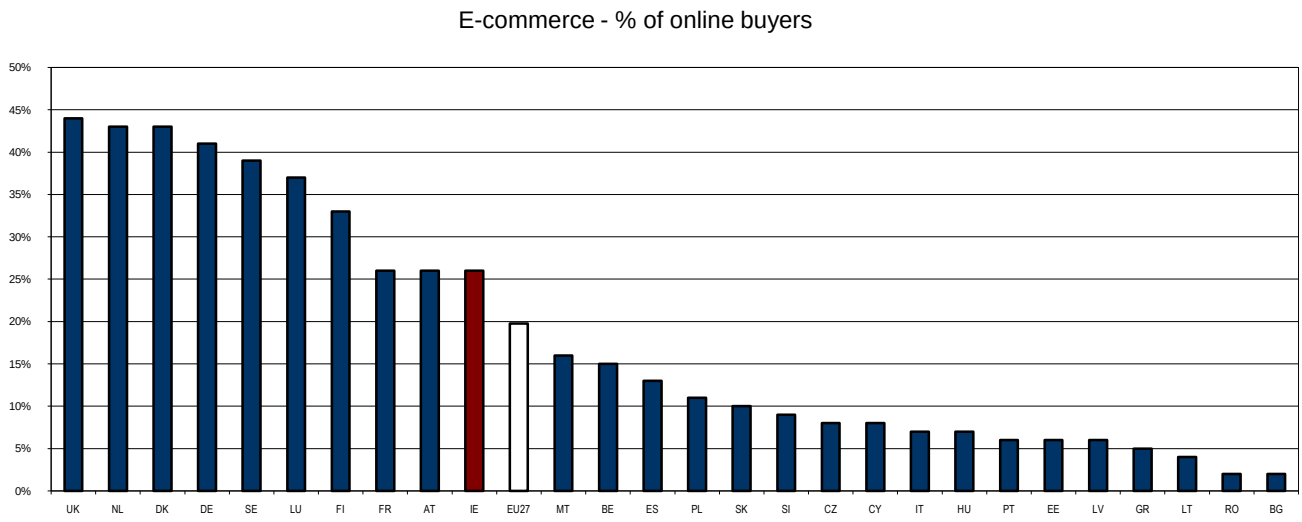
Ireland has very good e-commerce development and an average level of connectivity and usage of ICTs by citizens and businesses. Growth in broadband take-up has boosted the ratio of broadband to narrowband. ICT skill levels in the general population are improving. Ireland is noted for a high level of e-commerce usage.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

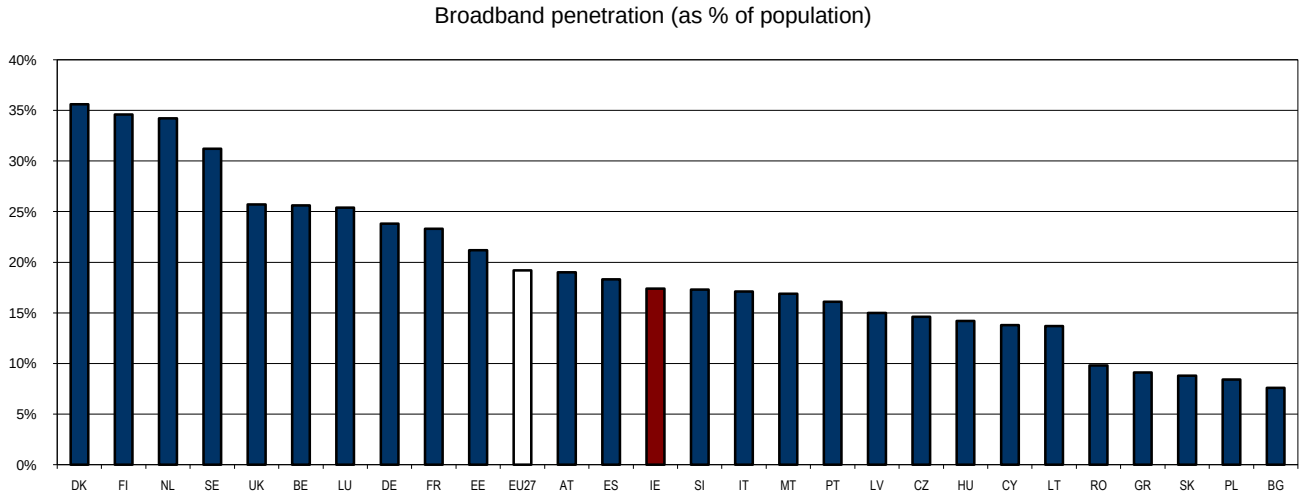
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Ireland does not have a single organization that is recognized among NIS stakeholders as the national security agency. Nor does the country have stakeholders recognized as responsible for information security development and implementation as they are more concerned with focusing on compliance with EU legislation.

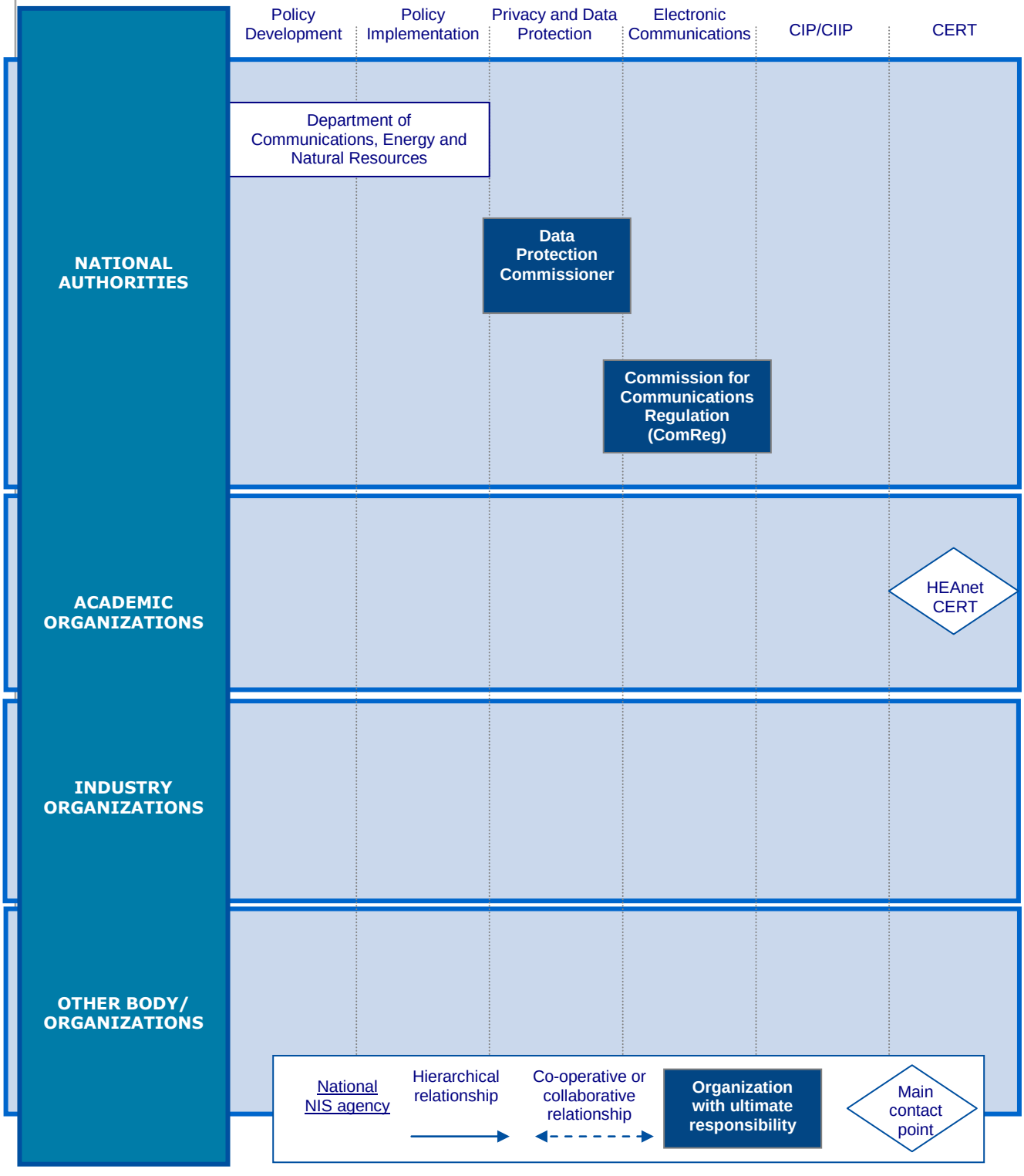
Data Protection Commissioner is responsible for implementing and ensuring compliance with privacy and data protection legislation in Ireland.

ComReg is charged with implementing and ensuring compliance with electronic communications regulations in Ireland. HEAnet is recognized in the country as the stakeholder serving as the national contact point for IT security.

There in no single agency viewed as responsible for CIP/CIIP in Ireland.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Ireland. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Department of Communications, Energy and Natural Resources (DCENR)							X	X
Data Protection Commissioner								X
ComReg			X	X			X	X
HEAnet-CERT	X							

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Ireland:

National Authorities in Network and Information Security	
Department of Communications, Energy and Natural Resources (DCENR)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.dcenr.gov.ie	
Areas of Activity: The Department of Communications, Energy and Natural Resources has responsibility for the Telecommunications, Broadcasting and Energy sectors. The department also regulates, protects and develops the Natural Resources of Ireland.	
Commission for Communications Regulation (ComReg)	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.comreg.ie	
Areas of Activity: ComReg is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications and broadcasting transmission) and the postal sector. It is the national regulatory authority for these sectors in accordance with EU law which is subsequently transposed into Irish legislation.	

Department of Justice, Equality and Law Reform	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.justice.ie	
Areas of Activity: The remit of the Justice family of agencies and services stretches across a range of human concerns. It touches on every aspect of national life from child protection and involvement in inquiries and tribunals to all elements involved in crime and punishment and the courts system, from the buying and selling of property to a range of immigration services and the areas of disability and diversity. On the international front, the Minister and the Department manage the interests of Ireland in relation to Justice and Home Affairs matters by participating fully in the European Union, the Council of Europe and the United Nations.	

National Crime Council	
Type of Organisation: National Government	Ownership: PPP
ENISA Focus Points: AR, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.irlgov.ie/crimecouncil/	
Areas of Activity: The council was established by the Minister for Justice, Equality and Law Reform. The Council has a broad mandate to provide a forum for the development, expression and contribution of a wide range of views on anti-crime strategies and policies and to raise public knowledge and awareness of crime.	

Internet Advisory Board	
Type of Organisation: National Government	Ownership: Non-profit
ENISA Focus Points: AR, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Independent, but collaborates with both the government and the Internet industry	
Weblink: http://www.iab.ie	

Areas of Activity: The IAB was established by the Minister of Justice, Equality and Law Reform in February 2000. The IAB assists and supports the Irish Internet Service Provider (ISPAI) industry to deliver an effective self-regulatory environment for internet content. The board also commissions research on internet downside issues and promotes awareness of internet safety, particularly with regard to children.

Data Protection Commissioner	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: Independent, co-operates with the Ministry of Industry and Trade	
Weblink: http://www.dataprotection.ie	
Areas of Activity: The Data Protection Commissioner is responsible for upholding the rights of individuals with respect to personal data. The Commissioner also has a role to play in the enforcement of Electronic Communications Data Protection and Privacy Regulations.	

Department of the Taoiseach - Information Society Policy Unit (ISPU)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: co-operates with the Ministry of Industry and Trade	
Weblink: http://www.taoiseach.gov.ie/index.asp?locID=175&docID=-1	
Areas of Activity: The Information Society Policy Unit (ISPU) in the Department of the Taoiseach (Head of the Irish Government) has overall responsibility for developing, co-ordinating and driving implementation of the Information Society agenda.	

Industry Organisations Active in Network and Information Security

ICT Ireland	
Type of Organisation: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: AR	

Relationships: part of the Irish Business Employers Confederation
Weblink: http://www.ictireland.ie
Areas of Activity: ICT Ireland is the representative lobby group for the high tech or knowledge sector within IBEC (Irish Business Employers Confederation). The association represents over 300 companies, both foreign owned and indigenous. Indirectly involved in security aspects but more focused on increasing the competitiveness of Ireland generally.

Telecoms and Internet Federation (TIF) - Irish Telecoms Security & Fraud Forum	
Type of Organisation: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Affiliated with the Irish Business Employers Confederation	
Weblink: http://www.tif.ie/	
Areas of Activity: The ITSFF has been established as an unincorporated association since April 1998 and has developed a reputation as an effective body operating in the field of telecommunication fraud and security issues within the industry. It exists because like every organisation the industry is susceptible to fraud and security related issues, there is an ongoing need for information relating to security risks, fraudster techniques, criminal activity, methods and means to be exchanged between telecommunication companies outside the normal competitive arena.	

Irish Internet Association (IIA)	
Type of Organisation: Other Industry Association	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.iia.ie	
Areas of Activity: The Irish Internet Association is the professional body for those conducting business via the internet from Ireland. It has been and remains one of the driving forces behind the adoption of the medium. Established in 1997, the IIA provides leadership to enterprises and society conducting business in Ireland.	

Internet Service Providers Association of Ireland (ISPAI)	
Type of Organisation: Other Industry Association	Ownership: Non-profit

ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy
Relationships: acts as a single point of contact between the ISP industry and the government
Weblink: http://www.ispai.ie
Areas of Activity: The Internet Service Providers Association of Ireland was formed in January 1998 by the leading Irish Internet Service Providers operating at that time. The aim of the association is to provide one voice for the Irish ISP industry at national, EU and International level. The ISPAI has agreed with the Irish government that a self-regulatory approach to the industry has greater opportunities for success and effectiveness. As part of this, the ISPAI established and funds the www.hotline.ie service to combat illegal content, especially child pornography, being hosted and distributed on the Internet. The ISPAI represents the industry on the Government's Internet Advisory Board.

Academic Organisations Active in Network and Information Security

HEAnet

Type of Organisation: Other Academic	Ownership: Non-profit
ENISA Focus Points: CERT	
Relationships: None	
Weblink: http://www.heanet.ie	
Areas of Activity: HEAnet is Ireland's National Education and Research Network. HEAnet-CERT operates by agreement with JANET CSIRT (Computer Security Incident Response Team). HEAnet utilizes the services of JANET CSIRT to provide a single, trusted point of contact for clients to deal with computer security incidents and their prevention.	

Other Organisations Active in Network and Information Security

Irish Computer Society (ICS)

Type of Organisation: Philanthropic, Educational and Professional Associations	Ownership: Non-profit
ENISA Focus Points: AR, Development of Security Technology and Standards	

Relationships: None

Weblink: http://www.ics.ie

Areas of Activity:

The Irish Computer Society was founded in 1967 as the national body for Information and Communication Technology (ICT) Professionals in Ireland. Since its foundation the ICS has promoted the continuous development of professional ICT knowledge and skills in Ireland by organising seminars, lectures and related activities. The ICS represents the views of members to Government on topics of relevance, such as budgets and taxation, data protection, education and training. The Society is a nominating body for the Industrial and Commercial Panel of Seanad Éireann. ICS members serve from time to time on commissions, boards and committees appointed by government.

Activities

Strategic Initiatives

Code of Practice on Data Protection for the Insurance sector

Type of Activity: Governmental Policies

Responsible Organisation(s): Data Protection Commissioner

ENISA Focus Points: Implementation of Security Technology and Standards

Weblink: http://www.dataprotection.ie/viewdoc.asp?DocID=841

Description:

The Office of the Data Protection Commissioner published a data protection Code of Practice for the insurance sector in Ireland in August 2008. The Code was prepared against a backdrop of significant public concern arising from media reports last year that personal information held by the Gardaí and by the Department of Social & Family Affairs was being routinely accessed by private investigators acting on behalf of insurance companies. This was confirmed by the Office's own investigations of insurance companies at the time. The Code is the latest stage in the response of the Office to those issues and follows the launch in 2007 of a data protection code of practice for An Garda Síochána.

hotline.ie

Type of Activity: Non-governmental Initiative

Responsible Organisation(s): ISPAI

ENISA Focus Points: AR

Weblink: http://www.hotline.ie

Description:

The hotline.ie service provides an anonymous facility for the public to report suspected illegal content encountered on the Internet, in a secure and confidential way. The primary focus of the Hotline is to combat Child Pornography. Other forms of illegal content and activities exist on the Internet and may be reported using this service. The Hotline, run by the Internet Service Providers Association of Ireland (ISPAI) since November 1999, is part financed by the European Commission's Safer Internet Plus Programme. It is supervised by the Department of Justice, Office for Internet Safety (OIS), in cooperation with An Garda Síochána and is a member of INHOPE, the International Network of Hotlines.

Funding Programmes & Financial Initiatives

Webwise

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s): National Centre for Technology in Education (NCTE)

ENISA Focus Points: AR

Weblink: http://www.webwise.ie

Description:

Webwise is the Irish Internet Safety Awareness Node of Insafe the European network of internet safety awareness nodes. Webwise provides parents, teachers, and children with educational resources, advice and information about potential dangers on the Internet and empowers users to minimise or avoid these risks. Webwise monitors and addresses emerging trends, and seeks to reinforce the image of the Internet as a place to learn. Webwise also raises awareness on reporting illegal content to hotline.ie and shares best practice, information and resources with European partners through the European Commission's Insafe network.

askcomreg.ie

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s): ComReg

ENISA Focus Points: AR

Weblink: http://www.askcomreg.ie

Description:

Askcomreg.ie is owned by ComReg and has been designed with the consumer in mind. The aim of askcomreg.ie is to provide consumers with a user friendly website that provides relevant information and answers on the main issues which affect them in their dealings with suppliers.

Events

Media Campaigns	
MakeITsecure	
Responsible Organisation(s): DCENR	Frequency: annual
ENISA Focus Points: AR, e-ID	
Target Groups: Major- Consumers/Citizens	
Weblink: http://www.makeitsecure.org	
Description: National internet security awareness campaign developed by DCENR.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, seven security breaches were reported in Ireland:

1. In August 2008 numerous bank customers have had their credit cards cancelled following the latest international scam to hit the financial services sector. Personal banking details of hundreds of customers were compromised after thieves hacked into the online database of one of the country's leading retailers. This so-called testing came to light when transactions for up to €1 appeared for items purchased on US website, Kosher.com. This allows fraudsters to determine if cards are still in use before using them for larger purchases. All the major banks were working non-stop yesterday to contact customers and cancel all cards affected and re-issue new ones. It is likely hackers got credit card details by getting into the retailer's website or obtaining details from an employee, according to the Irish Payment Service Organisation (IPSO).

   http://www.irishexaminer.com/irishexaminer/pages/story.aspx-qqqg=ireland-qqqm=ireland-qqqa=ireland-qqqid=69351-qqqx=1.asp

2. In August 2008 Satellite broadcaster Sky television has launched an investigation after personal details including bank account numbers of 33 people from several areas of Wexford became available online.

   http://www.examiner.ie/irishexaminer/pages/story.aspx-qqqg=ireland-qqqm=ireland-qqqa=ireland-qqqid=69420-qqqx=1.asp

3. Personal details of 380,000 social welfare recipients were stored on a laptop, which went missing in April 2007, was found in August 2008. Up to 106,000 of the records held on the laptop contained bank account details, as recipients were paid benefits directly into their accounts. Following an examination three of these laptops have been identified as containing data that could, if improperly disclosed, be misused.

   http://www.irishtimes.com/newspaper/breaking/2008/0811/breaking25.htm

4. In August 2008 data thieves, posing as bank technicians, fooled shop owners into giving them access to credit card terminals and managed to download the details of over 20,000 credit and debit cards. The Irish Payment Services Organisation has warned that individuals pretending to be from Irish banks convinced shop owners they were carrying out maintenance on behalf of banks. This enabled them to plug in wireless devices that pushed the data to the Internet and allowed the card numbers to be used overseas. The scam has forced banks to restrict cash withdrawals to €100 a day for card-holders travelling outside the country.

   http://www.siliconrepublic.com/news/article/11217/cio/20-000-credit-cards-skimmed-by-opportunistic-data-thieves

5. In August 2008 contact details for more than 17,000 members of the Institute of Chartered Accountants in Ireland were inadvertently published on the web in the latest data security breach to hit a high-profile organisation. The information includes members' personal addresses, contact details including e-mail addresses and phone numbers, and personal data such as date of birth. The file also includes membership numbers and the temporary passwords allocated to members before their first log-in to the website. During a redesign of the institute's website in July, a version of its membership database was mistakenly published on its site. As a result a number of search engines came across the page and indexed it. The Institute's own investigation suggests that the data was "crawled" by four Internet search engines.

   http://www.irishtimes.com/newspaper/finance/2008/0819/1218868113806.html

6. Thousands of people have reportedly had their financial details stolen during a recent card-skimming operation in the Galway area. Reports stated gardaí believe several thousand ATM and credit cards were skimmed at a large shop in the county. Some of the cards had already been cloned and large sums of money stolen before gardaí became aware of the situation.

   http://www.breakingnews.ie/ireland/mhqleymhqlql/rss2/

7. In October 2008 it was reported a laptop containing personal details of thousands of HSE staff was stolen. The major security blunder took place on September 17 at the HSE headquarters in the Carnegie Centre in Dublin. The computer is thought to contain thousands of staff names, pay details, staff numbers and work areas. It was not encrypted meaning identity thieves armed with simple software could get access to vital information. Gardai have been called in and are now investigating the matter alongside the Data Protection Commissioner.

   http://www.istockanalyst.com/article/viewiStockNews+articleid_2680211.html

Country Report – Italy

Country General Information

Political system:	Republic
Capital city:	Rome
Total area:	301 263 sq.km
Population:	58.8 million
Official language:	Italian
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Italy, we present a set of three indicators in the Country Highlights section.

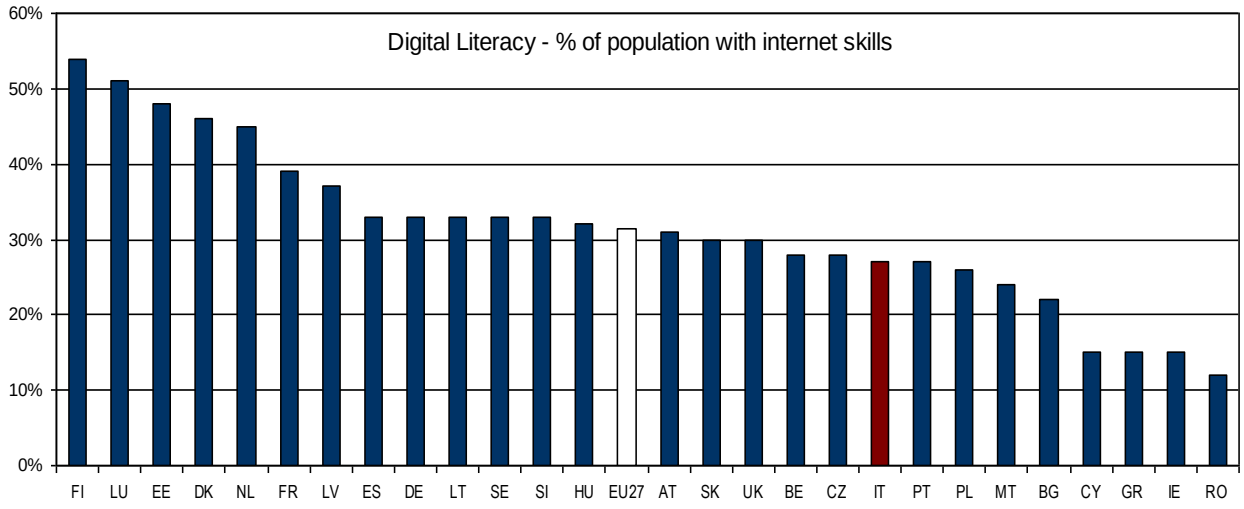
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Italy is fundamental to this NIS study.

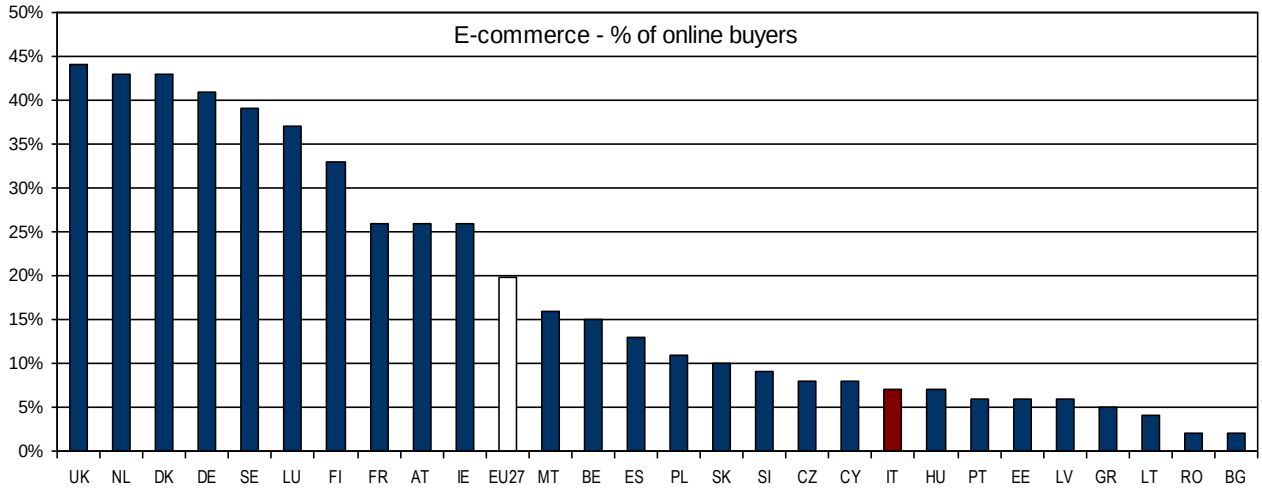
The development of the information society in Italy is still lagging behind in comparison with the general developments in the EU. There are mixed developments in the country as Italy belongs to leading countries in availability and quality of e-government services but lags behind the EU average in benchmarking indicators such as digital literacy, e-commerce activity indicator and broadband penetration.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

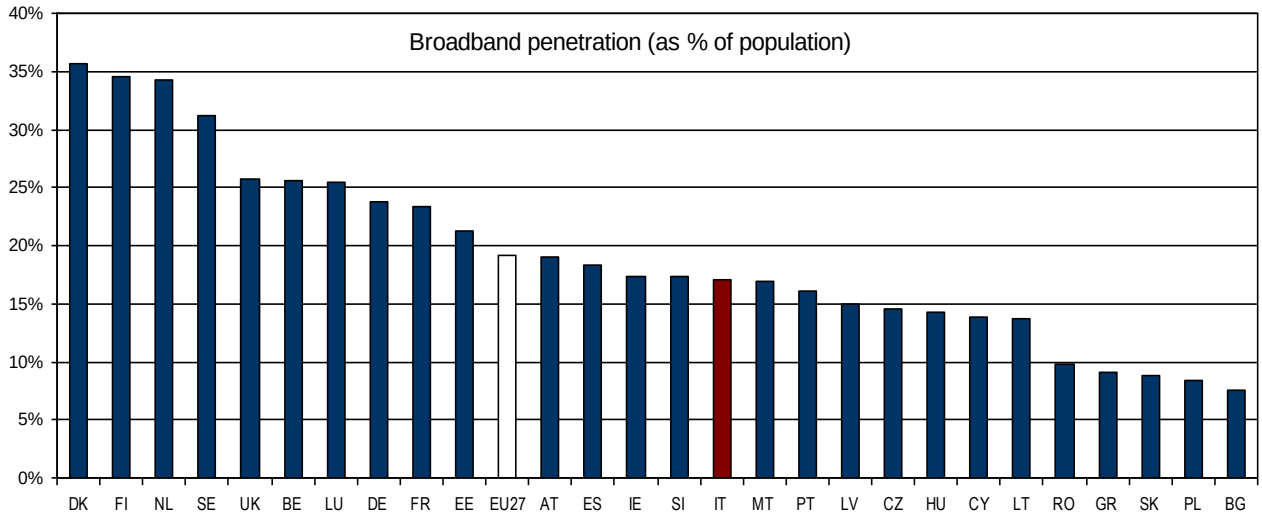
Digital Literacy Indicator



eCommerce Indicator



Broadband penetration Indicator



NIS Highlights

Italy does not have a single institution recognized among NIS stakeholders as the national security agency; there are various organization sharing the responsibilities and competencies concerning the classified information. The Ministry of Economic Development acts as the institution from among all NIS stakeholders in Italy as the one responsible for

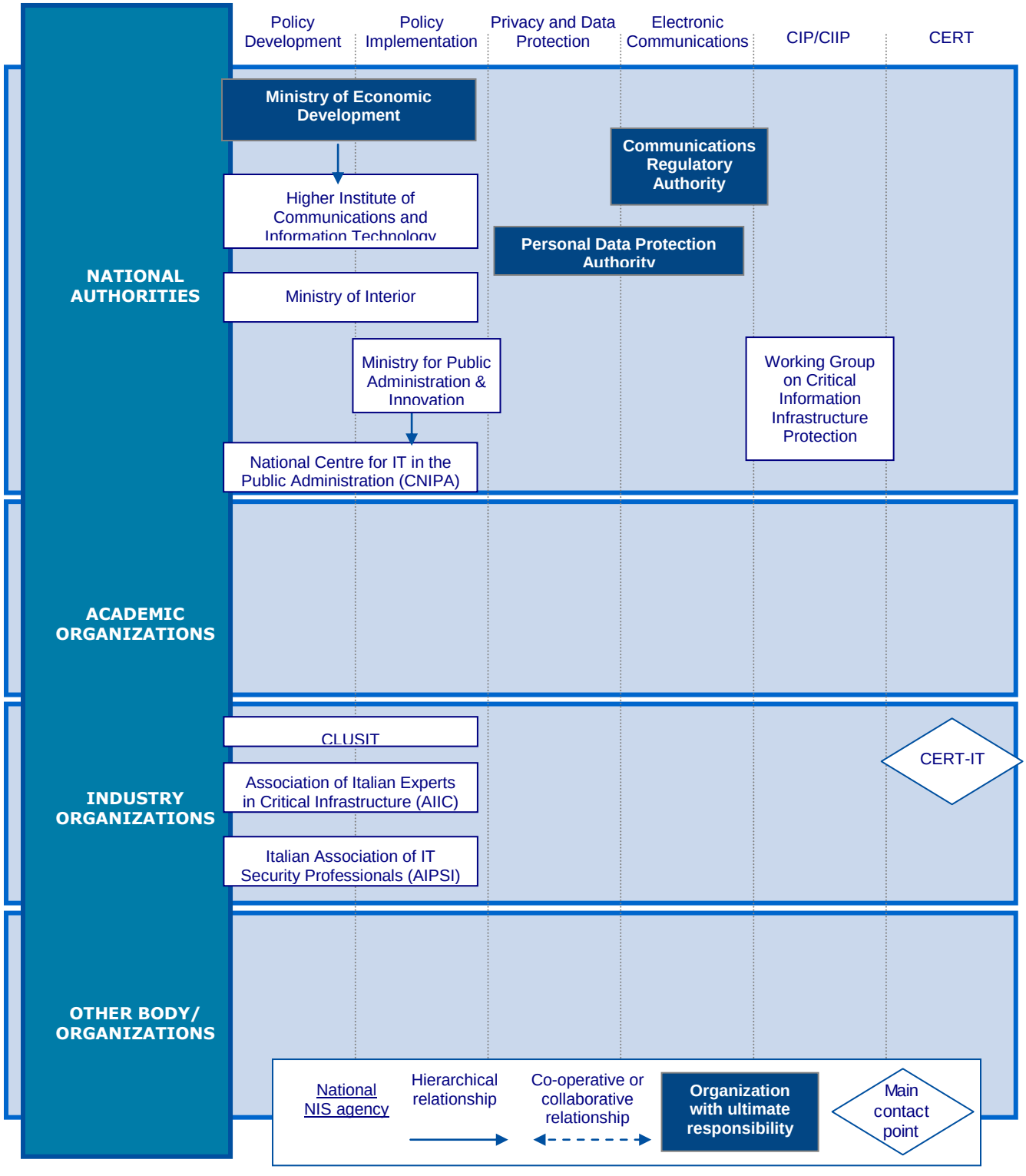
coordinating the development and implementation of national information security strategy.

Italy is committed to data protection and ensuring compliance in this regard. Italian Personal Data Protection Authority ensures compliance with the Privacy Directive. It is accountable to the Italian Parliament, which has established its powers, defined its statutes and elected its members.

Additionally, Italy has a working group on critical information infrastructure protection, established in 2003 as part of the Prime Minister's Office that composed of representatives from Government departments and agencies, and private sector operators. The country hosts a number of conferences on NIS - events organized prevalently by industry professional and associations.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Italy. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Economic Development			X	X			X	
Personal data protection authority			X	X			X	
Communications Regulatory Authority		X						X
Higher Institute of Communications and Information Technology				X			X	X
Ministry of the Interior				X		X		
National Centre for IT in the Public Administration (CNIPA)		X	X	X		X	X	X
Ministry for Public Administration and Innovation								X
CERT-IT	X							
CLUSIT			X					X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Italy:

National Authorities in Network and Information Security

Ministry of Economic Development

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging and Current Risks, Development of Security Technology and Standards Policy	
Relationships: N/A	
Weblink: http://www.sviluppoeconomico.gov.it, http://www.comunicazioni.it	

Areas of Activity:

The functions of the former Ministry of Communications were transferred to the Ministry of Economic Development in 2008. The ministry is the main regulator; it acts as policy coordinator, and supervisor. Is involved in analyses and development of economic, technical and legal aspects of Internet, Telephony services, and Broadband in Italy.

Takes and publishes technical measures regarding the type approval and the utilization of terminal apparatus to be connected, directly or indirectly, to telecommunications networks granting, afterwards, the relevant licences. Carries out type approvals for telecommunications apparatus. Grants licences, authorizations and permissions (as an example, for WiMax), adopting the relevant provisions taking great care of their observance; determines technical regulations considering both users' interests and services quality levels; arranges plans for radiofrequencies' grant and allocation making sure of their observance. It imposes measures to Service Providers in order to prevent the diffusion of pedo-pornographic content over Internet.

Higher Institute of Communications and Information Technology (ISCOM)

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging and Current Risks, Development and Implementation of Security Technology and Standards Policy	
Relationships: Part of the Ministry of Economic Development	
Weblink: http://www.isticom.it/	

Areas of Activity: ISCOM is the technical Body of the Ministry of Economic Development. Its activities (directed specifically towards firms of the ICT sector, public administration and end-users) include: consulting and training services, regulation development, applied research, tests, standards development, in the field of telecommunications networks. ISCOM is also the Italian certification body for security of ICT products and evaluation centre for ICT systems and products that contain classified data.

Ministry of Interior	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging and Current Risks, e-ID	
Relationships: N/A	
Weblink: http://www.interno.it/mininterno/export/sites/default/it/	
Areas of Activity: Oversees aspects as national security, electronic identity (Electronic Passport), and Intelligence and Cybercrime policies.	

National Centre for IT in the Public Administration (CNIPA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness raising, Emerging and Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: CNIPA is part of the Italian Government and the Technical Body of the Ministry for Public Administration and Innovation	
Weblink: http://www.cnipa.gov.it	
Areas of Activity: CNIPA provides the technical support to the Department for Innovation and Technologies within the Ministry for Public Administration and Innovation. Main technical areas are: PKI, electronic signatures, ICT awareness, e-Government. It comprises a Technical Committee (*Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni*) charged of setting Security procedures for the Public sector, and the Gov.CERT, the Public CERT to prevent and respond to issues coming from attacks and damages to ICT networks and systems.	

Personal Data Protection Authority (*Garante per la protezione dei dati personali*)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Awareness raising, Emerging and Current Risks, Development of Security Technology and Standards Policy	

Relationships: Independent body accountable to the Italian parliament.	
Weblink: http://www.garanteprivacy.it	
Areas of Activity: The Data protection Authority is mainly interested to ensure compliance with the Privacy Directive.	
Communications Regulatory Authority (Agcom)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Implementation of Security Technology and Standards Policy	
Relationships: Independent body accountable to the Italian parliament.	
Weblink: http://www.agcom.it	
Areas of Activity: The Communications Regulatory Authority (Agcom) is an independent authority, established in July 1997. Agcom is first and foremost a "guarantor". The two main tasks assigned to it: to ensure equitable conditions for fair market competition and to protect fundamental rights of all citizens.	
Postal and Communications Police Service	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Implementation of Security Technology and Standards Policy	
Relationships: Part of the National Police Service, which reports to the Ministry of the Interior; cooperates with G8 network, European Union, European Council, OCSE, Interpol, Europol.	
Weblink: http://www.poliziadistato.it/pds/informatica	
Areas of Activity: The Postal and Communications Police Service deals with offences and violations related to mail and telecommunications. It is composed of 19 field offices and 77 units operating throughout the Italian territory. Its main activities concern the prevention of, and response to, computer crime (hacking, anti-terrorism, e-commerce related frauds, telephony frauds, pedo-pornography), audiovisual piracy and copyright protection, protection of postal services. It also acts as a national point of contact for translational emergencies and relations with a number of other parties, as the "G8 network", the European Union, The European Council, OCSE, Interpol, and Europol. From 2007 it comprises also the National Centre for Cybercrime and Protection of Critical Infrastructures (CNAIPIC), with responsibilities over Critical Infrastructure protection.	
National Centre for Cybercrime and Protection of Critical Infrastructure (CNAIPIC)	
Type of Organisation: National Government	Ownership: Public

ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Implementation of Security Technology and Standards
Relationships: reports to the Postal and Communications Police Service
Weblink: N/A
Areas of Activity: Unit of the Postal and Communications Police Service specialized against attacks directed towards Critical Infrastructures.

Committee for the Diffusion of Broadband	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: N/A	
Weblink: http://www.comitatobandalarga.it	
Areas of Activity: Scope of the Committee (that was constituted in 2007 by the Italian Ministries of Communications, Regional Affairs and Local Autonomies, and Public Administration and Innovation) is to identify the main Public actions needed to promote the diffusion of Broadband services over the Italian territory; to monitor the evolution and availability of those services; to coordinate different projects run out by single Regions; to set guidelines and provide technical recommendations for those projects.	

Industry Organisations Active in Network and Information Security

Association for Telecommunications, IT and Consumer Electronics (ICT-CE)	
Type of Organisation: Other industry association	Ownership: Non-profit
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Relationships: N/A	
Weblink: http://www.ict-ce.it	
Areas of Activity: Association of Italian Industry in Telecommunication, Informatics and Consumer Electronics.	

AITech-Assinform	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness raising	
Relationships: N/A	
Weblink: http://www.assinform.it/	
Areas of Activity: AITech-Assinform is the Italian association of Information and Communication Technology companies and an affiliate of the Confindustria (Confederation of Italian Industry) AITech-Assinform Member Companies are suppliers of hardware and software; bespoke software development and software customisation services; installation and maintenance services; technical, application and management support and consultancy services; training services; outsourcing services, network services; multimedia content.	

Easy4	
Type of Organisation: Association	Ownership: Non-profit
ENISA Focus Points: Awareness raising	
Relationships: N/A	
Weblink: http://eden.saferinternet.it/	
Areas of Activity: It is part of the European internet safety network INSAFE within the framework of the Safer Internet Programme which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union.	

Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) - Italian Association of IT Security Professionals	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness raising	
Relationships: Italian Delegate of ISSA	
Weblink: http://www.aipsi.org/	

Areas of Activity: AIPSI is a non-profit association founded in 2005 with the scope of representing the community of Italian security professionals. It is the Italian delegate of ISSA (Information Systems Security Association) that counts more than 13.000 associates in 100 organizations around the world. AIPSI activities are: organization of educational forum, documents publication, interactions and links between security experts in order to improve their knowledge, promotion of the correct management of security in public and private organizations.

ISACA Roma	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness raising	
Relationships: Italian Delegate of ISSA	
Weblink: http://www.isacaroma.it/	
Areas of Activity: No-profit association for security experts, mainly interested to Educational activities.	

Association of Italian Experts in Critical Infrastructure (AIIC)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks	
Relationships: Italian Delegate of ISSA	
Weblink: http://www.infrastrutturecritiche.it/aiic/	
Areas of Activity: No-profit organization with the intent of promoting in Italy many activities in the field of Critical Infrastructures, their security and interdependencies: research, education, analysis of risks, awareness, consulting services.	

Other Bodies and Organisations Active in Network and Information Security

CERT-IT	
Type of Organisation: CERT	Ownership: Non-profit
ENISA Focus Points: CERT, Resilience, Awareness raising	
Relationships: N/A	

Weblink: http://idea.sec.dsi.unimi.it/
Areas of Activity: The Italian Computer Emergency Response Team (CERT-IT) was founded in February 1994. The CERT-IT is supported by Dipartimento di Informatica e Comunicazione (DICO) - Università degli Studi di Milano. CERT-IT became a member of the International Forum of Incident Response and Security Teams (FIRST) in 1995, as the first Italian CERT to be admitted. The main goal of CERT-IT is to contribute to the development of security culture in the computer world, in particular the Italian computer world. Promotes research and development activities in computer security. Assists the Italian Internet community in getting the most updated information about computer security; such an activity is developed in close contact with other CERTs in order to facilitate information exchange and update on security systems and incidents. Provides an expertise team in computer incident handling.

CERT SPC	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness raising	
Relationships: part of CNIPA	
Weblink: http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Sistema_Pubblico_di_Connettivit%c3%a0_(SPC)/CERT-SPC/	
Areas of Activity: From January 2008 the CERT SPC has been instituted in order to monitor and prevent intrusions, attacks, and other incidents, to the Central Public Connectivity System	

GovCERT	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness raising	
Relationships: part of CNIPA	
Weblink: http://www.govcert.it/	
Areas of Activity: Coordinates the CERT-AM, which are the CERTs of each unit of the Public Administration, in compliancy with the ICT security directive of the 16/1/2001	

GARR-CERT	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness raising	

Relationships: owned by the GARR consortium	
Weblink: http://www.cert.garr.it	
Areas of Activity: GARR-CERT is the Computer Emergency Response Team for GARR, the Italian Academic and Research Network. It deals with computer and network security incidents.	
CERT Difesa	
Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness raising	
Relationships: part of the Ministry of Defence	
Weblink: http://www.cert.difesa.it/	
Areas of Activity: The CERT-Difesa mission is to assist the national army in protecting the communication networks and promoting the sharing of information around IT security.	
CLUSIT (Italian Association for IT Security)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Relationships: N/A	
Weblink: http://www.clusit.it	
Areas of Activity: CLUSIT is a non-profit organization based on the experiences of other European Information Security Associations such as CLUSIB (B), CLUSIF (F), CLUSIS (CH), and CLUSSIL (L) to be the reference regarding Information Security. Activities: raise the computer security culture among companies, public administration and common citizens. Participate and contribute to development of laws, practical codes, and correct behaviour in computer security both at national and international level. Contribute to the definition of learning programs and of certifications for computer security professionals. Promote the adoption of methodologies and technologies, which can contribute to the improvement of the security level of the information infrastructure at all levels.	
EDEN	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: Awareness Raising	

Relationships: N/A	
Weblink: http://eden.saferinternet.it/	
Areas of Activity: It is part of the European internet safety network INSAFE within the framework of the Safer Internet Programme which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union.	
Altroconsumo	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: Awareness Raising	
Relationships: N/A	
Weblink: http://www.altroconsumo.it	
Areas of Activity: This is a consumer organisation. Its aim is to protect and educate consumers.	
SINCERT	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: N/A	
Weblink: http://www.sincert.it/	
Areas of Activity: SINCERT, National System for the Accreditation of Certification and Inspection Bodies, was founded in 1991 as a Non Profit Organization. The Association aims to accredit the following bodies: Business management systems Certification Bodies, i.e. quality management systems, ICT Security management systems, environmental management systems, occupational health and safety management systems, food safety management systems and many others. Product Certification Bodies. Personnel Certification Bodies. Inspection Bodies.	

Activities

Strategic Initiatives

Industria 2015

Type of Activity: Government Policy

Responsible Organisation(s): Ministry of Economic Development

ENISA Focus Points: Micro-enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards

Weblink: N/A

Description:

General Italian Industrial Policy: launched in September 2006, it has been taken in the Financial Law of 2007. It comprises all Governmental Funding to R&D done by SMEs and general Innovation activities done by the Industrial and Public system.

Funding Program of Lombardy Region

Type of Activity: Governmental Funding Program

Responsible Organisation(s): Regione Lombardia — Camere di Commercio lombarde

ENISA Focus Points: Micro-enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards

Weblink: N/A

Description:

Funding program to favour Innovation processes and the competitiveness of Region Lombardy SMEs.

Research Programmes

Online Sicuro

Type of Activity: Social & Other Research Programmes

Responsible Organisation(s): Clusit

ENISA Focus Points: CERT, AR, Emerging and Current Risks, Micro- enterprises

Weblink: http://www.clusit.it
Description: The project is that of the realization of a Web Security Awareness and Assistance Centre for Citizens and SMEs.

Events

Conference and Workshops

CRITIS'08 3rd International Workshop on Critical Information Infrastructures Security

Responsible Organisation: AIIC - Italian Society of Critical Infrastructures Experts (www.InfrastruttureCritiche.it) and ENEA - The Italian National Agency for New Technology, Energy and the Environment.	Frequency: biennial
ENISA Focus Points: Resilience, Emerging and Current Risks, Development of Security Technology and Standards Policy	
Target Groups: Large Enterprises, Government Organizations, Educational & Research Organizations, Security Professionals	
Weblink: http://critis08.dia.uniroma3.it/	
Description: CRITIS'08 wants to bring together experts from science, industry and public authorities involved in management, supervision and protection of critical infrastructures to provide an interdisciplinary and multi-faceted view about third millennium security strategies for Critical Information Infrastructures.	

Forum Expo ICT Security

Responsible Organisation: Nuovo Studio Tecna	Frequency: biennial
ENISA Focus Points: Awareness raising, Emerging and Current Risks, Implementation of Security Technology and Standards	
Target Groups: Consumers / Citizens, SMEs, Large Enterprises, Government Organizations, Educational & Research Organizations, Security Professionals	
Weblink: http://www.nstecna.com/eventi/ict2008/	
Description: Large exhibition dedicated to all aspect of NIS, from Security of networks and application, to Critical Infrastructures Protection, Risk Analysis, Access Control, Biometrics, Business Continuity, Compliance to norms and standards. The last edition reported large partecipation, with 2.500 presences.	

International Wireless Communications Exposition & Conference (IWCE)

Responsible Organisation: Wireless (Softpeople Group)	Frequency: biennial
ENISA Focus Points: Awareness raising, Emerging and Current Risks, Implementation of Security Technology and Standards	
Target Groups: SMEs, Large Enterprises, Government Organizations, Security Professionals	
Weblink: http://www.videogov.com/it/	
Description: Event dedicated to Public Security, Videosurveillence, Infomobility, Critical Infrastructures	
SMAU	
Responsible Organisation: SMAU	Frequency: annual
ENISA Focus Points: Resilience, Awareness raising, Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Citizens, SMEs, Large Enterprises, Government Organizations, Security Professionals	
Weblink: http://www.smau.it	
Description: Main Italian exhibition over Information & Communications Technologies (ICT). In 2008 there are 16 workshops dedicated to the Security topic.	
Sicurtech Expo	
Responsible Organisation: Fiera Milano Tech	Frequency: annual
ENISA Focus Points: Implementation of Security Technology and Standards	
Target Groups: SMEs, Large Enterprises, Government Organizations, Security Professionals	
Weblink: http://www.fieramilanotech.it/?id=MjQzLTM1MjktMzUxOS1JVEEg	
Main exhibition dedicated to Safety and Security issues, with some aspects connected with NIS, as video-surveillance and solutions for safety at work..	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, three security breaches were reported in Italy.

The most remarkable one happened in May 2008, when the information included names, birthdates, addresses, income and tax paid, arranged alphabetically and according to municipality appeared available on the tax agency website. The site was nearly taken down by the sheer number of people trying to see the information of their neighbours - or celebrities - before it was taken down for good by Italy's privacy agency.

http://technologyexpert.blogspot.com/2008/05/italys-deliberate-data-breach-has.html

Country Report – Latvia

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Riga
Total area:	65 000 sq.km
Population:	2.3 million
Official language:	Latvian
Time zone:	EET (GMT+2)
Currency:	Latvian Lati (LVL)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Latvia, we present a set of three indicators in the Country Highlights section.

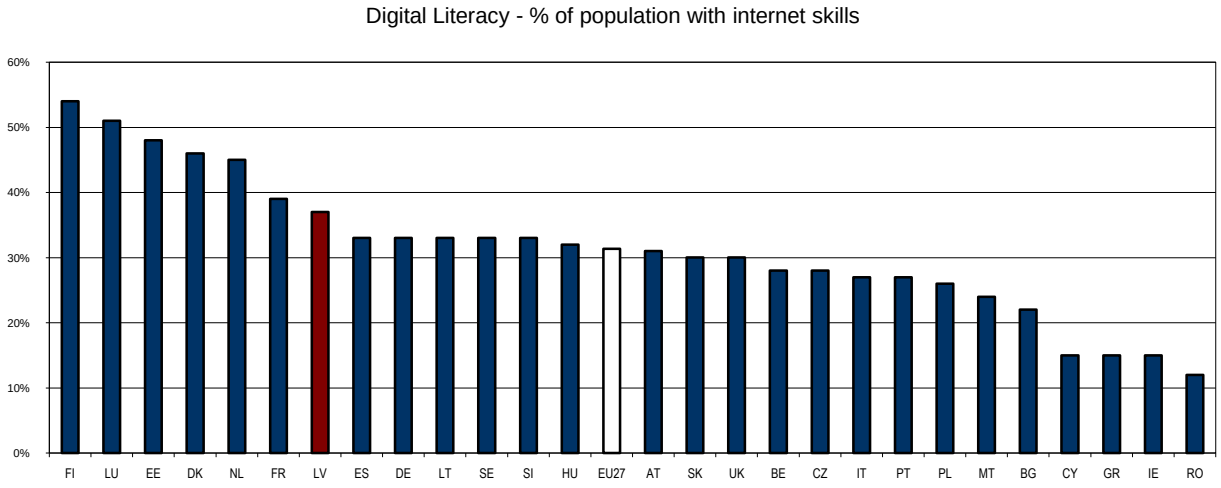
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Latvia is fundamental to this NIS study.

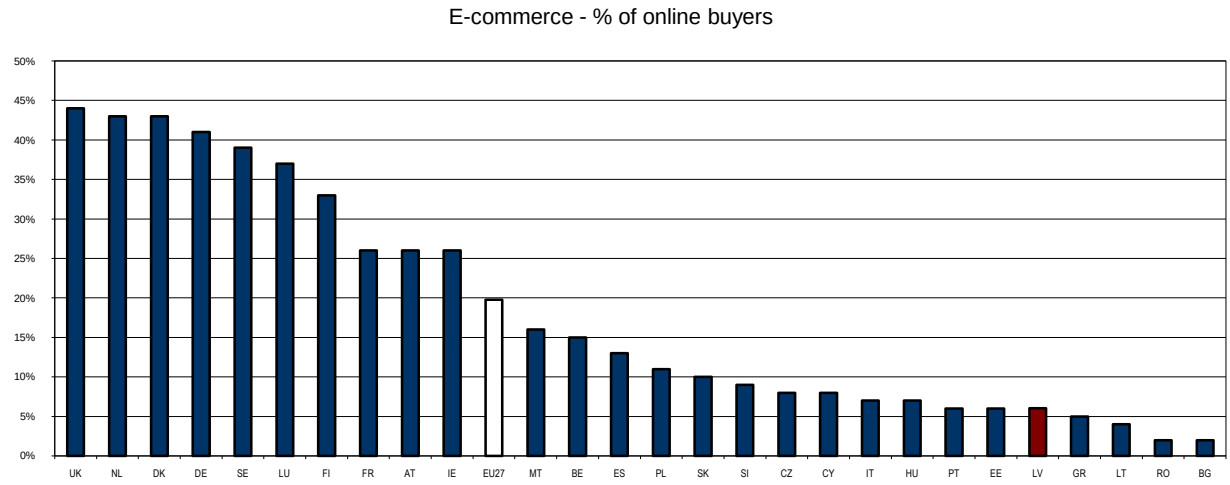
The development of the information society in Latvia is currently doing well, the situation may improve further with particularly strong progress in eGovernment, a rapid adoption of broadband by Internet users, and a business environment relatively favorable to ICT investment, which can rely particularly on a good eSkill base.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

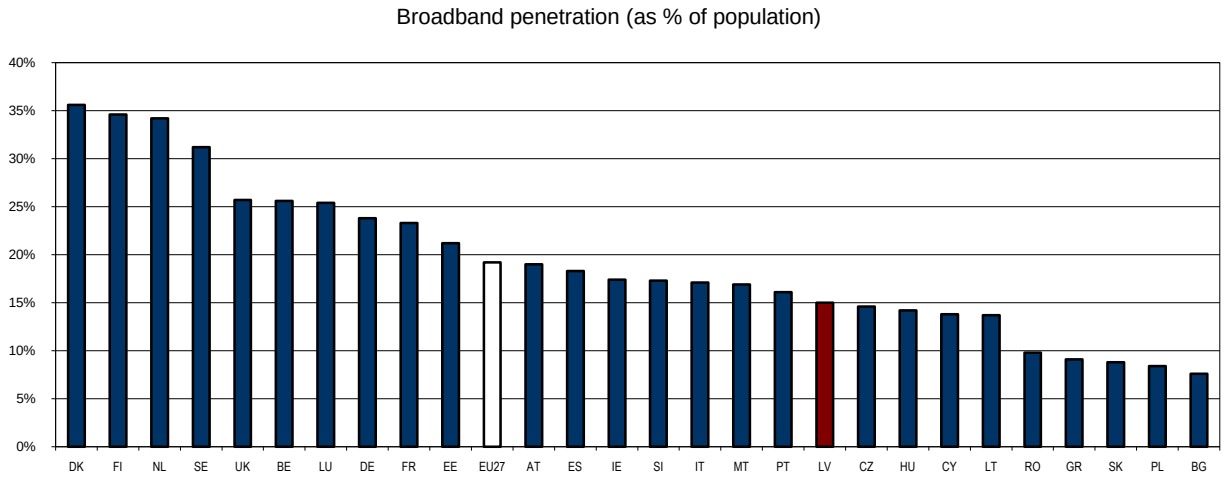
Digital Literacy Indicator



eCommerce Indicator



Broadband penetration Indicator



NIS Highlights

Latvia does not have a single agency or organization that is specialized in NIS or is recognized as the national agency for information security. There are many government bodies involved and the structure of information security responsibilities is unstructured.

The Secretariate of Special Assignments Minister for Electronic Government Affairs is responsible for both the development and implementation of information security policy at the national level in Latvia. The minister organizes and coordinates the development and implementation of the state policy in the field of electronic government, Information Society and IT, and also facilitates and coordinates the development of state and local governments electronic services.

The Data State Inspectorate is responsible for the protection of personal data in Latvia.

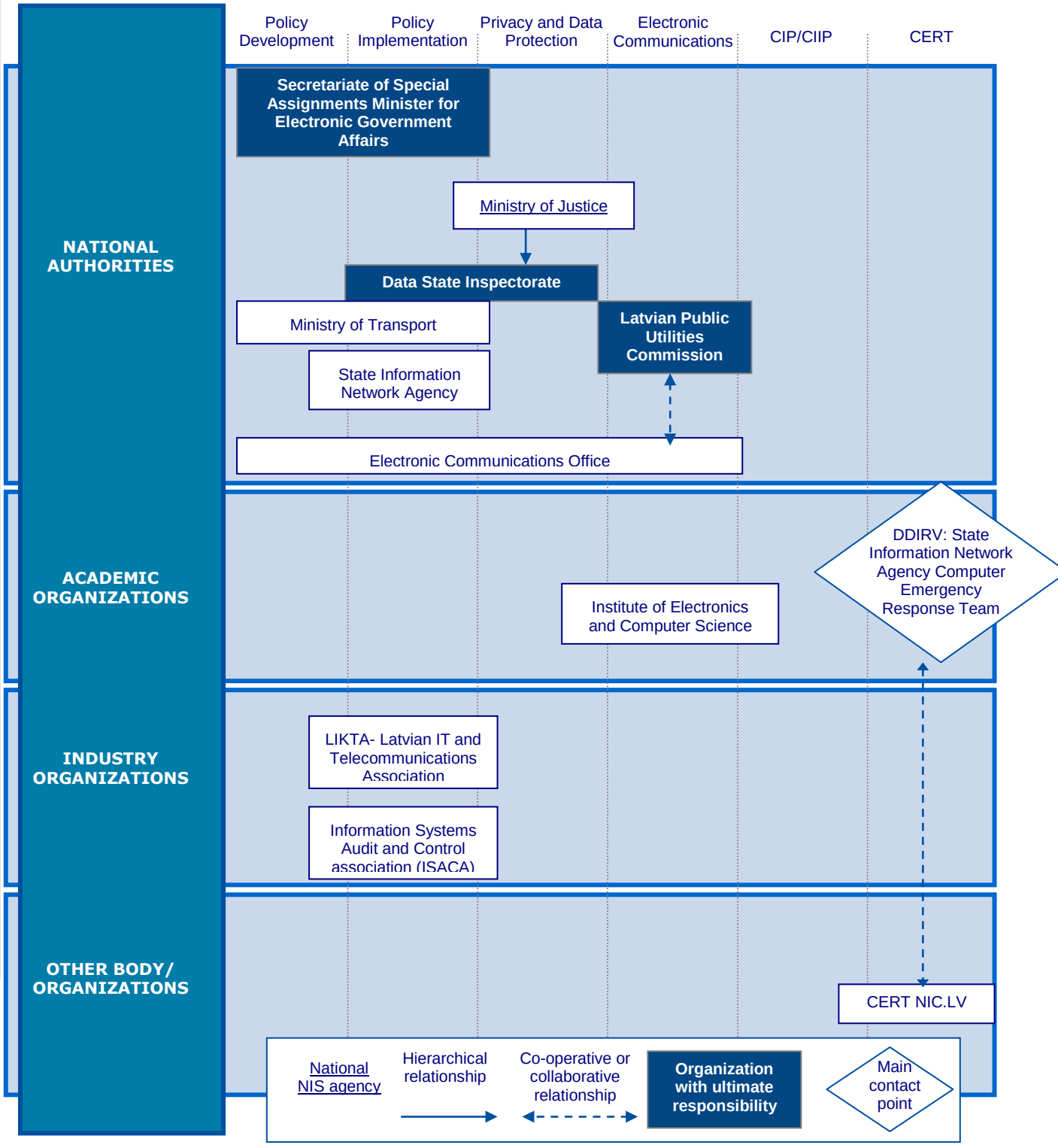
Electronic communications legislation is handled by the Latvian Public Utilities Commission. On 15 April 2004 the Cabinet of Ministers issued regulations No. 304 "Electronic Communications Law" according to the procedure of Article 81 of the Constitution. On 28 October 2004 the Saeima adopted the Electronic Communications Law, which replaced the previous Law On Telecommunications. The Electronic Communications Law introduces new norms of EU directives in the communications sector, particularizes the Commission's functions and specifies new procedures for implementation of these functions. With the approval of the new law the Commission must develop about 40 new secondary legislation acts – regulations, methodologies, procedures and orders.

DDIRV: State Information Network Agency Computer Emergency Response Team was established to provide quality recommendations and consultations for IT administrators in Latvia in case of security incidents. NIC.lv also has responsibilities in this area.

There is no single agency recognized at the national level for activities pertaining to CIP/CIIP.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Latvia. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Secretariate of Special Assignments Minister for Electronic Government Affairs			X	X			X	X
Data State Inspectorate			X	X				X
Latvian Public Utilities Commission							X	X
DDIRV: State Information Network Agency Computer Emergency Response Team	X	X						

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in the Latvia:

National Authorities in Network and Information Security	
State Information Network Agency	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.vita.gov.lv/	
Areas of Activity: The Agency is responsible for maintenance of the National Data Transmission Network. It is also responsible for operating government CSIRT – DDIRV.	
Ministry of Transport	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: part of Ministry of Interior	
Weblink: http://www.sam.gov.lv/	
Areas of Activity: The ministry is charged with elaboration of the transport network, communication policy, organization and coordination of the implementation of transport legislation, communication policy, as well the execution of other functions as laid out in normative acts. The ministry of Transport is a leading institution of state administration of transport and communication branches, which elaborates legal acts and policy planning documents regulating the branch. It provides the implementation of the transport policy.	
Data State Inspectorate	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: Part of Ministry of Justice	

Weblink: http://www.dvi.gov.lv/eng/
Areas of Activity: The Data State Inspectorate was established on 2 January 2001 to operate in accordance with the Personal Data Protection Law, based on the Cabinet of Ministers Regulations No 408 of 28 November 2000 Regulations on the Data State Inspectorate. The Inspectorate is a government authority providing the supervision of personal data protection under the auspices of the Ministry of Justice. The duties of Data State Inspectorate include: control and supervision of processing of personal data state-wide in compliance with requirements of the Personal Data Protection Law; control the compliance with safety requirements concerning the safety of information in personal data processing systems; to handle complaints, make decisions related to protection of personal data, draft recommendations: and, to register personal data processing systems to develop the Personal Data Processing Register.

Secretariate of Special Assignments Minister for Electronic Government Affairs	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Interior	
Weblink: http://www.eps.gov.lv	
Areas of Activity: Supervision of implementation of the Law on State Information; Systems and Government Regulations on Security of State Information Systems; and Technical Provisions for State information Systems; Coordination of Implementation of digital signature and e-government services; coordinates projects with the aim to raise society's awareness on information security.	

State Police Cybercrime	
Type of Organisation: Other Public Bodies	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade and the Ministry of Justice	
Weblink: n/a	
Areas of Activity: This department of the Latvia police deals specifically with cybercrime affairs.	

Ministry of Education and Science	
Type of Organisation: National Governmental Organizations	Ownership: Public
ENISA Focus Points: AR	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://izm.izm.gov.lv/58.html	
Areas of Activity: The ministry is charged with development of technological research and curriculum in Latvia. The Ministry ensures development and implementation of a policy in the fields of education, science, sports and state language promoting sustainable growth of welfare of the citizens of Latvia as educated, healthy, physically and mentally developed personalities and integrity of the society of Latvia. The Ministry strengthens and ensures provision of information to the public, explanation of the adopted resolutions and the link with the society by means of implementing the best practice of the administration process and transparent principles of operation of the state administration.	

Electronic Communications Office	
Type of Organisation: Other Public Bodies	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.esd.lv/index.php?lang=en	
Areas of Activity: State Joint Stock Company whose main functions include: management of radio frequency spectrum and numbering to ensure their rational and effective use; technical planning the use of radio frequency spectrum and assigning radio frequencies for radio equipment operation; the provision of electromagnetic compatibility and numbering services; and, assigning call-signs (identification) to radio stations.	

Latvia Public Utilities Commission	
Type of Organisation: National Authority	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: collaborates with the Electronic Communications Office	
Weblink: http://www.sprk.gov.lv/	

Areas of Activity:

Public Utilities Commission (PUC) is an independent state institution responsible for regulation of energy, telecommunications, post and railway sectors in accordance with the law "On Regulators of Public Utilities" and the corresponding normative acts in the regulated sectors.

Industry Organisations Active in Network and Information Security

LIKTA- The Latvian Information Technology and Telecommunications Association

Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Relationships: co-operates with the National Authorities	
Weblink: http://www.likta.lv	

Areas of Activity:

The Latvian Information Technology and Telecommunications Association - LIKTA - is a professional association, founded in 1998, that regroups over 60 important ITTE product and service providers and educational institutions, as well as over 150 individual professional members of the ITTE industry sector in Latvia, namely in computer hardware and software, electronics, and telecommunications infrastructure and service providers. LIKTA member organisations employ over 15 000 people. The principal objective of LIKTA is to promote and further the development of Information Society in Latvia, so that all citizens may be given the opportunity to benefit from ITT and contribute to the Knowledge based economy. LIKTA works toward increasing e-awareness in society by organizing conferences and educational endeavours and takes an active part in preparing professional study programs for ITT specialists. It has also set up the European Computer Driving Licence (ECDL) certification process in Latvia to allow non-specialists to confirm their computer skills. LIKTA also provides expert advice to Governmental institutions on legislative and other matters related to ITTE, and maintains close links to other more specific ITTE industry associations, as well as to corresponding organisations abroad. It is an active spokesman on behalf of the ITTE industry in Latvia. LIKTA is actively involved in discussing legislation and in monitoring public procurement procedures for ITT products and services.

LDTA- Association of Computer Technologies of Latvia

Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Development of Security Technology and Standards	
Relationships: none	
Weblink: http://www.itnet.lv	

Areas of Activity: Association of computer Technologies of Latvia (LDTA) is a non-profit organization that was founded on September 1997 and is the oldest association in IT industry in Latvia. The founders and members of the association are the biggest IT companies and juridical persons that deal with IT solution development and implementation as well as IT product whole seller's enterprises. LDTA is a member of LTA (Association of Telecommunications of Latvia) and LTA is a member of LDTA that provides close contact with telecommunication companies in Latvia. Currently LDTA consists of 15 legal members that represent the majority of Latvia's IT industry. At the moment the members of LDTA are taking part in processes that provide creation of Information Society infrastructure and are actively using and promoting the principles of New Economy. LDTA has developed a successful partnership with the Customs office and State's Revenue Service that secures the environment of a fair competition in the Latvian market.

Latvian Electrical Engineering and Electronics Association	
Type of Organisation: IT Association	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: none	
Weblink: http://www.letera.lv	
Areas of Activity: Develops Industry of Electronics and Electrical Engineering in the branch of Information and Communications Technology.	

Information Systems Audit and Control association (ISACA)- Latvia Chapter	
Type of Organisation: IT Association	Ownership: n/a
ENISA Focus Points: AR, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.isaca.lv	
Areas of Activity: Information systems security, control and audit.	

Internet Association of Latvia (LIA)	
Type of Organisation: IT Association	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: none	

Weblink: http://www.lia.lv
Areas of Activity: LIA regularly researches IT markets and determines problems, of which some are related to security on the Internet.

Academic Organisations Active in Network and Information Security

Institute of Electronics and Computer Science

Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks,	
Relationships: Part of the University of Latvia	
Weblink: http://www.ces.net/	
Areas of Activity: IECS was founded in 1960 as a research institution of the Latvian Academy of Sciences. In 1997 IECS was incorporated into the structure of the University of Latvia.	

Other Bodies and Organisations Active in Network and Information Security

Riga Information Technology Institute

Type of Organisation: Research Center	Ownership: private
ENISA Focus Points: Resilience, AR, Implementation of Security Technology and Standards	
Relationships: part of CESNET	
Weblink: http://www.riti.lv	
Areas of Activity: Riga Information Technology Institute is the research and development institution. RITI was established in 1995 as the subsidiary of Exigen Services Latvia. Major areas of research include: Software engineering methods and tools; Management and security of information systems; Terminology related to information and communications technologies; Methodologies and tools for software testing; Developing higher education in the field of information and communications technologies; Quality management in software design; and, Development of the Information Society. The National Data Inspectorate of Latvia has included RITI on the list of organizations, which have the right to provide certified services in terms of testing the security of information systems, equipment and procedures.	

Activities

Strategic Initiatives

Project Net-Safe

Type of Activity: Governmental Policies

Responsible Organisation(s): Secretariat of Special Assignments Minister for Electronic Government Affairs and the Latvian Internet Association (LIA)

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.drossinternets.lv

Description:

The aim of the project is to create a Latvian national awareness node in the Insafe network, which coordinates information about safe use of internet in Europe; to ensure safer use of Internet and other up-to-date communication technologies, to prevent distribution of illegal contents in the internet and to involve the society and internet service providers in the improvement of information environment quality. The project is further aimed at educating the target groups (children, youth, teachers and parents) about internet content safety and the potential threats (hostilities, racism, child pornography and paedophilia, cyber-bullying, personal data (identity) theft and data abuse, viruses etc.).

Electronic Signature Breakthrough Program

Type of Activity: Governmental Policies

Responsible Organisation(s): Government

ENISA Focus Points: Implementation of Security Technology and Standards

Weblink: n/a

Description:

In October 2006, the Lithuanian government and a number of leading companies signed the "Electronic Signature Breakthrough Program", which seeks to create favourable conditions for the development of the electronic signature so as to increase the use of the e-signature and its infrastructure very significantly over the next three years. Nearly all of the major post offices of the Latvia Post (LP) can handle requests for e-signatures.

Hotline

Type of Activity: Governmental Policies

Responsible Organisation(s): Secretariat of Special Assignments Minister for Electronic Government Affairs and the Latvian Internet Association (LIA)

ENISA Focus Points: AR
Weblink: http://www.drossinternets.lv http://www.ebaltics.com/forum2008/Presentations/Krike.pdf
Description: On 1 July 2007 the Secretariat of Special Assignments Minister for Electronic Government Affairs in cooperation with Latvian Internet association launched the project Hotline Latvia within the framework of European Community program Safer Internet plus. The duration of the project is 14 months. The main aim of the project is to make the Internet environment safe for children by providing the possibility to report on breaches on the Internet. Project Hotline is tightly connected with another project Net-Safe. In other European countries such hotlines function successfully already for several years, and, as a result, improvements on children safety on the Internet have been achieved. While implementing these projects, educational campaigns are organized for children, their parents and teachers about safe usage of Internet as one of the ways to protect yourself and others – ensured by the possibility to report on discovered breaches on the internet.
Education System Informatization Program
Type of Activity: Governmental Policies
Responsible Organisation(s): Latvian government
ENISA Focus Points: AR, Implementation of Security Technology and Standards
Weblink: http://www.liis.lv/english/main.htm
Description: The Programme Information and Communication Technologies for Education Quality (hereinafter – Programme) is a medium-term policy planning document with a set strategic goal and sub-goals, tasks for policy realization, activity directions, necessary resources, as well as activity results and progress indicators for the period from 2007 to 2013.
e-Latvia 2005-2008
Type of Activity: Governmental Policies
Responsible Organisation(s): Secretariat of Special Assignments Minister for Electronic Government Affairs and the Latvian Internet Association (LIA)
ENISA Focus Points: AR, Implementation of Security Technology and Standards
Weblink: http://www.eps.gov.lv

Description:

The Information Society programme "e-Latvia 2005-2008" aims to ensure the dynamic development and competitiveness of the country in the knowledge-based economy. Priority areas include e-Government, e-Learning, e-Business and welfare, e-Health, Broadband and access to services, and Security.

SIIS

Type of Activity: Governmental Policies

Responsible Organisation(s): Latvian Government

ENISA Focus Points: AR

Weblink: n/a

Description:

The new program of Informatics teaching in primary school, as well as a program for secondary school, corresponding to ECDL requirements were implemented in 2004. From 2008, after completing school, students will possess sufficient ICT skills. However the IT infrastructure in schools in Latvia is out of date and it is of insufficient capacity, as the amount of modern computers per 100 pupils is 4 times smaller than in Europe, thus the amount of out-of-date computers in 2003 exceeded the amount of new computers. It is necessary to improve ICT use in mastering other classroom disciplines.

Funding Programs and Financial Initiatives

Latvia@World project

Type of Activity: Non-Gov Funding Programmes & Financial Initiatives

Responsible Organisation(s):

LIKTA

ENISA Focus Points: AR

Weblink: http://www.csirt.cz

Description:

The Latvian Information and Communications Technology Association (LIKTA) has begun to offer free computer training to people in Riga under the auspices of the Latvia@World project. A new computer training class was opened in August, with 10 workstations. The plan was to train 30 instructors and then more than 1,000 residents of Riga by the end of 2006. Telco Lattelecom supported the installation of the training classroom, which allows the people of Riga to learn basic computer skills at no charge.

Events

Conference and Workshops

Baltic IT&T Forum

Responsible Organisation: Data Media Group; ENISA; LIKTA	Frequency: Annual
ENISA Focus Points: Resilience, AR, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major- Consumers/Citizens, Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises; Minor- Government Institutions	
Weblink: http://www.ebaltics.com/?sadala=106	
Description: Workshop will feature a professional discussion of information security, covering such issues as awareness raising, management of information security, legal aspects of this process, as well as specific information security incidents and how they have been resolved. Target audiences of the workshop are IT and information security managers and practitioners, security specialists and auditors, as well as state administration representatives and SME executives. 2008 was 12th such conference so 1997 is assumed to have been the first.	

Baltic Dynamics

Responsible Organisation: Latvian Technological Centre	Frequency: Annual, but rotates among three Baltic States every year
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Target Groups: Major- SMEs, Government Institutions, Large Enterprises, Security Professionals; Minor- Educational and Research Organizations	
Weblink: http://www.innovation.lv/baltdyn07/default.htm	
Description: From the 13th to 15th of September, the annual international conference 'Baltic Dynamics' took place in Riga again. Organized by Latvian Technology centre, the event gathered more than 400 participants from 35 countries, which is a record in the 12-year history of Baltic Dynamics event. Overall 85 reports were presented. Moreover - several governmental and other officials participated at Baltic Dynamics this year: the minister of education and science Baiba Rivþa, minister of economy Jurijs Strods and manager of LIDA (Latvian Investment and Development Agency) Andris Ozols. The president of Latvia Valdis Zatlers also attended an evening event.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

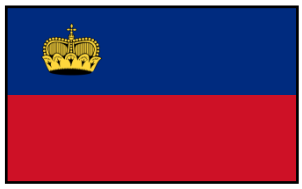
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Latvia.

Country Report – Liechtenstein

Country General Information



Source: European Commission

Political system:	Principality
Capital city:	Vaduz
Total area:	160 sq.km
Population:	0.03 million
Official language:	German
Time zone:	CET (GMT+1)
Currency:	Swiss Franc (CHF)

Source: Eurostat

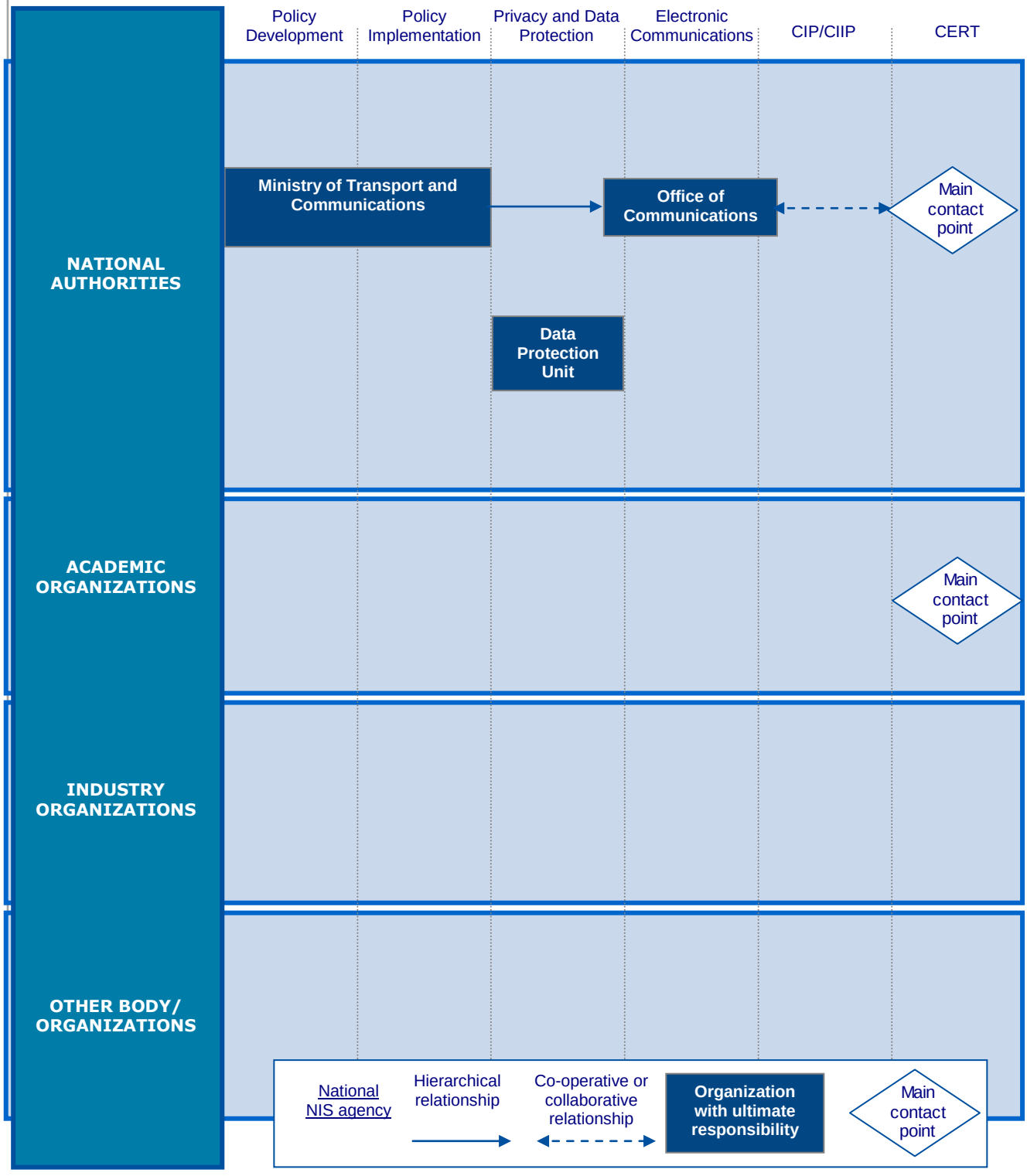
NIS Highlights

The Ministry of Transport and Communications is responsible for the development of electronic communication policy. Its body, the Office of Communications, is the national regulatory authority with the tasks of monitoring responsibilities in electronic communications, and administrative responsibilities of frequencies, numbering and Identification resources.

Liechtenstein is committed to data protection and ensuring compliance in this regard. The Data Protection Unit is an independent oversight body responsible for this task. It is in charge of supervision of both the protection of personal data, as well as access to public information. The tasks may include maintaining a register of databases, investigating complaints, imposing fines for violations, conducting audits and providing consultations on data protection, and commenting on legislative proposals.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Liechtenstein. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Transport and Communications							X	X
Data Protection Unit								X
Office of Communications								X
SWITCH-CERT	X							

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Liechtenstein:

National Authorities in Network and Information Security	
Ministry of Transport and Communications (*Ressort Verkehr und Kommunikation*)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.llv.li/amtsstellen/llv-rfl-verkehr.htm	
Areas of Activity: Responsible for the policy of electronic communications.	
Amt für Kommunikation (AK) - Office of Communications	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: reports to the Ministry of Transport and Communications	
Weblink: http://www.llv.li/amtstellen/llv-ak/llv-ak-home.htm	
Areas of Activity: National Regulatory Authority with the tasks of monitoring responsibilities in electronic communications, administrative responsibilities of Frequencies, numbering and Identification resources.	
Stabsstelle für Datenschutz - Data Protection Unit	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: reports to the Ministry of Justice	
Weblink: http://www.llv.li/amtstellen/llv-sds/llv-sds-home.htm	
Areas of Activity: Responsible for ensuring compliance with data and privacy protection policy.	

Amt für Personal und Organisation - Office of Human and Administrative Resources	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: reports to the Ministry of General Government Affairs	
Weblink: http://www.llv.li/amtsstellen/llv-apo-home.htm	
Areas of Activity: Responsible for the e-Government-strategy of Liechtenstein, and central IT provider for the government.	

SWITCH-CERT	
Type of Organisation: National-CERT	Ownership: Foundation
ENISA Focus Points: CERT	
Relationships: reports to office of communication	
Weblink: http://www.switch.ch/cert	
Areas of Activity: Point of contact for CERT issues for national agencies and academic institutions	

Activities

No significant activities related to NIS are ongoing in Liechtenstein.

Events

There are no significant security-related events held in Liechtenstein.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Liechtenstein.

Country Report – Lithuania

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Vilnius
Total area:	65 300 sq.km
Population:	3.4 million
Official language:	Lithuanian
Time zone:	EET (GMT+2)
Currency:	Litas (LTL)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Lithuania , we present a set of three indicators in the Country Highlights section.

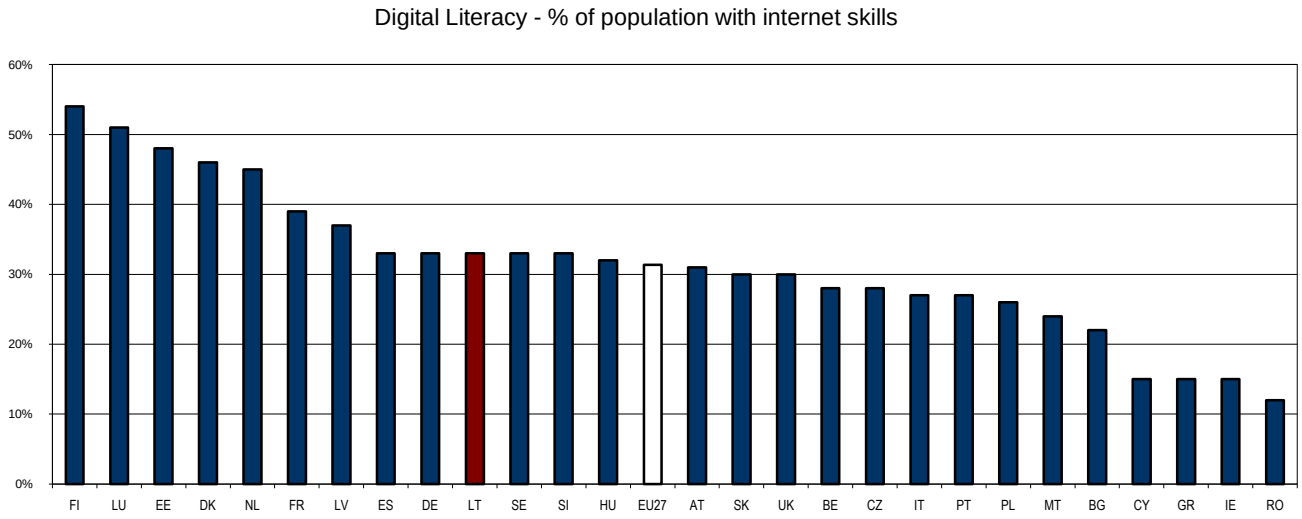
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Lithuania is fundamental to this NIS study.

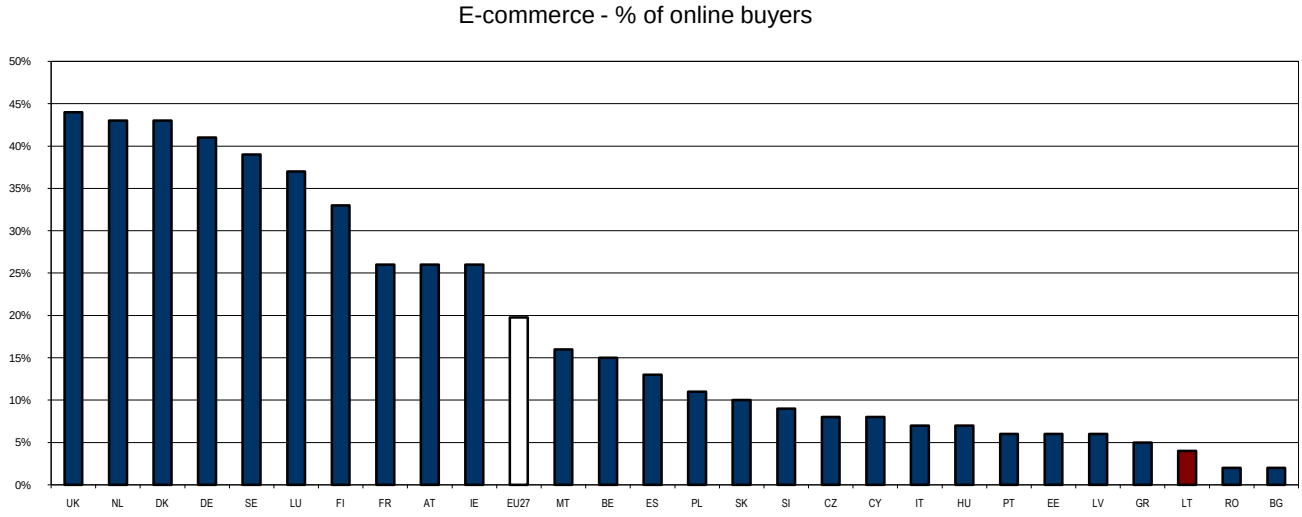
Lithuania experienced a rapid growth of computer and Internet usage, thanks also to special initiatives promoted by the local government, like the possibility to deduct the cost of a computer with software and/or Internet access from the taxes. More and more services rendered to the public are made available also in the form of e-services, among other we can count the declaration of residents' income, employment services, search for information stored by public libraries, social contributions, customs declarations and submission of statistics.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

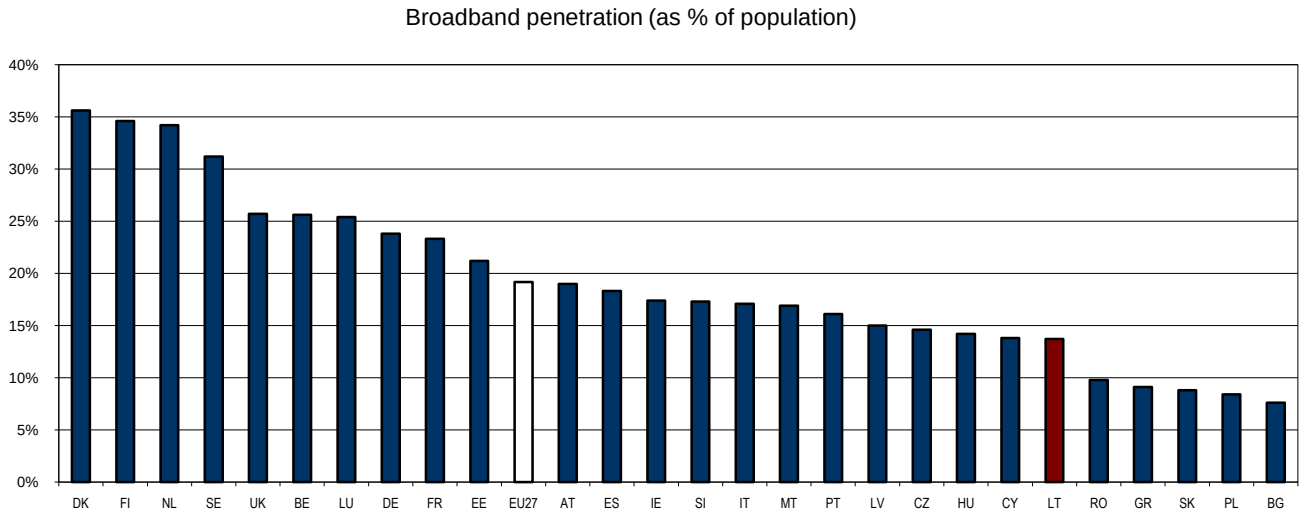
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

In Lithuania there is no organization recognized among the NIS stakeholders having the role of a national security agency. Several government bodies, private sector players, and educational institutions, however, are involved with the process.

Taking responsibility for the development and implementation of national information security policy is the Communications Regulatory Authority of the Republic of Lithuania (RRT), the Ministry of the Interior, Information Policy Department (MoI). The RRT is responsible for private sector supervision and the MoI is charged with setting security policy and coordination of security implementation in governmental sector, information society development policy, development and implementation of e-government projects, participation in electronic signature and personal identification projects.

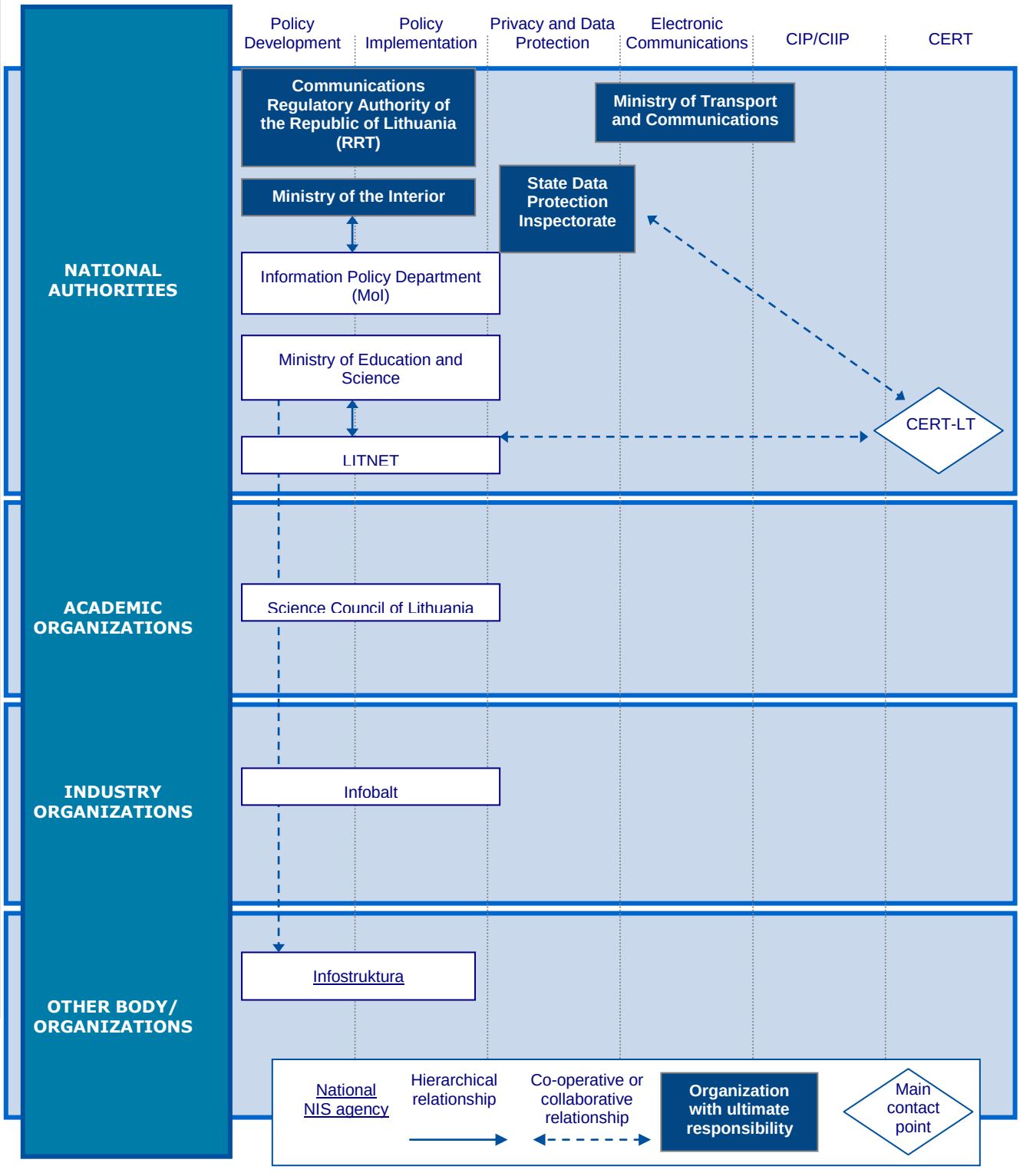
State Data Protection Inspectorate Personal is responsible for data protection in Lithuania. The Inspectorate is responsible for the supervision and control of enforcement of the Republic of Lithuania law on Legal Protection of Personal Data.

Ministry of Transport and Communications is responsible for implementing and ensuring compliance with electronic communications legislation in Lithuania. Officially the ministry is charged with oversight of transport, post and electronic communications legislation.

CERT-LT was established within RRT to coordinate existing Lithuanian CERTs andISPs activities on computer/network/information security. CERT started its activities on October 2, 2006.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Lithuania. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of the interior, Information Policy Department (MoI)							X	X
Communications Regulatory Authority of the Republic of Lithuania (RRT)	X		X				X	X
State Data Protection Inspectorate			X				X	X
Ministry of Transport and Communications							X	X
CERT-LT	X		X					

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Lithuania:

National Authorities in Network and Information Security	
Ministry of Transport and Communications	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.transp.lt	
Areas of Activity: The Ministry of Transport and Communications is authorized by law and other legal acts to perform the functions of administration in the areas of transport (air, water, railway, and road transport), post and electronic communications and implement the State policy in these areas.	
State Data Protection Inspectorate	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.ada.lt	
Areas of Activity: The Inspectorate is responsible for the supervision and control of enforcement of the Republic of Lithuania law on Legal Protection of Personal Data (hereinafter referred to as LPPDL), except its article 8, also for the Republic of Lithuania law on Electronic Communications (hereinafter referred to as ECL) section IX "Personal data processing and privacy security" implementation of provisions of articles (except provisions of articles 63 (5), 65(4) and 70(7)). The Government of the Republic of Lithuania by Resolution No. 1593 of 06/12/2004 "On granting authorization for implementation of the law on Electronic Communications of the Republic of Lithuania" by article 4 entitled the Inspectorate to perform control ensuring the inviolability of electronic communications users' private life according to the procedures established by the Government of the Republic of Lithuania. The Government by Resolution No.807 of 20/07/2005 approved the Rules for Inspections on Communication Secrecy, which specify the procedure of inspections carried out by Inspectorate establishing whether the requirements of ECL article 63(1) to ensure communications secrecy are complied with and also the procedure for formalizing such inspections results.	

Ministry of Education and Science	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development and Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.smm.lt	
Areas of Activity: The Ministry of Education and Science formulates and executes the national policy in the areas of education, science and studies, drafts strategic education plans, annual programmes, submits proposals and resolutions to the Government, organises matura examinations, approves the general content of teaching, training and studies under the framework of formal education (general programmes and subject programmes as well as teaching, training and study plans), national standards for attained education levels (except for higher education and PhD studies), standards for vocational training, guidelines for study areas in higher education, accreditation criteria applicable to curricula and the order of accreditation. Included in this would be curriculum for IT and security courses included within.	

LITNET	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: funded by Ministry of Education and Science	
Weblink: http://www.litnet.lt	
Areas of Activity: Academic and Research Network in Lithuania (LITNET) is an association of Academic research and other non-profit organizations. The members of this association manage and develop the network. The LITNET Network Operating Center (NOC) carries out about network activity. LITNET NOC is located in the Kaunas University of Technology. The main expert of this network is LITNET Technical Expert group.	

Ministry of the Interior, Information Policy Department	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: Part of the Ministry of the Interior	
Weblink: http://www.vrm.lt/index.php?id=291&lang=2	

Areas of Activity: The department is charged with setting security policy and coordination of security implementation in the governmental sector as well as information society development policy, development and implementation of e-government projects, participation in electronic signature and personal identification projects.

Information Society Development Committee	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development and Implementation of Security Technology and Standards Policy, Implementation and Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.ivpk.lt	
Areas of Activity: The principal objectives of the Information Society Development Committee is to participate in the process of shaping state information technologies and telecommunications (ITT) policy of the Republic of Lithuania and ensure the co-ordination of the implementation thereof. Ensure planning, creation and development of ITT infrastructure complying with the European Union requirements. In accordance with the ITT development strategy approved by the Government of the Republic of Lithuania, plan and organise the ITT development throughout the country - ensure equal access to ITT for all consumers based in Lithuania, promote competition of ITT service providers and expand the communication between population and legal entities, on one hand, and state and municipal institution, on the other hand.	

RRT- The Communications Regulatory Authority of the Republic of Lithuania	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, AR, Development and Implementation of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.rrt.lt	

Areas of Activity:
RRT was established under the provisions of the Law on Telecommunications and the Directives of the European Union on independent national communications regulatory authorities of the EU Member States. RRT started its activities in May 2001 after the reorganization of the state enterprise State Radio Frequency Service. The establishment of the independent national regulatory institution, i.e. RRT, was one of the prerequisites for closing the telecommunications negotiation chapter when Lithuania was joining the European Union. The mission of RRT is ensuring a variety of technologically progressive, high quality, safe and affordable electronic communications and postal services (products) to every citizen of Lithuania as a prerequisite for the development of the information society. The mission of RRT is aimed at purposive and integrated as well as flexible activities to ensure the infrastructure for the continuous process of the information society formation. The objective of RRT is to ensure a variety of technologically progressive, high quality, safe and affordable electronic communications and postal services (products) to every citizen of Lithuania while influencing the supply of such services in the market on the grounds of a flexible and harmonized framework of the single EU market.

National Consumer Rights Protection Board	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: None	
Weblink: http://www.vartotojoteises.lt	
Areas of Activity: The State Data Protection Inspectorate and National Consumer Rights Protection Board investigate cases of spam. Communications Regulatory Authority of the Republic of Lithuania works in consultation with State Data Protection Inspectorate and National Consumer Rights Protection Board and coordinates spam enforcement activities in Lithuania.	

Infostruktura	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises, Implementation and Implementation of Security Technology and Standards Policy	
Relationships: State enterprise under the watch of the Ministry of the Interior of the Republic of Lithuania	
Weblink: http://www.is.lt/	

Areas of Activity: State Enterprise "Infostruktura" is the administrator of the Secure State Data Communication Network (SSDCN) that is isolated from the Internet and provides the secure nation-wide communication services for public institutions in Lithuania. The enterprise also provides communications via SSDCN and TESTA with the National Networks of EU Member States, EU Institutions and EU Agencies. TESTA is the European Community's own private network, also isolated from the Internet and allows officials from different Ministries and administrations to communicate at a trans-European level in a safe and prompt way.

The Science Council of Lithuania	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.lmt.lt	
Areas of Activity: The Science Council of Lithuania advises the parliament and government of Lithuania on the issues of research and education. Established in 1991 the Science Council of Lithuania was and still remains an initiator or an evaluator of all the most important legislative proposals in the field of the Lithuanian science and studies system. The main aims of the Council are to seek that this system would efficiently develop studies, scientific research and experimental development projects, which are significant to the State economy, social development and international co-operation, and contribute to the creation of intellectual services and science-oriented high tech production as well.	

CERT-LT	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT	
Relationships: Cooperates with the State Data Protection Inspectorate, LITNET, and numerous other groups	
Weblink: http://www.cert.lt/en/institution.html	
Areas of Activity: CERT-LT is the Lithuanian national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security.	

Industry Organisations Active in Network and Information Security

Infobalt

Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Emerging Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.infobalt.lt	
Areas of Activity: Association "Infobalt" unifies Lithuanian IT, communications and electronics companies, as well as scientific institutions, seeking to represent national ICT sector. The association participates in solving strategic sector's development questions and influences the development itself. "Infobalt" unifies 116 members – Lithuanian companies, institutions, education institutions and non-government organizations operating in the fields of IT, telecommunications, e-services and other knowledge society creation activities. The association represents its members in state authorities and management institutions, stimulates cooperation and common activities preparing and implementing national development strategy for ICT sector. Simultaneously the association emphasizes the importance of cooperation among high education, scientific research und ICT sector and initiates activities of such cooperation.	

Activities

Strategic Initiatives

Lit-Grid Program

Type of Activity: Governmental Policies
Responsible Organisation(s): Vilnius University
ENISA Focus Points: Implementation of Security Technology and Standards Policy
Weblink: http://www.litgrid.lt/

Description:

This is a long-term program (2007-2012). It is a government-financed process aimed at deploying, developing, and supporting Lithuania's grid computing, service, and communications infrastructure for the purposes of research and education. The grid is to be integrated into the emerging European and Baltic grid infrastructures, and knowledge about grid technologies and the use of grids in Lithuania is to be brought up to the level which exists in those EU member states that have a longer history of experience with such issues. Furthermore, Lithuania is expected to do more work in defining grid technology policies and in setting standards in this process. The LitGrid program is working on grid-based, parallel and distributed algorithms and other high-performance computing procedures for various research applications that are of interest and importance to Lithuanian scientists.

Electronic Signature Outbreak Program

Type of Activity: Governmental Policies

Responsible Organisation(s): Lithuanian Government, Bank Hansabankas, Bank SEB Vilniaus Bankas, Bank DnB NORD, Bank PAREX, UAB OMNITEL, UAB "Bitė Lietuva", and Association "Langas į ateitį"

ENISA Focus Points: AR

Weblink: n/a

Description:

The "Electronic Signature Outbreak Program" was created in Lithuania in 2006. Its purpose is to use the best practice of neighbouring countries and exclusive advantages of the Lithuanian market to establish an operative infrastructure of electronic signature, as well as organize a critical mass of the users of this infrastructure.

Safer Internet LT Project

Type of Activity: Governmental Policies

Responsible Organisation(s): RRT, Ministry of Education and Science

ENISA Focus Points: AR

Weblink:
http://ec.europa.eu/information_society/activities/sip/projects/countries/lithuania/index_en.htm

http://www.draugiskasinternetas.lt

Description:

Based on the programme "Safer Internet Plus" of the EC, the project "Safer Internet LT" is being implemented in Lithuania from 2007–2009. The main tasks of this project are the following: Education of the society on the issues of a safe internet (awareness node), and Internet hotline operations.

esaugumas.lt
Type of Activity: Governmental Policies
Responsible Organisation(s): RRT
ENISA Focus Points: AR
Weblink: http://esaugumas.lt/
Description: The project consists in creating a new web site which is dedicated in raising the awareness on NIS. The web site is dedicated for Internet users, small/medium size enterprises and state institutions network administrators and is intended to be an interactive forum of NIS for all interested parties. The www.esaugumas.lt page is Lithuania's Internet gateway for all the concerned subjects, aimed at presenting relevant information on the issues of security of networks and information to the Internet users, enterprises and institutions.

Funding Programmes & Financial Initiatives

Fee-free Internet
Type of Activity: Non-Gov Funding Programmes & Financial Initiatives
Responsible Organisation(s): Numerous governmental bodies, private sector players, and the Lithuanian citizenry
ENISA Focus Points: n/a
Weblink: n/a
Description: Funds were obtained from the European Regional Development Fund to enable more residents to have free Internet access assistance was received from the European Regional development Fund for the establishment of public Internet assess points. The project will result in the establishment of 400 public Internet access points. At present, Lithuania has a total of 700 centers offering free Internet usage to the population.

Basics of Lithuanian e-citizens' computer literacy
Type of Activity: Non-Gov Funding Programmes & Financial Initiatives
Responsible Organisation(s): European Social Fund Agency
ENISA Focus Points: AR
Weblink: http://www.langasiateiti.lt/

Description: The main project goal is to provide 50 thousand Lithuanian citizens above 16 years old with basic knowledge in computers and safe use of the Internet during direct teaching in computer classrooms. Training programme has been elaborated upon minimal qualification in computer literacy programme approved by the Government. This programme was prepared in accordance with the European Computer Driving License (ECDL) programme designated for citizens (e - Citizen) that has been implemented in the European Union since the second half of the year 2005. The project ran until May 2008. According to data, 28 percent of the courses participants were citizens from large Lithuanian towns; citizens from other Lithuanian towns amounted to 46 percent; citizens from the countryside - 26 percent from the total amount of the courses participants. The major part of the courses participants are women (78 percent). Having analyzed the course participants by age groups, it became obvious that the courses participants the most interested in receiving basic computers skills are economically active senior citizens.

RAIN

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s): Government of Lithuania

ENISA Focus Points: AR

Weblink: http://www.rain.lt/

Description: Since 2005 during the first stage of the RAIN program there has been fulfilled the project „IT broadband network RAIN in rural areas" which value is 73 millions Lt (21,1 millions EUR). The project is financed in half by Lithuania and the European Union. After the implementation of RAIN project there will be laid 3,400 kilometers of optical cable lines; all 467 rural authorities will be connected with municipalities. With a help of this project phototransmissive channels will reach rural areas where 1/3 that is to say about 370 000 villagers live. The project was completed the 28th of February, 2008. The network is exploited in Klaipeda and Alytus regions; it is planned to start exploitation of RAIN network in Marijampole, Telsiai, Utena, Taurage, Kaunas, Panevezys and Siauliai regions by the end of 2007. The first 8 agreements with retail service operators have already been signed. These operators use RAIN resources and provide users with broadband communications services.

RAIN-2

Type of Activity: Governmental Funding Programmes

Responsible Organisation(s): Government of Lithuania

ENISA Focus Points: CERT

Weblink: http://www.rain.lt/

Description: RAIN-2 is a continuous project stemming from the creation of the RAIN network. The goal of RAIN-2 is to reach the remaining rural areas, where 2/3 of villagers live. It is planned to execute the RAIN 2 project in 2008 – 2011. Planned results of RAIN-2 include: Residents and organizations in 98% of the territory of rural areas will have the availability to use broadband communications services. Additionally a competitive environment for provision of broadband communications will be created, where users will have the possibility to choose a service provider. General knowledge centers in rural areas will include the following: schools, libraries and public internet centers, as well as state authorities. They all will be connected to broadband networks.

Events

Conference and Workshops

Infobalt 2008

Responsible Organisation: Infobalt	Frequency: Annual
ENISA Focus Points: AR, Emerging Risks	
Target Groups: Major- Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.infobalt.lt	
Description: The association "Infobalt" and JSC "Ekspozicijų centras" are hosted the15th exhibition of informational technologies, communications, e-services and electronics at INFOBALT 2008. Basic themes of the exhibition include: Business processes' optimization and E-business means; E-business: e-commerce, mobile commerce, mobile business; E-services for business; technologic platforms of e-service supply; E-business infrastructure, inter-operability; and, E-government, e-health and other e-services to society and business.	

European Network and Information Security Conference

Responsible Organisation: RRT; Ministry of Transport and Communications of the Republic of Lithuania; Ministry of the Interior of the Republic of Lithuania; European Network and Information Security Agency; and, Communications Regulatory Authority of the Republic of Lithuania	Frequency: annual
ENISA Focus Points: Emerging Risks	
Target Groups: Major- Government Institutions, Large Enterprises, Security Professionals, SMEs	
Weblink: http://www.securityconference.rrt.lt/	

Description:

The overall objective of the conference is to bring together actors in charge of different international collaboration instruments in the area of cyber-security. By means of synergy cooperation, the conference aims at enhancing cyber security and providing a forum for information sharing and networking with stakeholders in the private and public sectors as well as civil society. Main topics of the conference include: Framework for cooperation on cyber-security – best practice, Cyber-crime and enforcement, Management of security incidents. There is also a post-conference workshop. This post-conference workshop will target the ISP sector as a critical spot in safeguarding against security incidents and will attempt to deliver some organisational and technological solutions for ensuring protection and efficient management of incidents in the ISP networks. Target audience of the event includes the following groups: Senior representatives of governments and law enforcement organizations working in the field of network and information security; Senior ICT security experts from business and users organizations dealing with network and information security; and, CERT representatives.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Lithuania.

Country Report – Luxembourg

Country General Information

Source: European Commission

Political system:	Constitutional monarchy
Capital city:	Luxembourg
Total area:	2 586 sq.km
Population:	0.5 million
Official language:	French, German
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Luxembourg, we present a set of three indicators in the Country Highlights section.

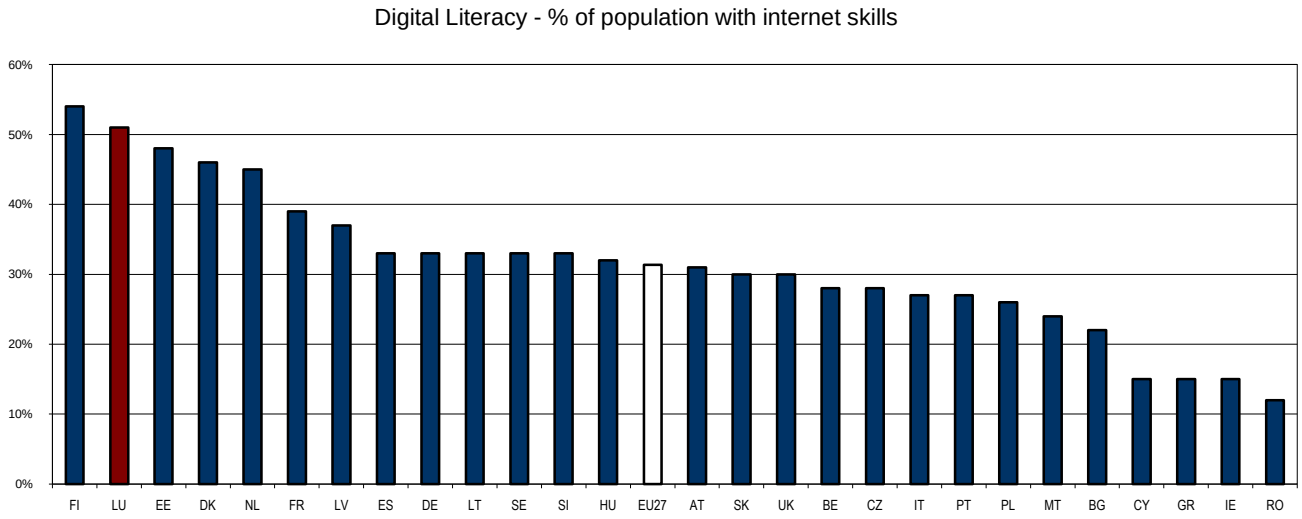
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Luxembourg is fundamental to this NIS study.

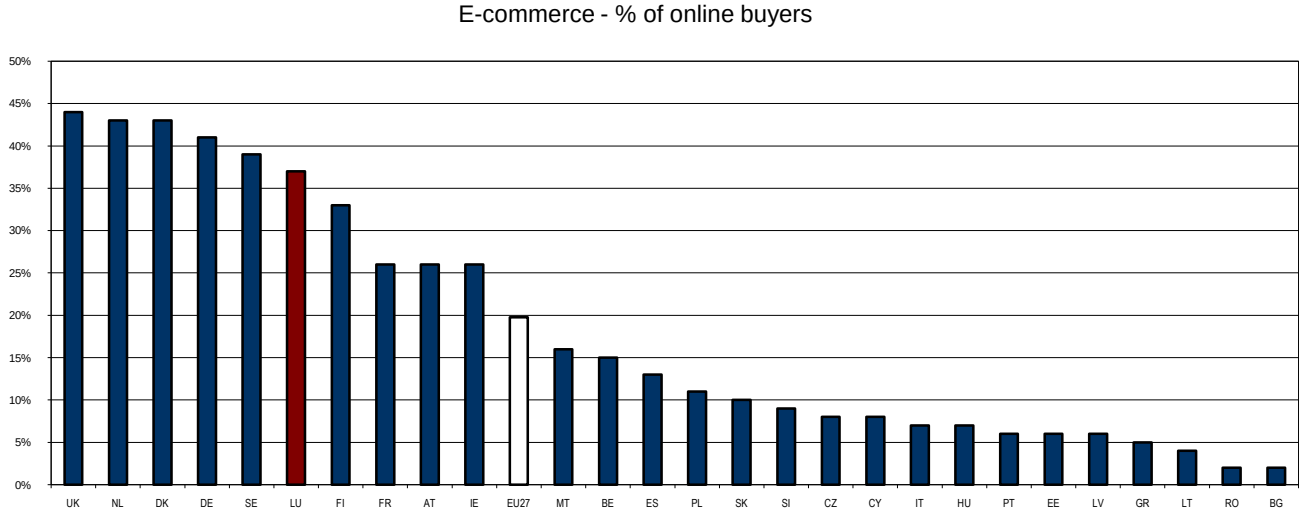
Luxembourg is well advanced in the information society, with strengths including broadband connectivity, households' Internet usage and e-Skills endowments. Take-up of broadband by households and enterprises is growing. Growth in the usage of online services is evident. In the wider economy, enterprise use of broadband and of e-business and e-commerce tools is improving. Skill levels are high both in the general population and in the workforce.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

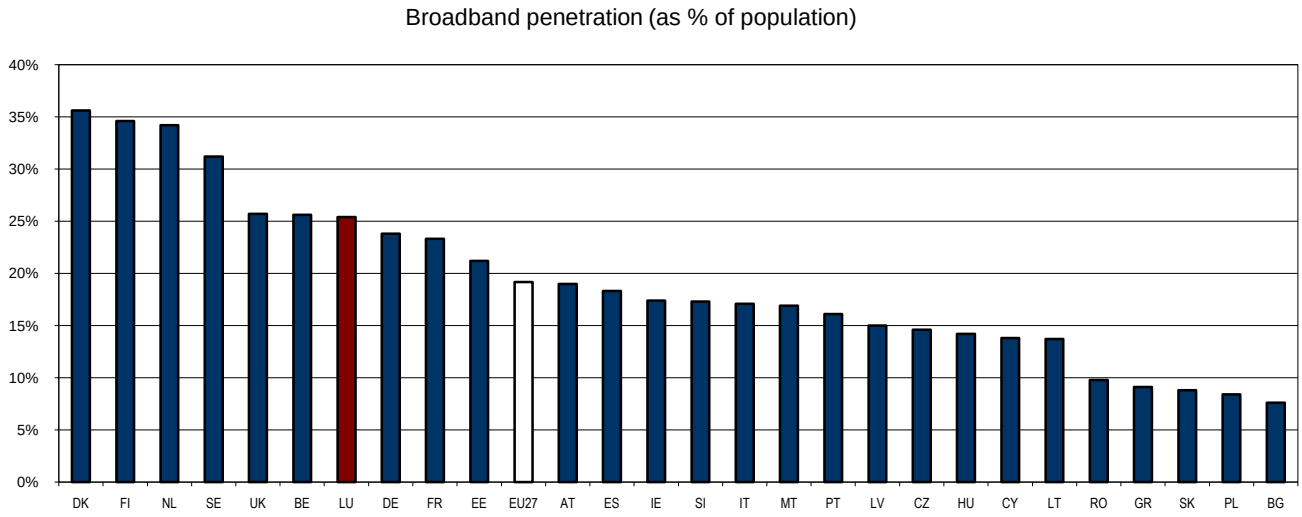
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Stakeholders in Luxembourg do not recognize a single body as the national security agency, although many actors are involved in the process. Additionally there is not a single agency recognized as being solely responsible for the development of national information security policy. The Ministry of the Economy and Foreign Trade is charged with administration and implementation of national security legislation once it is developed.

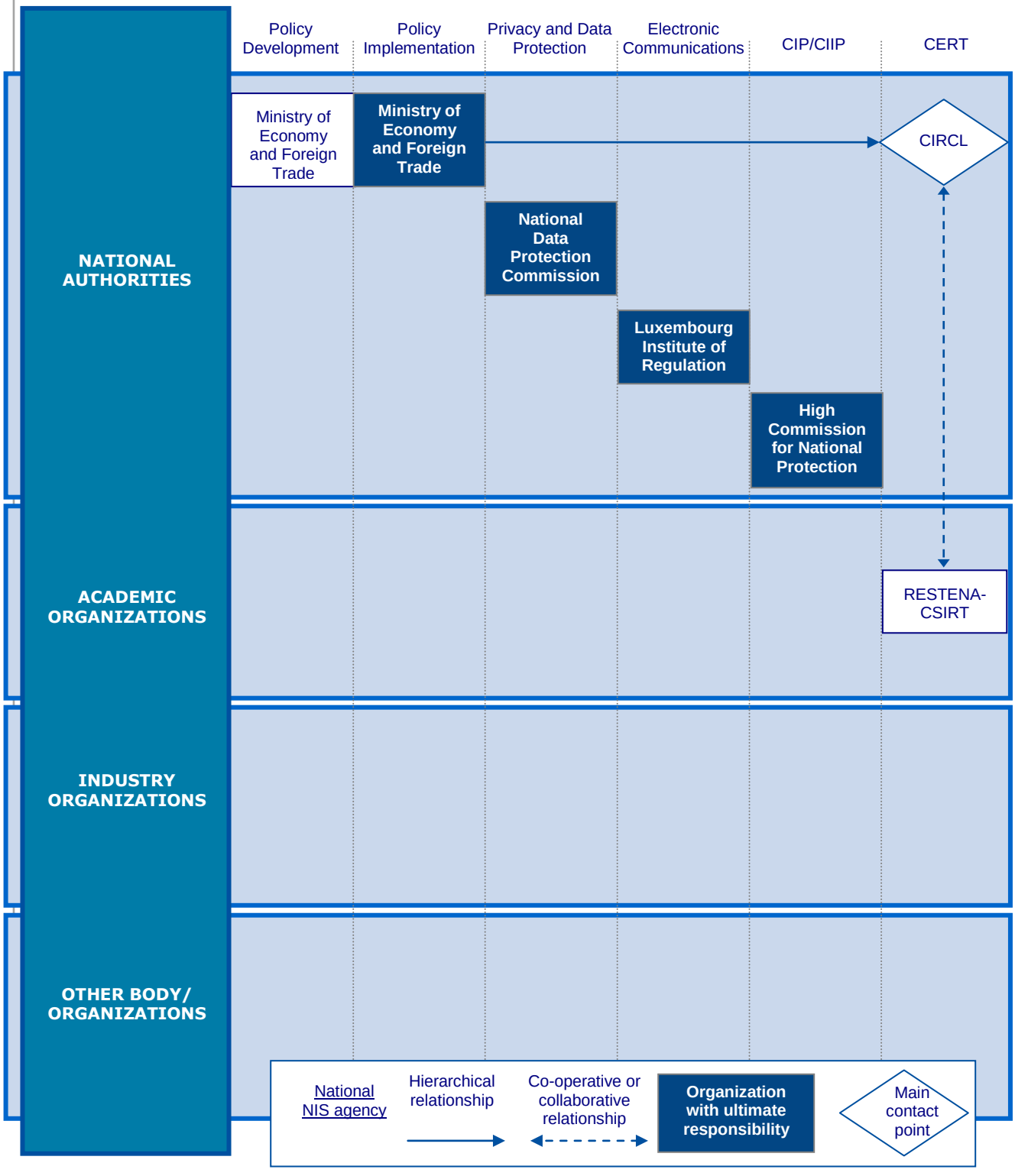
The National Commission for Privacy Protection is the recognized national body for data protection and privacy issues in Luxembourg.

Luxembourg Institute of Regulation is the independent regulatory body responsible for telecommunications, post, radio, electricity and gas regulation. Ensuring compliance with electronics communications legislation is among the body's responsibilities.

CIRCL is the recognized government CSIRT and national coordinator for CSIRT activities in Luxembourg. The High Commission for National Protection (HCPN) is responsible for inter-ministerial coordination of handling crisis management.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Luxembourg. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of the Economy and Foreign Trade			X	X			X	X
National Data Protection Commission (CNPD)			X				X	X
Luxembourg Institute of Regulation			X					X
High Commission for National Protection (HCPN)		X						
CIRCL	X							
RESTENA-CSIRT	X							

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Luxembourg:

National Authorities in Network and Information Security	
Ministère de l'Economie et du Commerce extérieur - Ministry of Economy and Foreign Trade	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Responsible for CASES and government involvement in LuxTrust	
Weblink: http://www.eco.public.lu	
Areas of Activity: Within the Ministry of Economy and Foreign Trade, the Directorate General for Energy, Electronic Commerce and IT Security is responsible for developing and implementing government policy in the area of electronic commerce including legislation related to electronic signature. The Directorate is also responsible for implementing policy in the area of IT security, and promoting awareness of information security.	
Cyberworld Awareness and Security Enhancement Structure (CASES)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: Part of the Ministry of Commerce and Foreign Trade	
Weblink: http://www.cases.lu	
Areas of Activity: CASES is a team within the Directorate General for Energy, Electronic Commerce and IT Security. The main aims of CASES are to raise awareness, promote the use of security measures, and promote confidence through knowledge and co-operation. CASES targets its activities towards citizens, SMEs and government institutions. CASES pursues its aims by developing glossaries, files, reports, rules and policies in the area of information security. These are propagated through various channels including an Internet portal, e-learning platform, workshops and conferences.	

La Commission nationale pour la protection des données (CNPD) – National Data Protection Commission	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: co-operates with the Ministry of Industry and Trade	
Weblink: http://www.cnpd.lu	
Areas of Activity: The CNPD is the national body for data protection and privacy issues. Its duties are to ensure compliance with legislation and the regulatory framework on personal data, and to provide input to the government on laws and measures in the area of the creation and processing of personal data.	

L'Institut Luxembourgeois de Régulation (ILR) – Luxembourg Institute of Regulation	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.ilr.public.lu	
Areas of Activity: Independent regulatory body responsible for the telecommunications, post, radio, electricity and gas sectors.	

Haut-Commissariat à la protection nationale (HCPN) – High Commission for National Protection	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience	
Relationships: co-operates with all relevant public bodies	
Weblink: http://www.hcpn.public.lu	
Areas of Activity: The HCPN is responsible for implementing national protection measures directed by the Ministerial Council for National Protection. Within the HCPN, the National Committee for Telecommunications (CONATEL) is responsible for protection of national communications infrastructure, while the National Committee for Critical Infrastructure (CONATIC) is responsible for other elements of information infrastructure.	

CIRCL - Computer Incident Response Centre Luxembourg	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, AR	
Relationships: Part of the Ministry of Economy and Foreign Trade	
Weblink: http://www.circl.lu	
Areas of Activity: CIRCL is the Computer Incident Response Centre of governmental administrations and ministries of the Grand-Duchy of Luxembourg.	

Le Centre informatique de l'Etat - Government IT Centre	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.cie.public.lu	
Areas of Activity: The Government IT Centre supports state administration in developing and implementing IT systems, promotes e-government and organises related project, and administers the government network RACINE. The Centre has specific responsibility for ensuring information security.	

Industry Organisations Active in Network and Information Security

There are no Industry Organisations in Luxembourg that engage in significant NIS-related activities.

Academic Organisations Active in Network and Information Security

University of Luxembourg, Faculty of Sciences, Technology and Communication	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks	

Relationships: None	
Weblink: http://www.uni.lu	
Areas of Activity: The Informatics research unit conducts research on security of information systems and intrusion detection, and hosts the Laboratory of Algorithmics, Cryptology and Security.	
Réseau Téléinformatique de l'Education Nationale et de la Recherche (RESTENA) - National Education and Research Network	
Type of Organisation: Other Academic	Ownership: Public
ENISA Focus Points: CERT, AR	
Relationships: co-operates with other CSIRT/CERT teams within Luxembourg and internationally	
Weblink: http://www.restena.lu	
Areas of Activity: The primary objective of RESTENA is to provide network services for all public and private institutions and organisations involved in the field of education, research, culture, health and administration. RESTENA operates the RESTENA CSIRT that offers support and coordinates security incident response within its constituency of education and cultural institutions and research centres. The CSIRT also serves as a trusted point of contact and acts as clearing house for security incident-related information, and works to improve awareness and knowledge of IT security,	
Le Centre de Recherche Public Henri Tudor – Public Research Centre Henri Tudor	
Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: Emerging/Current Risks	
Relationships: None	
Weblink: http://www.tudor.lu	
Areas of Activity: CRP Henri Tudor conducts research, often in partnership with the private sector, in a number of areas including information and communication technology, with a number of ongoing projects dedicated to IT security.	
Le Centre de Recherche Public Gabriel Lippmann – Public Research Centre Gabriel Lippmann	
Type of Organisation: Research Centres	Ownership: Public
ENISA Focus Points: Emerging/Current Risks	

Relationships: None
Weblink: http://www.crpgl.lu
Areas of Activity: CRP Gabriel Lippmann is devoted to applied scientific research and technological development, as well as permanent technology transfer and high-level training. The Centre is involved in a limited amount of research in IT security.

Other Bodies and Organisations Active in Network and Information Security

Computer Security Research and Response Team Luxembourg (CSRRT-LU)

Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: CERT, AR	
Relationships: partners with research institutes, the industrial sector and governmental institutions	
Weblink: http://www.cssrt.org.lu	
Areas of Activity: CSRRT-LU is a computer security research and response team association, engaged in computer security development and research projects in order to increase security awareness. CSRRT-LU is supporting multiple research projects to improve the overall technical expertise in Computer/Network Security.	

Luxembourg Information Society staNdardization Association (ANSIL)

Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Implementation of Security Technology and Standards Policy	
Relationships: independent	
Weblink: http://www.ansil.eu	
Areas of Activity: ANSIL is an association of experts in the fields of information security and quality standardisation. Its goals include: being an interface with official institutions; promoting standardisation; participating in research projects; serving as a pool of experts. One of ANSIL's committees focuses on information security.	

LuxTrust

Type of Organisation: Technical and Professional Certification	Ownership: PPP
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships:	
Weblink: http://www.luxtrust.lu	
Areas of Activity: LuxTrust is a certification authority established between the Luxembourg government and major private sector actors of Luxembourg, in particular the financial sector.	

CLUb de la Sécurité des Systèmes d'Information Luxembourg (CLUSSIL) – Luxembourg Association for the Security of Information Systems	
Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: AR, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.clussil.lu	
Areas of Activity: CLUSSIL is an association of experts in the field of information security, whose goals include the development and propagation of methodologies and recommendations in the area of information systems security, and the promotion of co-operation between various actors.	

Activities

Strategic Initiatives

Luxembourg Safer Internet (LuSI)
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): Telindus, CRP Henri Tudor, 12345 Kanner Jugend Telefon
ENISA Focus Points: AR
Weblink: http://www.lusi.lu/

Description: LuSI is the Luxembourg node of the European Safer Internet Programme.

Events

Conference and Workshops	
Internet Security Day	
Responsible Organisation: Ministry of the Economy	Frequency: annual
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Target Groups: Large Enterprises, Government Institutions, : Educational and Research Organizations, Security Professionals	
Weblink: http://www.cases.public.lu/fr/actualites/fc/2008/05/FlyerISD20.pdf	
Description: Internet Security Day is a general NIS conference. Topics covered in past conferences include: fighting cyber crime, information security in the enterprise, electronic signature, online authentication, e-banking security.	
ANSIL Ordinary General Assembly	
Responsible Organisation: ANSIL	Frequency: annual
ENISA Focus Points: Implementation of Security Technology and Standards	
Target Groups: Security Professionals	
Weblink: http://www.ansil.eu/	
Description: Annual meeting which includes breakout sessions on IT security standards.	
Hack.LU08	
Responsible Organisation: CSRRT-LU	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Consumers/Citizens, SMEs, Large Enterprises, Government Organisations, Educational and Research Organisations, Security Professionals	
Weblink: http://wiki.hack.lu/index.php/Main_Page	

Description: Hack.lu is a 3-day open convention/conference where people can discuss computer security, privacy, information technology and its cultural/technical implications for society.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

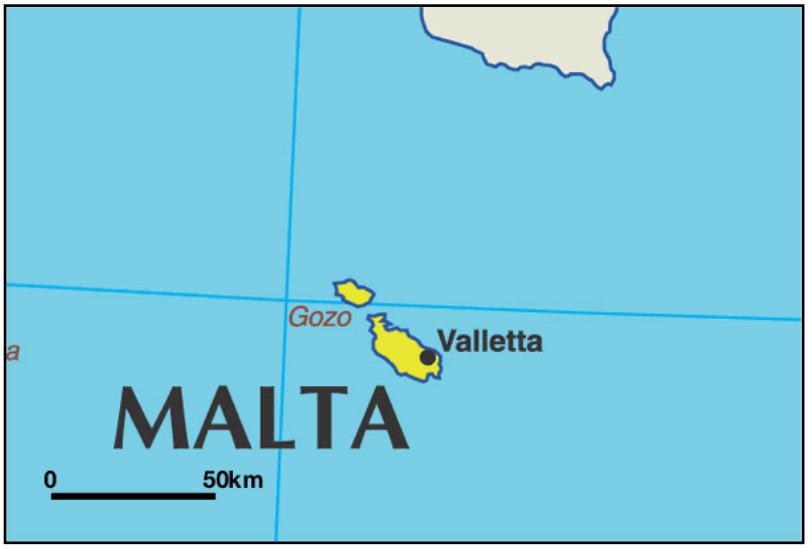
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Luxembourg.

Country Report –Malta

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Valletta
Total area:	316 sq.km
Population:	0.4 million
Official language:	Maltese, English
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Malta, we present a set of three indicators in the Country Highlights section.

The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

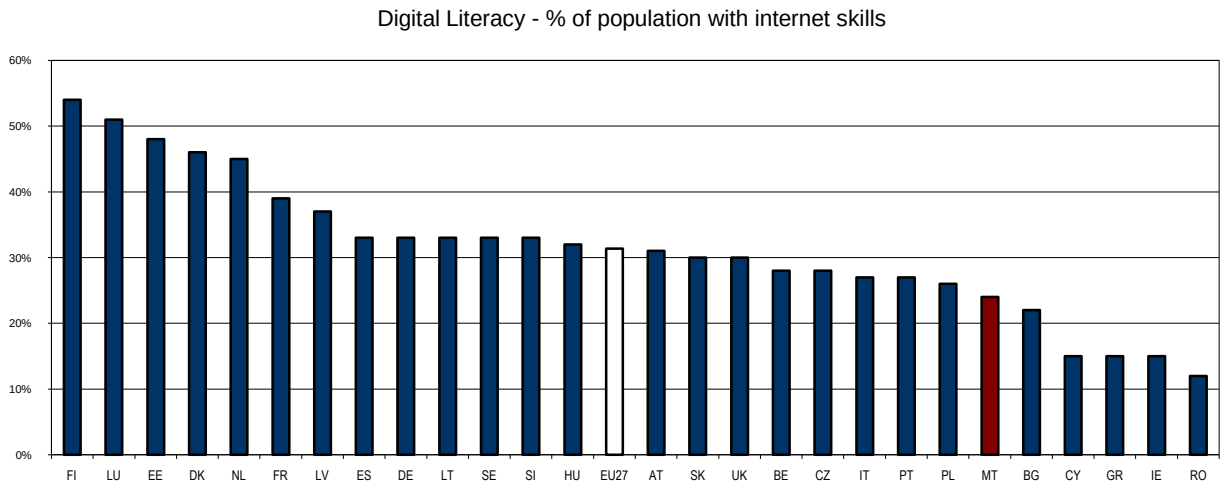
For these reasons, a general understanding of the stage of IT adoption in Malta is fundamental to this NIS study.

Malta recently registered a remarkable advancement on all fronts of the ICT adoption, household accessibility to ICTs has been considerably enhanced; eGovernment has developed into a mainstay of the ICT environment; students graduating in ICT specialisations are on the rise; ICT education has become amongst the most sought after vocational and undergraduate educational streams; the rate of local and foreign ICT investment is reaching unprecedented heights, thanks also to the efforts of the state in promoting Malta as a location for international IT companies.

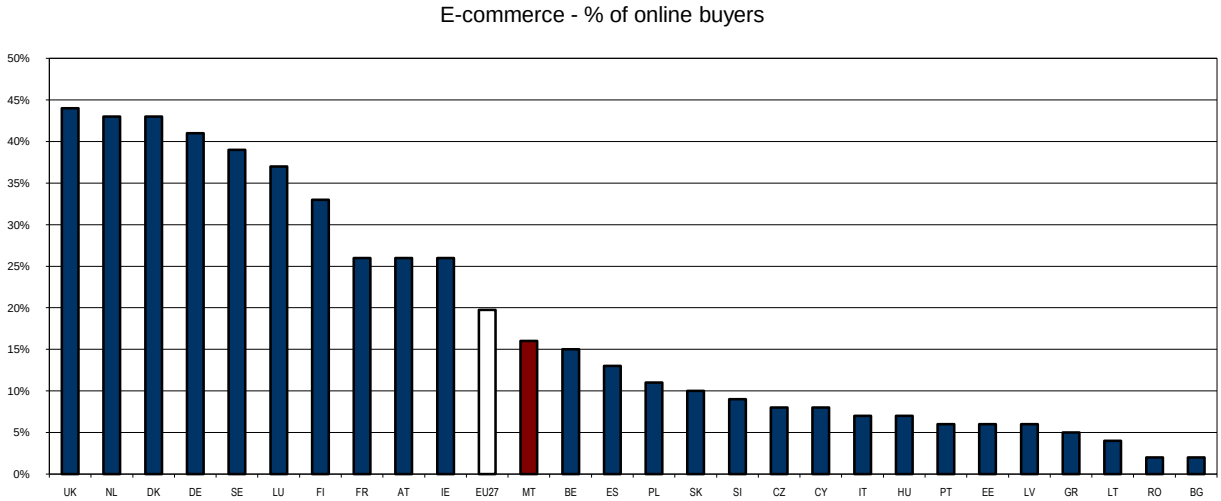
The development of the information society in Malta may improve further in the next years with particularly strong progress in eGovernment, a rapid adoption of broadband by Internet users, and a business environment relatively favorable to ICT investment, which can rely particularly on a good eSkill base.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

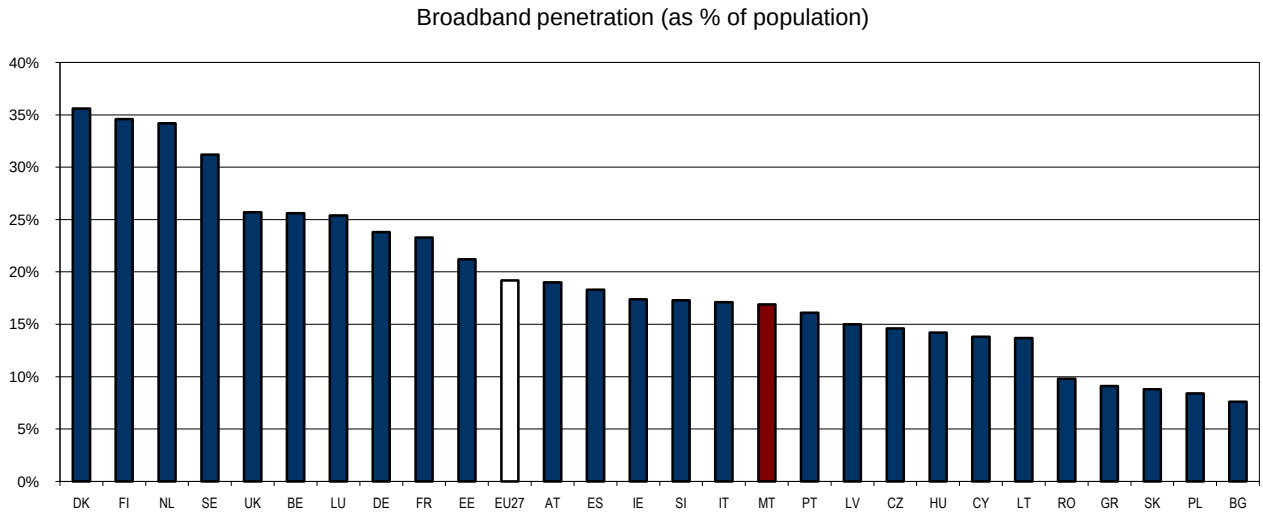
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Malta to date does not have a single organization that is recognized as an NIS agency responsible for leadership in the area of information security. However, in October, 2008, it was announced by the Ministry of IT that the National Information Security Agency would be set up in the coming days. The agency, would be separate but complimentary to the Malta IT Agency and the Malta Communications Authority in the sector of information security.

To date, the Ministry for Infrastructure, Transport and Communications takes responsibility for the development and implementation of national information security policy. The ministry is responsible for legislative framework pertaining to electronic communications, information society services, and signature certification services. The ministry is further charged with implementing initiatives according to the National ICT strategy, including initiatives related to building trust and confidence and confidence in technology usage.

Office of the Data Protection Commissioner is responsible for data protection as per Article 13, of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector on unsolicited communication has been transposed in Maltese law by LN 16 of 2003 under the Data Protection Act (CAP. 440 of the Law of Malta). The law empowers the Data Protection Commissioner to handle any complaints concerning unsolicited communications and to take the remedial action, as he deems necessary.

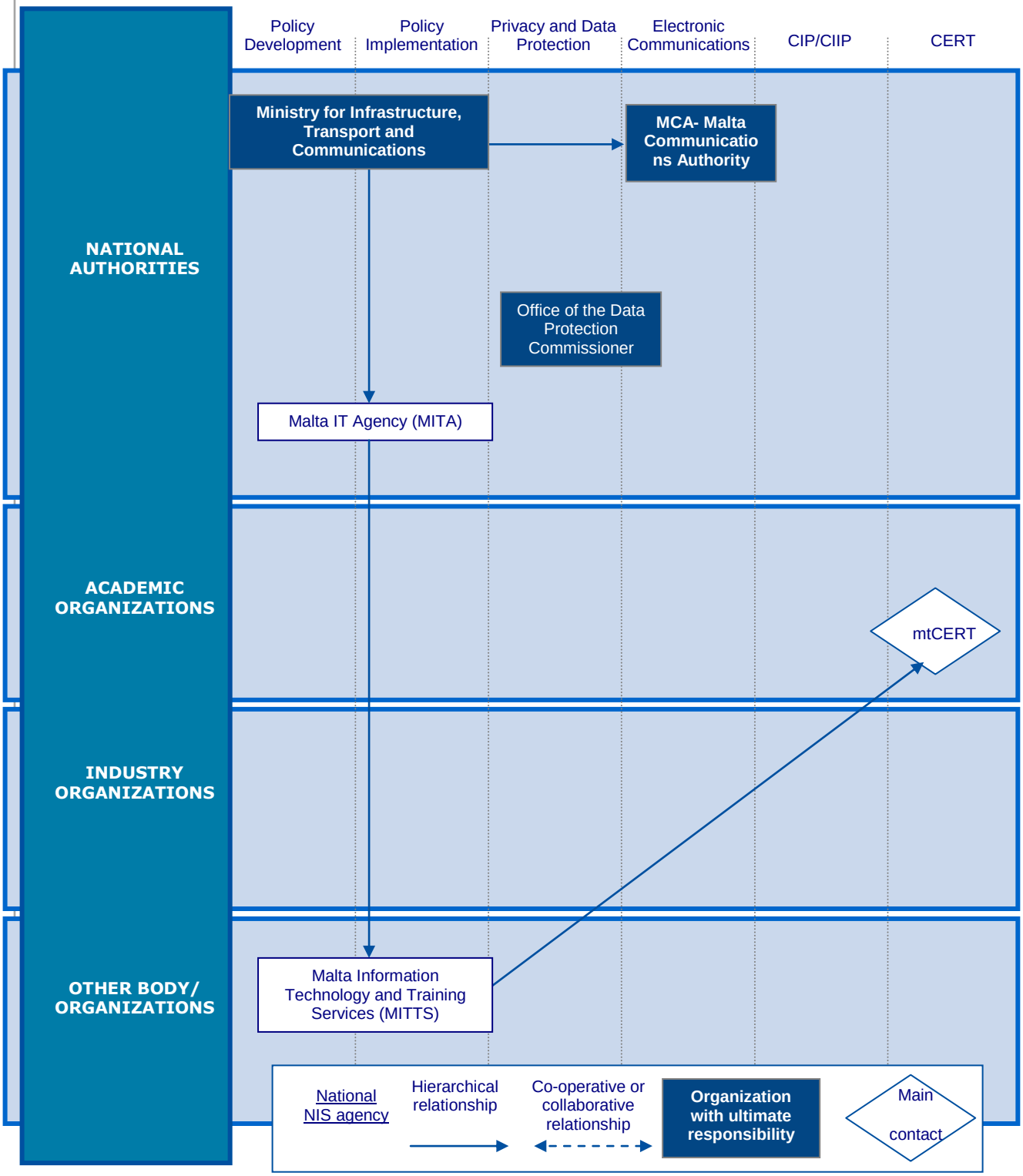
Malta has security response teams in place to handle security breaches and other incidents. mtCERT is responsible to proactively monitor for security threats and to try to prevent any security incidents, to respond to any reported security incidents on the

MAGNET (Maltese Government Network) and to educate all government employees who use computers on the prevention of such threats.

There are no single organizations in Malta that assume responsibility for CIP/CIIP at the national level.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Malta. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry for Infrastructure, Transport and Communications			X	X			X	
Data Protection Commissioner		X	X	X	X			X
MCA- Malta Communications Authority			X	X			X	
mtCERT- MITTS Ltd Computer Emergency Response Team	X							

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in the Czech Republic:

National Authorities in Network and Information Security

MCA- Malta Communications Authority

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: Falls under Ministry for Infrastructure, Transport and Communications	
Weblink: http://www.mca.org.mt	
Areas of Activity: The MCA is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications and broadcasting transmission), e-commerce and the postal sector. The MCA's mission, mandate and functions derive from the Malta Communications Authority Act (Cap 418). The MCA is the National Regulatory Authority (NRA) for these sectors in accordance with EU law, which is subsequently transposed into Maltese legislation.	

Ministru għall-Infrastruttura, Trasport u Komunikazzjoni (Ministry for Infrastructure, Transport and Communications)

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: part of Ministry of Interior	
Weblink: http://www.mitc.gov.mt	
Areas of Activity: The Ministry has been assigned responsibility for the Malta Communications Authority, The Information and Communications Technology Strategy and National Identity Management. The delivery of the latter is made possible by the fact that the Ministry also includes responsibility for the Public Registry, Land Registry, Civil Registration, Identity Cards and Passports. The Ministry is also responsible to ensure the national interest in the policy setting, regulation and operations of entities owned or partly owned by the Government.	

Malta Information Technology Agency (MITA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Micro-enterprises, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Interior	
Weblink: http://www.gov.mt/newsletterarticle.asp?a=545&l=2	
Areas of Activity: Since 2000, the Ministry of Infrastructure, Transport and Communications (MITC) has led and managed the national IT policy directly. However, the Government realised that the absence of a permanent structure within the public sector to manage this important policy area would represent a threat to the development of this policy in the long term. Hence, the newly established permanent IT Agency (MITA) will take over several of the functions that were previously carried out by the Ministry. The new Malta IT Agency will become the sole shareholder of MITTS Ltd and will eventually absorb that organisation as its operational arm.	
mtCERT	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT	
Relationships: co-operates with Ministry of Interior, it's part of MITTS Ltd	
Weblink: http://www.mtcert.gov.mt	
Areas of Activity: mtCERT stands for MITTS Ltd Computer Emergency Response Team. It is made up of 13 members within the Malta Information Technology and Training Services Ltd. Team members provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community.	
Awtorita' Maltija Dwar L-Istandards (Malta Standards Authority)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: n/a	
Weblink: http://www.msa.org.mt	

Areas of Activity: The Authority's mandate – besides being the National Standards Body entrusted to adopt, publish and disseminate voluntary standards – is very much broader and includes related standardization activities such as technical advice to various Ministries and governmental bodies, notification of standards and regulations and co-ordinating testing, certification, accreditation, and metrology activities in Malta. The Authority is also responsible for the running of the EU EMAS and Eco-label Schemes in Malta. The Authority is also responsible for all activities dealing with CE Marking, being the Designating Authority for Notified Bodies. MSA is presently made up of a Council, Central Administration and five directorates.

Office of the Data Protection Commissioner	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Micro-enterprises, Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.dataprotection.gov.mt/index.aspx	
Areas of Activity: The right to privacy is a fundamental human right, which is safeguarded and enshrined in Malta's Constitution. The enforcement of the right to privacy is facilitated by the protection of personal data from abuse. The Data Protection Act of 2001 was enacted in Malta on the 14th December 2001, with both sides of the House of Representatives voting in favour of the Act. The Data Protection Act 2001 provides for the protection of individuals against the violation of their privacy by the processing of personal data and for matters connected therewith or ancillary thereto. The Data Protection Act was brought fully into force on the 15th July 2003, enabling data subjects to enjoy their rights under the Act.	

Malta Council for Science and Technology	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.mcst.gov.mt/	
Areas of Activity: The Malta Council for Science and Technology (MCST) is the national advisory body to Government on science and technology policy. The MCST is also the national agency responsible for the management of the local RTDI programme, as well as the national contact organization for the Seventh Framework Programme (FP7).	

The Government of Malta	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.gov.mt/index.asp?l=2	
Areas of Activity: Government of Malta, involved partly in the country NIS activities, eGovernment in particular	

Malta Tourism Authority	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.mta.com.mt/	
Areas of Activity: Private entrepreneurs have entered the cultural sector by providing support for and initiating high-tech multi-media projects, many of which are targeted at tourists. Moreover, Malta's unique Hypogeum (a prehistoric underground burial site) has been installed with digital technology to protect it environmentally.	

Malta Resources Authority	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience	
Relationships: co-operates with Ministry of Industry and Trade	
Weblink: http://www.mra.org.mt	
Areas of Activity: The MRA is the regulatory authority for the energy sector. Would have strong links to eSecurity when it comes to CIIP.	

Industry Organisations Active in Network and Information Security

Malta Information Technology and Training Services LTD.

Type of Organisation: Other Industry Association	Ownership: Non-Profit
ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: owned by MITA, owns mtCERT	
Weblink: http://mitts.gov.mt	

Areas of Activity:

MITTS Ltd provides ICT services and professional project management and consulting services to the Government of Malta. It is dedicated to assisting the Government in transforming technological innovations into real business solutions. Its unique approach combines an innovative array of services with focused delivery capabilities using tried and tested methodologies to help maximise the benefits of investment in technology. By means of its ICT and project management services, MITTS Ltd helps Government implement technology to be able to fulfil its strategies and projects.

Chamber of Engineers

Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Micro-enterprises	
Relationships: none	
Weblink: http://www.coe.org.mt/	

Areas of Activity:

The Chamber of Engineers (CoE) is the only local organization catering for the interests of Maltese Professional Engineers. The Chamber was founded on the 28th April 1978. At both a local and European level, the Chamber actively participates in international discussion groups through the Chamber's affiliation with the European Federation of National Engineering Associations (FEANI) and the Council of Associations of long cycle Engineers of a University or Higher School of Engineering of the European Union (CLAIU-EU). The Chamber is also proud to hold a representative voice on a number of local Authorities and Government Boards. The Chamber organises courses for the Engineering Community on Health and Safety, Quality, Management, Building Services, Technical and Information Technology subjects, including security.

Academic Organisations Active in Network and Information Security

Malta College of Arts, Science & Technology- Institute of Information and Communication Technology	
Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR	
Relationships: none	
Weblink: http://www.mcast.edu.mt	
Areas of Activity: The college has an institute of Information and Telecommunications Technology that offers numerous diploma options in all areas of IT.	

Other Bodies and Organisations Active in Network and Information Security

The Malta Chamber of Commerce and Enterprise	
Type of Organisation: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: AR	
Relationships: n/a	
Weblink: http://www.chamber.org.mt/	
Areas of Activity: The chamber builds on its long tradition with dynamism and a forward looking approach, at the forefront of technology and developments in the business environment which it seeks to exploit to the advantage of its members, their employees and the nation at large.	

Activities

Strategic Initiatives

The Smart Island

Type of Activity: Governmental Policies

Responsible Organisation(s): Ministry for Infrastructure Transport and Communication

ENISA Focus Points: AR, Development of Security Technology and Standards

Weblink: https://secure2.gov.mt/SmartIsland//Pages/Data/StakeHolders.aspx

Description:

The National ICT Strategy 2008-2010, The Smart Island, is a vision for Malta where Information and Communication Technology (ICT) is not a mere information and communications tool but a primary vehicle for putting right social inequality, disadvantages and disabilities, while improving the quality of life of those people who live here and those who are staying for a short while.

Smart Learning - Malta's National e-Learning Strategy 2008-2010

Type of Activity: Governmental Policies

Responsible Organisation(s): Ministry for Infrastructure Transport and Communication

ENISA Focus Points: AR

Weblink: https://secure2.gov.mt/SmartIsland//Pages/Data/StakeHolders.aspx

Description:

The outcomes that the Government wants to attain through this vision are: All learners will have access to personalised, flexible learning content and opportunities; Through access to technology, children and young people will be able to develop and use independent learning skills that will support them in employment and throughout life-long learning; Educators and administrators will have the skills and support to deploy technology for the benefit of all learners; in addition, educators and administrators will have opportunities to use technology to support their own career development; Pedagogical use of technology will support and encourage sharing, collaboration, creativity and be a driver of innovation; Parents will have opportunities to support and play a part in their children's learning; Public-Private partnerships will support development and delivery of the National e-Learning Strategy; and, The National e-Learning Strategy will accelerate development of Malta's knowledge economy. An additional aim related to infrastructure is to establish standards for Internet and computer safety and security, technical standards for interoperability and compatibility and quality standards for content development.

Smart Careers
Type of Activity: Governmental Policies
Responsible Organisation(s): Ministry for Infrastructure Transport and Communication
ENISA Focus Points: AR
Weblink: https://secure2.gov.mt/SmartIsland/Pages/Initiatives/Initiative.aspx?id=12
Description: The increasing amount of career opportunities in the ICT Sector is becoming one of the major forces in today's economy. ICT has broadened its reach amongst all sectors across industry, placing ICT careers at a higher economical value than various other alternative careers. The challenge arising is that the supply of ICT graduates is not reaching the demand of the industry. To meet this challenge and promote a better future for students still undecided in their career choice, the Ministry for Infrastructure, Transport and Communication (MITC) is promoting a National ICT Careers Awareness Campaign: "Smart Careers". Together with the ICT industry and educational institutions, MITC is targeting both parents and students and making available information on ICT career paths and ICT studies which lead to such job positions.
m-Government
Type of Activity: Governmental Policies
Responsible Organisation(s): Ministry for Infrastructure Transport and Communication
ENISA Focus Points: AR, Implementation of Security Technology and Standards
Weblink: https://secure2.gov.mt/SmartIsland//Pages/Data/StakeHolders.aspx
Description: As an integral part of the e-Government programme, the Ministry aims to offer the e-Government services via a variety of service delivery channels apart from the world- wide-web. One of these service delivery channels is mobile telephony. This channel is made even more relevant following the gauging of the public perception earlier this year, where 43% of the respondents expressed their inclination to use e-Government services via their mobile telephone.

Research Programmes

National Research and Innovation Programme 2008

Type of Activity: Social & Other Research Programmes

Responsible Organisation(s):

Malta Council for Science and Technology

ENISA Focus Points: AR

Weblink: n/a

Description:

The MCST has just launched the National Research and Innovation Programme for 2008 with a nominal budget of €698,000. The focus of the R&I Programme 2008 shall be on technology transfer and collaboration between (1) academia and (2) industry or public entities. Selection and funding of projects under this programme shall be on a competitive basis.

Events

Conference and Workshops

MCA Annual Conference 2008

Responsible Organisation: MCA	Frequency: Annual

ENISA Focus Points: AR, Emerging/Current Risks

Target Groups: Major- Security Professionals, Educational and Research Organizations, SMEs, Large Enterprises, Government Institutions

Weblink: http://www.mca.org.mt/newsroom/openevent.asp?id=28&source=4

Description:

MCA Annual Conference 2008: e-COMMERCE - TOWARDS A BORDERLESS ECONOMY. During this conference the following topics are analyzed: the building blocks that underlie the core notion of 'e-readiness' and examining whether Malta's digital environment is conducive to foreign investment, the effects of e-Commerce on the supply chain – the efficiencies that can be gained, especially by micro-enterprises, which constitute the majority of businesses in Malta, and the role of Government as an enabler and driver of e-Commerce. The MCA event in 2006 focused solely on e-Security.

ICSEA 2008- The Third International Conference on Software Engineering Advances

Responsible Organisation: IARIA	Frequency: Annual, but not always in Malta
ENISA Focus Points: AR, Micro-enterprises, Implementation of Security Technology and Standards	
Target Groups: Major- Large Enterprises, Security Professionals, SMEs, Educational and Research Organizations	
Weblink: http://www.iaria.org/conferences2008/ICSEA08.html	
Description: This event breaks down the following topics: Security requirements, design, and engineering; Software safety and security; Security, privacy and safeness in software; Software vulnerabilities; Assessing risks in software; Software for online banking and transactions; Software trace analysis; Software uncertainties; Dynamic detection of likely invariants; Human trust in interactive software; Memory safety; Safety software reuse; High confidence software; Trusted computing; Next generation secure computing.	

Current Trends in Data Breaches

The field research and data collection phase showed how there is no specific trend for a particular country, but instead, common trends across all countries could be identified. The trends show a different strength in each country and are often driven either by the evolution of the same technology (e.g. Increased adoption of mobile devices) or by common policies (e.g. Adoption of EU guidelines).

However a lack of consistent statistics for most countries analyzed in this study, and a lack of a common approach in measuring the specific adoption and evolution of NIS gives a rather limited room for NIS trends evaluation validated by quantitative data.

For the aim of this study a specific NIS trend has been identified and analyzed: the analysis of the recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons among which include: the loss or theft of equipment where the data is stored, human error, equipment failure, unforeseen disasters (fires, floods, other natural calamities), hacking, and of ever increasing concern, the unauthorized use of data or information via inadequate access control to private or highly sensitive data.

In the last 12 months 0 security breaches were reported in Malta.

Country Report – Netherlands

Country General Information

Source: European Commission

Political system:	Constitutional monarchy
Capital city:	Amsterdam
Total area:	41 864 sq.km
Population:	16.3 million
Official language:	Dutch
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in the Netherlands, we present a set of three indicators in the Country Highlights section.

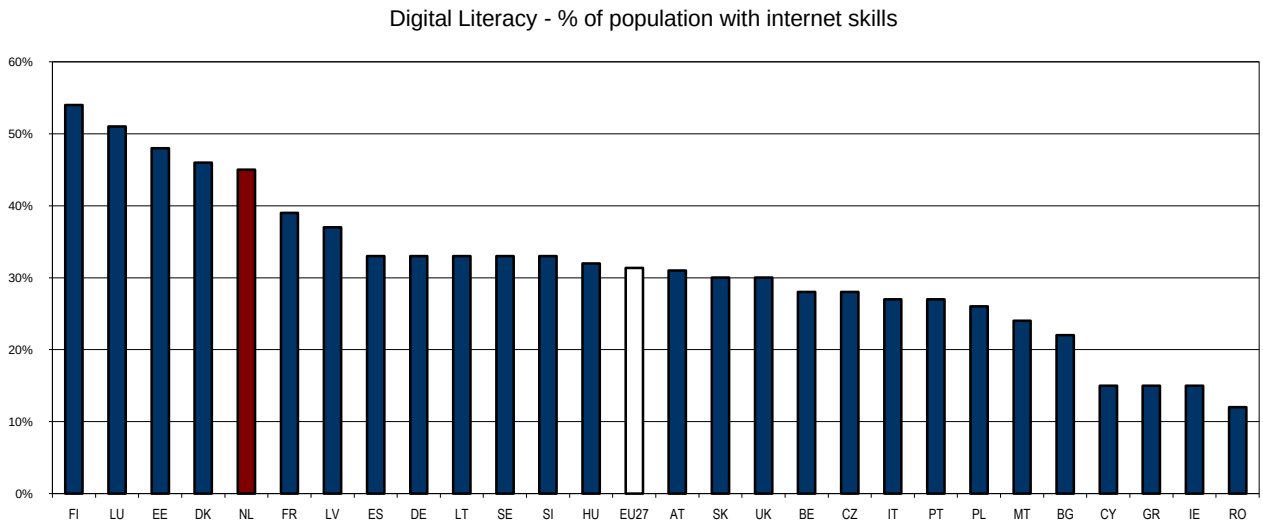
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in the Netherlands is fundamental to this NIS study.

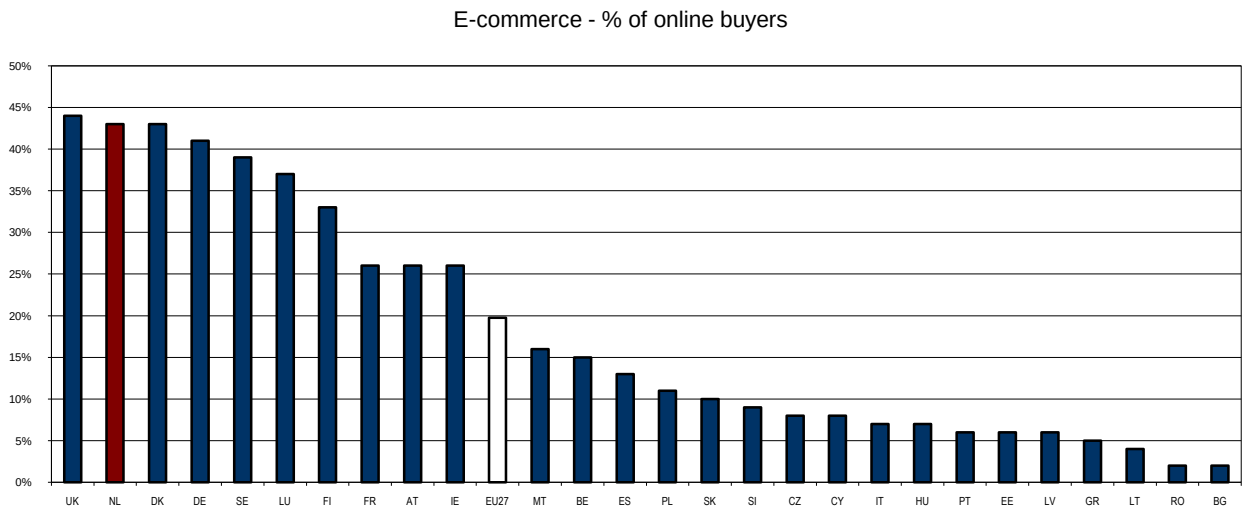
The Netherlands has reached one of the most advanced levels of development of information society without having a strong ICT sector or a high intensity in ICT research. Most other indicators show The Netherlands to be at the forefront of dissemination of ICTs in the economy, for example in use of e-business, in e-commerce and in the high level of ICT skills in the population and in the workforce.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

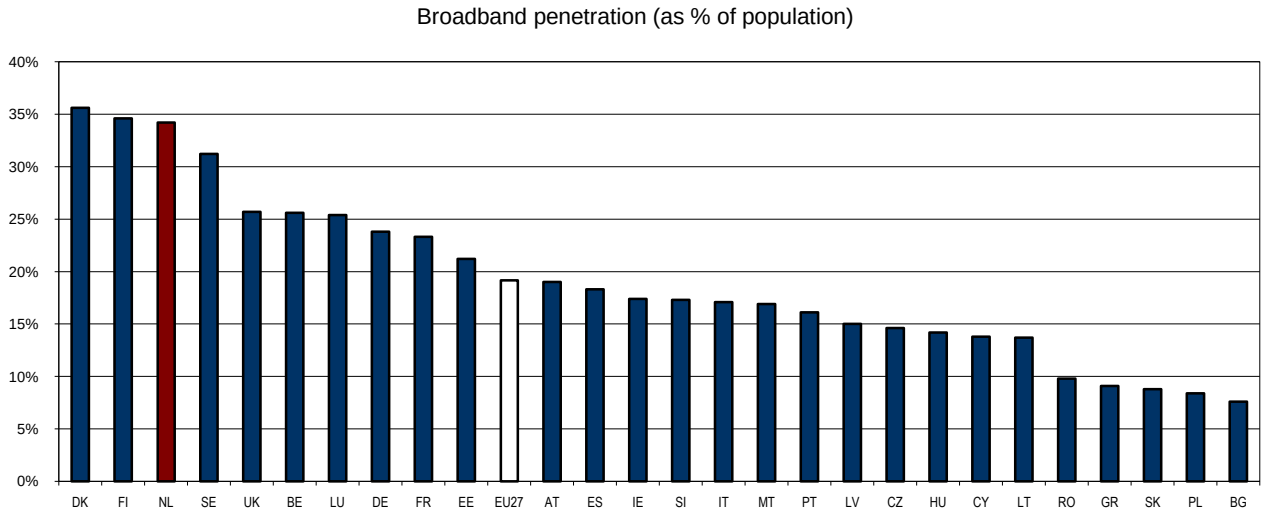
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

In The Netherlands there is not a single, independent government body recognized among NIS stakeholders as the national security agency. Nor is there a single body solely responsible for development of national information security policy.

The Ministry of Economic Affairs has a coordinating responsibility for providing the national policy on ICT, is the national point of contact for IT security in general in The Netherlands and gives also guidance to CIIP. The Ministry of the Interior and Kingdom Relations is responsible for the security of governmental IT systems and services and CIP in general.

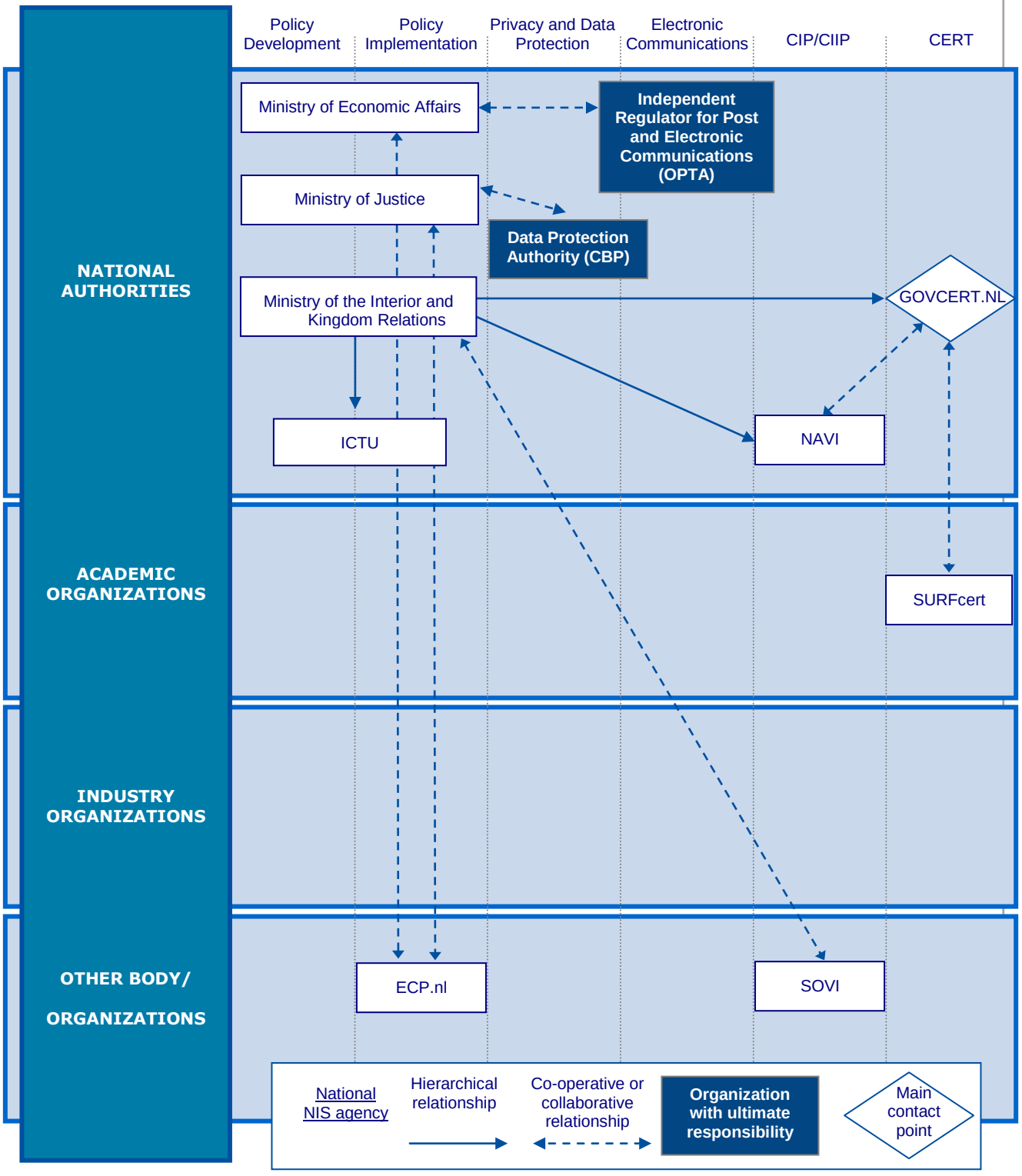
The CBP, Data Protection Authority, is responsible for ensuring compliance with privacy and data protection legislation in the Netherlands. Specifically the body regulates fair and lawful use and security of personal data in the country.

OPTA is charged with ensuring compliance with regards to electronic communications legislation.

The GovCert.NL is the national government point of contact and centre for expertise for warning, alerting and response services on ICT attacks and intrusions in The Netherlands.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Austria. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Economic Affairs		X	X	X		X	X	X
Independent Regulator for Post and Electronic Communications (OPTA)			X					
Ministry of the Interior and Kingdom Relations		X				X		
ICTU							X	X
GOVCERT.NL	X	X	X	X				X
National Advisory Centre for Critical Infrastructure (NAVI)		X		X				
CBP-Data Protection Authority			X	X				
SURFCert	X	X						
Strategic Forum on Critical Infrastructure (SOVI)		X		X				
ePlatform for the Netherlands (ECP.nl)			X	X				

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in the Netherlands:

National Authorities in Network and Information Security	
Ministry of Economic Affairs	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: collaborates with GovCert.nl, Platform for E-Netherlands, and ICTU/NICC; involved in the National Platform on Cybercrime (NPC)	
Weblink: http://www.ez.nl	
Areas of Activity: Development of the electronic communications market and IT including network and information security.	
Ministry of the Interior and Kingdom Relations	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, e-ID	
Relationships: responsible for GovCert.nl and ICTU	
Weblink: http://www.minbzk.nl	
Areas of Activity: Steering the development of EGOV (including governmental e-security).	
Ministry of Justice	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: responsible for National Platform on Cybercrime (NPC)	
Weblink: http://www.justitie.nl/	
Areas of Activity: IT security from a criminal security perspective, law enforcement and combating cybercrime.	

Independent Regulator for Post and Electronic Communications (OPTA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR	
Relationships: set-up by the Ministry of Economic Affairs, which has overall responsibility for the area of regulation	
Weblink: http://opta.nl	
Areas of Activity: Regulates telecommunications and postal industry; enforces legislation.	

GBO.Overheid	
Type of Organisation: Other Public Bodies	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards Policy	
Relationships: part of the Ministry of the Interior and Kingdom Relations	
Weblink: http://gbo.overheid.nl	
Areas of Activity: GBO.Overheid is the Dutch governmental shared service organization for ICT. It is responsible for the management and ongoing development of a number of ICT services for all government agencies. GBO.Overheid also develops shared standards to facilitate electronic messaging among government agencies, citizens and companies.	

GOVCERT.nl	
Type of Organisation: Other Public Bodies	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: Part of GBO.Overheid; Collaborates closely with National Infrastructure to Combat Cybercrime (NICC), National Police Services Agency (KLPD), General Intelligence and Security Service (AIVD), OPTA and NAVI	
Weblink: http://www.govcert.nl	
Areas of Activity: Central emergency point in dealing with ICT-related security incidents.	

National Advisory Centre for Critical Infrastructure (NAVI)

Type of Organisation: CIIP Bodies	Ownership: PPP
ENISA Focus Points: Resilience, Emerging/Current Risks	
Relationships: NAVI is part of the Ministry of the Interior and Kingdom Relations. NAVI works alongside the police, the General Intelligence and Security Service (AIVD), the National Coordinator for Counterterrorism (NCTb) and the relevant ministers. NAVI is also in close contact with GOVCERT.NL and the National Infrastructure to Combat Cybercrime (NICC).	
Weblink: http://www.navi-online.nl	
Areas of Activity: The National Advisory Centre on Critical Infrastructure (NAVI) connects government and business in the protection of the critical physical and digital infrastructure. Officials involved in the critical infrastructure in the Netherlands can contact the NAVI for information and independent advice about protection against malicious disruption. NAVI's four core activities are: Advice on security protection- NAVI gives advice on security protection to the owners and managers of critical infrastructure in the Netherlands. It conducts risk analyses, and it issues second opinions on existing security protection plans. It also evaluates risk analyses of existing and proposed security measures. NAVI provides this service in response to client need. Knowledge and information exchange on security protection- NAVI ensures that parties working in the critical sectors in the Netherlands can share knowledge and information. For this purpose, it maintains contacts with government bodies and business enterprises operating in the critical sectors and with relevant contacts and organisations abroad. It makes knowledge and information available in various ways, such as organising meetings, communicating via its website, and providing access to its knowledge bank. Product development- NAVI develops products that can be used within entire sectors or even multiple sectors. For instance, it is currently developing a series of manuals on various aspects of security protection. For example, one on risk analysis. NAVI can develop products for solutions at varying levels of maturity and make third-party products accessible for use in the Netherlands. Networking- NAVI maintains and develops a wide network of contacts among security professionals, and it serves as a meeting point for critical infrastructure parties in government, research and business at home as well as abroad. NAVI brings parties together by organizing and supporting knowledge and information hubs. There, parties from one or more sectors can meet regularly to share information about security protection.	
ICTU	
Type of Organisation: Other Public Bodies	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: reports to the Ministry of the Interior and Kingdom Relations, and the Association of the Netherlands Municipalities	
Weblink: http://ictu.nl/	

Areas of Activity: ICTU was founded by the Ministry of the Interior and Kingdom Relations, and the VNG (Association of the Netherlands Municipalities) on 11th April 2001. ICTU's statutory objective is to support authorities in the introduction and implementation of an innovative use of information and communication technology. ICTU is commissioned by authorities to work on IT issues of a generic nature. ICTU's aim is to maximize the government's IT objectives through collaborating with authorities. This means that ICTU is involved with policy development and implementation.

Team High Tech Crime	
Type of Organisation: National Security Actors	Ownership: Public
ENISA Focus Points: Emerging/Current Risks	
Relationships: Part of the National Police Services Agency (KLPD), which reports to the Ministry of the Interior and Kingdom Relations	
Weblink: http://www.politie.nl/klpd	
Areas of Activity: A crime unit of the Dutch police. The THTC was founded to police networks and communication systems in the Netherlands and tackle crimes using or directed against information and communication technology.	

Data Protection Authority (CBP)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: set up by the Ministry of Justice, which has overall responsibility for the area of data protection legislation	
Weblink: http://www.dutchdpa.nl/	
Areas of Activity: Regulates fair and lawful use and security of personal data.	

Academic Organisations Active in Network and Information Security

ICTRegie	
Type of Organisation: Other Academic	Ownership: Non-profit
ENISA Focus Points: Development of Security Technology and Standards policy	

Relationships: co-operates with the Ministry of Economic Affairs, supported by the Netherlands Organisation for Scientific Research (NWO) and SenterNovem (agency within the Ministry of Economic Affairs)
Weblink: http://www.ictregie.nl
Areas of Activity: ICTRegie has been established by the Dutch government to stimulate the innovative powers of the Netherlands by means of ICT research. The goal of the authority is to develop a national ICT research and innovation strategy that is aimed at strengthening the ICT knowledge infrastructure of the Netherlands and maximizing the benefits for society and the economy. ICTRegie is a compact, independent organization consisting of a supervisory board, an advisory council, a director and an office. The Ministers of Economic Affairs, and of Education, Culture and Science bear the political responsibility for ICTRegie. The organization is supported by the Netherlands Organization for Scientific Research (NWO) and SenterNovem. The organization has been founded for a limited period, until 2009.

SAFE-NL	
Type of Organisation: Other Academic	Ownership: Non-profit
ENISA Focus Points: Resilience, Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: supported by the research program Sentinels; co-operates with other R&D organisations in the field of ICT security	
Weblink: http://www.safe-nl.org	
Areas of Activity: SAFE NL provides a forum for researchers, practitioners, and implementers from research institutions, industry and government agencies to exchange ideas on the state of the art in security technology, current and novel application areas of this technology, and on the requirements for effective deployment of secure systems.	

SURFcert	
Type of Organisation: Other Academic	Ownership: Public
ENISA Focus Points: CERT, AR	
Relationships: None	
Weblink: http://www.surfnet.nl	
Areas of Activity: SURFcert is the CERT of the SURFnet network for higher education and research institutions in the Netherlands.	

Other Bodies and Organisations Active in Network and Information Security

Platform for eNetherlands (ECP.nl)	
Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: Ministry of Economic Affairs, Ministry of Justice	
Weblink: http://www.ecp.nl/	
Areas of Activity: Public and private platform to develop the digital economy.	

Safe Internet Foundation	
Type of Organisation: Other	Ownership: PPP
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: collaborates with the Ministry of Economic Affairs	
Weblink: http://www.sif.nl	
Areas of Activity: Public Private Partnership to promote awareness of viruses, hackers, content filtering, and privacy issues.	

Strategic Forum on Critical Infrastructure (SOVI)	
Type of Organisation: Other	Ownership: PPP
ENISA Focus Points: Resilience, Emerging/Current Risks	
Relationships: collaborates with the Ministry of the Interior and Kingdom Relationships	
Weblink: N/A	
Areas of activities: Public Private Partnership on cooperation in CIP.	

Activities

Strategic Initiatives

Digivaardig & Digibewust

Type of Activity: Governmental Policies

Responsible Organisation(s): ECP.NL, Ministry of Justice, Ministry of Economic Affairs

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.digibewust.nl/

Description:

Information portal for online safety and security.

Central College of Experts on Data Protection (CCvD-IB)

Type of Activity: Governmental Policies

Responsible Organisation(s): ECP.NL

ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards

Weblink: http://www.ecp.nl/projecten/id=2/Centraal_College_van_Deskundigen_Informatiebeveiliging_CCvDIB.html

Description:

Physical, logical and organisational measures for data protection by an independent certification institution.

Dutch National Alerting Service *(Waarschuwingsdienst)*

Type of Activity: Governmental Policies

Responsible Organisation(s): GOVCERT.NL

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: http://www.waarschuwingsdienst.nl/

Description:

Dutch National Alerting Service that provides citizens and SMEs with warnings regarding IT security related incidents.

DigiD
Type of Activity: Governmental Policies
Responsible Organisation(s): GBO.Overheid and the Dutch Tax Authorities
ENISA Focus Points: e-ID
Weblink: http://www.digid.nl/
Description: DigiD stands for Digital Identity and is a system shared between cooperating governmental agencies, allowing to digitally authenticate the identity of a person who applies for a transaction service via internet.
National Infrastructure against Cybercrime (NICC)
Type of Activity: Governmental Policies
Responsible Organisation(s): ICTU (commissioned the programme)
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: http://www.samentegencybercrime.nl
Description: The NICC programme is charged with the responsibility of creating a National Infrastructure against cyber-crime – not only by developing new features, but by collaborating with others as much as possible and by integrating existing initiatives in order to create the National Infrastructure. The programme supports, facilitates and finances initiatives by other public and private organizations that contribute to safer computer-supported work processes. The NICC's role is to monitor the entire process, to gather and disseminate information and to encourage public and private organizations to share their knowledge. The National Infrastructure consists of several components: a contact point, reporting unit, trend watching, monitoring and detection, information distribution, education, warning, development, knowledge sharing, surveillance, prevention, termination and mitigation.
National Forum on Continuity of Telecommunications
Type of Activity: Governmental Policies
Responsible Organisation(s): Ministry of Economic Affairs
ENISA Focus Points: Resilience, Emerging/Current Risks
Weblink: http://www.nco-t-ez.nl

Description:

The objective of the Forum is to promote co-operation between government and providers of public electronic communications services which are considered critical to society. The Forum aims to reduce vulnerabilities, to increase resilience of services and infrastructure, and to foster co-operation during major incidents. The Forum has very strong liaisons with programmes/projects in the fields of CIP, CIIP, and national security.

Project ICT Disturbance

Type of Activity: Governmental Policies

Responsible Organisation(s): Ministry of Economic Affairs

ENISA Focus Points: Resilience, Emerging/Current Risks

Weblink: N/A

Description:

The project is part of a national security programme. The aim of the project is to identify current and future risks in the ICT field and to propose measures for the improvement of the resilience of ICT infrastructure.

Research Programmes

Sentinels

Type of Activity: Technical Research Programme

Responsible Organisation(s): managed by the Technology Foundation STW; co-funded by STW, the Ministry of Economic Affairs, and the Netherlands Organisation for Scientific Research (NWO)

ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy

Weblink: http://www.sentinels.nl/

Description:

Sentinels is a Dutch research program on security in ICT, networks and information systems. The Sentinels program aims to give a very significant boost to security expertise in the Netherlands by providing and managing resources for scientific research in information security, by building a national IT-security community, and by disseminating the results into industry and government in the Netherlands.

Events

Conference and Workshops

Govcert.nl Symposium 2008	
Responsible Organisation: GovCert.nl	Frequency: annual
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major- Security Professionals, Educational and Research Organizations, Large Enterprises, Government Institutions; Minor- SMEs, Consumers/Citizens	
Weblink: http://www.govcert.nl/symposium/	
Description: Analysis of the IT security sustainability	

Vertrouwen 2.0	
Responsible Organisation: ECP.NL	Frequency: Up to 4 times per year
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Micro-enterprises, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major- Consumers/Citizens, Government Institutions, Large Enterprises, SMEs, Educational and Research Organizations; Minor- Security Professionals	
Weblink: http://www.ecp.nl/projecten/id=47/Vertrouwen_20.html	
Description: Copyright, protection of personal data and identity, cyber-crime, law enforcement, and consumer protection in the online world.	

Infosecurity	
Responsible Organisation: Private IT service providers	Frequency: annual
ENISA Focus Points: Resilience, Emerging Risks	
Target Groups: Major- Large Enterprises, Educational and Research Organizations, Security Professionals, SMEs, Government Institutions; Minor- Consumers/Citizens	
Weblink: http://www.infosecurity.nl/sites/www_infosecurity_nl/nl/index.asp	

Description: This is the premier security trade show in NL.

Media Campaigns

Digibewust	
Responsible Organisation: ECP.NL	Frequency: ongoing
ENISA Focus Points: AR	
Target Groups: Major- SMEs, Consumers/Citizens; Minor- Security Professionals, Educational and Research Organizations, Large Enterprises, Government Institutions	
Weblink: http://www.digibewust.nl/	
Description: Online portal for security and safety on the Internet.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, twelve security breaches were reported in the Netherlands:

1. In November 2007 a 340-page list with names, home addresses, functions and ranks of marine personnel was inadvertedly put on a Defense web site. Among them were the names and addresses of marines working for defense intelligence. The list was an internal document and not meant for publication. Defense removed the list after two days, but it lingered on several Defense operated servers for several days. After an assessment of the problem by prof. Chris Verhoef, the department finally took down the website in mid December.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

2. In December 2007 Vecozo, an organization set up by health insurance companies, has created a password and certificate protected web site where professionals can check whether patients are indeed insured. The newspaper Trouw discovered that 80,000 people could access the data: not only health professionals, but also nurses, home carers and taxi drivers. In other words: 1 out of every 200 in NL had access to the site. One can access name, date of birth, address and social security number of those insured. It's possible to find the addresses of well-known people and of people who have secret addresses (for instance, battered women who've fled their husbands).

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

3. In December 2007 CZ, a health insurance company, was informed that through sloppy security, the names, address, telephone number, social security number, bank information, date of birth and type of insurance of prospective clients who had filled in a web form for a quotation, were out in the open. CZ didn't do anything. But when the news hit the media five days after they were informed, they closed that part of their web site and apologized.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

4. In January 2008 one of the sysadmins of Planet, a Dutch ISP, stored a backup of all client data in a user account, as the result of a typing error (the user's account and the sysadmin's differed by only one letter). The user warned Planet, but Planet did not take any immediate action. The file contains the user names, aliasses, IP addresses, encrypted passwords and used services of all private and business Planet accounts. Using hashmaster, the user could decrypt all passwords. Planet ingored the matter until the story spread. It then asked the user to delete the file. Planet claims that it will change its back-up policy.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

5. In January 2008 Reader's Digest has moved its 'You might become a winner' direct mails over to e-mail, and spammed 46,962 people. The mail contained a link to 'your personal data' and 'your unique code'. By changing the code in the url, the name and full postal address of all 47,000 spam recipients could be seen.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

6. In April 2008 the Dutch National Pop Institute managed to briefly publish telephone numbers, home addresses and mail addresses of Dutch pop musicians, managers, music industry VIPs and pop music journalists on its website. Amongst those affected are a number of famous people. The data was removed. On its website, the NPI did not mention the incident.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

7. In May 2008 security firm Finjan discovered a web server controlled by criminals, containing more than 1.4 Gigabyte of business and personal data stolen from infected PCs. The data consisted of 5,388 unique log files. The compromised data came from all around the world and contained information from individuals, businesses, as well as renowned organizations, including healthcare providers. The server contained among others 571 log files from the US, 621 from Germany, 322 from France, 308 from India, 232 from Great Britain, 150 from Spain, 86 from Canada, 58 from Italy, 46 from the Netherlands, and 1,037 from Turkey. The web server contained malware that stole information from infected PC's and then stored that data on the web server, 'without any access restrictions or encryption, the data were freely available for anyone on the web, including criminal elements.' Finjan found compromised patient data, bank customer data, business-related email communications and Outlook accounts containing email communication.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

   In June 2008 the Indonesian Embassy had a vulnerability on their website visa4indonesia.nl, allowing visitors to see the data (name, address, travel information, passport numbers) of 25,000 Dutch people who had applied online for an Indonesian visa since 2007. The error was discovered by Orne Brocaar, as he himself was applying for a visa.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

8. In June 2008 a man who hacked into a third party Valve file server and stole the credit card numbers of Steam Cyber Cafe users was caught by police in the Dutch

town of Maastricht. According to the Dutch Ministry of the Interior, the 20 year old hacker had managed to "burn 13 million Euros playing poker online and shopping for notebooks, flat screens and MP3 players" before being caught. Known by the online handle MaddoxX, the man first made news when he boasted of the Valve hack in April of 2007. "We also don't want money from VALVe," he wrote on the No-Steam forum last year. "We want a simple message on their site." MaddoxX then posted an archived file that included unverified credit card numbers, transaction amounts, Valve's supposed bank balance, and data that reportedly allowed the creation of counterfeit cyber cafe certificates. Valve quickly responded to the breach of security, creating an email address titled "Catch_A_Thief@valvesoftware.com" to encourage citizens to help the authorities track down MaddoxX. In addition to the Valve caper, MaddoxX is being charged with hacking his way into an Activision server and subsequently downloading an unfinished version of Enemy Territory: Quake Wars. MaddoxX also stole 50,000 credit card numbers from an English ticketing website, according to the ITExaminer.

http://www.shacknews.com/onearticle.x/53369

9. In July 2008 a T-Mobile shop sent out a mail to 20 customers informing them that their reservation for an iPhone had been duly processed. The shop put all the addressees in the cc-field, allowing all of them to see one another's name. The main T-Mobile office sent a warning to all local shops, reminding them of the privacy procedures.

   http://www.spaink.net/dutch-data-breaches/#2008-09-22

10. In July 2008 Fortis MeesPierson Bank, who accepts only clients worth more than 1 million euro, had an internal document in an open directory. The file contained data about Fortis MeesPierson's richest clients: name, address, amount of savings, their investments, mortgage etc. The error was discovered by journalists from Z24.

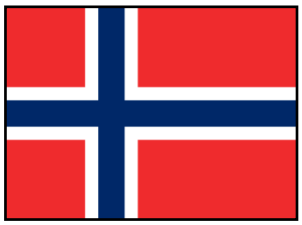
    http://www.spaink.net/dutch-data-breaches/#2008-09-22

11. In September 2008 due to a mail server configuration error, a member of one political party within the Provincial States of Limburg received the internal mail of another political party. Due to the often "explosive content" of those mails, Pierre Diederen (SP). the recipient, believed that somebody from within the CDA was actually leaking these e-mails.

    http://www.spaink.net/dutch-data-breaches/#2008-09-22

Country Report – Norway

Country General Information



Source: European Commission

Political system:	Monarchy
Capital city:	Oslo
Total area:	324 000 sq.km
Population:	4.4 million
Official language:	Norwegian
Time zone:	CET (GMT+1)
Currency:	Norwegian krone (NOK)

Source: Eurostat

NIS Highlights

The Ministry of Transport and Communications, an independent government body, is recognized among NIS stakeholders in Norway as the national security agency. The ministry is also responsible for development and implementation of information security policy at the national level.

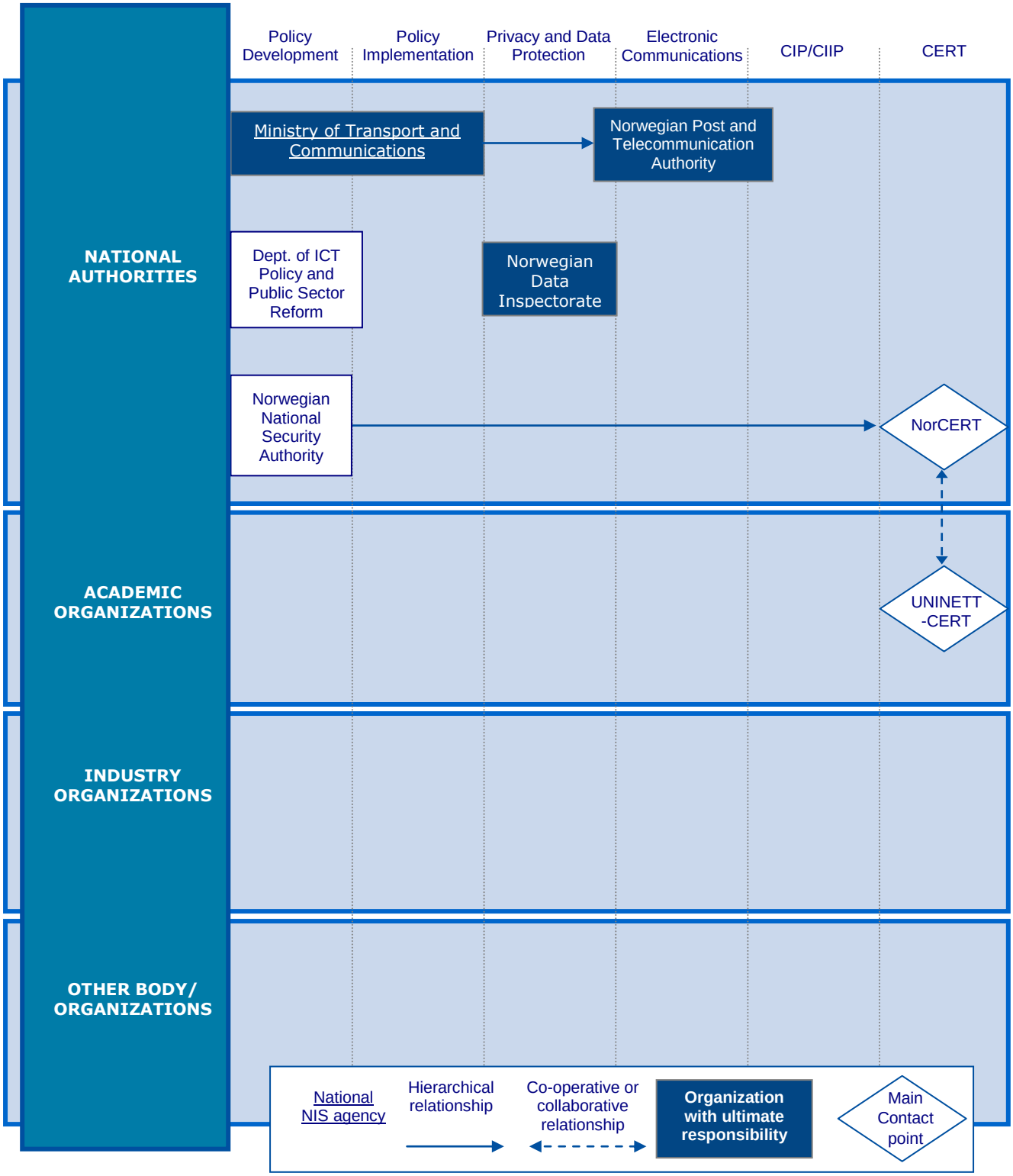
The Norwegian Data Inspectorate is responsible for implementing and ensuring compliance with privacy and data protection legislation in Norway. The inspectorate is charged with protecting persons from violation of their right to privacy through the processing of personal data. The agency shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.

The Norwegian Post and Telecommunication Authority is responsible for administering legislation in the area of post and telecommunications and for helping to ensure access to good and reasonably priced post and telecommunications services for users in Norway.

NorCERT is a part of the National Security Agency and coordinates preventative work and responses against IT security breaches aimed at vital infrastructure in Norway. The agency alerts of serious attacks, threats and other vulnerabilities related to serious IT security.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Norway. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Transport and Communications			X	X			X	X
Norwegian Data Inspectorate			X	X				
Norwegian Post and Telecommunication Authority				X			X	X
Dept. of ICT Policy and Public Sector Reform							X	
National Security Authority		X		X			X	
NorCERT	X	X						

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Norway:

National Authorities in Network and Information Security	
Ministry of Transport and Communications	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: The Norwegian Post and Telecommunications Authority is subordinate to the Ministry	
Weblink: http://www.regjeringen.no/en/dep/sd.html?id=791	
Areas of Activity: Within the Ministry of Transport and Communications, the Department of Civil Aviation, Postal Services and Telecommunications is responsible for policy formulation in the area of communications, drafting telecommunications legislation, and R&D within telecommunications and IT.	
Norwegian Post and Telecommunication Authority	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: reports to the Ministry of Transport and Communications	
Weblink: http://www.npt.no	
Areas of Activity: The Norwegian Post and Telecommunications Authority is a separate administrative body with responsibility for administering legislation in the area of post and telecommunications. The responsibilities of the Norwegian Post and Telecommunications Authority include: drafting and following up regulations, supervision of actors in the area of telecommunications, standardization, granting and control of licences, competition regulation, management of frequencies, authorization of suppliers and installers and international work in the telecommunications sector.	
Norwegian National Security Authority (NSM)	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public

ENISA Focus Points: CERT, Emerging/Current Risks, Development of Security Technology and Standards Policy
Relationships: reports to the Minister of Defence and the Minister of Justice
Weblink: http://www.nsm.stat.no
Areas of Activity: The Norwegian National Security Authority (NSM) is a cross-sectoral professional and supervisory authority within the protective security services in Norway. The purpose of protective security is to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. Among the Authorities tasks are: development of the Norwegian Computer Network Defence, strategy certification of information systems and products (through SERTIT), co-ordination of preventative work and responses against IT security breaches aimed at vital infrastructure in Norway (through NorCERT), development of security measures including R&D.

NorCERT	
Type of Organisation: Public and Private CERTS	Ownership: Public
ENISA Focus Points: CERT	
Relationships: a Department within of the Norwegian National Security Authority	
Weblink: http://www.nsm.stat.no/Engelsk-start-side/English2/	
Areas of Activity: NorCERT coordinates preventative work and responses against IT security breaches aimed at vital infrastructure in Norway. Its tasks include: gathering information related to serious IT security threatening incidents; coordinating early patching of serious vulnerabilities in vital computer systems; sharing information with other response teams regarding new threats; assisting other response teams and aiding national readiness measures; being Norway's point of contact for similar organizations abroad. NorCERT is an operational department in NSM consisting of two integrated sections: • VDI is the Norwegian Alert and Early Warning System for Digital Infrastructure identifying, classifying and issuing warnings about IT attacks against Norway. • Incident Handling is Norway's national centre coordinating the handling of attacks against vital Norwegian ICT security.	

Norwegian Centre for Information Security (NorSIS)	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public
ENISA Focus Points: AR	

Relationships: Reports to the Ministry of Government Administration and Reform	
Weblink: http://www.norsis.no	
Areas of Activity: The Norwegian Centre for Information Security (NorSIS) is responsible for coordinating activities related to ICT security in Norway. The primary target group is the small and medium enterprises and the public authorities. NorSIS reaches its objectives through: making the public aware of the importance of information security by means of training and information; compiling of guidelines and tutorials to help solve specific problems; and establishing an overall awareness towards information security.	
Ministry of Government Administration and Reform	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: The Norwegian Data Inspectorate is a subordinate enterprise	
Weblink: http://www.regjeringen.no/en/dep/fad/Selected-topics/ict-policyenorway.html?id=1367	
Areas of Activity: The Ministry of Government Administration and Reform is responsible for the implementation of egovernment in Norway. Within the Ministry, the Department of ICT Policy and Public Sector Reform is responsible for the work associated with preventive ICT security, including a number of issues relating to personal data protection. The Department of Government Services has the Norwegian Data Inspectorate and Government Administration Services as a subordinate enterprises.	
Norwegian Data Inspectorate	
Type of Organisation: Public Network & Information Security Bodies	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: Reports to the Ministry of Government Administration and Reform	
Weblink: http://www.datatilsynet.no	

Areas of Activity:

The Norwegian Data Inspectorate ensures enforcement of the Personal Data Act of 2000. Its tasks include: keeping a systematic, public record of all processing that is reported or for which a licence has been granted; dealing with applications for licences; verifying that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified; providing information on general national and international developments in the processing of personal data and on the problems related to such processing; identifying risks to protection of privacy, and provide advice on ways of avoiding or limiting such risks; providing advice and guidance in matters relating to protection of privacy and the protection of personal data to persons who are planning to process personal data or develop systems for such processing, including assistance in drawing up codes of conduct for various sectors; on request or on its own initiative giving its opinion on matters relating to the processing of personal data.

Agency for Public Management and eGovernment	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Overseen by the Ministry of Government Administration and Reform	
Weblink: http://www.difi.no/	

Areas of Activity:

The Agency for Public Management and eGovernment (DIFI) was established in January 2008. The agency aims to strengthen the government's work in renewing the Norwegian public sector and to improve the organisation and efficiency of government administration. The Agency's tasks include: providing assistance with reorganisation processes in the public sector; developing a good national information policy; encouraging coordinated and cost-efficient use of ICT within the public sector; making public information and services more accessible for citizens and public agencies.

Government Administration Services	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: Reports to the Ministry of Government Administration and Reform	
Weblink: http://www.dss.dep.no/templates/Page 111.aspx	

Areas of Activity:

Government Administrative Services (GAS) is a governmental agency. The main purpose of GAS is to provide synergy for the ministries with cost-effective and reliable shared services, including running computer systems.

Academic Organisations Active in Network and Information Security

UNINETT-CERT

Type of Organisation: Other Academic	Ownership: Public
ENISA Focus Points: CERT	
Relationships: funded by the Ministry of Education and Research	
Weblink: http://cert.uninett.no/	

Areas of Activity:

UNINETT is a CERT with a constituency comprising the UNINETT member organizations and their networks. UNINETT's basic service is to provide assistance with handling and investigating incidents, including spam, portscanning, denial of service, break-ins, piracy and phishing attempts, that involve one or more members of its constituency.

Norwegian Information Security Laboratory (NISLab)

Type of Organisation: Universities	Ownership: Public
ENISA Focus Points: AR, Emerging Risks	
Relationships: None	
Weblink: http://www.nislab.no	

Areas of Activity:

The Norwegian Information Security laboratory (NISlab) is the information security group at Gjøvik University College. NISlab is part of the Faculty for Computer Science and Media Technology. The group conducts international competitive research in several areas of information security, supervises Ph.D. research projects in this field and teaches courses in information security at the master and bachelor level. Activities related to information security at GUC were initiated in spring 2001 in reaction to a request by the Norwegian telco Telenor. NISlab employs 5 full professors, 1 associate professor, 1 researcher, 1 assistant professor, 6 adjunct professors and lecturers and 9 PhD students. NISlab carries out research in many areas of information security including: Information Security Management, System security, Cryptology, Network security, Privacy, Attacks and forensics, Information warfare and critical infrastructure protection, Content protection, and Dependable computing.

Activities

There are no significant security-related activities ongoing in Norway.

Events

Conference and Workshops	
Security Valley	
Responsible Organisation: NISLab	Frequency: annual
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Security Professionals, Educational and Research Organizations	
Weblink: http://www.securityvalley.no/	
Description: Conference focusing on ID theft. Participating delegates attend lectures by national and international industry experts.	
Information Security for the Energy Sector	
Responsible Organisation: NorSIS	Frequency: annual
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Large Enterprises, Security Professionals; Minor- SMEs	
Weblink: http://www.norsis.no/nyheter/2008-10-03-Energiseminar.html	
Description: NorSIS is arranging this workshop focusing on security issues for the energy sector. The goal of the conference is to increase awareness on issues related to information security as well presenting prevention methods. Attendees will typically be IT security managers and other managers from the energy industry.	
Risk	
Responsible Organisation: mnemonic	Frequency: annual
ENISA Focus Points: Resilience, Emerging/Current Risks, Implementation of Security Technology and Standards	

Target Groups: Major- Security Professionals
Weblink: http://www.mnemonic.no/features/risk-2008-2/view?set_language=en
Description: This is a yearly risk management and information security conference with national as well as corporate-level speakers. The conference has three main themes: IT security, application security and security management. The conference is primarily aimed at IT specialists.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, one security breach was reported in Norway:

In September 2008 it was reported that Norway's national tax office erroneously sent CD-ROMs loaded with the 2006 tax returns of nearly four million people living in Norway to national newspapers, radios and television stations. Although tax statements have been open to public scrutiny in Norway since 1863, the social security number of each citizen remains highly confidential. According to the tax authorities, the documents can only be opened by a secret code and so damage may be limited. Nonetheless this mishap occurred on the eve of a historic transatlantic pact between Norway and the US to share data about the private lives of its citizens. Travel plans, email addresses, mobile telephone numbers and even surfing habits will be made available to American security services in an effort to

combat terrorism. The Norwegian government says it wants assurances that the information given will be protected in a secure manner. Privacy advocates and rights groups in Europe have strongly criticised such deals with Washington.

http://www.spaink.net/dutch-data-breaches/#2008-09-22

Country Report – Poland

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Warsaw
Total area:	313 000 sq.km
Population:	38.1 million
Official language:	Polish
Time zone:	CET (GMT+1)
Currency:	Zloty (PNL)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Poland, we present a set of three indicators in the Country Highlights section.

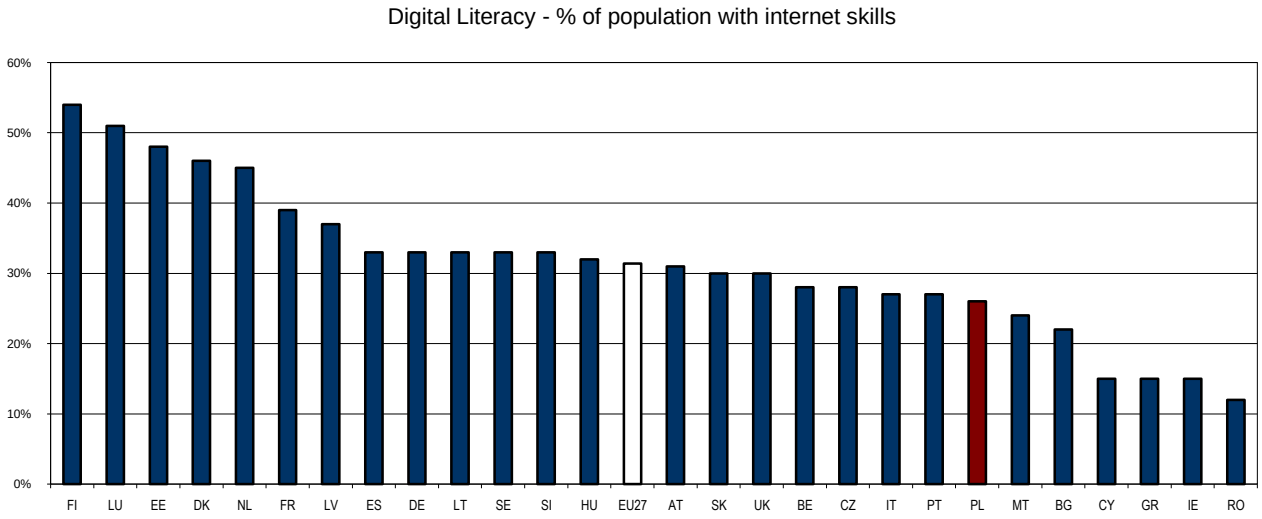
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Poland is fundamental to this NIS study.

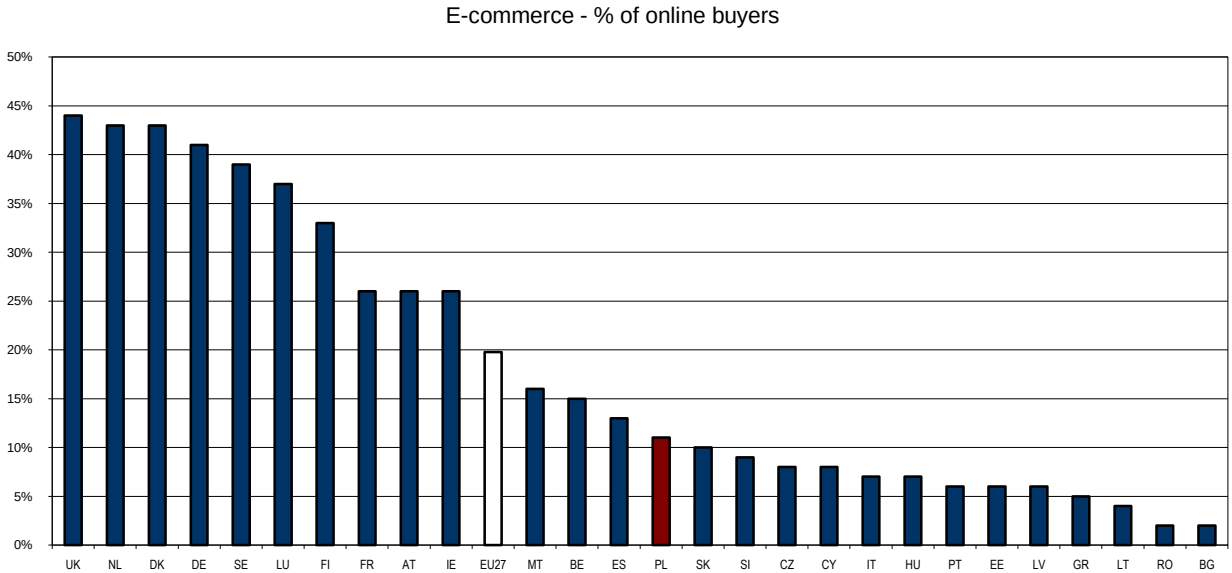
The information society in Poland is developing and the activities planned for 2008-2013 aim to launch further services for citizens and enterprises and linking up the various public administration systems. The remodeling of the national data registers is also underway in order to simplify the administrative procedures for enterprises and citizens and to create conditions for the development of integrated public services, mortgage register and other records.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

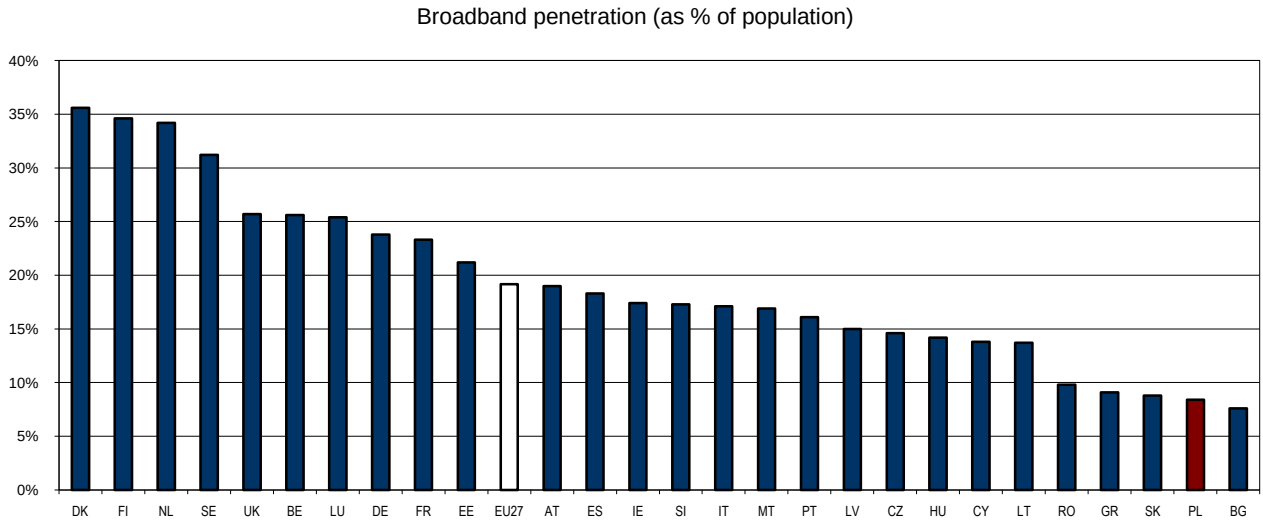
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

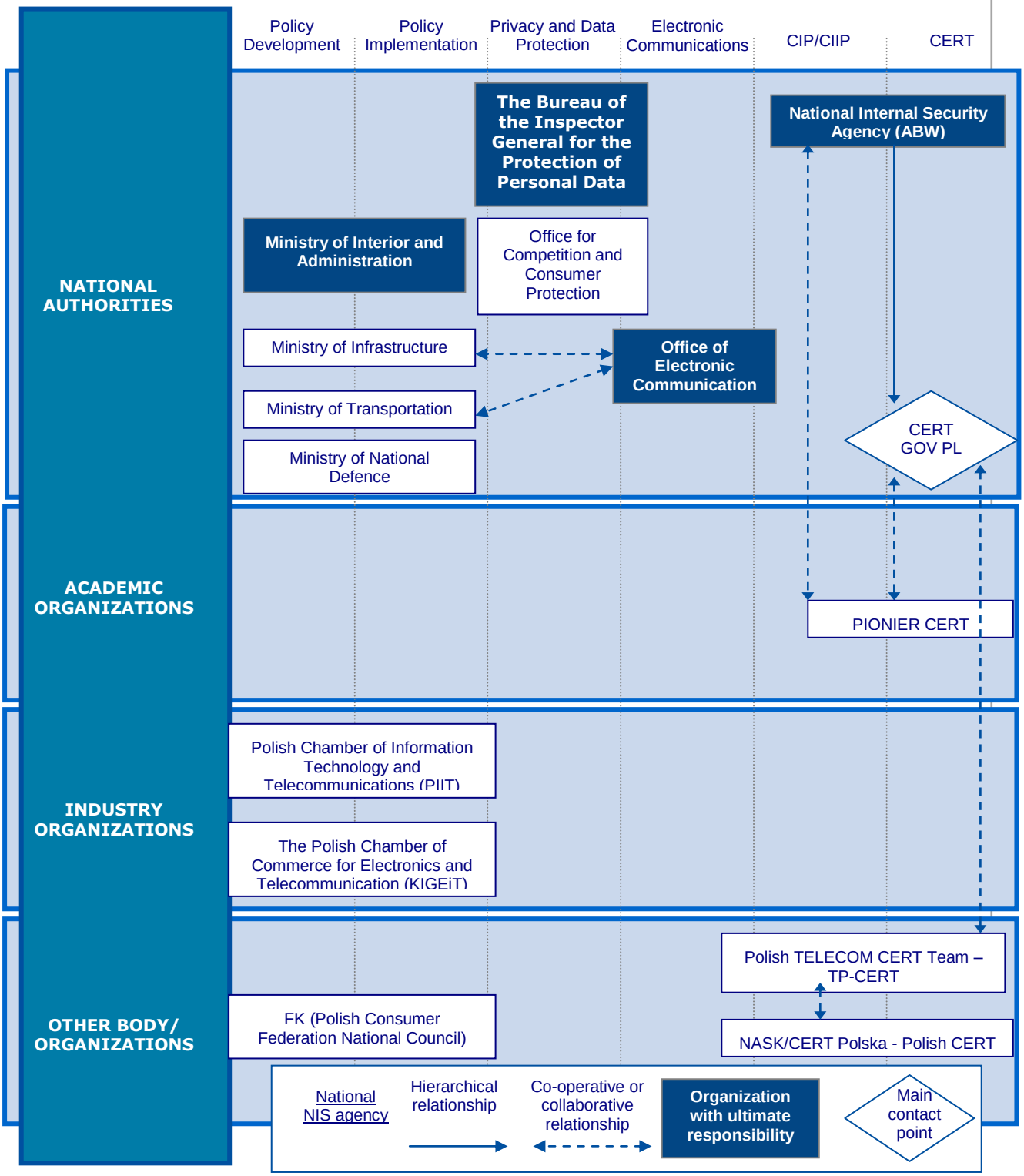
There is no single body recognized among NIS stakeholders in Poland as the national security agency. The Ministry of Interior and Administration and Office of Electronic Communications both hold responsibility for the development and implementation of information security policy. The Ministry of the Interior and Administration is charged with oversight of information technology, national tele-information systems, and national information administrative registers. The Office of Electronic Communications is the regulating body within the scope of postal, telecommunications, and management of broadcast frequencies, and is responsible for electromagnetic controls and requirements. It is also responsible for implementing and ensuring compliance with electronic communications legislation.

The Bureau of the Inspector General for the Protection of Personal Data is responsible for implementing and ensuring compliance with privacy and data protection legislation.

Additionally, Poland has security response teams in place to handle security breaches and other incidents. NASK/Computer Emergency Response Team Polska, Polish CERT, CERT GOV PL, and National Internal Security Agency (ABW) are the main national points of contact for IT security. The National Internal Security Agency (ABW) is also responsible for key elements of CIP/CIIP at the national level in Poland.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Poland. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Name of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Interior and Administration						X	X	X
Office of Electronic Communications							X	X
Bureau of the Inspector General for the Protection of Personal Data			X	X			X	X
CERT GOV PL National Internal Security Agency (ABW)	X	X	X	X				
NASK/Computer Emergency Response Team Polska – Polish CERT	X	X	X	X			X	X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Poland:

National Authorities in Network and Information Security	
Ministry of Interior and Administration	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Cooperates with Ministry of Industry and Trade	
Weblink: http://www.mswia.gov.pl/portal/en/	
Areas of Activity: The ministry is ultimately responsible for information technology, national tele-information systems, and national information administrative registers. Departments under the ministry's control include the Department of Information Technology Development, Information Society Department, and Center of Information Projects.	
Office of Electronic Communications	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: The activities of the President of the Office of Electronic Communications are supervised by the minister competent for communications (currently, the Minister of Transportation is in charge of the communications sector).	
Weblink: http://www.uke.gov.pl	
Areas of Activity: The office regulates postal, telecommunications, and broadcast frequencies activities, and regulates electromagnetic compatibility. Among the tasks that the office is charged with are: ensuring that all citizens have access to universal service; ensuring a high level of protection for consumers in their dealings with telecommunications; encouraging a high level of personal data protection; and ensuring the integrity and security of the public telecommunications network.	

The Bureau of the Inspector General for the Protection of Personal Data	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.giodo.gov.pl/	
Areas of Activity: Protection of personal data is the primary responsibility of the bureau.	

National Internal Security Agency (ABW)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: CERT, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Cooperates with Ministry of Interior	
Weblink: http://www.abw.gov.pl	
Areas of Activity: A government institution that protects the internal security of the Republic of Poland and its citizens, ABW's primary objective is to obtain advance knowledge in order to effectively neutralize threats to the state's internal security. Activities include combating cyber-crime and cyber-terrorism and prosecution of infringements. The agency is charged with investigating, detecting, and preventing crimes connected with production of and trade in goods, technologies, and services of strategic importance for national security.	

CERT GOV PL National Internal Security Agency (ABW)	
Type of Organization: National Security	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks	
Relationships: Cooperates with CERT Polska (and other CERTS within Poland)	
Weblink: http://www.cert.gov.pl	
Areas of Activity: As part of the National Internal Security Agency (ABW), this is the Computer Emergency Response Team for the Polish governmental sector.	

Ministry of National Defense (Centrum Wsparcia Technicznego Sekcja Reagowania na Incydenty Komputerowe WBBŁiI)	
Type of Organization: National Security	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks	
Relationships: Cooperates with other Polish CERTs	
Weblink: http://www.czst.wp.mil.pl/zglosz.php	
Areas of Activity: Polish military CERT.	
Polish Committee for Standardization	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: Cooperates with Ministry of Industry and Trade	
Weblink: http://www.pkn.pl	
Areas of Activity: The committee is responsible for standardization and adoption of international standards. There are technical departments within the committee that have responsibilities for information security.	
Office for Competition and Consumer Protection	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy	
Relationships: Cooperates with Ministry of Industry and Trade	
Weblink: http://www.uokik.gov.pl/	
Areas of Activity: The office is one source of consumer protection in Poland. If citizens feel they have been compromised or that their personal details have been stolen or used against them, they can contact the office for assistance, thus making the office a stakeholder in the security of Polish citizens' personal data.	
Ministry of Infrastructure	
Type of Organization: National Government	Ownership: Public

ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy
Relationships: Supervisory responsibilities for the Office of Electronic Communications
Weblink: http://www.en.mi.gov.pl/
Areas of Activity: The Ministry of Infrastructure is part of government administration that serves the minister responsible for issues related to construction, zoning and housing, maritime economy, communications, and transport.

Industry Organizations Active in Network and Information Security

The Polish Chamber of Commerce for Electronics and Telecommunication (Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji – KIGEiT)	
Type of Organization: Other Industry Associations	Ownership: Non-profit
ENISA Focus Points: AR, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.spis.cz	
Areas of Activity: The Polish Chamber of Commerce for Electronics and Telecommunication (KIGEiT) is an independent organization of economic entities involved in the manufacturing, export, import, trade, services, and R&D work in the area of electronics. The Chamber affiliates over 200 companies. KIGEiT is member of European Information, Communications and Consumer Electronics Technology Industry Associations (EICTA).	

The Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji – PIIT)	
Type of Organization: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.piit.org.pl	

Areas of Activity:

The Polish Chamber of Information Technology and Telecommunications (PIIT) was established in 1993, to assemble companies operating within the IT and telecommunications sector. PIIT is member of EICTA and at present has over 180 members. PIIT has declared its support for proposal concerning Internet safety of children via general education addressed to kindergartens, primary schools, first-level secondary schools, and schools of higher levels, as prepared by Nobody's Children Foundation and the Research and Academic Computer Network.

The Polish Chamber for Electronic Communication (Polska Izba Komunikacji Elektronicznej)

Type of Organization: IT Association	Ownership: Non-profit

ENISA Focus Points: Implementation of Security Technology and Standards Policy

Relationships: None

Weblink: http://www.pike.org.pl/

Areas of Activity:

The Polish Chamber of Electronic Communication (PIKE) represents 130 companies – broadband electronic communication operators and producers and distributors of equipment and services used by operators in their businesses. PIKE members serve over 4.5 million subscribers (75% of the market). PIKE supports members in their everyday business activity, representing their interests in relations with legislative bodies, the parliament, and the president, as well as many regulators and market participants. PIKE participates in the creation of legislation governing activities on the market, such as the Radio and Television Act, and telecommunications, copyright, and cinematography laws. PIKE represents the communications community with its most important business partners, such as broadcasters and copyright management organizations, as well as branch business partners such as self-government organizations from Poland and abroad. PIKE is also involved in educating its members on legal issues as well as supporting the implementation of ethical values in business. Twice a year, the chamber organises the PIKE Conference and Exhibition, which is the largest meeting for electronic media representatives in Poland.

Academic Organizations Active in Network and Information Security

PIONIER CERT, Security Team of Poznan Supercomputing and Networking Center

Type of Organization: Public and Private CERTS	Ownership: Public

ENISA Focus Points: CERT, Resilience, AR, Emerging Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy

Relationships: None

Weblink: http://cert.pionier.gov.pl/

Areas of Activity:

The PIONIER-CERT (formerly: POL34-CERT) is a Computer Security Incident Response Team that has been established to provide effective incident response service to members and users of Polish Scientific Broadband Network PIONIER (and POL34/622). The main purpose of this initiative is to establish a single point of contact for all security incidents involving hosts classified as belonging to the constituency of PIONIER-CERT. The primary goal is to provide active incident handling with high quality technical support, which can be guaranteed by five-year experience acquired by the Security Team of Poznan Supercomputing and Networking Center. As dealing with such incidents is mainly related to the information analysis process, the team can also be considered as the coordination center managing actual responses and exchanging critical information among various interested parties. The PIONIER-CERT Initiative should also be considered as the representative entity of PIONIER (and POL34/622) in security matters for any outside organizations.

Academic Computer Centre in Gdansk - TASK (Centrum Informatyczne Trójmiejskiej Akademickiej Sieci Komputerowej)

Type of Organization: Universities	Ownership: Public
ENISA Focus Points: AR, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.task.gda.pl/english/	

Areas of Activity:

Founded in 1994 by the State Committee for Scientific Research (KBN), the Academic Computer Centre in Gdansk (CI TASK) is an inter-university unit that manages one of the biggest and most modern metropolitan area networks (MAN) in Poland. The TASK network covers the territory of the whole so-called Tri-City – i.e. the complex of three adjacent towns Gdansk, Sopot, and Gdynia. It connects 70 LAN networks of various research institutes, in which over 6,000 computers, workstations, and servers are now installed. The network has about 16,000 users (not including students).

The Academic Computer Centre CYFRONET AGH

Type of Organization: Universities	Ownership: Public
ENISA Focus Points: AR, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.cyf-kr.edu.pl/en/	

Areas of Activity:

The Academic Computer Centre CYFRONET AGH, established over 30 years ago, is an autonomous organizational and financial entity of the AGH University of Science and Technology. The center currently employs around 60 people and incorporates the High-Performance Computing Department, Software Department, Computer Networks Department, Storage & Security Data Department, Technical Department, Administration Department, Financial and Accounting Department, and the Operators Section. Furthermore, it includes the European Cooperation Group and the Research and Development Group.

ICM – Interdisciplinary Centre for Mathematical and Computational Modelling	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: AR, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.icm.edu.pl/web/guest/home	

Areas of Activity:

ICM is a center involved in scientific research, computational sciences, development and implementation research, education in computational science and modelling, and informational technology, as well as being a resource of knowledge and an organization strongly involved in the promotion of science.

Wroclaw Centre for Networking and Supercomputing	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: AR, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.wcss.wroc.pl/english/	

Areas of Activity:

Wroclaw Centre for Networking and Supercomputing is an organizational unit of Wroclaw University of Technology. Founded in 1995, its main tasks include operation and development of the Wroclaw Academic Computer Network (WASK), operation and development of high performance computing services, and operation and development of network information services for all academic institutions in city of Wroclaw. The center is working on a project called Policy-based Security Tools and Framework (POSITIF) under the 6th Frame Programme of European Union. WCSS is responsible for management of the test bed for other project partners, workshops organization, knowledge dissemination in the security sector, and conducting scientific research on high-speed networks' security systems.

Other Bodies and Organizations Active in Network and Information Security

NASK/Computer Emergency Response Team Polska – Polish CERT	
Type of Organization: CERT	Ownership: public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.cert.pl	
Areas of Activity: This CERT organization operates within NASK. The CERT is a member of FIRST and TERENA TF-CSIRT and an Accredited Team within the Trusted Introducer (TI) initiative. It responds to computer incident reports and is involved in numerous security projects and awareness campaigns.	

Nobody's Children Foundation	
Type of Organization: CERT	Ownership: Non-Profit
ENISA Focus Points: Emerging/Current Risks	
Relationships: None	
Weblink: http://www.fdn.pl/	
Areas of Activity: The organization is the coordinator of AWARENODE (Safer Internet Action Plan project carried out with NASK), and offers assistance to children, their parents, and guardians in connection with internet abuse.	

SIT	
Type of Organization: Philanthropic, Educational & Professional Associations	Ownership: Non-Profit
ENISA Focus Points: Emerging/Current Risks	
Relationships: Part of INSAFE	
Weblink: http://www.saferinternet.pl/en	

Areas of Activity: As part of the European internet safety network INSAFE, within the framework of the Safer Internet Programme (a coherent approach by the European Union), SIT aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal and unwanted content by the end-user.

Polish TELECOM CERT Team – TP-CERT	
Type of Organization: CERT	Ownership: Private
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: TP CERT collaborates with other CERTs in Poland, including CERT Polska and CERT GOV.pl	
Weblink: http://www.tp.pl/prt/en/tpcert	
Areas of Activity: In 1997, Telekomunikacja Polska established the Computer Security Incident Response Team (CSIRT) with Information and Communication Technology (ICT) security of Internet users in mind. Since September 2006, CSIRT has been operating under the name TP CERT. TP CERT provides monitoring services for TP's constituency regarding network and computer security incident response and prevention. TP CERT's constituency is the Internet community of TP (including both individual users and corporate customers). The main goals of TP CERT are as follows: 1) To assist users of the TP network in implementing proactive measures to reduce the risks of computer security incidents, in particular by providing consultancy and education services, information on network and computer security, and warnings of possible attacks 2) To assist users of the TP network in responding to such incidents when they occur, in particular by providing a single, trusted point of contact in TP for Internet users to deal with network and computer security incidents, and coordinating incident handling with an emphasis on exchange of information between interested parties.	

FK (Polish Consumer Federation National Council)	
Type of Organization: Other	Ownership: Private
ENISA Focus Points: AR, Development of Security Technology and Standards	
Relationships: CERT Poland (NASK)	
Weblink: http://www.federacja-konsumentow.org.pl	
Areas of Activity: FK is a consumer organization dedicated to protecting and educating consumers.	

TP Group Foundation (Fundacja Grupy TP)	
Type of Organization: Other	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.fundacjagrupytp.pl/	
Areas of Activity: This foundation is part of the European internet safety network INSAFE within the framework of the Safer Internet Programme, which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal and unwanted content, as part of a coherent approach by the European Union.	

Kidprotect.pl Foundation	
Type of Organization: Other	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.kidprotect.pl/	
Areas of Activity: The Kidprotect.pl Foundation is the first organization in Poland that is dedicated to the safety of children on the internet. Active since 2002, Kidprotect.pl is a non-profit organization, depending on sponsor support and the work of volunteers. The Foundation does not use any public funds and does not pursue any business activity. As part of carrying out the program Safe Internet (www.bezpiecznyinternet.org), it also conducts trainings for teachers, parents, educators, and crime prevention officers, as well as classes for children to learn how to practice internet safety. Kidprotect.pl operates a hotline that enables anonymous internet users to report incidents of sexual crimes against children, and enacted a social campaign called Stop Pedophiles (www.stoppedofilom.pl). Kidprotect.pl also trains police officers and prosecutors in combating this sort of crime. The Foundation further takes care of adult victims of sexual abuse and carries out an online support group for male and female victims and their relatives.	

Activities

Strategic Initiatives

The Safer Internet Academy (Akademia Bezpiecznego Internetu)

Type of Activity: Non-governmental Initiative

Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: http://www.fdn.pl/strona.php?p=25

Description:

Nobody's Children Foundation has worked for improving online safety for children and young people since 2003. Comprehensive research, education, media, and help activities have been conducted within the Safer Internet Academy (SIA) program. Programs within SIA include the Child in the Web campaign, Stop Cyberbullying campaign, Sieciaki.pl project, and Helpline.org.pl.

Przedszkolaki Sieciaki

Type of Activity: Non-governmental Initiative

Responsible Organization(s): Nobody's Children Foundation, Egmont, TV MiniMini

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.przedszkolaki.sieciaki.pl/

Description:

The Safer Internet Academy team, in cooperation with Egmont (a publishing company specializing in children's books), operate the website Przedszkolaki.Sieciaki.pl, dedicated to younger children.

Sieciaki.pl

Type of Activity: Non-governmental Initiative

Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT, TP Group Foundation (Fundacja Grupy TP)

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: http://www.sieciaki.pl

Description:

Sieciaki.pl is an educational project run by the Nobody's Children Foundation since February 2005. Its main component is a dedicated website, www.sieciaki.pl, focusing on internet safety for children and young people. Additionally, the project involves meetings with children, open-air events, concerts, and educational sessions. Films, songs, and multimedia materials have also been developed. Goals of the Sieciaki.pl project include educating children about safety on the Internet and how to use the Web and certifying and promoting safe websites.

Helpline.org.pl

Type of Activity: Non-governmental Initiative

Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT, TP Group Foundation (Fundacja Grupy TP)

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: http://helpline.org.pl/

Description:

Helpline.org.pl is a joint project of the Nobody's Children Foundation and the TP Group Foundation, co-financed by the European Commission within the Safer Internet Plus program. Helpline.org.pl was launched in February 2007 on the Safer Internet Day, with the goal of helping children and young people face threats on the Internet. Moreover, the Helpline's consultants provide advice for parents, caregivers, and professionals who work with children and young people.

Child in the Web (Dziecko w sieci)

Type of Activity: Non-governmental Initiative

Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT, NASK

ENISA Focus Points: CERT

Weblink: http://www.dzieckowsieci.pl/

Description:

Since January 2005, this campaign has been carried out within the European Commission's Safer Internet program as a comprehensive educational project designed to improve children and young people's safety online. The main partner of the campaign has been the TP (Polish Telecom) Group Foundation (TPGF).

Saferinternet.pl

Type of Activity: Non-governmental Initiative

Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska - Polish CERT, NASK

ENISA Focus Points: AR

Weblink: http://saferinternet.pl/

Description:

Since January 2005, the Nobody's Children Foundation has been the national coordinator of the awareness project carried out in cooperation with Research and Academic Computer Network (NASK) within the European Commission's program Safer Internet Plus (SIP). The project involves national efforts and international cooperation for preventing threats to children and young people who use electronic media. The Foundation runs the Saferinternet.pl project within the Safer Internet Academy. In cooperation with NASK, the following initiatives have been undertaken within the Saferinternet.pl project: Safer Internet Day, Keeping Children and Young People Safe Online international conference, and the dedicated website www.saferinternet.pl.

Polish HOTLINE

Type of Activity: Non-governmental Initiative

Responsible Organization(s): NASK

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: http://www.dyzurnet.pl

Description:

The National Initiative for Children Hotline (NIFC) Polska is a team acting within the framework of the Research and Academic Computer Network, qualified to receive and react to notifications regarding illegal content on the Internet under Polish law. The hotline is the result of a competition announced within the framework of the Safer Internet Action Plan of the European Commission. In October 2003, NASK notified its readiness to open hotline services and signed a contract to take leadership of the project in September 2004.

Abuse-forum

Type of Activity: Non-governmental Initiative

Responsible Organization(s): NASK

ENISA Focus Points: CERT, AR, Emerging/Current Risks

Weblink: N/A

Description:

Cooperation between Polish security teams and ISP representatives; includes more than 10 "incident handling capability" teams.

WOMBAT Project
Type of Activity: Non-governmental Initiative
Responsible Organization(s): NASK/CERT Polska
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks
Weblink http://www.wombat-project.eu/
Description: The goal of the WOMBAT project is to create a global system of monitoring and analysis of online threats, with particular focus on malicious software, which in recent years has become a powerful tool in the hands of cyber-criminals. The project started in January 2008 within the 7th Framework Program of the European Union and will last until the end of 2010. The project is developed by IT security experts from renowned companies and research institutions, involved in monitoring activities and increasing the security of the Internet. Research within the WOMBAT project will concentrate on the creation of new methods of analyzing the threats appearing on the Internet on a mass scale, the identification of their sources, and reasons for their occurrence. Also, as trends of threats are changing, there is a special need for novel sources of data, collected from all over the world and analyzed in a wide context. Information intended to serve this end will be culled from: the Leurre.com globally dispersed system of honeypots serviced by the Eurecom Institute; the world's biggest collection of malicious software gathered by Hispasec Company (within the framework of Virustotal project); the CERT Polska team originating from the ARAKIS early warning system and the HoneySpider Network honeyclient system; and the global Symantec DeepSight Threat Management System.
ARAKIS Project
Type of Activity: Non-governmental Initiative
Responsible Organization(s): NASK/CERT Polska
ENISA Focus Points: CERT, AR, Emerging/Current Risks
Weblink: http://www.arakis.pl
Description: ARAKIS is a CERT Polska (NASK) project that aims to create an early warning and information system for novel network threats. The system focuses on detection and characterization of new automated threats. Currently the system detects threats that propagate actively through scanning. ARAKIS aggregates and correlates data from various sources, including honeypots, darknets, firewalls and antivirus systems. Each of these sources gives a different perspective on what is happening in the network.
CLOSER (CLuster Of SEcurity Resources)
Type of Activity: Non-governmental Initiative

Responsible Organization(s): NASK/CERT Polska
ENISA Focus Points: CERT
Weblink: None
Description: Program awarded by NATO to NASK (and others) the task of establishing and coaching new CSIRT teams in CEE region. Additional goals of the program are to: provide training and mentoring services; instruct in usage of IR systems; increase cooperation among CERTs worldwide; help in establishing CERT standards and procedures in countries where this may be necessary; and introduce new CERT stakeholders to worldwide forms and assist in their collaboration.
Safer Internet
Type of Activity: Non-governmental Initiative
Responsible Organization(s): Kidprotect.pl Foundation
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: http://www.saferinternet.pl
Description: Web site with advice and materials concerned with online safety and how to protect against malicious provocations online.
Honeyspider Network (HSN)
Type of Activity: Non-governmental Initiative
Responsible Organization(s): NASK/CERT Polska
ENISA Focus Points: CERT
Weblink: http://www.honeyspider.net/
Description: The HoneySpider Network Project is a joint venture between NASK/CERT Polska, GOVCERT.NL and SURFnet. The goal is to develop a complete client honeypot (or honeyclient) system, based on existing state-of- the-art client honeypot solutions and a novel crawler application tailored for the bulk processing of URLs. The system focuses on attacks against, or involving the use of, Web browsers. These include the detection of drive-by downloads, malicious binaries and phishing attempts. Apart from identifying browser exploits (including 0-day attacks), the system is expected to automatically obtain and analyze the attacking malware and ultimately generate its signature. The major incentive to start this project is the rapidly growing number of browser exploits involving varying degrees of user interaction. These types of attacks lie outside the scope of current monitoring systems in use by the three parties.

Research Programmes

Positif

Type of Activity: Technical Research Programme

Responsible Organization(s): Wroclaw University of Technology and stakeholders of other EU countries

ENISA Focus Points: Resilience, Implementation of Security Technology and Standards

Weblink: http://www.positif.org/

Description:

The main task of the POSITIF project is to create a security framework that enables automatic management of a network infrastructure beyond networking devices and software. This platform ensures security of networking infrastructure on several levels. The platform consists of tools that provide efficient management of the network infrastructure and definition and installation of proper security policies on the network blocks. This solution is semi-automated and provides proactive solutions of monitoring system security. There is the option to integrate the platform with many types of intrusion detection components. It is also possible to monitor operating systems using appropriate scanning tools.

Measurement and Analysis of P2P Activity Against Paedophile Content (MAPAP)

Type of Activity: Social and Other Research Programmes

Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT and stakeholders of other EU countries

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://antipaedo.lip6.fr

Description:

A project run within the European Commission's Safer Internet Plus program, designed to explore P2P networks in order to develop an effective system of combating child pornography.

Events

Conference and Workshops

Keeping Children and Young People Safe Online

Responsible Organization(s): Nobody's Children Foundation. Computer Emergency Response Team Polska – Polish CERT, TP Group Foundation (Fundacja Grupy TP), NASK, Landeszentrale für Medien und Kommunikation/Klicksafe.de, Insafe	Frequency: Annual
ENISA Focus Points: CERT, AR, Emerging/Current Risks	
Target Groups: Major – Security Professionals, Educational and Research Organizations; Minor – Consumers/Citizens	
Weblink: http://konferencja.saferinternet.pl/	
Description: The Warsaw conference brings together representatives from the education sector, NGOs, law enforcement, government, and industry. It addresses a wide variety of issues relating to children and young people's safety online, such as cyber-bullying, social networking sites, mobile phones, and online gaming. The aims of the conference are to raise awareness of the new challenges and opportunities in fighting Internet threats and to help share best practices across different sectors. Numerous sessions at the event are led by recognized international experts in the field of child protection.	
SECURE	
Responsible Organization(s): NASK Computer Emergency Response Team Polska – Polish CERT, ENISA, Ministry of Interior and Administration, National Internal Security Agency (ABW)	Frequency: Annual
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks	
Target Groups: Security Professionals	
Weblink: http://www.secure.edu.pl/en/index.html	
Description: SECURE is the oldest IT security conference in Poland. The conference structure and program is specifically aimed at: senior managers directly charged with protecting their corporate infrastructure; technical experts who determine security requirements and implement solutions; policy and decision makers with overall security responsibility; legal/compliance/regulatory professionals who work with policy and decision makers in establishing security policies; and government executives and practitioners who are responsible for protecting systems and critical infrastructures. Every year current issues concerning security matters of IT systems and networks are discussed at the conference, which for 10 years has been organized by CERT Polska team acting within NASK.	

The Personal Data Protection Day	
Responsible Organization: The Bureau of the Inspector General for the Protection of Personal Data	Frequency: Annual
ENISA Focus Points: CERT, AR, e-ID	
Target Groups: Security Professionals, Government Institutions	
Weblink: http://www.giodo.gov.pl/410/	
Description: Polish event for Data Protection Day, which aims to draw the attention of all citizens of European countries to issues related to data protection and to help raise the level of knowledge in this area.	

ENIGMA	
Responsible Organization: ENIGMA Systemy Ochrony Informacji	Frequency: Annual
ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Target Groups: Major – Security Professionals; Minor – Government Organizations, Educational and Research Organizations	
Weblink: http://www.enigma.com.pl/index.php?option=com_content&task=view&id=201&Itemid=165	
Description: The oldest national conference of cryptography and Information Security. Several stakeholders and experts on new technologies present standards and procedures for the protection of information.	

Media Campaigns

Stop Cyber-Bullying (Stop cyberprzemocy)	
Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT, TP Group Foundation (Fundacja Grupy TP), NASK	Frequency: Annual
ENISA Focus Points: CERT, AR, Emerging/Current Risks	
Target Groups: Consumers/Citizens	
Weblink: http://www.saferinternet.pl/wiadomosci/inauguracja_kampanii_stop_cyberprzemocy.html	

Description: In February 2007, a joint project of the Nobody's Children Foundation and the TP Group Foundation was launched within the Safer Internet program – helpline.org.pl. Its mission is to help children and young people who face threats when using the Internet and mobile phones, and to introduce system changes to provide more effective protection for the youngest users of new technologies.

You Never Know Who Is On the Other Side (Nigdy nie wiadomo, kto jest po drugiej stronie)	
Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT	Frequency: Once
ENISA Focus Points: CERT, AR, Emerging/Current Risks	
Target Groups: Consumers/Citizens	
Weblink: http://www.dzieckowsieci.pl/strona.php?p=147	
Description: A media campaign conducted under the slogan "You Never Know Who Is On the Other Side" is the first project carried out by the Child On the Web campaign. Action has been devoted to the problem of child abuse on the Internet and initiating a discussion on this issue in Poland. The media campaign gained more than 70% visibility among the public (Gemius 2005).	

The Internet Is a Window on the World, the Whole World	
Responsible Organization(s): Nobody's Children Foundation, Computer Emergency Response Team Polska – Polish CERT, NASK	Frequency: Annual
ENISA Focus Points: CERT, AR, Emerging/Current Risks	
Target Groups: Consumers/Citizens	
Weblink: http://www.dzieckowsieci.pl/strona.php?p=70	
Description: In 2005 and 2006 the campaign was co-organized by Research and Academic Computer Network (NASK) and the Nobody's Children Foundation. The media and educational campaign addressed the problem of harmful content on the Internet. Press, radio, and TV ads were created under the slogan "The Internet is a window on the world, the whole world".	

Stop Pedophiles	
Responsible Organization: Kidprotect.pl Foundation	Frequency: N/A
ENISA Focus Points: AR, Emerging/Current Risks	

Target Groups: Consumers/Citizens	
Weblink: http://www.stoppedofilom.pl/kampania/	
Description: This is a public service campaign warning against pedophilia.	
Safer Internet Day	
Responsible Organization(s): Nobody's Children Foundation. Computer Emergency Response Team Polska – Polish CERT, NASK Computer Emergency Response Team Polska – Polish CERT, European Commission Information Society and Media	Frequency: Annual
ENISA Focus Points: AR	
Target Groups: Major – Consumers/Citizens; Minor – Educational/Research Organizations	
Weblink: http://www.saferinternetday.pl/	
Description: Starting as an initiative in 2004, SID has become a major annual event crowning the awareness activities of Insafe, the European safer internet network. The growing network of nodes from Europe and beyond has a mission to promote media literacy and the safe, ethical, and efficient use of the internet and mobile phones.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing

concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Poland.

Country Report –Portugal

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Lisbon
Total area:	92,000 sq.km
Population:	10.6 million
Official language:	Portuguese
Time zone:	GMT
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Portugal, we present a set of three indicators in the Country Highlights section.

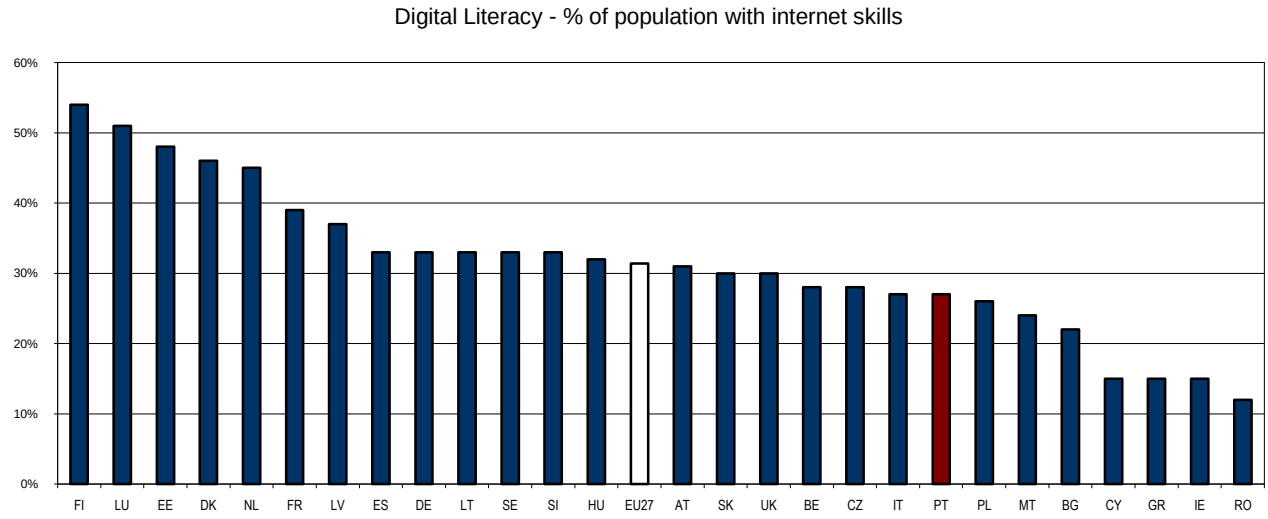
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Portugal is fundamental to this NIS study.

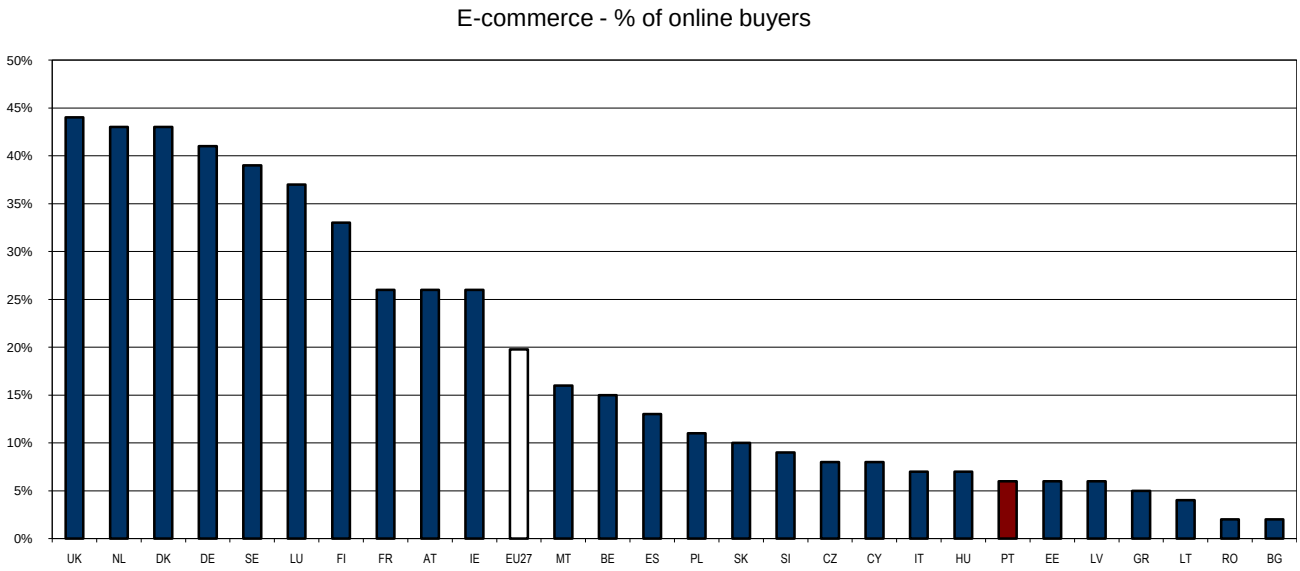
Portugal is in the middle rank of EU countries in terms of information society development.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

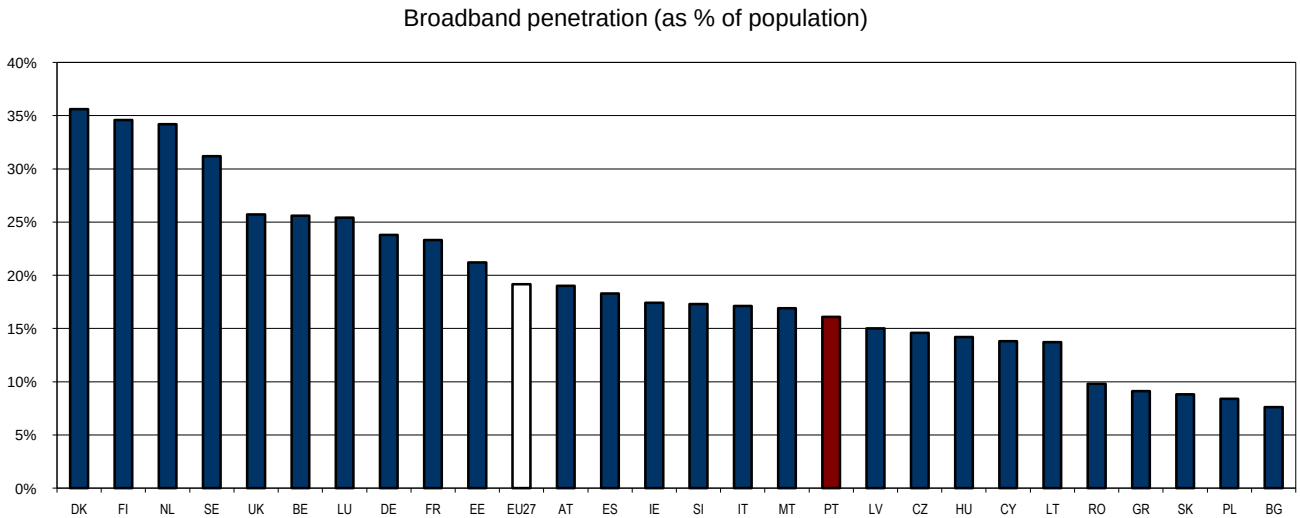
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The Knowledge Society Agency is the Portuguese national security agency. The agency is responsible for information security development and implementation, which includes coordinating the policies for the information society and its mobilization through the promotion of dissemination, qualification and research activities. Among other tasks, it is in charge of promoting security and privacy in the use of the Internet and information and communication technologies.

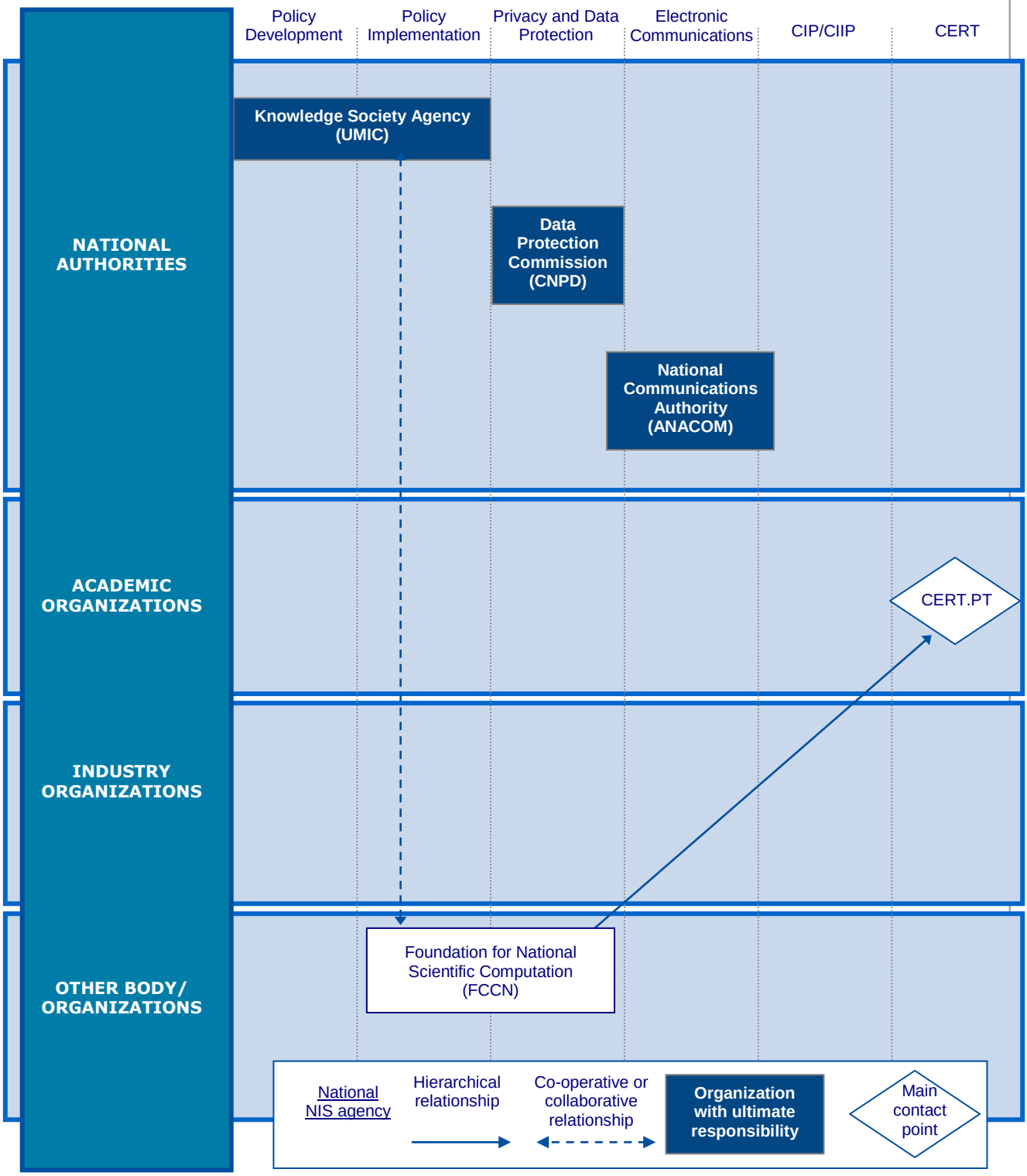
The CNPD – Portuguese Data Protection Authority is responsible for ensuring compliance with privacy and data protection legislation. The CNPD is an independent body, with powers of authority throughout Portuguese territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law.

The Portuguese National Communications Authority is responsible for implementing and ensuring compliance with electronic communications legislation in Portugal.

Additionally Portugal has a national security response team in place to handle security breaches and other incidents. CERT.PT acts as a national point of contact for IT security.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Portugal. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Knowledge Society Agency (UMIC)	X	X	X					X
Data Protection Commission (CNPD)			X	X				X
National Communications Authority (ANACOM)		X						X
FCCN (CERT.PT)	X		X					X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Portugal:

National Authorities in Network and Information Security	
Agência para a Sociedade do Conhecimento (UMIC) - Knowledge Society Agency	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: autonomous but under the supervision of the Ministry of Science, Technology and Higher Education	
Weblink: http://www.umic.pt/	
Areas of Activity: The Knowledge Society Agency (UMIC) is the Portuguese public agency tasked with the mission of coordinating the policies for the Information Society and mobilizing it through dissemination, qualification and research activities.	
Autoridade Nacional de Comunicações (ANACOM) – National Communications Authority	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Development of Security Technology and Standards	
Relationships: independent	
Weblink: http://www.anacom.pt	
Areas of Activity: The National Communications Agency (ANACOM) is the regulator, supervisor and representative of the communications sector in Portugal. The authority is responsible for ensuring compliance with the Electronic Communications Law.	
Comissão Nacional de Protecção de Dados (CNPD) – National Data Protection Commission	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Relationships: independent, co-operates with the Ministry of Interior	

Weblink: http://www.cnpd.pt/
Areas of Activity: The National Data Protection Commission (CNPD) is an independent body, with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection.

Industry Organisations Active in Network and Information Security

Associação Nacional das Empresas das Tecnologias de Informação e Electrónica (ANETIE) – National Information Technologies and Electronics Association	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Relationships: co-operates with the National Authorities	
Weblink: http://www.anetie.pt/	
Areas of Activity: The National Information Technologies and Electronics Association (ANETIE) has as it members most of the national technology companies active in the electronics, software, communication and information industries.	

Associação dos Operadores de Telecomunicações (APRITEL) – Association of Telecommunications Operators	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.apritel.org/	
Areas of Activity: The purpose of the Association of Telecommunications Operators (APRITEL) is to promote a legal and regulatory environment supporting investment in the industry of electronic communications and to contribute for the development of the Information Society.	

Other Bodies and Organisations Active in Network and Information Security

Fundação para a Computação Científica Nacional (FCCN) - Foundation for National Scientific Computation	
Type of Organisation: Other	Ownership: Non-profit
ENISA Focus Points: CERT, AR	
Relationships: part of CESNET	
Weblink: http://www.fccn.pt/	
Areas of Activity: The Foundation for National Scientific Computation (FCNN) runs the research and education network and the CERT for this community.	

CERT.PT	
Type of Organisation: CERT	Ownership: Non-profit
ENISA Focus Points: CERT, AR	
Relationships: Part of FCCN	
Weblink: http://www.cert.pt	
Areas of Activity: CERT.PT's priorities include: offering technical support to computer users in resolving security incidents, advising on best-practices, analysing artefacts, and coordinating actions with the parties involved; gather and disseminate a set of information about vulnerabilities and recommendations, pertaining to potential security risks and ongoing malicious activities; gather from accredited sources information related to security vulnerabilities, and act on the community with the goal of minimizing impact at the National level; and, promote the creation of new CERT/CSIRTs in Portugal, and raise awareness of security issues on computer users. CERT.PT maintains the hotline service of Linha Alerta.	

Internet Segura – Safe Internet	
Type of Organisation: Other	Ownership: Private
ENISA Focus Points: AR	
Relationships: consortium of UMIC, the Ministry of Education, FCCN, and Microsoft Portugal	
Weblink: http://www.internetsegura.pt/	

Areas of Activity:

Internet Segura was created in the scope of European Program Safer Internet plus and it has the following main strategic goals: 1) fight against illegal content; 2) Minimize the illegal and harmful content impact on the citizens; 3) Promote a safe Internet usage; and 4) Society Awareness about the Internet usage risks. Among the projects that Internet Segura has carried out are the Internetsegura.pt and SeguraNet portals and Linha Alerta.

Activities

Strategic Initiatives

InternetSegura.pt Portal

Type of Activity: Non-Governmental Initiatives

Responsible Organisation(s): Internet Segura

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.internetsegura.pt

Description:

InternetSegura.pt is a portal dedicated to: fighting illegal content; minimizing the effects of illegal and harmful content on citizens; promotion of safe use of the Internet; and awareness of society to the risks associated with the use the Internet.

SeguraNet Portal

Type of Activity: Non-Governmental Initiatives

Responsible Organisation(s): Internet Segura

ENISA Focus Points: AR, Emerging/Current Risks

Weblink: http://www.seguranet.pt

Description:

Seguranet is a portal whose main goal is to promote a secure Internet usage among parents, teachers, children and youngsters.

Linha Alerta

Type of Activity: Non-Governmental Initiatives

Responsible Organisation(s): Internet Segura

ENISA Focus Points: CERT, AR, Emerging/Current Risks, Implementation of Security Technology and Standards
Weblink: http://linhaalerta.internetsegura.pt/
Description: Linha Alerta is part of a combined project – awareness node and hotline service – called Internet Segura and is co-funded until December 2008 by the European Commission under the Safer Internet plus program. The mission of Linha Alerta is to block illegal content on the Internet and prosecute their disseminators in an effective way. In order to carry out this core activity Linha Alerta has a website to which anonymous complaints can be sent.

Events

Conference and Workshops

Safer Internet in Youth places "JA"	
Responsible Organisation: SeguraNet	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major- Consumers/Citizens	
Weblink: N/A	
Description: The objective is to promote a use and insurance of the Internet, clarified and critical, by the children and young, as also by the workers and citizens in the general.	

Media Campaigns

Internet Safety Day	
Responsible Organisation: UMIC	Frequency: biennial
ENISA Focus Points: AR, Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Citizens/Consumers	
Weblink: N/A	

Description: Promotes sensibilities, and clarifies tools and tips for safer internet usage. Organized with the European Community.	
Unique European Program	
Responsible Organisation: Linha Alerta	Frequency: n/a
ENISA Focus Points: Implementation of Security Technology and Standards	
Target Groups: Major- Consumers	
Weblink: N/A	
Description: Integrated in the "unique European Program" for children	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

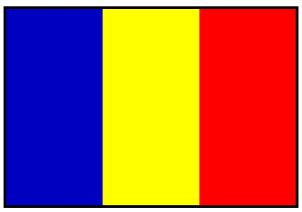
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Portugal.

Country Report – Romania

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Bucharest
Total area:	238 000 sq.km
Population:	21.6 million
Official language:	Romanian
Time zone:	EET (GMT+2)
Currency:	Leu (RON)

Source: Eurostat

Country Highlights

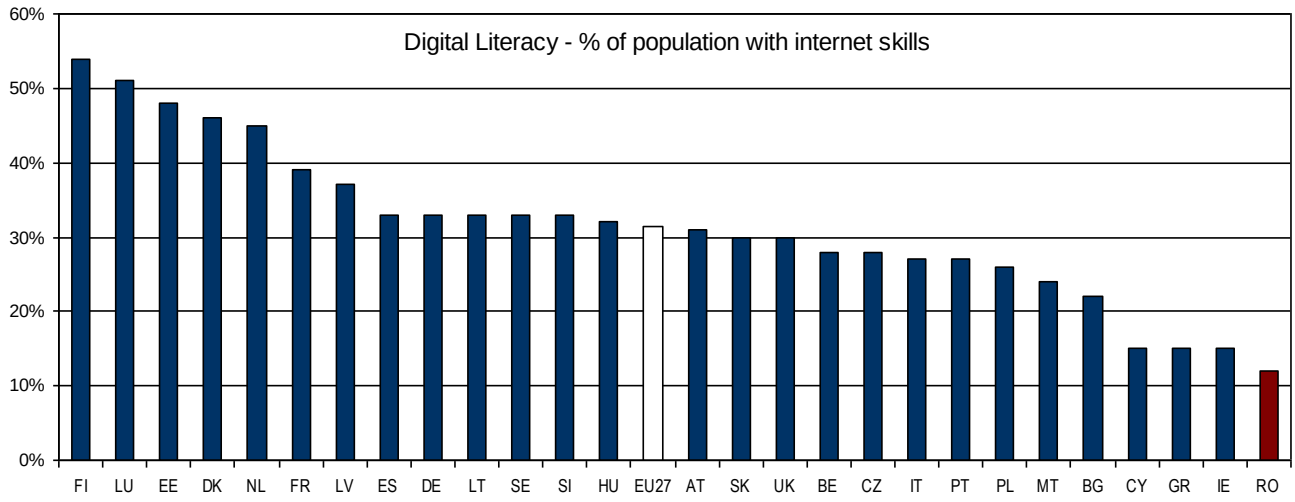
In order to provide an overview of recent IT developments in Romania, we present a set of three indicators in the Country Highlights section.

The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

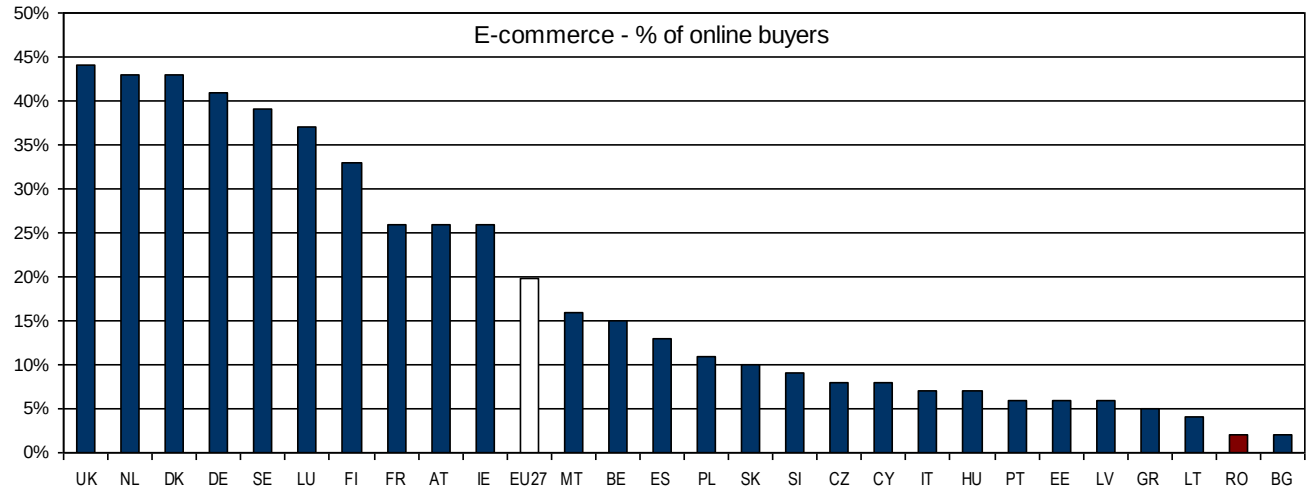
For these reasons, a general understanding of the stage of IT adoption in Romania is fundamental to this NIS study.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

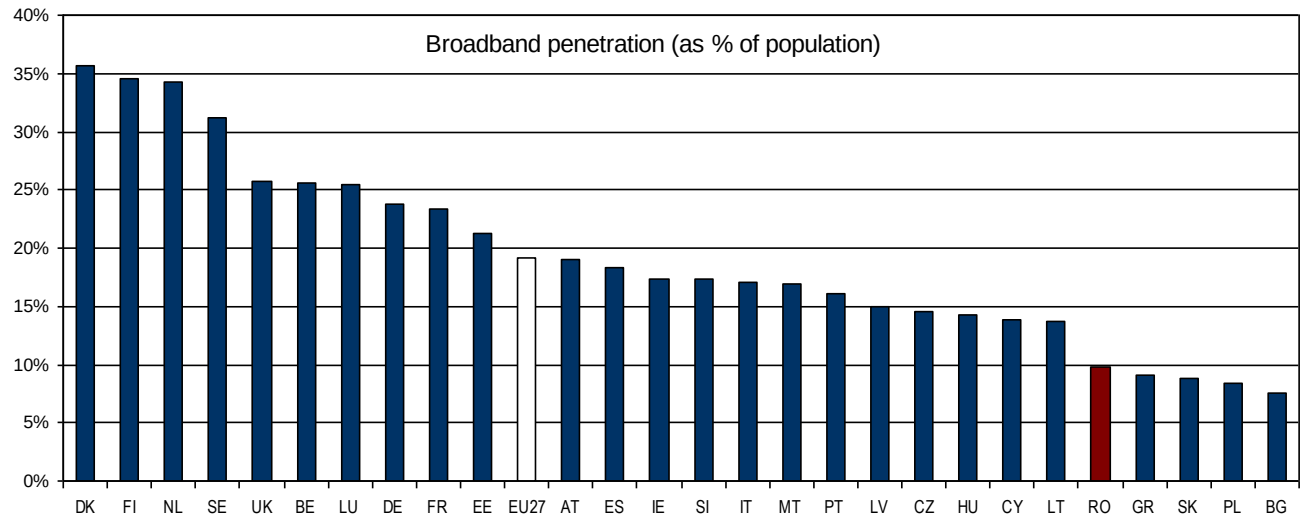
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Romania does not have one single institution recognized among NIS stakeholders as the national security agency; there are various organization sharing the responsibilities and competencies concerning the classified information. Concerning the state classified information, National Registry Office for Classified Information performs regulation,

authorization, evidence and control tasks in conformity with the provisions on the protection of classified information.

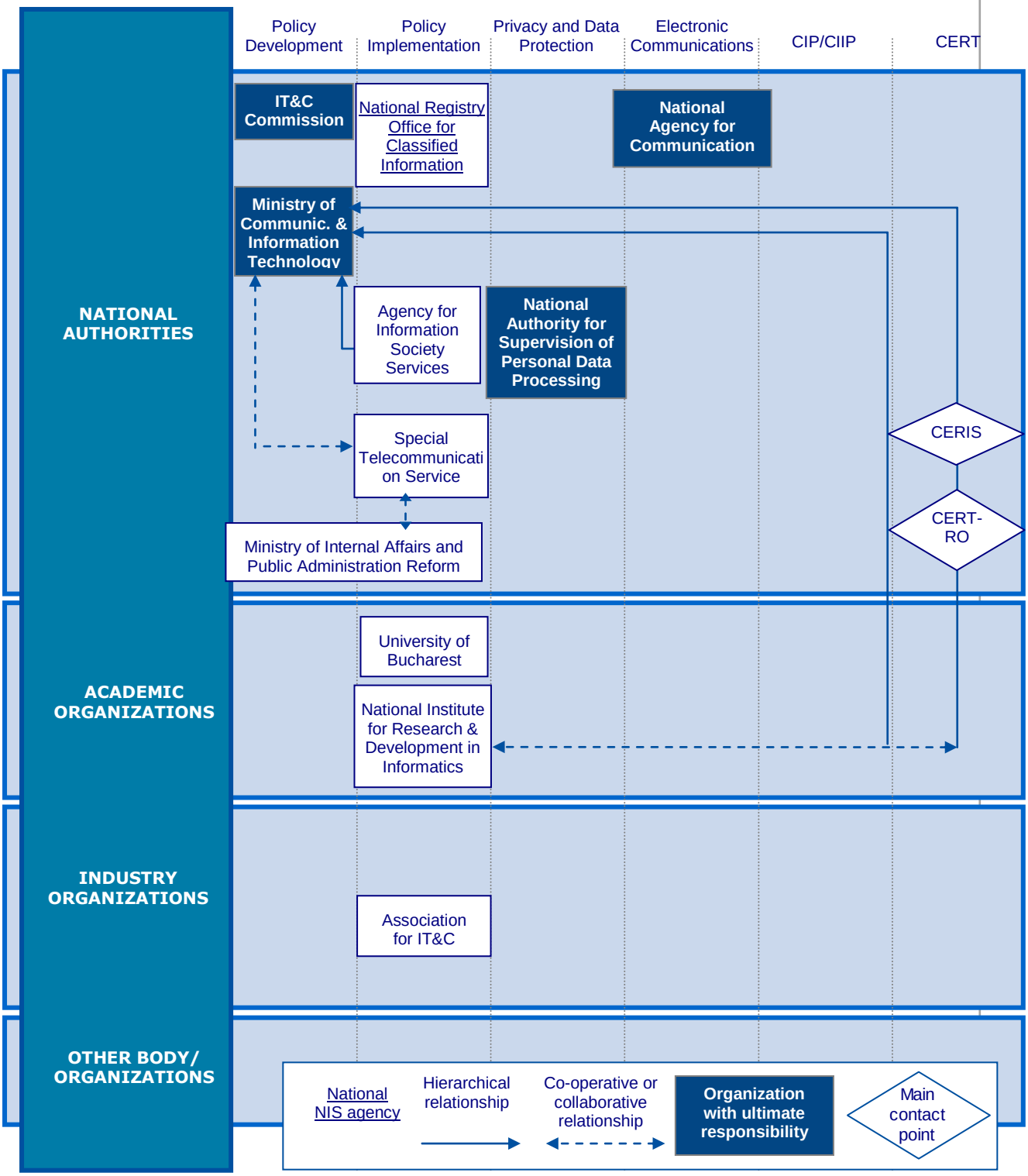
The Romanian Ministry of Communication and Information Technology is the institution that holds the responsibility for the development and implementation of the Information Society Strategy and beyond, support the development of the Romanian IT&C industry, develop and implement Information Security Strategy. Several other organizations in cooperation with the Ministry of Communication and Information Technology participate at the implementation of security policies at national level.

Romania is committed to data protection and ensuring compliance in this regard. The National Authority for the Supervision of Personal Data Processing is a public authority, autonomous and independent from any authority of the public administration, as well as from any natural or juridical person from the private area that regulates the data protection and processing, monitors and controls the operators. It aims at protecting the fundamental rights and freedoms of the natural persons in connection with the processing of personal data and the free circulation of these data.

Additionally, Romania has security response teams in place to handle security breaches and other incidents. CERT-RO (Computer Emergency and Response Team - Romania) coordinates security incidents and offers information exchange platform for IT specialists responsible for the IT security of all kinds of organizations, including government institutions and enterprises. CERT-RO operations are in its infancy in Romania - it is subordinated to the Ministry of IT&C and was founded temporarily as a department within the National Institute for Research and Development in Informatics.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Romania. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Communication and Information Technology	X						X	X
IT&C Commission							X	
National Agency for Communication								X
Agency for Information Society Services								X
National Authority for the Supervision of Personal Data Processing								X
National Registry Office for Classified Information								X
IT Security Incidents Reports and Expertise Centre		X	X	X				
CERT-RO	X							
Special Telecommunications Service		X		X				X
Ministry of Internal Affairs and Public Administration Reform						X	X	X

Association for IT&C			X	X				
Romanian Intelligence Service		X	X	X				
University of Bucharest								

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Romania:

National Authorities in Network and Information Security	
Ministry of Communication and Information Technology	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.mcti.ro	
Areas of Activity: The ministry develops and implements the Information Society Strategy 2004-2008, supports the development of the Romanian IT&C industry, and develops and implements Information Security Strategy.	
IT&C Commission – Chamber of Deputies	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://www.cdep.ro/	
Areas of Activity: The chamber is a parliamentary commission whose objective is to launch legislative initiatives.	
National Agency for Communication and Information Technology (ANRCTI)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: The Prime Minister names the president of the organization.	
Weblink: http://www.anrcti.ro/	

Areas of Activity: The National Agency is an independent institution that sets the rules for the Romanian communications market and monitors the enforcement of those rules. ANRCTI's major objectives include: promotion of competition, protection of the end-users' interests, encouragement of effective investments into infrastructure, and stimulation of innovations.

Agency for Information Society Services (ASSI)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: The Agency is subordinated to the Ministry of Communication and Information Technology	
Weblink: http://www.assi.ro/	
Areas of Activity: The organization is in charge of running IT systems for the central governmental bodies offering electronic services to the public.	

National Authority for the Supervision of Personal Data Processing	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.dataprotection.ro/	
Areas of Activity: The National Authority for the Supervision of Personal Data Processing is a public authority, autonomous and independent from any authority of the public administration, as well as from any natural or juridical person from the private area. According to the law, the Authority can't be subjected to any imperative or representative mandate and can't be compelled to submit to the instructions and orders of another public authority or private entity. The President of the Authority is named by the parliament. The Authority focuses on protection of fundamental rights and freedom of the natural persons, especially the right of intimate, family and private life in connection with the processing of personal data and the free data circulation.	

National Registry Office for Classified Information (ORNISS)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	

Relationships: ORNISSS is a public institution with legal power, subordinated to the Government and directly coordinated by the Prime Minister.
Weblink: http://www.orniss.ro/
Areas of Activity: ORNISS performs regulation, authorization, evidence and control tasks in conformity with the protection of classified information, the National Standards for the protection of classified information in Romania, and the Norms of the North Atlantic Treaty Organization on the protection of classified information in Romania. In order to accomplish the tasks assigned, ORNISS is empowered to require the necessary information from the heads of public authorities and bodies, of economic operators with integral or partial state share capital and of other public or private legal persons. The heads of the authorities and public bodies, of economic units with integral or partial state share capital and of other public or private legal bodies are bound to place at ORNISS' disposal the data and information related to the protection of classified information in their field of activity, except for the cases stipulated by law.

Special Telecommunications Service (STS)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: The activity of the Special Telecommunications Service is organized and coordinated by the Supreme Council of National Defence and is placed under the control of the Romanian Parliament, through the Defence, Law Enforcement and National Security Commissions in the two Chambers of Parliament. STS cooperates with the ministries and the other public administration entities to ensure the security and resiliency of the networks.	
Weblink: http://www.stsnet.ro/	

Areas of Activity:

STS manages, operates and develops special telecommunications networks under its management or assigned to it for use; develops programs and documents for the modernisation, development, operation and maintenance of the special telecommunications networks; establishes the communications security policy and ensures application of the methods and measures required for the protection of the information processed, stored or transmitted through the special telecommunications networks according to the national standards for information protection; manages and ensures protection of the government-assigned frequency bands used to achieve its legal attributions or those of the institutions competent in the field of national security and public order; monitors across the country, for protection purposes, the government-assigned frequency bands under its management and keeps a record of their use; develops co-operation relations with other institutions within the national system of defence and provides special communications for the High National Headquarters and the National Command and Control Authority, under the terms of the law; co-operates with the institutions within the national system of defence, as well as with other legal entities carrying out activities in this field, in order to harmonise and ensure compatibility of their communication systems; organises the electronic signature authentication system.

Ministry of Internal Affairs and Public Administration Reform (MIRA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.mira.gov.ro/	

Areas of Activity:

According to the law, the ministry sets measures for defending the human fundamental rights and liberties, as well as for defending the public and private property; according to its competence, it organizes and develops, through specialized structures, activities for preventing and countering terrorism, organized crime, illicit trafficking and consumption of drugs, trafficking in persons, illegal migration, computer crime, as well as other crimes and antisocial deeds; monitors the enforcement of provisions contained by the strategies and programs of reform and restructuring of the central and local public administration, elaborated on basis of the Governing Programme, in compliance with the European Union standards and the domestic legislation and it ensures the achieving of strategies and programs in its own activity field.

National Institute for Criminology	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: part of Ministry of Justice	
Weblink: http://www.criminologie.ro/	

Areas of Activity: The organization performs research activities related to crime inlcuding cyber crime.	
Ministry of Defence	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging and Current Risks, Development of Security Technology and Standards Policy	
Relationships:	
Weblink: http://www.mapn.ro/	
Areas of Activity: The Ministry of Defence is a specialized body of the central public administration submitted to the Government conducting national defence activities according to the stipulations of the law and to the strategy of national security, with a view to safeguarding national sovereignty, state independence and unity, territorial integrity and constitutional democracy.	
Romanian Intelligence Service (SRI)	
Type of Organisation: National Security Actor	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: Cooperates with other public institutions such as the Ministry of Defence, MIRA or SIE for matters of national security	
Weblink: http://www.sri.ro/	
Areas of Activity: The Romanian Intelligence Service is the official institution of Romania with competences in gathering and making the effective use of national security-related intelligence. The activities are carried out mainly on the national territory but also outside borders, in cooperation with other institutions with responsibilities in the field of monitoring and preventing cross-border threats.	
Foreign Intelligence Service (SIE)	
Type of Organisation: National Security Actor	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: The activity of the Foreign Intelligence Service is organized and coordinated by the Country's Supreme Defence Council (CSAT); Cooperates with other public institutions such as the Ministry of Defence, MIRA or SIE for matters of national security.	
Weblink: http://www.sie.ro/	

Areas of Activity:
Under the Law no. 1/1998, the Foreign Intelligence Service (SIE) is the state body specialized in foreign intelligence concerning the national security and the safeguarding of Romania and its interests..

Industry Organisations Active in Network and Information Security

ISACA Romania	
Type of Organisation: IT Association	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: none	
Weblink: http://www.isaca.ro/	
Areas of Activity: ISACA Romania is a Romanian chapter of ISACA International. The association builds knowledge and facilitates the CISA and CISM exams and certifications for IT security professionals.	

National Association of Romanian ISPs (ANISP)	
Type of Organisation: IT Association	Ownership: Public
ENISA Focus Points: Emerging and Current Risks, Development of Security Technology and Standards Policy	
Relationships: Cooperates with public and private authorities to build knowledge. Does lobbying for its members.	
Weblink: http://www.anisp.ro/	
Areas of Activity: ANISP does lobbying for the members and involves actively in legislative initiatives related to the communications market.	

Employers' Association of the Software Industry and Services (ANIS)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Cooperates with public and private authorities to build knowledge. Does lobbying for its members.	

Weblink: http://www.anis.ro/	
Areas of Activity: The Employers' Association of the Software and Services Industry – ANIS upholds the interests of Romanian software producers and services providers. The association was founded in 1998, and at present, counts more than 100 members, some of which are the foremost IT companies in the field. One of ANIS strategic objectives is to be involved in legislative issues impacting the IT sector, by collaborating in the process of elaborating and applying national IT policies, with main focus on software production and service providing.	
Association for IT&C (ATIC)	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: none	
Weblink: http://www.atic.org.ro/	
Areas of Activity: ATIC does lobbying for the members and involves actively in legislative initiatives that relate to the communications market. Build co-operation between members.	
Association of Telecommunications Operators	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness raising	
Relationships: none	
Weblink: http://www.aotr.ro/	
Areas of Activity: ATO does lobbying for the members and involves actively in legislative initiatives that relate to the communications market. Build co-operation between members.	
Association of Telecommunications Operators	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness Raising	
Relationships: none	
Weblink: http://www.aotr.ro/	

Areas of Activity: ATO does lobbying for the members and involves actively in legislative initiatives that relate to the communications market. Build co-operation between members.

Romanian Standards Association (ASRO)	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Cooperates with public authorities and private entities for standards development and certification.	
Weblink: http://www.asro.ro/	
Areas of Activity: ASRO is a non-lucrative association, a Romanian private legal entity of public interest, non governmental and apolitical, set up as a national standards body on basis of the Government Ordinance No.39/1998, Law 177/2005 and Law No.355/2002 and is recognized as a national standards body by the Government Decision 985/2004..	

Academic Organisations Active in Network and Information Security

National Communications Research Institute (INSCC)	
Type of Organisation: Research Centre	Ownership: Public
ENISA Focus Points: Resilience, Emerging and Current Risks	
Relationships: none	
Weblink: http://www.inscc.ro/	
Areas of Activity: National Communications Research Institute - INSCC Bucharest performs fundamental and applicative research, technological development, technical and economical studies. INSCC also carries out tests, measurements and trials, conformity assessment and certification of communications equipments and services.	

National Institute for Research and Development in Informatics (ICI)	
Type of Organisation: Research Centre	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: Cooperates with public and private authorities to build knowledge.	

Weblink: http://www.ici.ro/
Areas of Activity: ICI's mission is the development of the scientific and technological support in ITC, necessary for the achievement of the specific structures and services of the knowledge - based information society.

University of Bucharest	
Type of Organisation: Research Centre	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: Co-operates with the Ministry of Education and industry associations for building knowledge.	
Weblink: http://www.unibuc.ro/	
Areas of Activity: The Department of Technology is a partner of Cisco Academy. In cooperation with the University, the academy has introduced Cisco Courses within the Information Technology Faculty. The courses are dedicated to information technologies, network security, wireless LANs and other IT areas.	

Military Technical Academy	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy	
Relationships: none	
Weblink: http://www.mta.ro/	
Areas of Activity: The Academy organizes courses on information security.	

Other Bodies and Organisations Active in Network and Information Security

IT Security Incidents Reports and Expertise Center (CERIS)	
Type of Organisation: CERT	Ownership: public
ENISA Focus Points: CERT	
Relationships: Part of Ministry of Communications and Information Technology.	

Weblink: http://www.ceris.ro/
Areas of Activity: CERIS is the place where IT staff within public administration organizations can call for receiving guidance and solutions in IT security events they deal with. CERIS promotes the necessity of building the information security culture within public administration organizations.

CERT-RO	
Type of Organisation: CERT	Ownership: public
ENISA Focus Points: CERT, Resilience, Awareness Raising, Emerging and Current Risks	
Relationships: CERT is subordinated to the Ministry of IT&C and was founded temporarily as a department of ICI (National Institute of Research and Development in Informatics).	
Weblink: http://www.cert-ro.eu	
Areas of Activity: The CERT-RO offers an information exchange frame for IT specialists responsible of the IT security of all kinds of organizations, including government institutions and enterprise.	

Activities

Strategic Initiatives

Knowledge Based Economy
Type of Activity: Government Funding Program
Responsible Organisation(s): Ministry of IT&C (MCTI)
ENISA Focus Points: Implementation of Security Technology and Standards
Weblink:
Description: In the next years, approximately 200 communities will benefit from Local Communities Electronic Networks (LCEN), as knowledge centres for offering citizens information and online services throughout the Knowledge Economy Project. The project was initiated by the Romanian government, with the support of World Bank and coordinated by Ministry of Communication and Information Technology.

AXA III, IT&C Structural funds for public and private sectors
Type of Activity: Government Funding Program
Responsible Organisation(s): Ministry of IT&C (MCTI)
ENISA Focus Points: Micro- enterprises
Weblink:
Description: The project has three main focus points: increasing the role of IT&C usage, development and increasing efficiency of modern electronic communications and development of e-Economy. These focus points mainly refer to increasing broadband penetration for SMEs, Education and Public Administration, support for e-Health development including hardware, software and broadband, broader usage of e-Learning systems, ERP and CRM acquisition, increasing usage and administration of databases.
CERT
Type of Activity: Governmental Policy
Responsible Organisation(s): Ministry of IT&C (MCTI)
ENISA Focus Points: CERT
Weblink:
Description: At this stage, CERT RO is still a department of the National Institute for Research and Development in Informatics.
WiMAX
Type of Activity: Governmental Policy
Responsible Organisation(s): Ministry of IT&C (MCTI)
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy
Weblink:
Description: WiMAX is a project started back in 2006, but still no licenses were issued yet.
Safer Internet Plus
Type of Activity: Governmental Funding Program

Responsible Organisation(s): Ministry of IT&C (MCTI)
ENISA Focus Points: Awareness Raising, Emerging and Current Risks
Weblink:
Description: Safer Internet Plus program aims at promoting safer use of the Internet and new online technologies, particularly for children and teenagers, and to fight against illegal content and content unwanted by the end-user. This program funds projects that are specially targeted towards parents, educators, and children with a view to raise awareness on the risks involved by the Internet use and to depict harmful content.
ICT-PSP
Type of Activity: Governmental Funding Program
Responsible Organisation(s): Ministry of IT&C (MCTI)
ENISA Focus Points: Micro- enterprises
Weblink:
Description: The program will be focused on e-Government, e-Inclusion and e-Heath as well as on data protection and sustained IMM sector growth.

Events

Conference and Workshops	
International Security Expert Conference	
Responsible Organisation: Provision	Frequency: annual
ENISA Focus Points: Resilience, Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: SMEs, Large Enterprises, Government Organizations	
Weblink: http://www.isec.ro/	

Description:
The International Security Expert Conference is annual security conference organized by provision with international audience and speakers. Provision is confirming through this event its commitment in raising awareness on security issues, promoting cross-national and cross-sector collaboration, identifying industry trends and highlighting information security best practices and experiences. Further, this event will reunite specialists involved in fighting against cyber-crime and cyber-terrorism, securing critical infrastructures and setting up global institutions to address security incidents.

Media Campaign	
Safer Internet Day	
Responsible Organisation: Ministry of IT&C (MCTI)	Frequency: annual
ENISA Focus Points: Emerging and Current Risks	
Target Groups: Consumers / Citizens	
Weblink: http://www.sid2008.sigur.info/	
Description: The contest was organized in January for K-12, with the prime focus to determine the main advantages and risks related to the virtual world.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen

disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Romania.

Country Report – Slovakia

Country General Information

Source: European Commission

Political system:	Republic
Capital city:	Bratislava
Total area:	49 000 sq.km
Population:	5.4 million
Official language:	Slovak
Time zone:	CET (GMT+1)
Currency:	Slovak koruna (SKK) – Euro (EUR) from 1.1.2009

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Slovakia, we present a set of three indicators in the Country Highlights section.

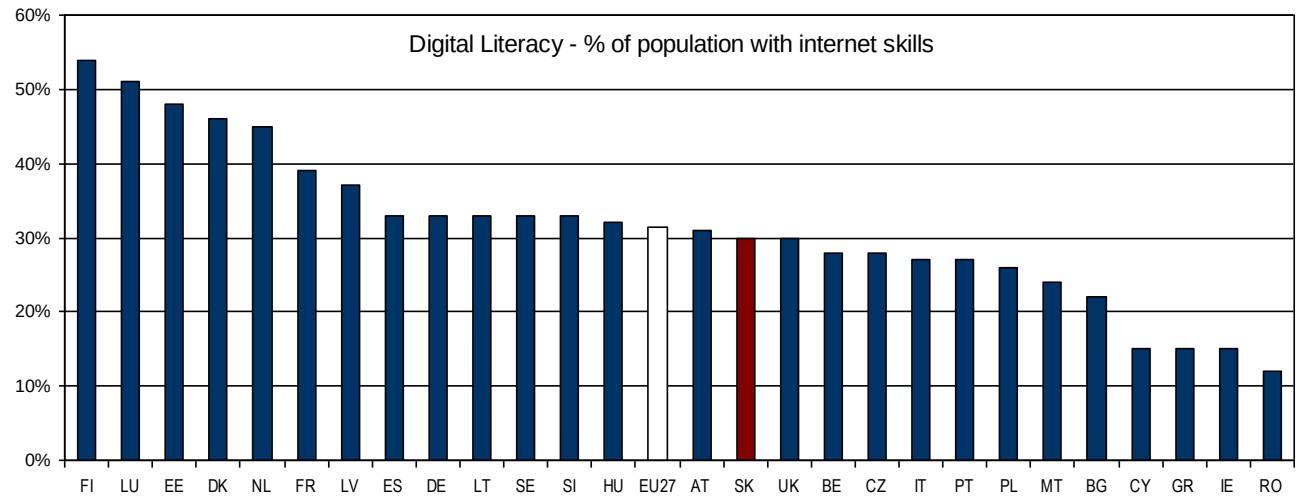
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Slovakia is fundamental to this NIS study.

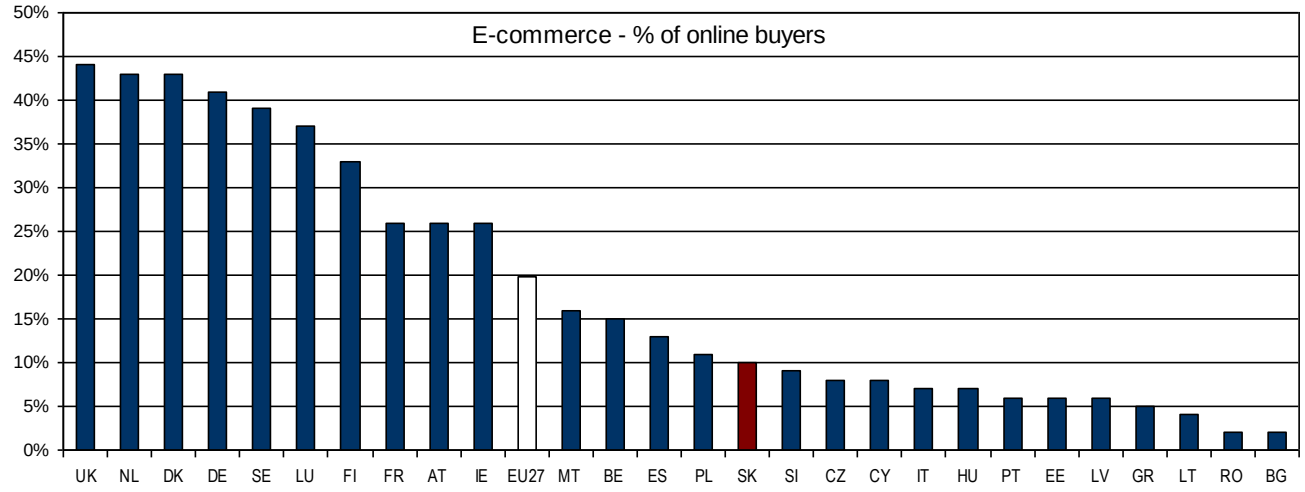
The development of the information society in Slovakia is currently doing well, the situation may improve further with particularly strong progress in eGovernment, a rapid adoption of broadband by Internet users, and a business environment relatively favorable to ICT investment, which can rely particularly on a good eSkill base.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

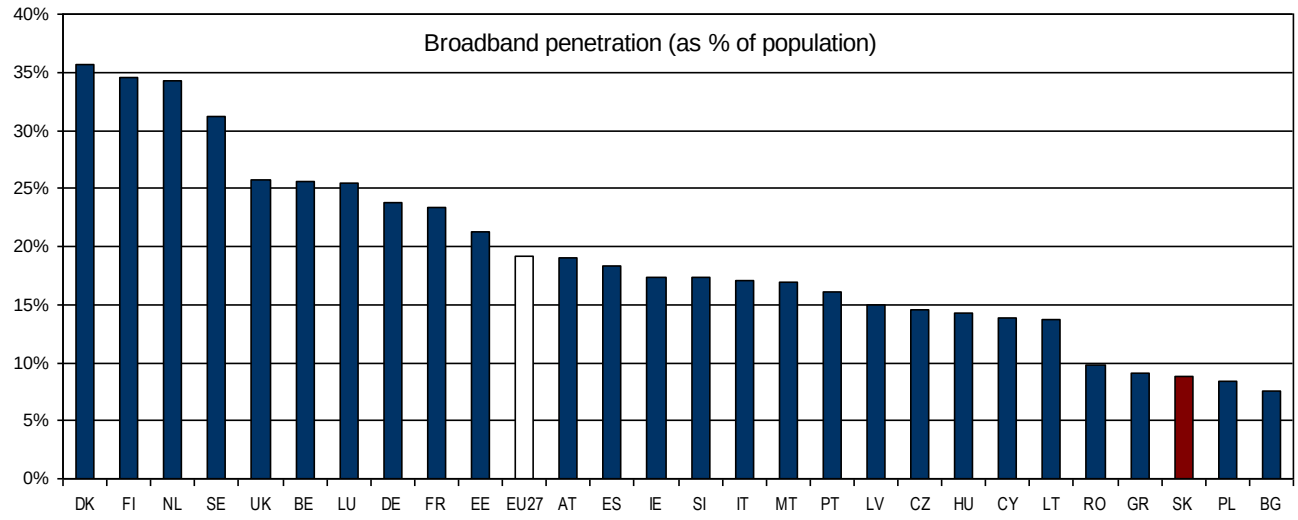
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

The National Security Authority, an independent government body, is recognized among NIS stakeholders in the Slovak Republic as the national security agency responsible for the area of classified information.

The Commission for Information Security under the Ministry of Finance, together with Slovak government, acts as national decision-making authorities in developing the information security policy in the Slovak Republic. The Commission is a working group consisting of employees of Ministry of Finance, national network and information security stakeholders (such as other ministries) and external experts in the field of information security. The Ministry of Finance oversees all execution concerning methodical and legislative activities connected to information society and information security issues at the national level as well as is responsible for implementation of all above mentioned.

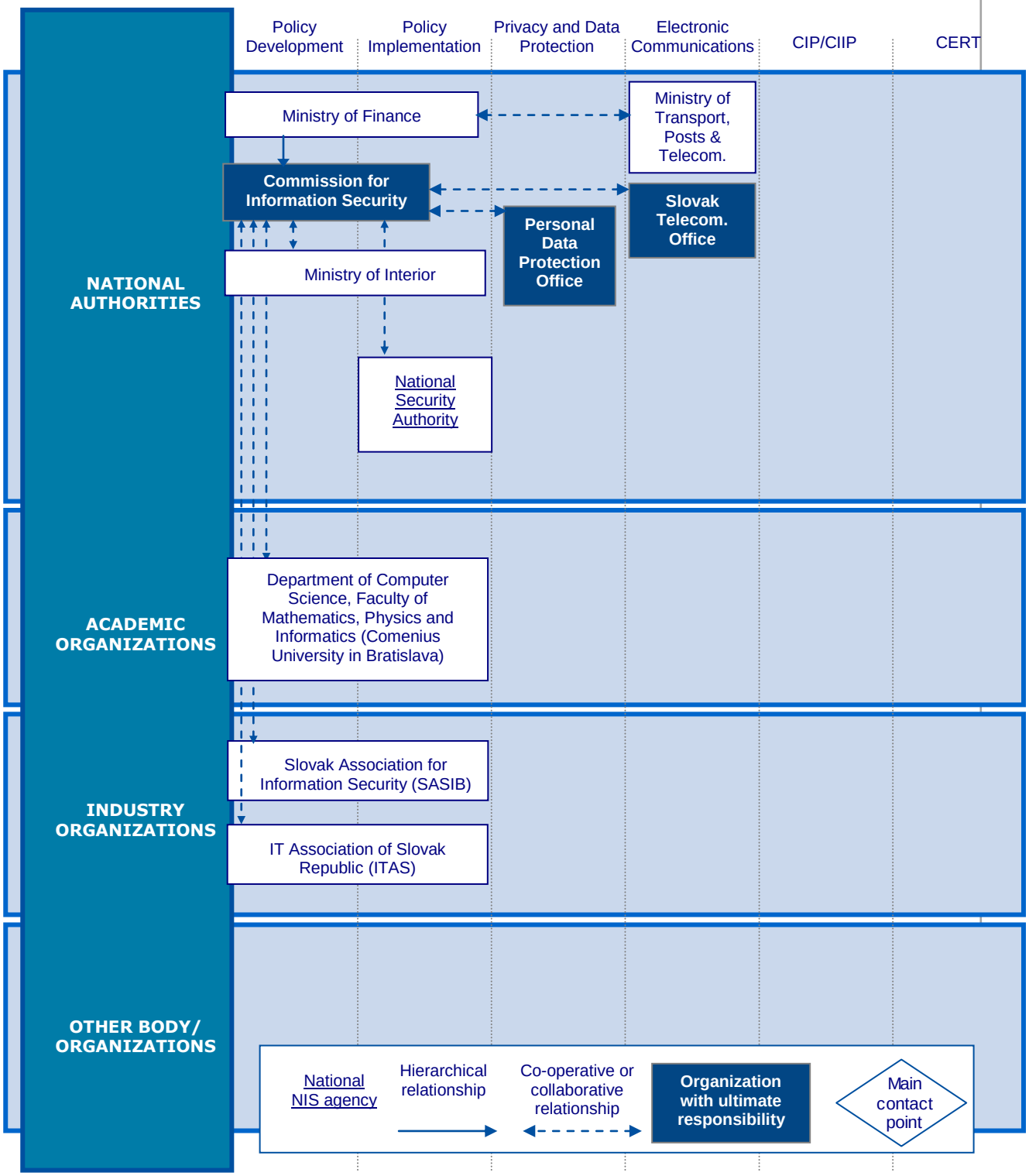
The Slovak Republic is committed to data protection and ensuring compliance in this regard. Personal Data Protection Office is an independent oversight body responsible for this task. The Office is also charged with maintaining a register of databases; investigating complaints; imposing fines for violations; conducting audits and providing consultations on data protection; and commenting on legislative proposals.

The Slovak Republic does not have security response teams yet. Currently, the Commission for Information Security is working on conditions under which a CERT will operate and legal aspects of creating a national CERT in April 2009 the latest.

The National strategy of information security has been approved recently in Slovakia; strategy for protection of cyberspace and critical infrastructure is in the conceptual phase. The country hosts a number of conferences on NIS - events organized prevalently by industry professional and associations.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Slovakia. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Finance (Department for Information Society)			X			X	X	X
Commission for Information Security (Ministry of Finance)		X	X	X			X	X
Personal Data Protection Office							X	X
Slovak Telecommunication Office		X					X	X
National Security Authority							X	X

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in the Slovak Republic:

National Authorities in Network and Information Security	
Ministry of Finance – Department for Information Society	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness Raising, Development and Implementation of Security Technology and Standards Policy	
Relationships: co-operates with all key stakeholders	
Weblink: http://www.finance.gov.sk/Default.aspx?CatID=5797&ContentID=2285%22%20target=_self http://www.informatizacia.sk/	
Areas of Activity: The Ministry of Finance is responsible for information society governance, development of the standards and recommendations for area of information society and security of information and public infrastructure. The ministry acts also in the area of non-classified information. The Department for Information Society consists of the following divisions: For information society strategy and international cooperation; For legislation, methods, standards and information system security; For public administration informatization; For managing Operational program of information society; and For implementation of Operational program of information society.	
Commission for Information Security	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness raising, Emerging and Current Risks, Development and Implementation of Security Technology and Standards Policy	
Relationships: part of Ministry of Interior, members are representatives of all key NIS stakeholders	
Weblink: http://www.finance.gov.sk/Default.aspx?CatID=5797&ContentID=2285%22%20target=_self http://www.informatizacia.sk/vdok_simple-zoznam-clenov-komisie-pre-ib/616s3247c	

Areas of Activity:

The commission is a working group consisting of employees of Ministry of Finance and external experts in the field of information security. It prepares expert proposals and standpoints in the field of protection and security of government and public administration information systems. Its scope includes security standards, relevant legislation and appointment of specific working groups. Its scope of activity includes: Evaluation of proposed security standards for protection and security of public administration information systems in the scope of non-classified information, proposals of security standards, change or modification of existing security standards for security of public administration information systems, presentation of expert opinion concerning norms and legislation related to NIS, and appointing working groups so that the NIS-related tasks could be carried out.

The members of the commission recruit from Ministry of Finance, Ministry of the Interior, National Security Authority, Slovak Association for Information Security, Slovak National Accreditation Service, Office for Personal Data Protection, Government Office of Slovak Republic, Department of Computer Science, Faculty of Mathematics, Physics and Informatics (Comenius University in Bratislava), IT Association of Slovak Republic (ITAS), and independent expert.

National Security Authority	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	
Relationships: co-operates closely with Ministry of Finance and other key stakeholders	
Weblink: http://www.nbusr.sk/	

Areas of Activity:

The National Security Authority is responsible for the protection of classified information. It provides support in domain of information security and information systems certification, crypto – security and crypto - certification, personal security, R&D, and administrative security for the Slovak Republic. Electronic signature scheme root certification authority for Slovakia.

Ministry of Transport, Posts, and Telecommunications	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: co-operates with Ministry of Finance, and Telecommunication Office	
Weblink: http://www.mpo.cz/en/e-comm-and-post/default.html	

Areas of Activity: The Ministry of Transport, Posts, and Telecommunications is primarily responsible for coordination and fulfilment of national policy for electronic communications. The main tasks include: the Ministry elaborates necessary documents related to electronic communications, prepares and coordinates research activities in the electronic communication sector, cooperates on development strategy of new electronic communication services, and works with the Telecommunication Office on implementation of electronic communication policy.

Ministry of Interior - Department of Crisis Management and Civil Protection	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, e-ID	
Relationships: co-operates with all key stakeholders	
Weblink: http://www.minv.sk/?ochrana-kritickej-infrastruktury, www.minv.sk	
Areas of Activity: The Ministry of Interior coordinates the activities related to development of information systems for public administration, creates conditions for information systems securization, manages and coordinates the tasks connected to integrated rescue system, and cooperates with public institutions on development of automated support systems.	

Slovak Telecommunication Office	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: cooperates with National Security Authority, Ministry of the Interior, Ministry of Finance and others if required.	
Weblink: http://www.teleoff.gov.sk/en/	
Areas of Activity: The main activities of the office comprise carrying out state regulation of electronic communication, managing the frequency spectrum, maintaining international relations with regulatory authorities in the area of electronic communications, cooperating with the Council for Broadcasting and Retransmission, exercising state supervision, and imposing sanctions in the electronic communications field.	

Personal Data Protection Office	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development and Implementation of Security Technology and Standards Policy	

Relationships: cooperates with all key NIS stakeholders if required.
Weblink: http://www.dataprotection.gov.sk/buxusnew/generate_page.php?page_id=93
Areas of Activity: The Personal Data Protection Office as a state body participates in protection of fundamental rights and freedoms of persons in the course of processing their personal data. The Office performs its tasks and duties indecently and in course of the law. Its tasks include: continuous inspection of the state of personal data protection, recommendations for the measures of personal data protection in the filing systems, issuing a binding decision in the case of doubts, provides inspection of the processing of personal data in the filing systems, imposes sanctions in the case of a breach, executes registration of filing systems and provide access to the registration, issues generally binding legal regulations within the scope of its power, and gives opinions on draft laws and other generally binding legal regulations, which regulate processing of personal data.

Industry Organisations Active in Network and Information Security

IT Association Slovakia (ITAS)

Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: Resilience, AR, Implementation of Security Technology and Standards	
Relationships: cooperates with the government	
Weblink: http://www.itas.sk/	
Areas of Activity: IT Association Slovakia (ITAS) is a professional association representing the most significant local and international companies operating in the Slovak market in the field of information and communication technologies (ICT). ITAS was founded in September 1999 and presently incorporates 65 professionally registered members. The stated mission of the ITAS is to promote and develop an information society. NIS aspect: the members of ITAS include IT vendors specializing in network and information security that contribute to primary ITAS functions that include: to actively encourage the creation of a developing information society, to participate in any new legislation which may impact on ICT, to support the competitiveness of Slovak ICT companies in international markets, to demonstrate the potential and possibilities of ICT for the efficient growth of the public and private sectors, and to promote the interests of the ICT sector. ITAS is a member of the EU association EICTA and cooperates with the Association for an Information Society (SPIS), Czech Republic.	

Slovak Association for Information Security (SASIB)

Type of Organisation: IT Association	Ownership: Private

ENISA Focus Points: CERT, AR, Emerging and Current Risks, Micro-enterprises, Development and Implementation of Security Technology and Standards Policy	
Relationships: none	
Weblink: http://www.sasib.sk/	
Areas of Activity: The goal of the organization is to increase knowledge and awareness of security legislation and expert knowledge of its members in the domain of professionals and public in information security and software protection. SASIB supports the NIS research activities of government and public administration, and prepares recommendation in the field of NIS and cyber-criminality.	
ISACA Slovakia	
Type of Organisation: IT Association	Ownership: Private
ENISA Focus Points: AR, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.isaca.sk/	
Areas of Activity: ISACA Slovakia was founded in 1999 and cooperates closely with the international association ISACA. Is supports its members (currently around 50 security professionals) and promotes consistent approach to information system and security audit and control in line with international standards. The members operate as auditors and security specialists.	

Academic Organisations Active in Network and Information Security

Faculty of Mathematics, Physics and Informatics (Comenius University), Department of Computer Science	
Type of Organisation: Academic Organization	Ownership: Public
ENISA Focus Points: AR	
Relationships: Commission for Information Security (Ministry of Finance), other academic institutions	
Weblink: http://www.dcs.fmph.uniba.sk/english/index.html	

Areas of Activity:

The department, established in 1974, continues to be responsible for organizing the major part of the undergraduate and graduate computer science education to this date. The distinguishing feature is a balanced coverage of the mathematical foundations, theoretical computer science, and practical computer science. The faculty covers courses on computer architecture, system software, networks, databases, software design, design and analysis of algorithms, formal languages, computational complexity, discrete mathematics, cryptology, data security and others. NIS related courses: Cryptography.

A faculty professor is a member of the Commission for Information Security that acts as an expert group in developing national security policy and security standards for public information systems.

Faculty of Electrical Engineering and Information Technology (Slovak University of Technology)

Type of Organisation: Academic Organization	Ownership: Public

ENISA Focus Points: AR

Relationships: other academic institutions

Weblink: http://www.fei.stuba.sk/generate_page.php?page_id=793

Areas of Activity:

The faculty is one of the most successful, largest and the most experienced (opened in 1941) technical faculty aimed at electrical engineering, information and communication technologies in Slovakia. In the NIS area it cooperates closely with security professionals in the project based education form. NIS with related courses: Cryptography in communication networks, Information security, Classical cryptography.

Activities

Strategic Initiatives

National Strategy for Information Security

Type of Activity: Strategic initiative – Government policy

Responsible Organisation(s): Ministry of Finance and Slovak Government

ENISA Focus Points: Resilience, Emerging and Current Risks, Security Technology and Standards Policy

Weblink: http://www.rokovania.sk/appl/material.nsf/0/D407B2290ECCC4C8C12574A400441715?OpenDocument

Description: National Strategy for Information Security is the main document covering all aspects of information security policy at the national level. The strategy aims to influence positively business environment in Slovakia through enhanced data integrity, increased authority, goodwill and transparency of all institutions and organizations. The strategy is set through 2008-2013.
Kry sa!
Type of Activity: Governmental Funding Programme
Responsible Organisation(s): Ministry of Transport, Posts, and Telecommunications and ITAS
ENISA Focus Points: AR, Emerging and Current Risks, Security Technology and Standards Policy
Weblink: http://www.kry-sa.sk
Description: The project aims at rising awareness of internet users about the security risks connected with internet usage, internet banking and PC usage in general. Project lasted three months in the form of publishing technical/scientific articles, interviewing security professionals and discussions. The project continues through maintaining website providing online advice.
Strategy for Protection of Cyberspace and of Critical Infrastructure
Type of Activity: Strategic initiative – Government policy
Responsible Organisation(s): Ministry of Finance and Slovak Government
ENISA Focus Points: Resilience, Emerging and Current Risks, Security Technology and Standards Policy
Weblink:
Description: This government strategic initiative is currently in working process – not officially approved yet. At this stage the involved stakeholders are working on the conceptual aspects of the strategy.

Events

Conference and Workshops

Information Security	
Responsible Organisation: SASIB & Eset	Frequency: annual
ENISA Focus Points: AR, Emerging and Current Risks	
Target Groups: Security Professionals, Large Enterprises, Government Institutions, Educational and Research Organizations	
Weblink: http://www.eset.cz/konferencia-informacna-bezpecnost-2008	
Description: The conference started three years ago in a form of a seminar and gradually developed to a conference; last year still being a local event, international participation is expected next year. The topics included news from security happenings: Security standards, security software, recent threats, public network security, and the role of state in information security policy.	

ITAPA	
Responsible Organisation: APPEL together with all major IT players in the country, government and IT associations	Frequency: annual
ENISA Focus Points: AR, Emerging and Current Risks	
Target Groups: Government Institutions, Large Enterprises, Educational and Research Organizations	
Weblink: http://www.itapa.sk/index.php?ID=5188	
ITAPA congress aims to help speeding up the information society development in public administration actively, mainly by: Increasing demand for information society development in public administration; creating space where representatives of politics, public administration, academic field and commercial subjects meet and exchange their knowledge; Presenting various solutions related information technologies; Awarding and supporting the best-of-breed solutions related to public administration's processes.	

SOFT-TRONIK Security Day	
Responsible Organisation: SOFT-TRONIK	Frequency: annual
ENISA Focus Points: AR, Emerging and Current Risks	
Target Groups: Large Enterprises, Security Professionals; SMEs, Government Institutions	
Weblink: http://www.soft-tronik.cz/web/infobaze.nsf/0/85FAF70D872E22FFC1257441004C3DC6	

Description: Introduction of available security solutions; discussion among security professionals.	
IDC IT Security Roadshow	
Responsible Organisation: IDC CEMA	Frequency: semi-annual
ENISA Focus Points: AR, Emerging and Current Risks	
Target Groups: Large Enterprises, Security professional, Government Institutions;	
Weblink: http://www.idc-cema.com/?showproduct=34368	
Description: IDC's IT Security Roadshow has become the seminal annual event for CIOs and IT managers looking for the latest information on IT security trends and wanting to meet IT security gurus and industry professionals.	
ABIT (Audit and Security in IT)	
Responsible Organisation: University of Defence	Frequency: biennial
ENISA Focus Points: AR, Emerging and Current Risks	
Target Groups: Large Enterprises, Government Institutions, Educational and Research Organizations, Security Professionals, SMEs	
Weblink: http://www.isaca.sk/index.php?option=com_content&task=blogcategory&id=23&Itemid=86	
ABIT is a professional event with an independent program. The aim of the conference is to facilitate the discussion among experts and professionals. The topic of ABIT 2007 was Euro conversion from the point of view of IT governance including topics on security aspects of Euro conversion.	

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

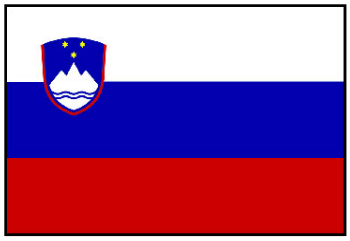
For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Slovakia.

Country Report – Slovenia

Country General Information



Source: European Commission

Political system:	Republic
Capital city:	Ljubljana
Total area:	20 000 sq.km
Population:	2 million
Official language:	Slovenian
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Slovenia, we present a set of three indicators in the Country Highlights section.

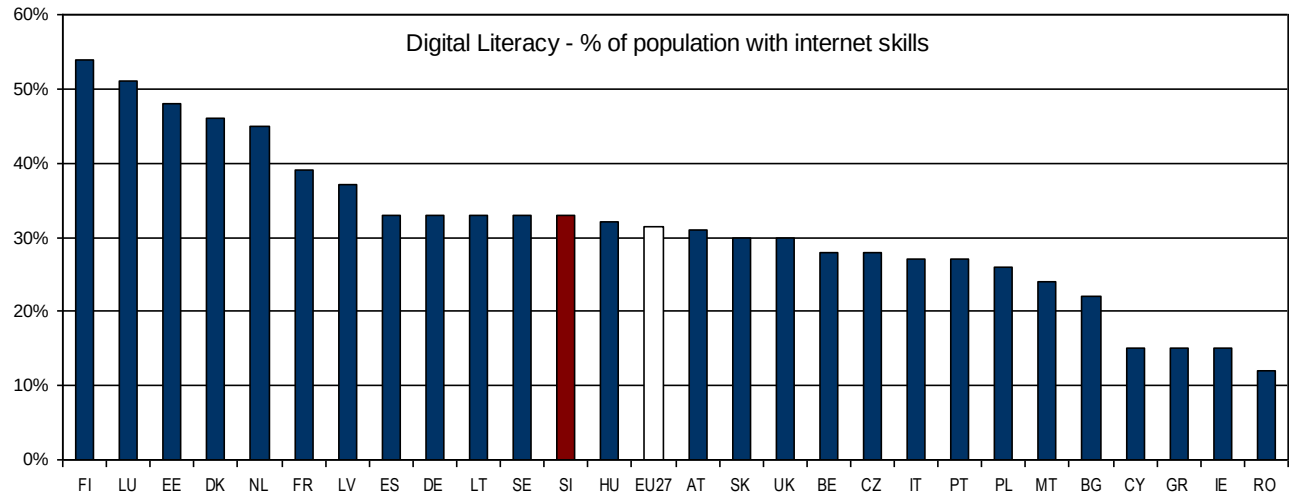
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Slovenia is fundamental to this NIS study.

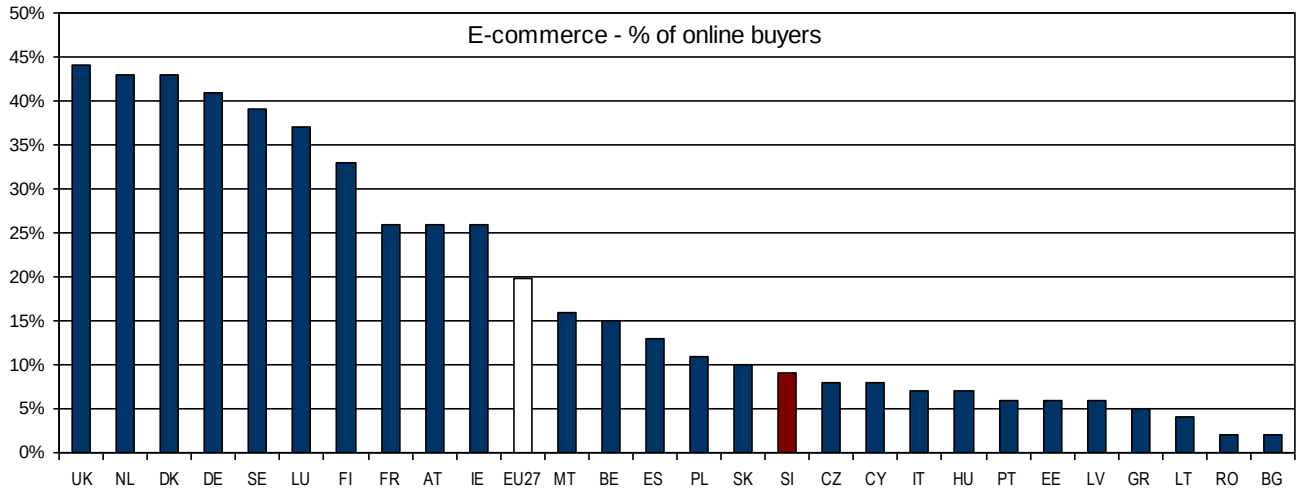
The development of the information society is well advanced in Slovenia. ICT investments have grown significantly in the last three years, both in private and public sector. This resulted in high availability of e-government services as well as business services.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

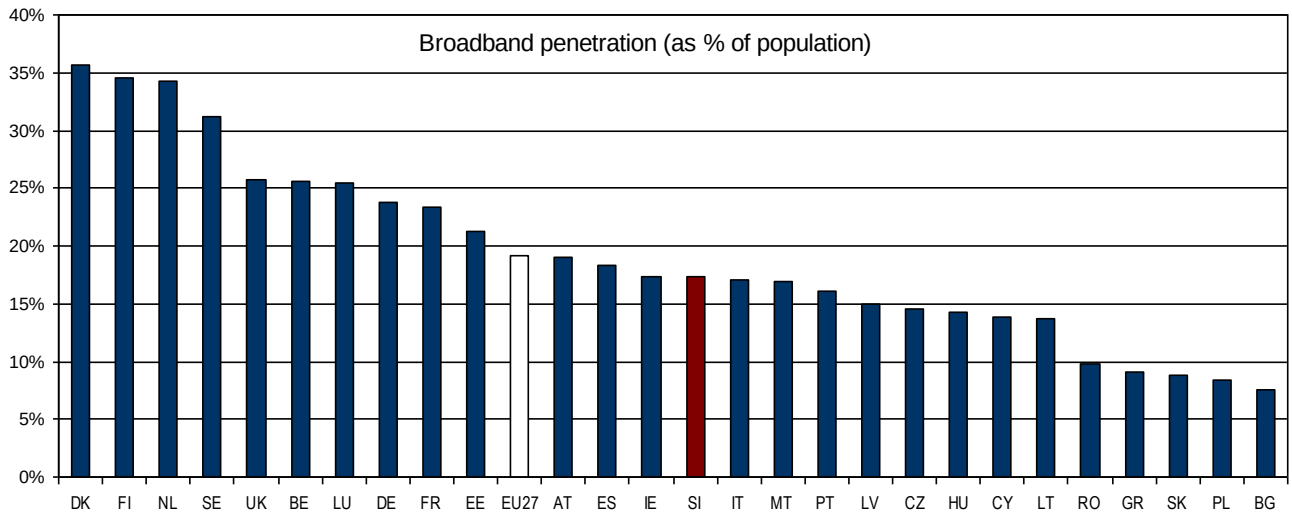
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

Slovenia does not have a single institution recognized among NIS stakeholders as the national security agency; there are various organizations sharing the responsibilities and competencies concerning the non-classified and classified information. The Government Office for the Protection of Classified Information is one of them and is responsible for monitoring the situation in the field of classification and protection of information and for

ensuring the development and implementation of physical, organizational and technical standards of classified information protection in government agencies, local community agencies, holders of public authorizations and those commercial organizations that obtain or have at their disposal classified information.

The Ministry of Higher Education, Science and Technology, through its Directorate for the Information Society, coordinates the development and implementations activities and programs in the field of the information society at the national level, which includes aspects relating to information security.

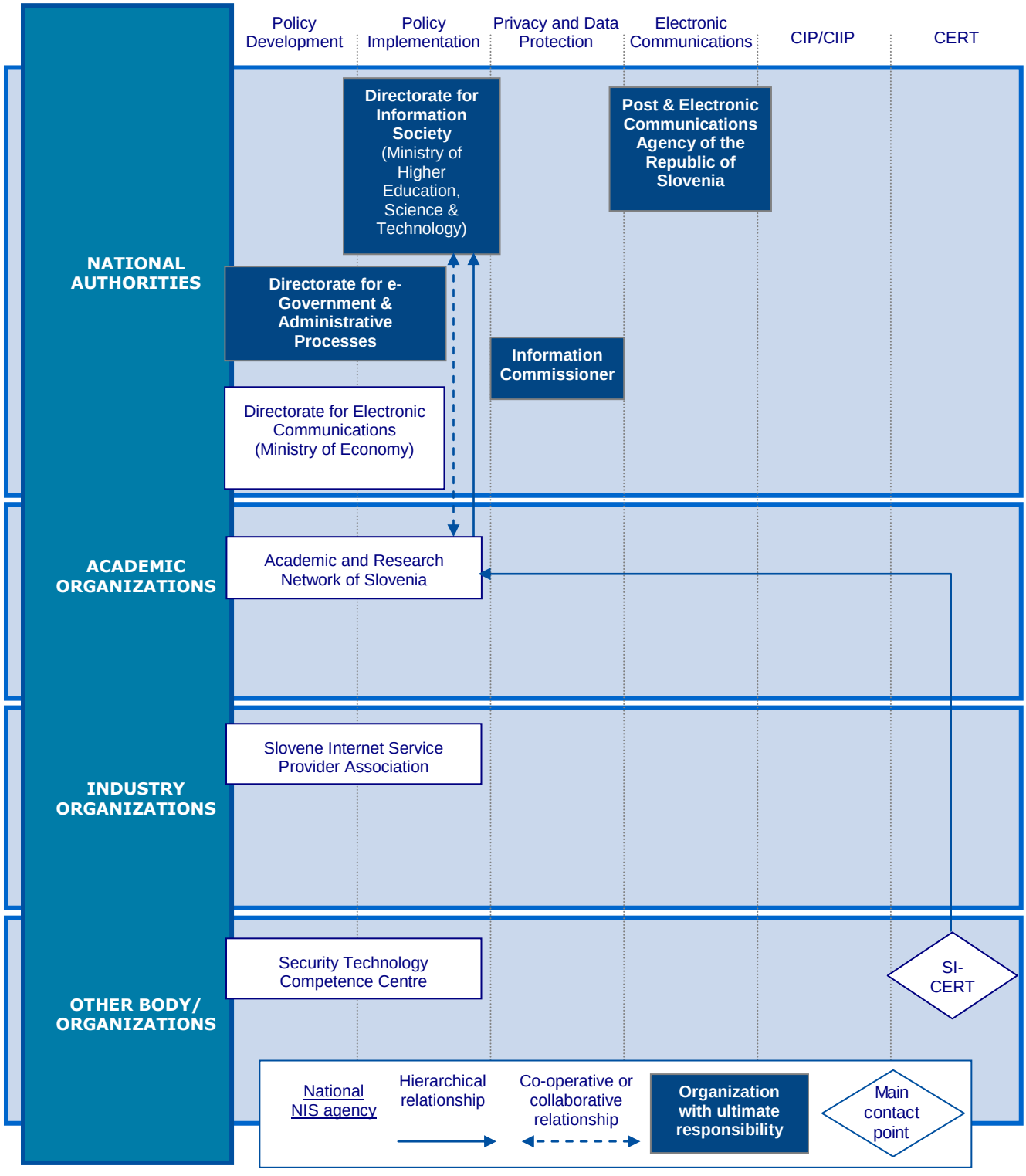
Slovenia is committed to data protection and ensuring compliance in this regard. The Information Commissioner is an autonomous and independent body responsible for this task. The Commissioner is in charge of supervision of both the protection of personal data, as well as access to public information. The tasks may include maintaining a register of databases, investigating complaints, imposing fines for violations, conducting audits and providing consultations on data protection, and commenting on legislative proposals.

Additionally, Slovenia has security response teams in place to handle security breaches and other incidents. SI-CERT is a service offered by ARNES (Academic and Research Network of Slovenia) and is extended to all computer networks in Slovenia, both academic and commercial. SI-CERT's main services include coordination of security incidents involving networks or systems in Slovenia, distribution of security-related information to the constituency, and providing technical expertise on network security related issues.

There are a number of projects currently underway in the country, many of which are closely connected to network infrastructure security. The country hosts a number of conferences on NIS. Main NIS stakeholders are prevalently organizing these events.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Slovenia. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Directorate for Information Society							X	X
Information Commissioner			X					
Post and Electronic Communications Agency of the Republic of Slovenia		X	X					
Directorate for e-Government and Administrative Processes						X		
SI-CERT	X							
Directorate for Electronic Communications							X	X
Office for the Protection of Classified Information				X			X	X
Academic and Research Network of Slovenia		X	X	X				

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Slovenia:

National Authorities in Network and Information Security

Ministry of Higher Education, Science and Technology, Directorate for Information Society

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards Policy	
Relationships: part of Ministry of Higher Education, Science and Technology; cooperates with ARNES	
Weblink: http://www.mvzt.si/index.php?id=249&L=1#c3998	

Areas of Activity:

The Directorate for the Information Society co-ordinates the implementation of the programme in the field of the information society. Accelerated development of the information society will have a significant impact on the competitiveness of the Slovenian economy and society, number of work places with high added value, quality of life and balanced regional development. In line with its mission to set up an inclusive information society that will integrate the potential and knowledge of the Information Communications Technologies into accelerated development of the Slovenian society as a whole, this Directorate dedicates an essential part of its activity to fostering the development of the information society and co-ordination of activities in this field.

Ministry of Economy, Directorate for Electronic Communications

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: part of Ministry of Economy	
Weblink: http://www.mvzt.si/index.php?id=249&L=1#c3998	

Areas of Activity:

The Electronic Communications Directorate is responsible for drafting modern legislation in the area of postal services, electronic communications and electronic commerce, it monitors the situation on markets, and, by applying strategies, policies and concrete measures, is responsible for establishing conditions for the approximation to the developed European countries in the area of postal services, electronic communications, electronic commerce operations in the market, and other information and communication technologies.

Ministry of Public Administration, Directorate for e-Government and Administrative Processes	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: part of Ministry of Public Administration	
Weblink: http://www.mju.gov.si/index.php?id=132	
Areas of Activity: The Directorate for e-government and administrative processes has the following tasks: to reform processes and rapidly develop e-government in order to bring services closer to citizens and corporate entities; to improve electronic support to relations among public administration subjects and beyond with the introduction of up-to-date information and communication technology; to ensure interconnection of public records and integration of databases with information support to processes; to keep up-to-date with information infrastructure developments worldwide and to prepare policy guidelines and standards for public administration; to reduce administrative burdens; to monitor the implementation of regulations governing the general administrative procedure, the administrative operation and the access to information of public character; to exercise administrative control; to co-ordinate the guidance of local administrative units; to prepare invitations to public tenders for the award of information infrastructure contracts; and to co-operate with non-governmental organisations.	

Information Commissioner	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: None	
Weblink: http://www.ip-rs.si/?id=195	
Areas of Activity: Information Commissioner is an autonomous and independent body, established in December 2005. The body supervises both the protection of personal data, as well as access to public information. The competencies of the Information Commissioner are: deciding on the appeal against the decision with which a body refused or dismissed the applicant's request for access or violated the right to access or re-use of public information in some other way, and within the frame of appellate proceedings also for supervision over implementation of the Act regulating the access to public information and regulations adopted hereunder; inspection supervision over implementation of the Act and other regulations, governing protection or processing of personal data or the transfer of personal data from Slovenia, as well as carrying out other duties, defined by these regulations; deciding on the appeal of an individual when the data controller refuses his request for data, extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the Act governing personal data protection.	

Post and Electronic Communications Agency of the Republic of Slovenia (APEK)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness Raising	
Relationships: None	
Weblink: http://www.apek.si	
Areas of Activity: The mission of the Post and Electronic Communications Agency of the Republic of Slovenia is to regulate the electronic communications and postal market in order to ensure competitiveness and thus make it possible to choose high-quality, modern and affordable services and a variety of radio and television programmes.	

Office for the Protection of Classified Information (NSA)	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Emerging and Current Risks, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards Policy	
Relationships: part of Government Office	
Weblink: http://www.uvtp.gov.si/en/	
Areas of Activity: The Government Office for the Protection of Classified Information shall perform the following tasks: To monitor the situation in the field of classification and protection of information and ensure the development and implementation of physical, organisational and technical standards of classified information protection in government agencies, local community agencies, holders of public authorisations and those commercial companies and organisations that obtain or have at their disposal classified information; to attend to the implementation of the accepted international obligations and international treaties on the protection of classified information, and cooperate in this field with the corresponding agencies of foreign countries and international organisations.	

Slovenian Governmental Certification Authority (SIGOV-CA)	
Type of Organisation: Public Network & Information Security Body	Ownership: Public
ENISA Focus Points: e-ID	
Relationships: part of Ministry of Public Administration	
Weblink: http://www.sigov-ca.gov.si/index-en.htm	

Areas of Activity: The organization issues qualified digital certificates for employees and servers of public administration institutions. Functioning as a part of the Slovenian Governmental Certification Authority at the Ministry of Public Administration. The Slovenian Time Stamping Authority issues trusted time stamps for applications of public administration institutions and functions as a part of the Slovenian Governmental Certification Authority at the Ministry of Public Administration.

Slovenian General Certification Authority (SIGEN-CA)	
Type of Organisation: Public Network & Information Security Body	Ownership: Public
ENISA Focus Points: e-ID	
Relationships: part of Ministry of Public Administration	
Weblink: http://www.sigen-ca.si/eng/eng-index.php	
Areas of Activity: The institution issues qualified digital certificates for citizens and for legal and natural persons, registered for performing activities. Functioning as a part of the Slovenian Governmental Certification Authority at the Ministry of Public Administration.	

Industry Organisations Active in Network and Information Security

Slovene Internet Service Provider Association (SISPA)	
Type of Organisation: IT Association	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: co-operates with the National Authorities	
Weblink: http://www.sispa.org	
Areas of Activity: The ultimate goal of the association is to support quick development of the Slovenian information society by means of the active and innovative use of the Internet.	

Chamber of Commerce and Industry (GZS) / Association of Informatics and Telecommunications (ZIT)	
Type of Organisation: IT Association	Ownership: Public
ENISA Focus Points: Awareness Raising	

Relationships: None
Weblink: http://www.gzs.si/slo/panoge/zdruzenje_za_informatiko_in_telekomunikacije
Areas of Activity: The basic tasks of the Association include: To promote interests of the members in Slovenia and abroad; communicate with government bodies, local partners and international organizations; provide technical assistance to members in the form of information, advice and training; develop business opportunities with end-user and public organizations, promote the development of the information society in the country.

Academic Organisations Active in Network and Information Security

Academic and Research Network of Slovenia (ARNES)

Type of Organisation: Research Centre	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness Raising, Emerging and Current Risks	
Relationships: Reports to Ministry of Higher Education, Science and Technology, Directorate of Information Society;	
Weblink: http://www.arnes.si/english/	
Areas of Activity: The Academic and Research Network of Slovenia (ARNES) is a public institute, which provides network services for research, educational and cultural organizations and enables them to connect and cooperate with each other and with related organizations abroad. ARNES builds, maintains and manages infrastructure which links universities, institutes, research laboratories, museums, schools, databases and digital libraries. It offers its users the same services as the national academic networks in other countries with which it cooperates in European Commission projects in testing, development and the introduction of new Internet protocols and services. It also performs services which are not offered by commercial organizations but which are preconditions for the operation of the Internet in Slovenia.	

University of Ljubljana, Faculty of Social Sciences

Type of Organisation: University	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: University of Ljubljana	
Weblink: http://www.ris.org/	

Areas of Activity: Faculty of Social Sciences and ARNES are running the Slovenian awareness node SAFE.SI, financed through Safer Internet Plus programme. The organizations also analyzes social aspects of the Internet usage in Slovenia.	
Institute of Informatics, Faculty of Electrical Engineering and Computer Science	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Emerging and Current Risks, Development of Security Technology and Standards Policy	
Relationships: None	
Weblink: http://lisa.uni-mb.si/index_ang.htm	
Areas of Activity: The members of the institute are involved in many international projects, where the research topics of software process quality assurance, application of multimedia technologies and defining efficient approaches to component based development of information systems are actively discussed and developed. The institution accommodates Information Systems Laboratory, Database Technology Laboratory, Computer Mediated Communication Laboratory, and Real-time Systems Laboratory.	
Faculty of Criminal Justice and Security, University of Maribor	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: None	
Weblink: http://www.fvv.uni-mb.si/defaultEng.htm	
Areas of Activity: The Faculty organizes a number of courses focused on information security, legal aspects of information security, security systems and ethics and human rights. The Faculty also organizes events on information security, for example a meeting "Private policing and security - Relationships between the private and public sectors" held in December 2008.	
Faculty of Computer and Information Science, University of Ljubljana, Laboratory for System Research and Information Technologies	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: None	

Weblink: http://www.fri.uni-lj.si/en/
Areas of Activity: The Faculty of Computer and Information Science was founded on 1st January 1996 when the previous Faculty of Electrical Engineering and Computer Science was split into two new faculties. Research activities (as well as most Diploma, Master and Doctoral theses research) at the Faculty of Computer and Information Science are performed in fourteen research laboratories, including Laboratory for Cryptography and Computer Security.

Laboratory for Telecommunication, Faculty of Electrical Engineering, University of Ljubljana	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Resilience	
Relationships: None	
Weblink: http://lt.fe.uni-lj.si/default.asp	
Areas of Activity: Laboratory for Telecommunications was founded in 1946, and is thus the oldest laboratory in the field of telecommunications in Slovenia. The development (project) work is related to development of information technology systems and services. Covered are all key telecommunication technologies, such as NGN; IP, xDSL, MPLS, ATM, GSM, GPRS, UMTS, and TM, as well as XML, and Web applications. Important fields of work represent design and development of signaling system no. 7, converged services and multi-accessible portal systems based on fixed, mobile, IP and voice platforms. An important area of research, development and implementation is the role of telecommunications and networking technologies in distance education. Laboratory for Telecommunications closely co-operates with the Slovenian telecommunications industry, including vendors, service providers and content providers.	

Faculty of Organisational Sciences, University of Maribor	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: None	
Weblink: http://ecom.fov.uni-mb.si/ecomENG/index.htm	
Areas of Activity: The Faculty is an educational and research institution focusing on e-government, e-commerce, e-business (with emphasis on SMEs), e-market services and related issued in the field on information security.	

Other Bodies and Organisations Active in Network and Information Security

SI-CERT	
Type of Organisation: CERT	Ownership: private
ENISA Focus Points: CERT	
Relationships: Functions within the Academic and Research Network of Slovenia (ARNES)	
Weblink: http://www.arnes.si/english/si-cert	
Areas of Activity: SI-CERT is a service offered by ARNES (Academic and Research Network of Slovenia). The constituency is extended to all computer networks in Slovenia, both academic and commercial. SI-CERT's main services include coordination of security incidents involving networks or systems in Slovenia, and providing technical expertise on network security related issues.	

Security Technology Competence Centre (SETTCE)	
Type of Organisation: Other body	Ownership: Non-profit
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.setcce.si/eng	
Areas of Activity: Security Technology Competence Centre is an association of organizations for research, development and technology transfer in the area of security technology and electronic business. The centre brings its clients the latest achievements in the field of secure e-business through development, consulting and educational activities.	

Jozef Stefan Institute Laboratory for Open System and Networks	
Type of Organisation: Other body	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: None	
Weblink: http://www.ijs.si/ijsw/E5	

Areas of Activity:

Laboratory for open systems and networks was established in 1992. Laboratory activities are aimed at research and development of next generation networks, telecommunication technologies, and promotion of the concept of information society. The main areas of research include also security and privacy in information systems.

SAFE-SI

Type of Organisation: Other body	Ownership: Non-profit

ENISA Focus Points: Awareness raising

Relationships: Faculty of Social Sciences, ARNES,

Weblink: http://www.safe.si

Areas of Activity:

The organization supports the protection and education of children and teenagers in relation with the use the Internet and new online technologies. The project is a part of Safer Internet Plus Programme.

Activities

Strategic Initiatives

Protection of the Local Networks of the Organizations Connected to ARNES Network

Type of Activity: Non-governmental Initiative

Responsible Organisation(s): ARNES

ENISA Focus Points: Resilience, Emerging and Current risks, Implementation of Security Technology and Standards

Weblink: N/A

Description:

Implementing a more strict access control rules on the ARNES access routers. Development of the interactive online system where local network administrators can submit their security requests to ARNES.

Development of Slovenian Grid Network

Type of Activity: Non-governmental Initiative

Responsible Organisation(s): ARNES

ENISA Focus Points: Resilience
Weblink: N/A
Description: ARNES joins the European Grid Network project under the "SiGNET" name (Slovenian Grid Network). In 2008, it will start implementing a test grid network, which will be used for testing and developing the central national network infrastructure.
Network infrastructure Vulnerability Testing
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): SI-CERT
ENISA Focus Points: Resilience, Emerging and Current Risks
Weblink: N/A
Description: In 2008, a new service that will allow organizations to order a network vulnerability test will be implemented.
SPLETNO OKO (Web Eye)
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): University of Ljubljana, Faculty of Social Sciences; SISPA
ENISA Focus Points: Awareness Raising
Weblink: N/A
Description: SPLETNO-OKO.SI is a Slovenian hotline, which provides means for anonymous reporting of illegal Internet contents. “Spletno oko” is dealing with the reports concerning child pornography and hate speech on the Internet.
DIADEM (Distributed Adaptive Security by Programmable Firewall)
Type of Activity: Non-governmental Initiative
Responsible Organisation(s): Jozef Stefan Institute Laboratory for Open System and Networks
ENISA Focus Points: Resilience, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: N/A

Description: Development of a solution for protection of broadband services.
Encouragement of technology development projects in SMEs
Type of Activity: Government Funding Program
Responsible Organisation(s): Ministry of Higher Education, Science and Technology, Directorate of Information Society
ENISA Focus Points: Micro-enterprises
Weblink: N/A
Description: An initiative aimed at rising technology development programmes in SMEs.
Netflow analyzing system change
Type of Activity: Non-governmental initiative
Responsible Organisation(s): SI-CERT
ENISA Focus Points: Emerging and Current Risks
Weblink: N/A
Description: Change from flow-tools to a new nfdump/NfSen analyzing applications.

Research Programmes
Digital Identity Management at University of Ljubljana
Type of Activity: Technical Research Programme
Responsible Organisation(s): Digital identity management at University of Ljubljana - University of Ljubljana
ENISA Focus Points: Emerging and Current Risks, Implementation of Security Technology and Standards
Weblink: N/A

Description: The project includes analysis, design, and deployment strategy and prototype implementation of an identity management system across the whole University of Ljubljana - almost 60,000 users.

Events

Conference and Workshops

SirIKT

Responsible Organisation: ARNES	Frequency: annual
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Target Groups: Educational and Research Organizations	
Weblink: http://www.sirikt.si/index-2008.html	

Description:

The event is an annual meeting of teachers and students organized in cooperation with ARNES. The main topic is the use of information technologies in educational and research programs. This year (2008) it included seminars and workshops on topics such as Web 2.0 applications and privacy, user protection, security in educational networks, etc.

INFOSEK

Responsible Organisation: Palsit, ENISA	Frequency: annual
ENISA Focus Points: Awareness Raising, Implementation of Security Technology and Standards	
Target Groups: Security professionals	
Weblink: http://www.infosek.net/index.php?page=28	

Description:

A conference dealing with leading security topics, with leading experts: up-to date sessions, best practices, emerging trends and a lot of opportunities for networking and exchanging opinions: SOA & Security- Security Management, Business Continuity Management and Risk Management, Hacking. In 2008, the topic of the conference will be "How to protect yourself" focusing on biometrics, hacking, and outsourcing - network security.

Frisk 2008

Responsible Organisation: Gibanje za mladino	Frequency: annual
ENISA Focus Points: Awareness Raising , Emerging and Current Risks, Implementation of Security Technology and Standards	

Target Groups: Consumers / Citizens, SMEs, Large Enterprises, Government Organizations, Educational & Research Organizations, Security Professionals

Weblink: http://www.frisk.si/

Description: The festival is promoting all aspects of ICT technologies, and also includes security related workshops and presentations.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Slovenia.

Country Report – Spain

Country General Information

Source: European Commission

Political system:	Constitutional Monarchy
Capital city:	Madrid
Total area:	504 000 sq.km
Population:	45.2 million
Official language:	Spanish
Time zone:	CET (GMT+1)
Currency:	Euro (EUR)

Source: Eurostat

Country Highlights

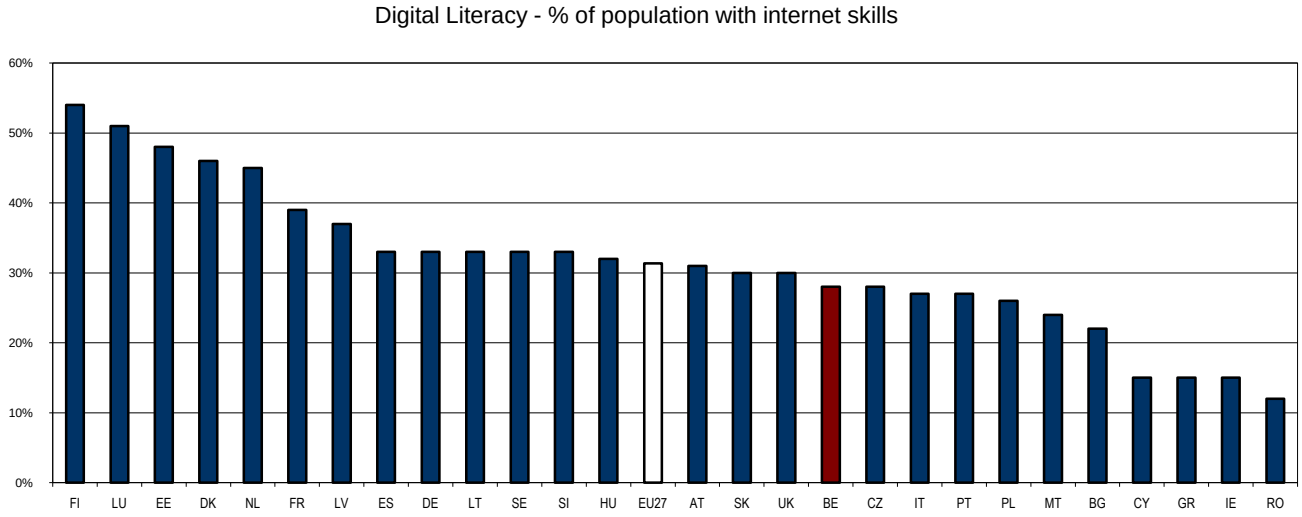
In order to provide an overview of recent IT developments in Spain, we present a set of three indicators in the Country Highlights section.

The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

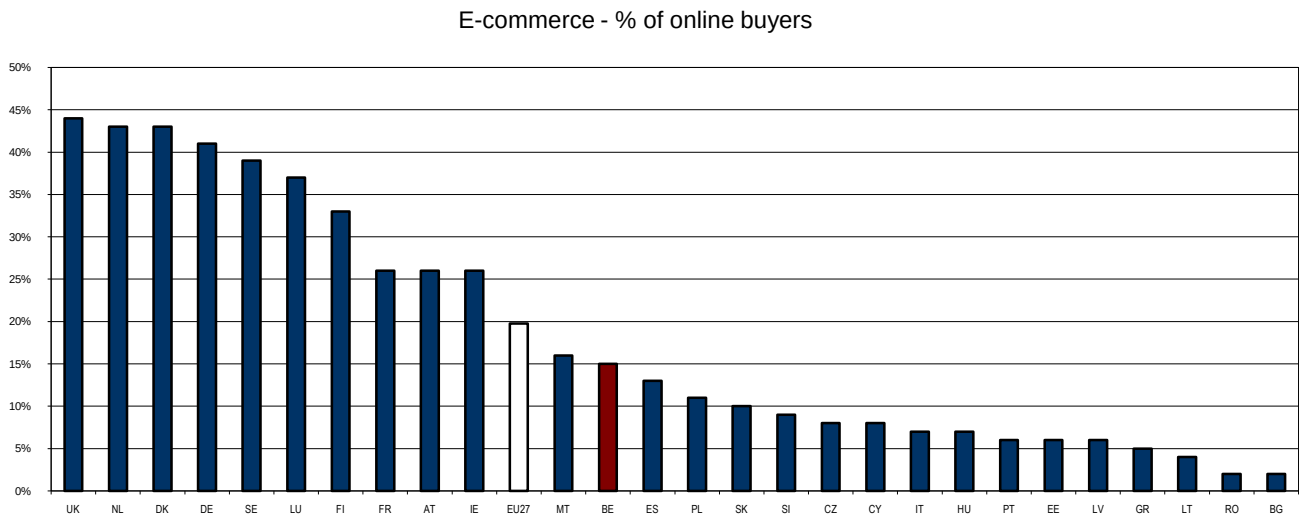
For these reasons, a general understanding of the stage of IT adoption in Spain is fundamental to this NIS study.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

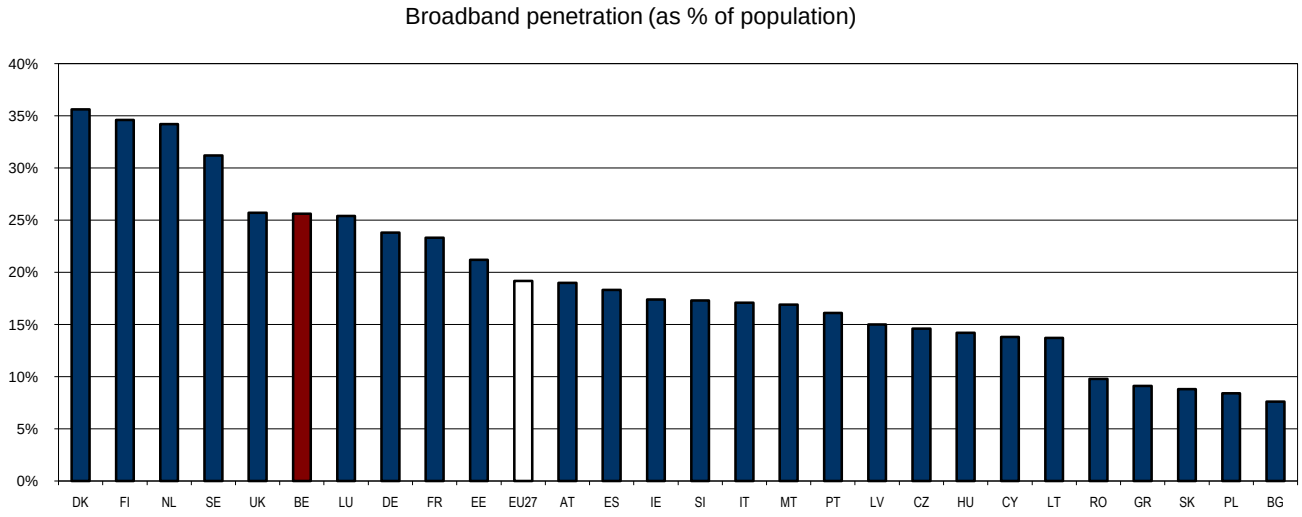
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

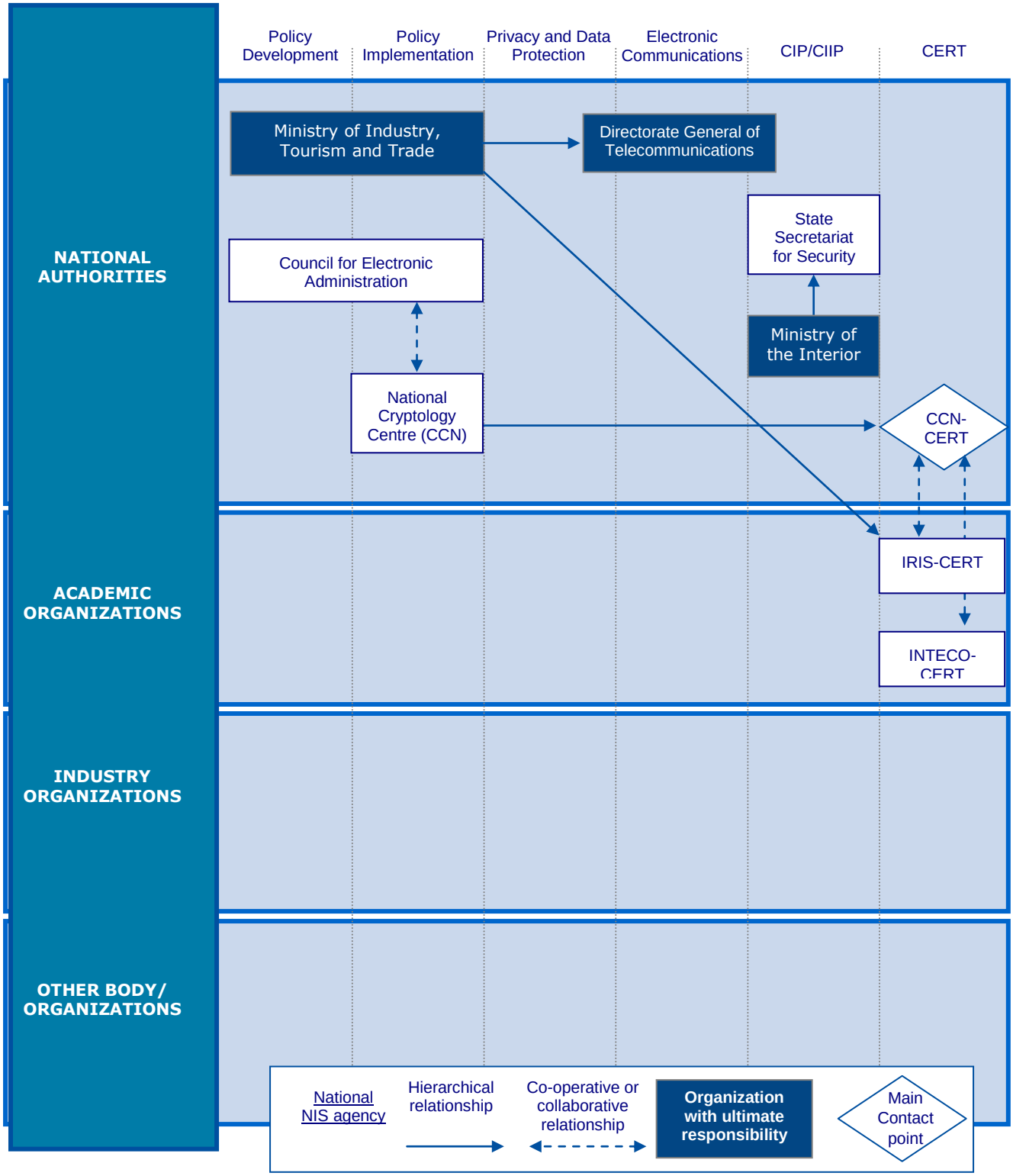
In Spain there is no single agency responsible for NIS. The Ministry of Industry, Tourism and Commerce has overall responsibility for developing and implementing national information security policy. Responsibility for implementing and ensuring compliance with electronic communications legislation is held by the Directorate General of Telecommunications, which is part of the Ministry of Industry, Tourism and Commerce.

The Ministry of Interior has overall responsibility for critical infrastructure protection (CIP/CIIP). Within the Ministry, the State Secretariat for Security is responsible for development of the National Critical Infrastructure Protection Plan.

The National Cryptology Centre (CCN) acts as a certification body, and runs the government CERT, which has a co-ordinatory role and acts a main point of contact with international organizations.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Spain. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Industry, Tourism and Trade			X				X	X
Directorate General of Telecommunications								X
Ministry of the Interior		X				X		
State Secretariat for Security		X		X			X	
Council for Electronic Administration							X	X
National Cryptology Centre (CCN)		X						X
CCN-CERT	X		X	X				
IRIS-CERT	X		X	X				
INTECO-CERT	X		X	X				

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Spain:

National Authorities in Network and Information Security	
Secretaría de Estado de Telecommunicaciones y Para la Socieded de la Información – State Secretariat for Telecommunications and Information Society	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: AR, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: part of the Ministry of Industry, Tourism and Trade	
Weblink: http://www.mityc.es/en-US/Ministerio/Estructura/SecretariaEstadoTelecomunicaciones/TitularesOrganosDirectivos/Titulares.htm	
Areas of Activity: Regulation regarding Telecommunications and Information Society: electronic communications, information society services and ecommerce, electronic signature.	
Consejo Superior de Aministración Electrónica – Council for Electronic Administration	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: part of the Ministry of Public Administration, collaborates with the National Cryptology Centre	
Weblink: http://www.csi.map.es	
Areas of Activity: The Council is responsible for the development and implementation of ICT policy and strategy and e-government within the public administration.	
Secretaría de Estado de Segurided – State Secretariat for Security	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risks, Development of Security Technology and Standards Policy	
Relationships: part of the Ministry of the Interior	

Weblink: http://www.mir.es/SES	
Areas of Activity: Within the Secretariat are: the General Directorate of Security Infrastructure and Material; the Centre of Intelligence against Organised Crime (CICO); and the Office of State Security Infrastructure and Equipment (GIESE). The Secretariat is responsible for developing the National Critical Infrastructure Protection Plan, and in particular Critical Information Infrastructures.	
Centro Criptológico Nacional - National Cryptology Centre	
Type of Organisation: National Security Actor	Ownership: Public
ENISA Focus Points: Resilience, Implementation of Security Technology and Standards	
Relationships: part of the National Intelligence Centre, which is associated with the Ministry of Defence	
Weblink: http://www.ccn.cni.es/	
Areas of Activity: The National Cryptology Centre (CCN) is responsible for providing ICT security assurance for public administration and is also an information security certification body.	
CCN-CERT	
Type of Organisation: National Security Actor	Ownership: Public
ENISA Focus Points: CERT, Emerging/Current Risks, AR	
Relationships: part of the National Cryptology Centre	
Weblink: https://www.ccn-cert.cni.es/english/	

Areas of Activity:

CCN-CERT is the Spanish governmental CERT. Its mission is to become the National Alert Centre, to cooperate and assist public administration in giving a quick and efficient response to security incidents and to actively face new threats to which they are currently exposed. CCN-CERT offers its services through the following:

- Support and coordination for the resolution of incidents suffered by national, provincial or local administration.
- Research and diffusion of the best practices on information security among all the members of public administrations. The series CCN-STIC, offers standards, instructions, guidelines and recommendations to ensure security of ICT systems in the public administration.
- Training through courses in the area of ICT security aimed at specialised public administration staff.

The CCN-CERT provides the necessary information and tools for the different administrations to develop their own CERTs, allowing CCN-CERT to act as a catalyst and as coordinator of governmental CERTs.

Academic Organisations Active in Network and Information Security

Instituto Nacional de Tecnologías de la Comunicación (INTECO) – National Institute of Communication Technologies

Type of Organisation: Other Academic	Ownership: Public
ENISA Focus Points: CERT, AR, Emerging/Current Risks, Micro-enterprises	
Relationships: promoted by the Ministry of Industry, Tourism and Trade	
Weblink: http://www.inteco.es	

Areas of Activity:

The National Institute of Communication Technologies (INTECO) is a platform for the development of the Knowledge Society through projects in the area of innovation and technology. INTECO's goal is to promote and develop innovation projects in the Information Society that are related to Information and Communication Technologies (ICT), which will improve the position of Spain and increase its competitiveness. The institute is tasked with developing, among other things, initiatives of technological security, accessibility and inclusion in the digital society and communications solutions for companies and individuals.

In the area of security INTECO runs the following projects with the aim of delivering a service to citizens and SMEs:

- Computer Emergency Response Team for SMEs and Citizens: it supports the development of the national business network and offers the typical services of an Incidents Response Centre, providing reactive solutions to computer incidents, prevention services against possible threats and services of information, awareness and training in computer security matters to SMEs and Spanish citizens.
- Information Security Observatory: its main aim is to analyse, describe, assess and propagate the culture of security and trust in the Information Society, through the creation of knowledge specialised in this area, and the development of recommendations and proposals that will allow defining valid trends for decision making processes in the security field.
- Security Technologies Show-Room for SMEs: it offers free and detailed information about the methods that guarantee the security of IT equipment in companies and other entities. Its main objectives are implementing different tests with security products, promoting the use of security technologies in Spanish SMEs and promoting the international visibility of Spanish security technologies.

IRIS-CERT

Type of Organisation: Other Acadamic	Ownership: Public
ENISA Focus Points: CERT, AR, Emerging/Current Risks	
Relationships: part of the Ministry of Industry, Tourism and Trade	
Weblink: http://www.rediris.es/cert/	

Areas of Activity:

IRIS-CERT is the security service of RedIRIS, the national academic and research network. RedIRIS has more than 300 affiliated institutions, essentially universities and public research centers.

Industry Organisations Active in Network and Information Security

Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España (AETIC) – Spanish Electronics, Information Technology and Telecommunications Industry Association

Type of Organisation: IT Associations	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Micro-enterprises	
Relationships: promotes links with relevant public institutions	
Weblink: http://www.aetic.es/	
Areas of Activity: AETIC has 1,000 members, of which 300 are individual companies and the rest are industry groups. AETIC works on NIS through its "eSEC Industry Platform", which is supported by the Ministry of Industry, Tourism and Trade; the Ministry of Science and Education; and the Centre for Development of Industrial Technology (CDTI).	

Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España (ASIMELEC) – Spanish Electronic and Communications Multisectorial Industry Association

Type of Organisation: IT Associations	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Relationships: promotes links with relevant public institutions	
Weblink: http://www.asimelec.es/	
Areas of Activity: ASIMELEC has 230 members, representing a total of 2,000 companies. ASIMELEC works on NIS through its "Security in Information Technology and Trust in the Network" and "Digital Identity and the National Identity Card" working groups.	

Asociación Nacional de Empresas de Internet (ASIMELEC) – National Association of Internet Enterprises

Type of Organisation: IT Associations	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises	
Relationships: promotes links with relevant public institutions	
Weblink: http://www.asimelec.es/	
Areas of Activity: ANEI works on NIS through its "Security" working group.	

Other Bodies and Organisations Active in Network and Information Security

Protegeles	
Type of Organisation: Philanthropic, Educational & Professional Associations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: promotes links with relevant public institutions	
Weblink: http://www.protegeles.com	
Areas of Activity: Protegeles is part of the European internet safety network INSAFE within the framework of the Safer Internet Programme. The organisation runs a hotline for dealing with harmful and illegal content over Internet, and is an awareness raising node.	

Asociación de Usuarios de Internet (AUI) – Association of Internet Users	
Type of Organisation: Other Bodies and Orgnisations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: promotes links with relevant public institutions	
Weblink: http://www.aui.es	
Areas of Activity: Association for individual and corporate Internet users whose goals are to influence Internet regulation and the Internet-related initiatves of public administration.	

Asociación de Internautas – Association of "Internauts"	
Type of Organisation: Other Bodies and Orgnisations	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: promotes links with relevant public institutions	
Weblink: http://www.internautas.org	
Areas of Activity: Association for individual Internet users whose goals are to influence Internet regulation and the Internet-related initiatves of public administration.	

Activities

Strategic Initiatives

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) – Certification Body of the Spanish Information Technology Evaluation and Certification Scheme

Type of Activity: Governmental Policies

Responsible Organisation(s): National Cryptology Centre

ENISA Focus Points: Implementation of Security Technologies and Standards

Weblink: http://www.oc.ccn.cni.es

Description:

The Certification Body operates under request of any private or public parties that wish to act as IT security evaluation laboratories, as well as under request of any private or public manufacturers/developers of IT products or systems that may wish to certify the security of their products. The "Common Criteria" certificates issued by this Certification Body are recognized by more than twenty countries.

Centro Demostrador de Seguridad para la Pyme – Security Technologies Showroom for SMEs

Type of Activity: Governmental Policies

Responsible Organisation(s): INTECO

ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises, e-ID

Weblink: http://www.inteco.es/Security/ShowRoom_for_SME

Description:

The Security Technologies Showroom for SMEs offers free and detailed information about the methods that guarantee the security of IT equipment in companies and other entities. It's main objectives are:

- Implementing different tests with security products.
- Promoting the use of security technologies in Spanish SMEs.
- Promoting the international visibility of Spanish security technologies.

Funding Programs and Financial Initiatives

Avanza R&D

Type of Activity: Government Funding Programs
Responsible Organisation(s): Ministry of Industry, Tourism and Trade
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards
Weblink: http://www.planavanza.es/
Description: Strategic Action of telecommunications and Information Society within the National Plan of Scientific Research, Development and Technological Innovation, 2008-2011
Avanza PYME
Type of Activity: Government Funding Programs
Responsible Organisation(s): Ministry of Industry, Tourism and Trade
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Micro-enterprises, Implementation of Security Technology and Standards
Weblink: http://www.planavanza.es/
Description: Among the goals of this programme is to promote the adoption of NIS products and services by SMEs
Research Programess
Observatorio de la Seguridad de Información – Information Security Observatory
Type of Activity: Social & Other Research Programmes
Responsible Organisation(s): INTECO
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises
Weblink: http://www.inteco.es/Seguridad/Observatorio
Description: The Observatory has been created by INTECO with the aim to generate specialized and useful knowledge about security matters, as well as to draft recommendations and proposals that can be used to define trends for future decision-making processes by public authorities. This plan of activities includes research, analysis, study, guidance and promotion tasks.

Events

Conference and Workshops	
"Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)" – IT Security Management Course	
Responsible Organisation: National Cryptology Centre (CCN)	Frequency: annual
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Government Organizations	
Weblink: http://www.ccn.cni.es/relacion_cursos.html	
Description: The CCN has developed a set of diverse courses to promote awareness related to IT usage at public administration, providing the necessary training for risk management and executing adequate security procedures.	
Encuentro Nacional de la Industria de la Seguridad en España (ENISE) – National Meeting of the Spanish Security Industry	
Responsible Organisation: INTECO	Frequency: annual
ENISA Focus Points: Resilience, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards	
Target Groups: Major- Large Enterprises, SMEs, Government Organizations, Security Professionals,	
Weblink: https://2enise.inteco.es/	
Description: ENISE is a meeting for the Spanish security industry. It's focused in three key sectors: Financial & Insurance, Defence and Public Administration (at every level, from national to local) and Utilities, Industry and Transport.	
Jornadas de Seguridad de la Información en Defensa – Information Security in Defence Congress	
Responsible Organisation: Ministry of Defence	Frequency: annual
ENISA Focus Points: Resilience, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards	
Target Groups: Major- Governmental Organisations, Educational and Research Organisations, Security Professionals	

Weblink: http://www.mde.es/jornada_sid.html
Description: The aim of this congress is to share knowledge about information security in the defence sector. Part of the conferences are restricted to Spanish Ministry of defence personnel only, and part are open to security companies.

Jornadas Técnicas RedIRIS – RedIRIS Technical Congress	
Responsible Organisation: RedIRIS	Frequency: annual
ENISA Focus Points: Resilience, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards	
Target Groups: Major- Governmental Organisations, Educational and Research Organisations, Security Professionals	
Weblink: http://www.rediris.es/jt/	
Description: RedIRIS is the Spanish academic and research network. Security and privacy in the network is one of the primary focuses of this meeting.	

SECURMÁTICA	
Responsible Organisation: SIC Magazine	Frequency: annual
ENISA Focus Points: Resilience, Emerging/Current Risks, e-ID, Implementation of Security Technology and Standards	
Target Groups: Major- Educational and Research Organisations, Security Professionals	
Weblink: http://www.securmatica.com	
Description: Spanish conference for security professionals, focused on the technical, management and legal aspects of information security.	

Mundo Internet – Internet World	
Responsible Organisation: Association of "Internauts"	Frequency: annual
ENISA Focus Points: Emerging/Current Risks, Implementation of Security Technology and Standards	
Target Groups: Major- Consumers/Citizens, SMEs, Educational and Research Organisations, Security Professionals	

Weblink: http://www.mundointernet.es
Description: International (Iberoamerican) congress on Internet, telecommunications and the information society.

Media Campaigns

Exprime la Red – Squeeze the Web	
Responsible Organisation: Protegeles	Duration: unlimited
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major- Consumers/Citizens, Educational and Research Organisations	
Weblink: http://www.exprimelared.com	
Description: This campaign is intended to show children the huge possibilities the Internet offers to them as well as some rules and suggestions to use Internet on a satisfactory way, preventing counter-productive effects. Moreover, the campaign is also targeting at Teacher-Parents Associations and Secondary School teachers. This is an online campaign with educative conference talks in Spanish schools. There is no end date scheduled.	

Me Gusta Internet – I Love Internet	
Responsible Organisation: AUI	Duration: unlimited
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major- Consumers/Citizens	
Weblink: http://www.megustainternet.es	
Description: The idea is to generate trust in the use of the Internet, so that citizens and businesses benefit from all the possibilities offered. It is an ongoing campaign, with no plans for ending.	

sentido común– common sense	
Responsible Organisation: AUI	Duration: unlimited
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Major- Consumers/Citizens, SMEs	

Weblink: http://sentidocomun.inteco.es/

Description:

The themes of this campaign are leisure time and communications; online fraud; and SME's security. This is an online campaign with no end date scheduled.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, zero security breaches were reported in Spain.

Country Report – Sweden

Country General Information

Source: European Commission

Political system:	Constitutional monarchy
Capital city:	Stockholm
Total area:	450,000 sq.km
Population:	9.0 million
Official language:	Swedish
Time zone:	CET (GMT+1)
Currency:	Swedish krona (SEK)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in Sweden, we present a set of three indicators in the Country Highlights section.

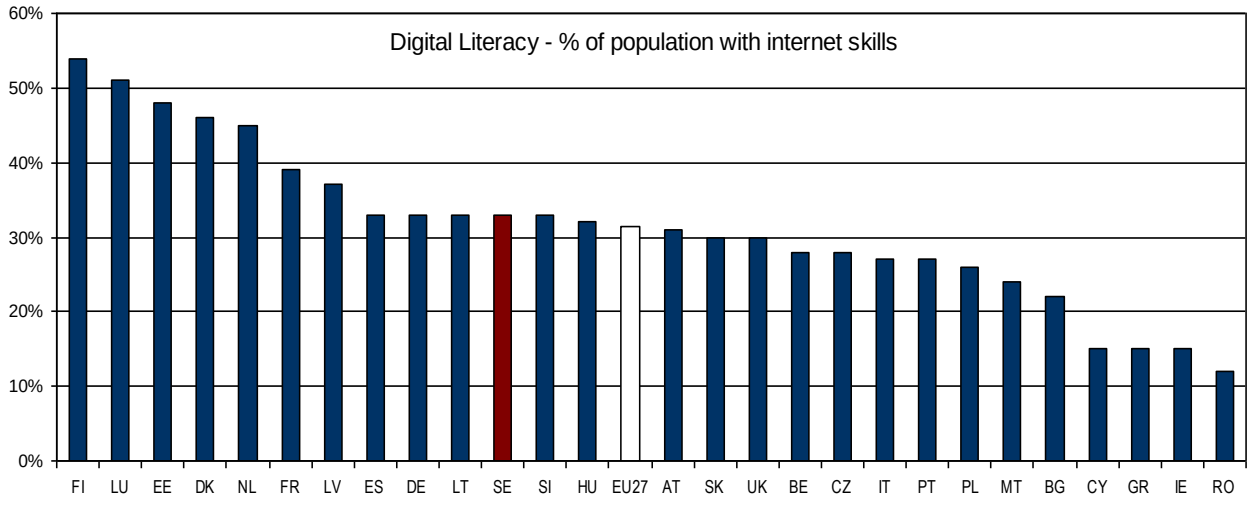
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in Sweden is fundamental to this NIS study.

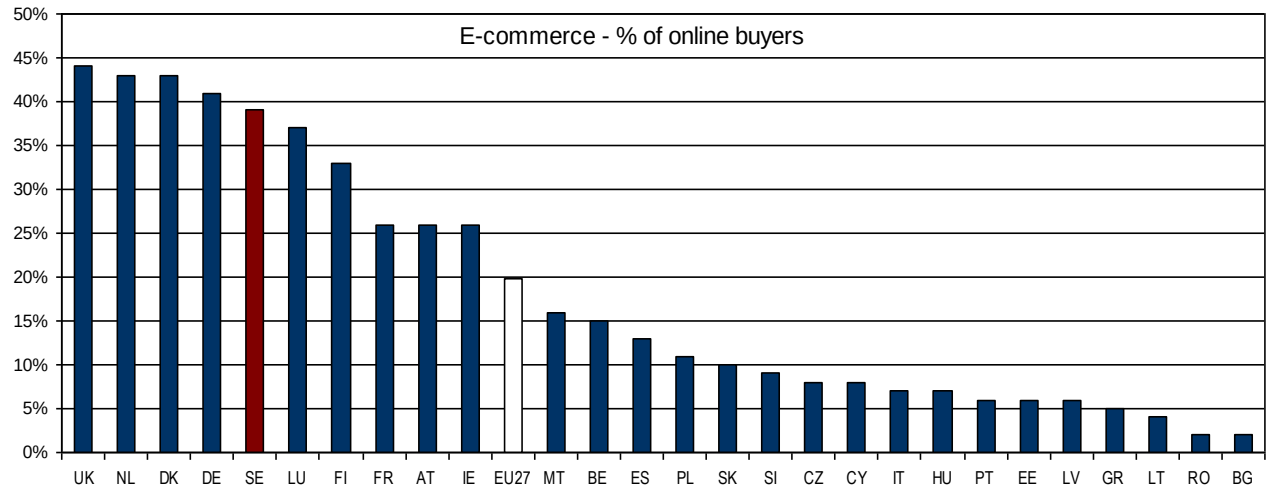
Sweden belongs to the group of the most developed countries for information society development. The country and is one of the leading countries for use of information and communication technologies in the economy, which is underlined by the high proportion of ICT specialists and above average level of digital literacy. Sweden is one of European leaders in electronic commerce with very high availability and sophistication of business and public services online.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

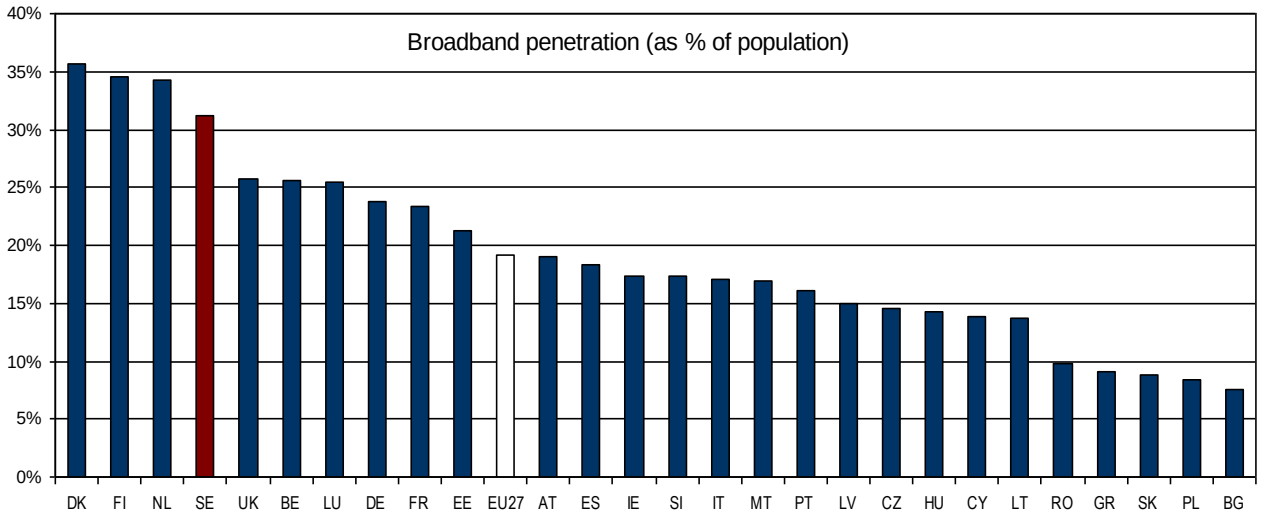
Digital Literacy Indicator



E-commerce Indicator



Broadband penetration Indicator



NIS Highlights

Sweden does not have a single government body that is recognized among NIS stakeholders as the national security agency – various institutions (National Post and Telecom Agency, Swedish Data Inspection Board, Swedish Emergency Management Agency, National Defense Radio Establishment, Swedish Defense Materiel Administration and Swedish Security Service) share the tasks and competencies.

The Ministry of Enterprise, Energy and Communications, Ministry of Justice and Ministry of Defense are responsible for the coordination of the development of national information security policy/ strategy, legislation and research in the NIS domain. The execution of strategic policies is carried out by the organizations that are overseen by the mentioned ministries.

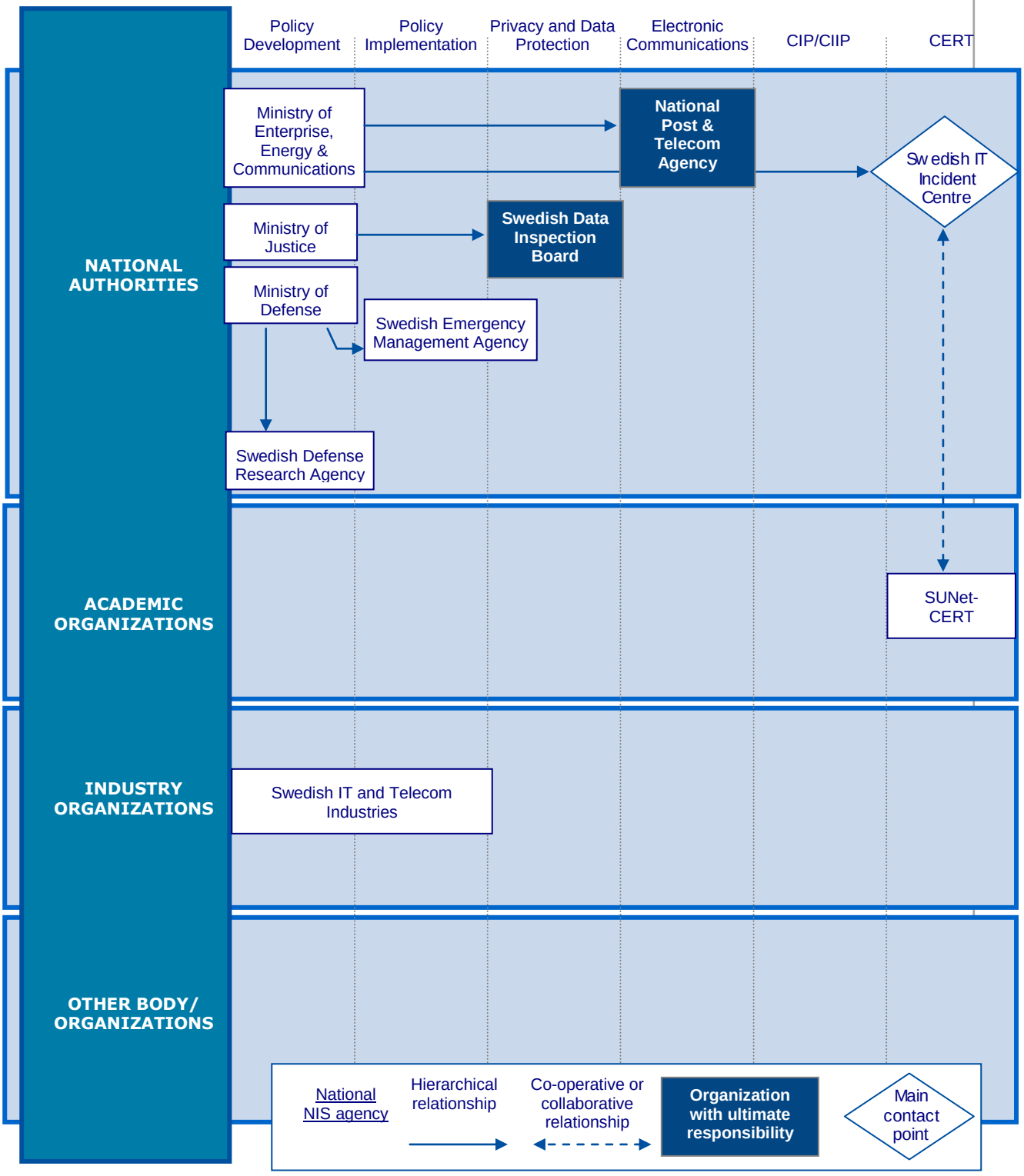
National Post and Telecom Agency overseen by Ministry of Enterprise, Energy and Communications, Swedish Data Inspection Board overseen by Ministry of Justice, Swedish Emergency Management Agency (will be replaced by MBS in January 2009) and National Authority for Signals Intelligence overseen by Ministry of Defense, and Swedish Security Service cooperate together so that information and infrastructure security is ensured in Sweden.

Sweden is committed to data protection and ensuring compliance in this regard. The Swedish Data Inspection Board is an independent oversight body responsible for protection of the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. The Board works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes.

Sweden has security response teams in place to handle security breaches and other incidents. Swedish IT Incident Centre (Sitic) is an independent organisation that supports the society against threats within the IT security area. Sitic is a part of the National Post and Telecom Agency (PTS). Sitic assess and inform continuously about threats against the IT security that involve risks against public authorities, county councils, municipalities and companies, acting as a state and governmental CERT.
There are a number of advanced e-government projects currently underway in the country as well as Internet security related ones. Sweden hosts a number of conferences prevalently organized by the main NIS stakeholders.

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in Sweden. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activity of the Key Stakeholders in the eight ENISA focus point areas:

	ENISA Focus Points							
Names of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
Ministry of Enterprise, Energy & Communications					X		X	X
National Post and Telecom Agency		X	X	X	X	X		
Swedish IT Incident Centre	X	X	X	X				
Ministry of Defence		X					X	X
Swedish Emergency Management Agency (MBS in Jan 2009)		X	X					
Swedish Defence Research Agency		X	X	X			X	
Ministry of Justice							X	X
Swedish Data Inspection Board							X	X
SUNeT-CERT	X							
Swedish Media Council			X	X				
Swedish IT and Telecom Industries			X	X	X			

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in Sweden:

National Authorities in Network and Information Security	
Swedish Data Inspection Board	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Reports to Ministry of Justice	
Weblink: http://www.datainspektionen.se/	
Areas of Activity: The Data Inspection Board's task is to protect the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. The Board works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes. The Board also handles complaints and carries out inspections. By examining government bills the Data Inspection Board ensures that new laws and ordinances protect personal data in an adequate manner.	
Ministry of Enterprise, Energy and Communications	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Micro-enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.sweden.gov.se/enterprise	
Areas of Activity: Infrastructure and responsibility for coordination on issues relating to the use of information technology.	
National Post and Telecom Agency	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks, Micro- enterprises, e-ID	

Relationships: Reports to Ministry of Enterprise, Energy and Communications	
Weblink: http://www.pts.se	
Areas of Activity: The Swedish Post and Telecom Agency (PTS) monitor the electronic communications (telephony, the Internet and radio) and postal sectors in Sweden. The Agency works with consumer and competition issues, efficient utilisation of resources and secure communications. The authority is an independent agency according to the Swedish public authority model. PTS's work concerning secure communications involves supervision under the Electronic Communications Act. The authority may require that all networks for electronic communications should satisfy reasonable requirements for good functionality and security. One important component of enhancing security on the Internet is well-informed and aware users. PTS has consequently taken initiatives to inform consumers about these areas. Furthermore, supervision is conducted in this area to verify that the stakeholders in the market comply with the legal provisions concerning protection of privacy. This supervision comprises for example dealing with complaints received, inspections and follow up of demands imposed.	
Ministry of Justice	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.sweden.gov.se/justice	
Areas of Activity:	
Ministry of Defence	
Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: resilience, Development of Security Technology and Standards Policy , Implementation of Security Technology and Standards	
Relationships: none	
Weblink: http://www.sweden.gov.se/defence	
Areas of Activity: The Ministry has two organizations to assist it with IT security matters: National Defence Radio Establishment and Swedish Emergency Management Agency.	
Ministry of Finance	

Type of Organisation: National Government	Ownership: Public
ENISA Focus Points: e-ID	
Relationships: none	
Weblink: http://www.sweden.gov.se/finance	
Areas of Activity: The Ministry is working with the major banks on e-ID solutions.	
Swedish IT Incident Centre	
Type of Organisation: Public NIS Body	Ownership: Public
ENISA Focus Points: CERT, Resilience, Awareness raising, Emerging and Current Risks	
Relationships: Reports to National Post and Telecom Agency	
Weblink: http://www.sitic.se	
Areas of Activity: Sitic is an independent organisation that supports the society against threats within the IT security area. Sitic is a part of the National Post and Telecom Agency, PTS. Sitic assess and inform continuously about threats against the IT security that involve risks against public authorities, county councils, municipalities and companies. Sitic provides a function for information exchange about IT-incidents among society's organisations and disseminates information in the society about new problems that can disturb IT systems. Sitic also submits information and advice about preventive measures and puts together and gives out statistic as base for continuous improvements in the preventive work. Sitics main competence is technology, technology analysis and strategic analysis within the area IT security, information security, IT incident handling and infrastructure protections. All personnel at Sitic are in a higher security protection class. Sitic can request competence from PTS, for example in administrative, legal, and human resource questions.	
Försvarets radioanstalt (FRA) - Swedish National Authority for Signals Intelligence	
Type of Organisation: Public NIS Body	Ownership: Public
ENISA Focus Points: Emerging and Current Risks	
Relationships: Reports to Ministry of Defence; Works with Defence and Police organizations as well as international collaboration	
Weblink: http://www.fra.se/	

Areas of Activity: FRA is engaged in information assurance. On demand, the Authority supports government authorities and state owned companies regarding current IT threats as well as giving general advice to improve security. It monitors radio and cable-based communication in order to identify and asses potential threats. FRA's main customers are the Foreign Ministry, the Ministry of Defence, the Military Intelligence And Security Directorate (MUST) and the Security Police.

Agency for Civil Protection and Preparedness (MSB)	
Type of Organisation: National NIS Body	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current Risks , e-ID	
Relationships: none	
Weblink: http://www.krisberedskapsmyndigheten.se/defaultEN____224.aspx, http://www.verva.se	
Areas of Activity: MSB is an organization that will replace the Swedish Emergency Management Agency (SEMA) and the Swedish Administrative Development Agency (Verva) in January 2009 and so integrate their competences. SEMA coordinates the work to develop the preparedness of Swedish society to manage serious crises. It works together with municipalities, county councils and government authorities, as well as the business community and several organisations, to reduce the vulnerability of society and improve the capacity to handle emergencies. In January 2007, SEMA was commissioned by the government to prepare proposals for an action plan for information security in Sweden. The action plan consists of 47 proposed measures. Verva coordinates the development of central government in Sweden and is one of the Government's central advisory agencies. Verva is the expert in the field of public administration development, it promotes and supports the development of public administration, it supports human resource development and strategic human resource management, and it enhances coordination in government administration. Verva coordinates the procurement of framework contracts concerning products and services for the entire public sector in the fields of information and communications.	

Swedish Defence Research Agency (FOI)	
Type of Organisation: Other Public Body (Research centre)	Ownership: Public
ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks , Development of Security Technology and Standards Policy	
Relationships: Reports to Ministry of Defence	
Weblink: http://www.foi.se	

Areas of Activity: FOI is one of Europe's leading research institutes in the defence and safety area. The agency is financed on contracts' basis and is responsible to the ministry of defence. The core business is research, method and technology development and studies. FOI carries out security policy studies and analyses, evaluate different types of threats and develop tools for, as an example, adaptation of society due to climate change. FOI develops systems for crisis management in connection with major accidents and catastrophic events.	
Swedish Institute for Transport and Communications Analysis (SIKA)	
Type of Organisation: National Security Actor	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: Reports to Ministry of Enterprise, Energy and Communications	
Weblink: http://www.sika-institute.se	
Areas of Activity: Produces statistics and forecasts within the communications sector.	
National Police	
Type of Organisation: Other Public Body	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: Reports to Ministry of Justice	
Weblink: http://www.polisen.se	
Areas of Activity: The Police inform about IT security and crime in addition to enforcing IT-related legislation.	
Swedish National Financial Management Authority (ESV)	
Type of Organisation: Government Organization	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: Reports to Ministry of Finance	
Weblink: http://www.esv.se	
Areas of Activity: Responsible for implementing e-invoicing.	
Ins@fe	

Type of Organisation: Regional Government	Ownership: Public
ENISA Focus Points: Awareness Raising, Emerging and Current risks	
Relationships: Reports to the Swedish Media Council	
Weblink: http://www.saferinternet.org/ww/en/pub/insafe/focus/sweden.htm	
Areas of Activity: This is an international EU network with a local presence, organizing events and promoting awareness.	

Swedish Consumer Agency	
Type of Organisation: Governmental Organization	Ownership: Public
ENISA Focus Points: Awareness Raising	
Relationships: Reports to Ministry of Integration and Gender Equality	
Weblink: http://www.konsumentverket.se	
Areas of Activity: The Swedish Consumer Agency has the responsibility of protecting all aspects of consumer rights.	

Industry Organisations Active in Network and Information Security

Swedish IT and Telecom Industries	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, Micro- enterprises	
Relationships: Part of Almega organization	
Weblink: http://www.itotelekomforetagen.se/	
Areas of Activity: The Swedish IT & Telecom Organization is a membership organization with the objective to promote and further develop the IT market and conditions for IT enterprises. Swedish IT & Telecom Industries is one of seven branch and employer associations who work together as Almega. Basic membership offers companies advice on sector issues and the opportunity to access collective agreements and employer support.	

ISACA Sweden	
Type of Organisation: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: Part of international ISACA network	
Weblink: http://www.isaca.se	
Areas of Activity: ISACA provides security certificates.	

SIG Security	
Type of Organisation: IT Association	Ownership: Non-profit
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: Part of international ISACA network	
Weblink: http://www.sigsecurity.se	
Areas of Activity: The organization’s main issue is to give rise to the understanding of and inspire to the work within the information security area.	

Swedish Risk Management and Security organization	
Type of Organisation: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: Awareness Raising, Emerging and Current Risks	
Relationships: Part of the Confederation of Swedish Enterprise	
Weblink: http://www.svensktnarinsgliv.se	
Areas of Activity: The organization's task is to promote awareness in the field of risk by monitoring current events, expert interaction etc.	

Swedish Consumers’ Association	
Type of Organisation: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: Awareness Raising	

Relationships: none
Weblink: http://www.sverigeskonsumentrad.se
Areas of Activity: Independent, non-partisan cooperative organisation consisting of 28 member organisations.

Academic Organisations Active in Network and Information Security

ICT, Royal Institute of Technology (KTH)	
Type of Organisation: University	Ownership: Public
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Relationships: Reports to the Swedish National Agency for Higher Education	
Weblink: http://www.kth.se	
Areas of Activity: The ICT faculty provides IT-related research and education.	
Chalmers Institute of Technology	
Type of Organisation: University	Ownership: Private
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Relationships: Reports to the Swedish National Agency for Higher Education	
Weblink: http://www.chalmers.se/	
Areas of Activity: This is the home to the Swedish IT Security Network.	
Department of Computer and Systems Sciences (DSV)	
Type of Organisation: University	Ownership: Private
ENISA Focus Points: Emerging and Current Risks	
Relationships: Reports to the Swedish National Agency for Higher Education	
Weblink: http://www.dsv.su.se/en/seclab/	

Areas of Activity:

The Department of Computer and Systems Sciences (DSV) is a joint department between Stockholm University and the Royal Institute of Technology. The DSV hosts SecLab, a laboratory for research and education in Computer Security and Security Informatics.

Other Bodies and Organisations Active in Network and Information Security

Swedish Media Council

Type of Organisation: Philanthropic, Educational & Professional Association	Ownership: Public
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Relationships: The Swedish Media Council is a committee under the Ministry of Culture	
Weblink: http://www.medieradet.se	

Areas of Activity:

The Council is the expert organisation on children and media in Sweden, and the aim of the Council's work is to protect children and minors from harmful effects of media content and media use. The Media Council's tasks are to: Be an expert on developments in the media and the effects of the media on children and young people; Follow research on the effects of the media and to spread factual information and provide guidance; Press for self-regulation in the media industry; Work for increased media knowledge in schools; Protect and strengthen children and young people in the new media landscape through cooperation with other actors; and Follow international developments and take part in international cooperation in its field.

SUNet-CERT

Type of Organisation: CERT	Ownership: Public
ENISA Focus Points: CERT	
Relationships: Part of Uppsala University	
Weblink: http://www.cert.sunet.se	

Areas of Activity:

SUNet CERT works with academic organizations attached to the SUNet network in security assistance. SUNet CERT helps University, college and other organisations connected to SUNet network with coordination of incidents. SUNet CERT also helps to keep the competence at IT security organisation within University's and colleges. SUNet CERT keeps a close contact with other ISPs in Sweden and abroad and cooperates with national and international CERT organisation.

Swedish Defence Materiel Administration	
Type of Organisation: Certification Provider	Ownership: Public
ENISA Focus Points: Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Relationships: Reports to Ministry of Defence	
Weblink: http://www.fmv.se	
Areas of Activity: The agency is responsible for carrying out certification in accordance with the Common Criteria Recognition Agreement (CCRA).	

Activities

Strategic Initiatives

National Action Plan for eGovernment
Type of Activity: Governmental Policy
Responsible Organisation(s): Ministry of Finance, Ministry of Enterprise, Energy and Communications
ENISA Focus Points: Resilience, Emerging and Current Risks, Micro- enterprises, e-ID
Weblink: http://www.regeringen.se/content/1/c6/09/65/12/4ffd1319.pdf
Description: The purpose of the initiative is to prepare the nation for electronically based public administration by the year 2010

eProcurement
Type of Activity: Governmental Policy
Responsible Organisation(s): Swedish National Financial Management Authority
ENISA Focus Points: Awareness raising, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: http://www.esv.se/

Description: The agency has assessed how the government could facilitate realizing fully electronic procurement by December 2013.
eInvoicing
Type of Activity: Governmental Policy
Responsible Organisation(s): Swedish National Financial Management Authority
ENISA Focus Points: Awareness raising, Emerging and Current Risks, Micro-enterprises, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards
Weblink: http://www.esv.se
Description: The government launched a target of being able to receive electronic invoices by July 2008.
Broadband 2013
Type of Activity: Governmental Policy
Responsible Organisation(s): Ministry of Enterprise, Energy and Communications
ENISA Focus Points: Awareness raising, Implementation of Security Technology and Standards
Weblink: http://www.sou.gov.se/bredband2013/
Description: The project assessed the resources required to provide broadband (+50MBps) for less populated areas.
Answer2
Type of Activity: Non-Governmental Initiative
Responsible Organisation(s): Swedish Media Council, Insafe
ENISA Focus Points: Awareness raising, Emerging and Current Risks
Weblink: http://www.saferinternet.org/ww/en/pub/insafe/focus/sweden.htm

Description:

The Swedish Media Council coordinates the Swedish node for internet safety awareness. In February 2007 BRIS-Children's Right in Society joined the project as helpline partner. Together they coordinate a strong, consistent and up-to-date safety message and ensure that it reaches all relevant target groups.

Security Arena Lindholmen

Type of Activity: Governmental Funding Program

Responsible Organisation(s): SEMA, Lindholmen Science Park, Chalmers University of Technology, Ericsson AB, Saab AB and AB Volvo

ENISA Focus Points: Resilience, Awareness Raising, Emerging and Current Risks

Weblink: http://www.lindholmen.se/ext/securityarena_en.php

Description:

The Security Arena brings together academia, industry and end-users. A three-year framework agreement has been entered into between the Swedish Emergency Management Agency (SEMA) and Lindholmen Science Park, Security Arena. Under this agreement, SEMA is contributing funds to applied research, technology and method development in the field of societal safety and security. The Security Arena performs research and concept development in many areas including information and communication security, interoperability, transport security and surveillance and early warnings.

Child Pornography Filter

Type of Activity: Non-governmental initiative

Responsible Organisation(s): National Criminal Investigation Department, Swedish ISPs

ENISA Focus Points: Awareness Raising

Weblink: N/A

Description:

The IT department of the Swedish Police's National Criminal Investigation Department maintains a list of proscribed Web sites that the ISPs, through the use of filters, prevent their users from accessing.

Strategy to Improve Internet Continuity in Sweden

Type of Activity: Government Policies

Responsible Organisation(s): National Post and Telecom Agency, electronic communications network owners and service providers

ENISA Focus Points: Resilience, Emerging and Current Risks, Development of Security Technology and Standards Policy
Weblink: http://www.pts.se/en-gb/Documents/Reports/Internet/2006/Strategy-to-improve-Internet-security-in-Sweden---PTS-ER-200612/
Description: The National Post and Telecom Agency (PTS) was assigned by the Government to develop a strategy to improve Internet security in Sweden. The goal of the strategy is to secure critical functions in the Internet infrastructure, which, if they were not maintained, would cause substantial disruption or interruption and in this way impede or prevent the use of the Internet for large groups of individual users or vital public businesses, authorities or organisations.

Research Programmes

Swedish IT Security Network (SWITS)
Type of Activity: Technical Research Programme
Responsible Organisation(s): Universities, SEMA
ENISA Focus Points: Resilience,Awareness Raising, Emerging and Current Risks
Weblink: N/A
Description: SWITS was launched in 2001 to promote collaboration between PhD students active in the IT security area.

SurfaLugnt - Browse with ease
Type of Activity: Research Programme
Responsible Organisation(s): National Post and Telecom Agency, Swedish Emergency Management Agency, Swedish IT and Telecom Industries
ENISA Focus Points: Awareness Raising, Emerging and Current Risks, Micro- enterprises
Weblink: http://www.surfalugnt.se/
Description: This activity has the purpose of increasing public trust toward using the internet by providing advice and recommendations.

Events

Conference and Workshops

Methodology for Crisis Communication

Responsible Organisation: Swedish Emergency Management Agency	Frequency: annual
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Target Groups: Security Professionals, Educational and Research Organizations; SMEs, Large Enterprises, Government Institutions	
Weblink: http://www.krisberedskapsmyndigheten.se/templates/Page____8864.aspx	
Description: The course deals with communication in the event of a crisis or emergency. It is primarily aimed at information managers, press representatives etc. The scope is to give a preparation in how to communicate with media in a crisis environment.	

SWITS 2008

Responsible Organisation: Karlstad University	Frequency: annual
ENISA Focus Points: Resilience, Awareness raising, Emerging and Current Risks	
Target Groups: Educational and Research Organizations	
Weblink: http://www.cs.kau.se/~simone/SWITS/AnnualSeminars/SWITS-8/SWIST%202008%20Program.htm	
Description: Yearly event organized by the Swift network. This event is aimed at IT security PhD. students. It gives the opportunity to share current research within specific topics.	

SIG Security "External Threats"

Responsible Organisation: SIG Security	Frequency: annual
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Target Groups: Security Professionals, Educational and Research Organizations	
Weblink: http://www.sigsecurity.se/web-content/z03_aktiviteter/z03_aktiviteter-04.asp	

Description: The event is aimed at all SIG members, i.e. any of the 1,700 security professionals. During the yearly meeting, a topic of discussion is chosen, and this year it is the area of "external threats".	
Skydd-Security, Fire and Rescue Expo	
Responsible Organisation: SIG Security	Frequency: biannual
ENISA Focus Points: Awareness raising, Emerging and Current Risks	
Target Groups: Security Professionals	
Weblink: http://www.skydd.net	
Description: This trade fair is aimed at all professionals within the areas of security, fire and rescue. It includes seminars on crisis management and methodologies for handling these issues.	
Internetdagarna	
Responsible Organisation: IIS	Frequency: annual
ENISA Focus Points: Resilience, Emerging and Current Risks, e-ID, Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards	
Target Groups: Large Enterprises, Government Organizations, Educational & Research, Organizations, Security Professionals	
Weblink: http://www.internetdagarna.se	
Description: Yearly event organized by the IIS and sponsored by several other organizations for instance PTS. One topic was IT security and speakers covered the areas of cyberterrorism, data intrusion etc. Attendee range from CIO's to help desk staff.	

Media Campaign	
Safer Internet Day	
Responsible Organisation: Swedish Media Council	Frequency: annual
ENISA Focus Points: Awareness raising	
Target Groups: Consumers / Citizens	
Weblink: http://www.medieradet.se/templates/Page 1502.aspx	

Description: The event has the scope of assisting field social workers in their work with children. The project is aimed at school children, who are encouraged to share their digital experiences by making short films. The films can then generate more collaboration, thereby creating an insight in the way school children utilize digital media.

Current Trends in Data Breaches

The field research and data collection phase showed how there is no specific trend for a particular country, but instead, common trends across all countries could be identified. The trends show a different strength in each country and are often driven either by the evolution of the same technology (e.g. Increased adoption of mobile devices) or by common policies (e.g. Adoption of EU guidelines).

However a lack of consistent statistics for most countries analyzed in this study, and a lack of a common approach in measuring the specific adoption and evolution of NIS gives a rather limited room for NIS trends evaluation validated by quantitative data.

For the aim of this study a specific NIS trend has been identified and analyzed: the analysis of the recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons among which include: the loss or theft of equipment where the data is stored, human error, equipment failure, unforeseen disasters (fires, floods, other natural calamities), hacking, and of ever increasing concern, the unauthorized use of data or information via inadequate access control to private or highly sensitive data.

In the last 12 months 0 security breaches were reported in Sweden.

Country Report – United Kingdom

Country General Information

Source: European Commission

Political system:	Constitutional monarchy
Capital city:	London
Total area:	242 500 sq.km
Population:	60.4 million
Official language:	English
Time zone:	GMT
Currency:	Pound sterling (GBP)

Source: Eurostat

Country Highlights

In order to provide an overview of recent IT developments in the UK, we present a set of three indicators in the Country Highlights section.

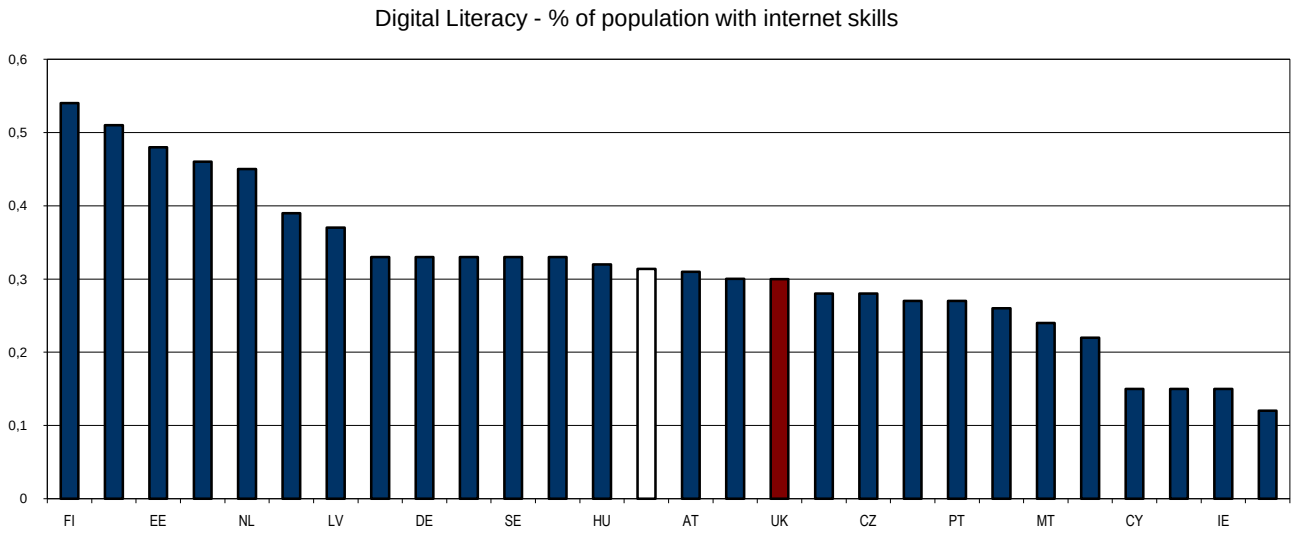
The indicators show the current IT market development stage of each EU member state. General IT developments clearly impact on network and information security (NIS); in general, the more a country relies on IT for its business and governmental activities, as well as for private purposes, the more NIS gains in importance. Increasing broadband penetration, for example, translates to increased usage of online services, which raises the likelihood of exposure to online threats; likewise, a generally higher level of computer literacy among the general populace results in increased online activity, and greater usage of ecommerce increases the risk of online fraud; in short, an individual's online security risk increases in parallel with the time he or she spends online.

For these reasons, a general understanding of the stage of IT adoption in the UK is fundamental to this NIS study.

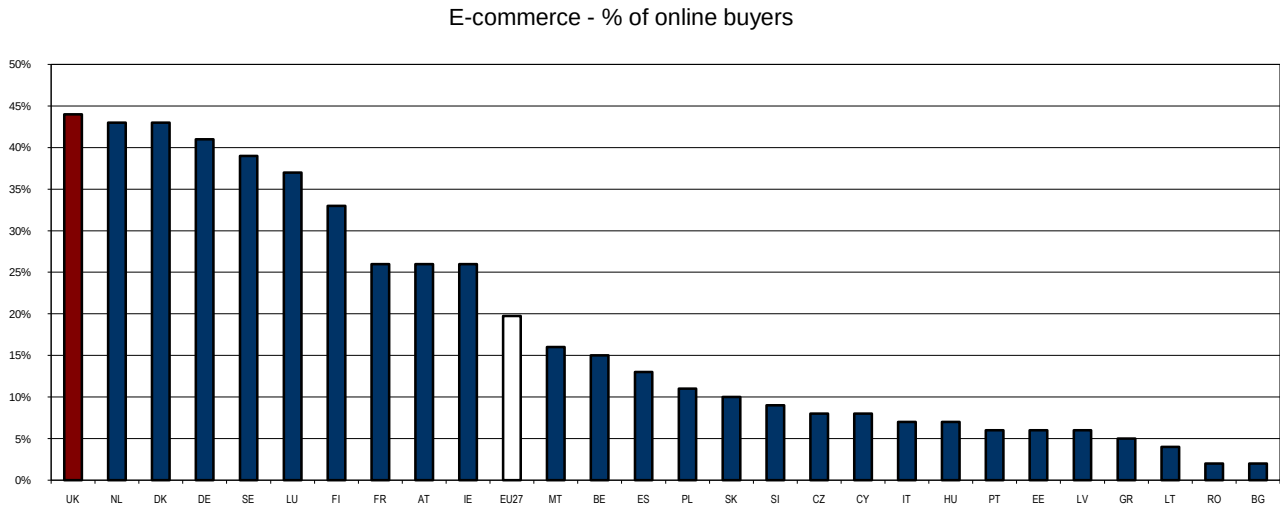
The United Kingdom is very strong in terms of the country's ICT development. Progress is also very fast in areas where the UK has a relative comparative advantage, namely the supply of e-Government services and the use of Internet by households. Broadband usage is high. That said the economic aspects of information society are not quite as well developed as broadband and public services and investment in ICT research is relatively low.

The shown indicators – Digital Literacy, E-commerce Buyers, Broadband penetration – provide an overview on key development areas, and have been chosen particularly as statistics are consistently available for all EU Member States (EU27).

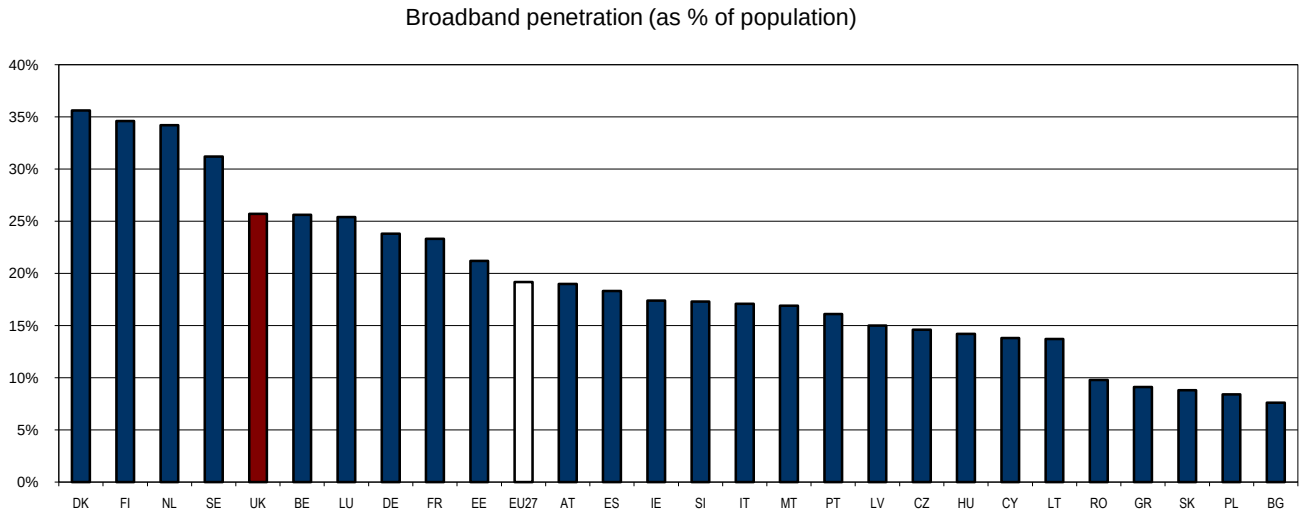
Digital Literacy Indicator



eCommerce Indicator



Broadband Penetration Indicator



NIS Highlights

No single UK organization is recognized as the national agency for information security.

Several public stakeholders are involved in the development and implementation of IS policy in the UK, including the Home Office, the Information Commissioner's Office, the Serious Organized Crime Agency (SOCA), and the Department for Business Enterprise and Regulatory Reform (BERR). The Information Assurance Policy and Program Board (IAPPB), and the Chief Information Officer (CIO) Council are responsible for NIAS implementation. Several academic and industry organizations are also involved at various stages of the development and implementation of national information security policy (see diagram below).

In terms of data protection and privacy, the Information Commissioner's Office (ICO), the UK's independent supervisory authority, oversees and ensures compliance with both the Data Protection Act 1998 and the Freedom of Information Act 2000.

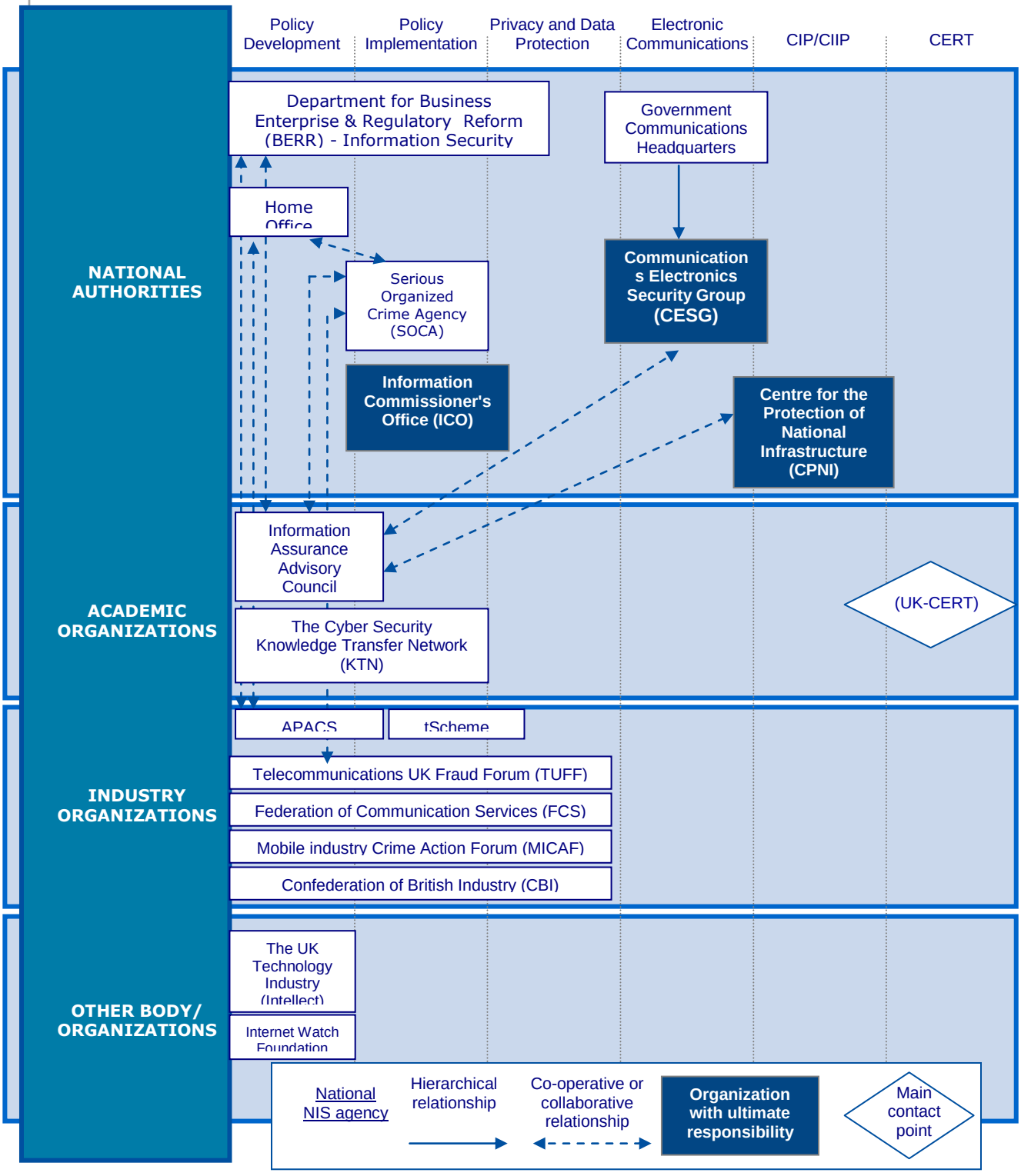
The Communications-Electronics Security Group (CESG) is the national technical authority for information assurance.

The United Kingdom Computer Emergency Response Team (UK-CERT) handles security breaches and other incidents.

The Center for the Protection of National Infrastructure (CPNI) is responsibility for key elements of CIP/CIIP at the national level. The center provides protective security advice to businesses and organizations across the national infrastructure (communications, emergency services, energy, finance, food, government, health, transport and water).

Overview of Key Stakeholders

The below diagram provides an immediate overview of the key NIS stakeholders active in the United Kingdom. Stakeholders are active in a variety of areas concerning IS security, including the development and implementation of IS policy, data privacy and compliance, passing and implementing electronic communications policy, and serving as national points of contact regarding information security.



Key Stakeholders activities within ENISA focus points areas

This table shows the activities of key stakeholders in ENISA's eight areas of focus:

	ENISA Focus points							
Name of Key Stakeholders	CERT	Resilience	AR (Awareness Raising)	Emerging Risks / Current Risks	Micro- enterprises	e-ID	Development of Security Technology and Standards Policy	Implementation of Security Technology and Standards
BERR Information Security Policy Team			X	X			X	X
Information Commissioner's Office (ICO)			X					X
Communications-Electronics Security Group (CESG)	X	X	X	X			X	X
United Kingdom Computer Emergency Response Team (UK-CERT)	X	X	X					
Central Sponsor for Information Assurance (CSIA)			X	X			X	X
Center for the Protection of National Infrastructure (CPNI)	X	X	X	X				
Information Assurance Advisory Council (IAAC)			X	X			X	

Detailed Stakeholders Overview

This section contains more detailed information on all NIS stakeholders in the United Kingdom:

National Authorities in Network and Information Security	
National Consumer Council (NCC)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks	
Relationships: None	
Weblink: http://www.ncc.org.uk	
Areas of Activity: NCC is focused on protecting the consumer. *Note: NCC will merge with Postwatch and Energywatch to form a new consumer representation and advocacy body.*	
Department for Business Enterprise & Regulatory Reform (BERR) – Information Security Policy Team	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: Works with regional commerce organizations to support policy development	
Weblink: http://www.berr.gov.uk/sectors/infosec/index.html	
Areas of Activity: Formerly the Department of Trade and Industry (DTI), BERR's role is to help ensure business success in an increasingly competitive world. It does this by: Promoting the creation and growth of business and a strong enterprise economy across all regions. Ensuring that all Government Departments and agencies deliver better regulation for the private, public and third sectors. Delivering free and fair markets, with greater competition, for businesses, consumers and employees. Ensuring Government acts as an effective and intelligent shareholder. BERR's Communications Supply Policy Team focuses on policy, both domestic and international, to embed good security practice within the UK business community.	

Communications-Electronics Security Group (CESG)	
Type of Organization: National Security Actor	Ownership: Public
ENISA Focus Points: CERT, Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: CESG is the information assurance arm of the Government Communications Headquarters (GCHQ) and the Government's National Technical Authority for Information Assurance. GCHQ is an intelligence and security civil service organization reporting to the Foreign Secretary and working closely with MI5 and MI6 intelligence agencies.	
Weblink: http://www.cesg.gov.uk	
Areas of Activity: The CESG is the information assurance (IA) arm of the Government Communications Headquarters (GCHQ) and the government's and the Government's National Technical Authority for IA, responsible for ensuring secure knowledge sharing, which helps customers achieve their aims. The CESG aims to protect and promote the vital interests of the UK by providing advice and assistance on the security of communications and electronic data.	

Central Sponsor for Information Assurance (CSIA)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: In the field of Information Assurance, the CSIA works principally with: CPNI, CESG, BERR, Home Office, SOCA, ICO	
Weblink: http://www.cabinetoffice.gov.uk/csia	
Areas of Activity: The Central Sponsor for Information Assurance (CSIA) is a unit within the UK government's Cabinet Office providing a central focus for Information Assurance (IA) activity across the UK. The CSIA produces and maintains the National Information Assurance Strategy and, along with partner organizations; and coordinates and sponsors work programs to deliver on the strategy's recommendations.	

Center for the Protection of National Infrastructure (CPNI)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, CERT	

Relationships: CPNI is an interdepartmental organization, with resources from a number of government departments and agencies. These include MI5, CESG, and other government departments responsible for national infrastructure sectors. CPNI sponsors research and works in partnership with academia, other government agencies, research institutions, and the private sector.
Weblink: http://www.cpni.gov.uk
Areas of Activity: CPNI was formed in 2007 from the merger of the National Infrastructure Security Coordination Center (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Center (NSAC). CPNI provides integrated (combining information, personnel, and physical) security advice to the businesses and organizations making up the national infrastructure. CPNI runs a CERT service called CSIRTUK for its partners in the private sector who operate elements of the national infrastructure.

Home Office	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: CERT, Resilience, Emerging/Current Risks, e-ID, Development of Security Technology and Standards	
Relationships: None	
Weblink: http://www.homeoffice.gov.uk	
Areas of Activity: The Home Office leads the national effort to protect the public from terrorism, crime, and antisocial behavior. In terms of information security, this is heavily related to terrorism (The Office for Security and Counter-Terrorism, OSCT) and Freedom of Information.	

Serious Organized Crime Agency (SOCA)	
Type of Organization: National Security Actor	Ownership: Public
ENISA Focus Points: Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.soca.gov.uk	
Areas of Activity: The Serious Organized Crime Agency (SOCA) is an executive, non-departmental public body sponsored by, but operationally independent of, the Home Office. The Home Secretary may set SOCA strategic priorities and judge the success of its efforts. Within that framework, SOCA sets its priorities, including how it will exercise the functions given to it by statute, and what performance measures it will adopt.	

Information Commissioner's Office (ICO)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: AR, Implementation of Security Technology and Standards	
Relationships: None	
Weblink: http://www.ico.gov.uk	
Areas of Activity: The ICO is the UK's independent authority to promote access to official information and protect personal information. It enforces the Data Protection Act, the Freedom of Information Act, the Privacy and Electronic Communications Regulations and the Environmental Information Regulations. It maintains the public register of data controllers under the Data Protection Act, approves publication schemes of public authorities under the Freedom of Information Act.	

Defence Science and Technology Laboratory (Dstl)	
Type of Organization: National Government	Ownership: Public
ENISA Focus Points: Resilience, Emerging/Current Risk, Development of Security Technology and Standards	
Relationships: Dstl is an agency of the Ministry of Defence.	
Weblink: http://www.dstl.gov.uk	
Areas of Activity: The Dstl is an agency of the Ministry of Defence, the main objective of which is ensuring the UK Armed Forces and government are supported by world-class scientific advice. Dstl delivers defense research, specialist technical services, and the ability to track global technological developments.	

British Standards Institute (BSI)	
Type of Organization: Technical & Professional Certification Providers	Ownership: Non-profit
ENISA Focus Points: AR, Development of Security Technology and Standards	
Relationships: None	
Weblink: http://www.bsi-global.com	

Areas of Activity:

BSI, the UK's national standards body, certifies management systems and products; provides product testing services; develops private, national and international standards; provides training and information on standards and international trade; and provides performance management software solutions. It specifically addresses information security and IT network security.

London Resilience Partnership

Type of Organization: Regional Government Organization	Ownership: Public

ENISA Focus Points: Resilience, AR, Emerging/Current Risk

Relationships: All major London services team members (including health, fire, ambulance, transport, councils, police force)

Weblink: http://www.londonprepared.gov.uk

Areas of Activity:

Established in 2002 to plan and prepare for potential emergencies, the London Regional Resilience Forum oversees the work of the partnership. It reports directly to the Minister for Local Government, the Minister for London, and the Mayor of London. It consists of several panels which allow partners to focus on particular areas, e.g., transport, faith organizations, utilities, health.

Industry Organizations Active in Network and Information Security

Institute of Information for Security Professionals (IISP)

Type of Organization: Other Industry Association	Ownership: Non-profit

ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards

Relationships: Supported by many companies and government departments including CESG, BERR, CPNI, and SOCA

Weblink: http://www.instisp.org

Areas of Activity:

Sets standards for professionalism in information security. The principal objective is to advance the professionalism of information security practitioners. It offers training, qualifications, and operating practices and also acts as an accreditation authority for the industry.

British Security Industry Association (BSIA)	
Type of Organization: Other Industry Association	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risk	
Relationships: BSIA lobbies key organizations to form valuable working partnerships e.g., Home Office	
Weblink: http://www.bsia.co.uk	
Areas of Activity: The BSIA disseminates information to members, potential members, users of security products/services, related organizations and the general public to raise awareness and understanding of issues relating to security and crime prevention. It draws up industry codes of practice and technical documents which are often considered by the BSI.	

The UK Technology Industry (Intellect)	
Type of Organization: IT Association	Ownership: Non-profit
ENISA Focus Points: Resilience	
Relationships: none	
Weblink: http://www.intellectuk.org	
Areas of Activity: Intellect is the trade association for the UK technology industry. It provides a voice for its members (800 companies ranging from SMEs to multinationals) in both government and business to create a commercial environment. It works in both markets and policy fields including the Data Breach Notification Working Group, the Defense and Security Commercial Council, the Digital Communications Market Group, the Identity Management Working Group, the Security and Privacy Group, and the Security and Resilience Group.	

British Computer Society - Information Security Specialist Group (BCS-ISSG)	
Type of Organization: IT Association	Ownership: Non-profit
ENISA Focus Points: AR, Emerging/Current Risk, Development of Security Technology and Standards	
Relationships: None	
Weblink: http://www.bcs.issg.org.uk	

Areas of Activity: ISSG is a specialist sub-group of BCS. ISSG's objective is to raise awareness of risks to information systems and identify technical and non-technical methods for attaining acceptable levels of security.	
CIFAS	
Type of Organization: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: AR	
Relationships: The Office of Fair Trading (OFT) and the National Consumer Council were involved in establishing CIFAS. CIFAS was also developed in consultation with the Information Commissioner's Office, which continues to consult on major changes. The police have been involved from the outset and have close links with CIFAS.	
Weblink: http://www.cifas.org.uk	
Areas of Activity: The UK's fraud prevention service with 270 members (mainly financial services). Members share data about identified frauds.	
Confederation of British Industry (CBI)	
Type of Organization: Other Industry Association	Ownership: Non-profit
ENISA Focus Points: Development of Security Technology and Standards, Implementation of Security Technology and Standards	
Relationships: Works in collaboration with UK government, international legislators, and policy makers	
Weblink: http://www.cbi.org.uk	
Areas of Activity: The CBI is the most powerful lobbying organization for UK business on national and international issues, working with the UK government, international legislators, and policymakers to help UK businesses compete effectively.	
Telecommunications UK Fraud Forum (TUFF)	
Type of Organization: IT Association	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risk, Development of Security Technology and Standards	
Relationships: Information is shared with MI5 Security Services, Metropolitan Police, SOCA, and CIFAS	

Weblink: http://www.tuff.co.uk	
Areas of Activity: A forum for the exchange of information and the promotion of a united effort against telecommunications fraud.	
Mobile Industry Crime Action Forum (MICAF)	
Type of Organization: Industry Organization	Ownership: Private
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: None	
Weblink: http://www.micaf.co.uk	
Areas of Activity: An organization set up by the United Kingdom mobile telecommunications industry, including mobile handset manufacturers, to address the issues of mobile phone theft. The forum meets regularly to exchange information and agree crime prevention strategies to reduce mobile phone theft and associated activity in the United Kingdom.	
APACS	
Type of Organization: Other Industry Organization	Ownership: Private
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards	
Relationships: APACS has a role in government and EU relations and lobbying takes place on a range of payments-related issues which involve the BERR, HM Treasury, the Home Office, and the European Commission.	
Weblink: http://www.apacs.org.uk	
Areas of Activity: APACS is the UK trade association for payments and for those institutions that deliver payment services to customers. It provides a forum for its members to come together on non-competitive issues relating to the payments industry. Currently, we have 31 members. APACS is the payments industry voice on a wide range of topics and the industry's representative in Europe. APACS forecasts payment trends, conducts market research, carries out lobbying activities, collates industry statistics, and helps develop industry standards and best practices.	
Federation of Communication Services (FCS) – FCS Industry Forum	
Type of Organization: Other Industry Organization	Ownership: Private

ENISA Focus Points: Emerging/Current Risks, e-ID, Development of Security Technology and Standards
Relationships: None
Weblink: http://www.fcs.org.uk
Areas of Activity: FCS is the Trade Association for businesses delivering communications products and services to customers in the UK by radio, mobile, fixed and IP telephony. FCS' mission is to help establish a favorable operating environment for its member organizations and address specific issues.

tScheme	
Type of Organization: Other Industry Organization	Ownership: Non-Profit
ENISA Focus Points: AR, e-ID, Development of Security Technology and Standards, Implementation of Security Technology and Standards.	
Relationships: Participating members include British Chamber of Commerce, CBI, DCSF (Department for Children, Schools, and Families), and CSIA as well as industry.	
Weblink: http://www.tscheme.org	
Areas of Activity: The tScheme initiative became an independent limited company in May 2000. Its members have contributed significant resources to the successful development and implementation of an objective, transparent, proportionate, and non-discriminatory scheme for trust services industry self-regulation, within the context of the EC Directive 1999/93/EC 'Electronic Signatures.'	

Academic Organizations Active in Network and Information Security

The Cyber Security Knowledge Transfer Network (KTN)	
Type of Organization: National Security Actor	Ownership: Non-Profit
ENISA Focus Points: AR, Emerging/Current Risks, e-ID	
Relationships: Works in partnership with the British Computer Society, CSIA, the Get Safe Online campaign, and IISP	
Weblink: http://www.ktn.qinetiq-tim.net	

Areas of Activity:
Aims to be the single Focus point for UK Cyber Security expertise, to collaboratively identify universal challenges and develop effective responses, influence UK investment strategy and government policy, accelerate innovation and education, harness and promote UK capability internationally, and help improve the UK security baseline.

Information Security Group (ISG) at Royal Holloway University of London	
Type of Organization: Universities	Ownership: Public
ENISA Focus Points: N/A	
Relationships: None	
Weblink: http://www.isg.rhul.ac.uk/	
Areas of Activity: The ISG is one of the largest academic security groups in the world. It brings together in a single institution expertise in education, research, and practice in the field of information security. The ISG offers an active research environment. It has a thriving PhD community, and offers world-leading masters degree programs (campus-based and online), as well as postgraduate diploma programs in information security. The ISG also includes the Smart Card Center of Excellence which it founded with Vodafone and Giesecke & Devrient.	

Other Bodies and Organizations Active in Network and Information Security

Information Assurance Advisory Council (IAAC)	
Type of Organization: Other	Ownership: Non-Profit
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: Partners with other major national security agents such as BSIA. The government liaison panel includes CESG, BERR, CSIA, SOCA, CPNI, and the Ministry of Defence	
Weblink: http://www.iaac.org.uk	
Areas of Activity: IAAC's mission is to advance information assurance to ensure the UK information society can count on a robust, resilient, and secure foundation. The IAAC is a partnership that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. It makes policy recommendations to government and corporate leaders at the highest levels. IAAC's sponsors and members comprise leading commercial end users, government policy makers, and the research community. IAAC's aim is to work for the creation of a safe and secure information society.	

Internet Watch Foundation (IWF)	
Type of Organization: Other	Ownership: PPP
ENISA Focus Points: AR, Emerging/Current Risks, Development of Security Technology and Standards	
Relationships: IWF works with numerous UK government bodies to influence initiatives to combat online abuse and this dialog goes beyond the UK and Europe to ensure greater awareness of global issues, trends, and responsibilities	
Weblink: http://www.iwf.org.uk	
Areas of Activity: The IWF is the UK's Internet 'hotline' for public and IT professionals reporting potentially illegal online content. The IWF works in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimize the availability of this content, specifically, child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK.	

Activities

Strategic Initiatives

WARP Initiative
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: AR, Emerging/Current Risks
Weblink: http://www.warp.gov.uk
Description: A community-based service where members can receive and share up-to-date advice on information security threats, incidents, and solutions. The initiative is led by a warning, advice, and reporting point (WARP) operator that understands the information security needs of its members. The operator will filter relevant information, deliver it to the community, and facilitate the sharing of advice and best practices within the community. This will help build trust, thereby encouraging community members to report incidents to each other; these reports may be shared with other WARPs, although the source remains anonymous. WARP is part of the information sharing strategy of the CPNI.

The Aerospace and Defense Manufacturer's Information Exchange (ADMIE)
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: Resilience, AR, Emerging/Current Risks
Weblink: http://www.cpni.gov.uk/Products/information.aspx
Description: The CPNI set up this information exchange so that confidential, mutually beneficial information regarding electronic security threats in the aerospace and defense sector could be shared. The ADMIE comprises UK-based organizations involved in this sector.
The UK Financial Services Information Exchange (FSIE)
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID
Weblink: http://www.cpni.gov.uk/Products/information.aspx
Description: The FSIE was set up to share confidential, mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions in the UK financial sector. FSIE members come from UK-based financial organizations including banking, insurance, securities, service providers, exchanges, and CPNI.
The UK Network Security Information Exchange (UK-NSIE)
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID
Weblink: http://www.cpni.gov.uk/Products/information.aspx

Description: The UK-NSIE was set up to share sensitive information in the information and communications technologies sector. It currently includes IP providers, core mobile operators, traditional telecommunications providers, and the CPNI. Participating companies now represent over 80% of the telecommunications market in the UK. It is linked to NSIE in the United States, of which BT is a member, acting as the channel for information between the two exchanges. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include a guide to the procurement of resilient telecoms and best practice guidance on the secure implementation of Border Gateway Protocol (BGP).
Pharmaceutical Industries Information Exchange (PIIE)
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: Resilience, AR, e-ID
Weblink: http://www.cpni.gov.uk/Products/information.aspx
Description: The PIIE was set up to share confidential, mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions in the pharmaceutical industry. All PIIE members are from global pharmaceutical corporations that have a significant UK interest.
Vendor Security Information Exchange (VSIE)
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: AR, Emerging/Current Risks, Micro-enterprises
Weblink: http://www.cpni.gov.uk/Products/information.aspx
Description: The VSIE was set up to share confidential, mutually beneficial information regarding electronic security threats among the major companies involved in the ICT industry. The VSIE comprises members of major international companies in the ICT sector.
The Security Researchers Information Exchange (SRIE)
Type of Activity: Government Funding Programs
Responsible Organization(s): CPNI
ENISA Focus Points: AR, Emerging/Current Risks, e-ID

Weblink: http://www.cpni.gov.uk/Products/information.aspx

Description:

The SRIE was set up to share confidential, mutually beneficial information regarding electronic security threats in the penetration testing and security research sector. The SRIE comprises of members of UK penetration testing and security research companies.

Research Programs

Next Generation Networks Telecom Services Assurance Project

Type of Activity: Technical Research Program

Responsible Organization(s): CESG

ENISA Focus Points: Resilience, AR, Emerging/Current Risks

Weblink: http://www.cesg.gov.uk/policy_technologies/ngn/index.shtml

Description: The NGN Assurance project has been initiated to design, develop, and implement an independent assurance scheme for telecoms systems and services. The project builds on the Ofcom initiative to support industry adoption of a 'minimum' level for interconnect security. The project covers only the UK and is led by CESG.

UK Biometrics Working Group (BWG)

Type of Activity: Technical Research Program

Responsible Organization(s): CESG / CPNI

ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards

Weblink: http://www.cesg.gov.uk/policy_technologies/biometrics/

Description: The BWG's remit is broad ranging and includes providing general advice on biometric technology and procurement, addressing privacy and human rights issues, directing technical areas such as evaluation and testing, and offering biometric policy advice and security assurance. CESG administers the BWG and leads the security assurance and policy areas. The BWG comprises representatives from government departments, independent biometrics specialists, and other relevant contributors from the UK and elsewhere.

Funding Programs and Financial Initiatives

Get Safe Online

Type of Activity: Government and Private Funding Program (Public Private Partnerships)

Responsible Organization(s): CSIA, BERR, Home Office, CPNI, SOCA

ENISA Focus Points: AR

Weblink: http://www.getsafeonline.co.uk

Description: Get Safe Online is a major public-private sector national initiative aimed at raising awareness of online security. It is largely internet based and is a one-stop-shop for reliable, up-to-date information about online safety, to give home users and small businesses the advice they need to use the Internet safely.

Security and Resilience Group

Type of Activity: Non-Government Funding Programs & Financial Initiatives

Responsible Organization(s): Intellect

ENISA Focus Points: Resilience, AR, Emerging/Current Risks, Development of Security Technology and Standards

Weblink: http://www.intellectuk.org/content/view/3614/47/

Description: Thought leadership, policy consultation, and market/business development, utilizing industry experience and expertise to help policy makers address threats and hazards.

Identity Management Working Group

Type of Activity: Non-Government Funding Programs & Financial Initiatives

Responsible Organization(s): Intellect

ENISA Focus Points: AR, Emerging/Current Risks, e-ID, Development of Security Technology and Standards

Weblink: http://www.intellectuk.org/content/view/409/47/

Description: Provides a channel for government and other stakeholders to exchange views with industry on technology issues as they arise and draw on private-sector expertise in shaping future policy and projects.

ThinkuKnow Campaign
Type of Activity: Social & Other Research Programs
Responsible Organization(s): Child Exploitation and Online Protection Center (CEOP), Police Force, NSPCC
ENISA Focus Points: AR, e-ID
Weblink: http://www.thinkuknow.co.uk
Description: The Child Exploitation and Online Protection (CEOP) Center is dedicated to eradicating the sexual abuse of children. It is part of UK policing and very much about tracking and bringing offenders to account, either directly or in partnership with local and international forces. CEOP compiles intelligence, informs operational deployments, steers CEOP Academy programs to law enforcement, child protection and educational sectors, and drives the campaign's dedicated Thinkuknow program for children and parents of all ages.

Events

Conferences and Workshops	
British Retail Consortium (BRC) – Annual Crime & Loss Prevention Conference 2008: Partners In Crime; Preventing Losses; Protecting Reputations	
Responsible Organization: British Retail Consortium	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks, e-ID	
Target Groups: SMEs, Large Enterprises, Government Organizations	
Weblink: http://www.brc.org.uk/brceventdetails05.asp?id=502	
Description: Annual conference for retail crime and loss prevention specialists.	
RSA European Conference 2008	
Responsible Organization: RSA Conference	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Security Professionals	
Weblink: http://www.rsaconference.com/2008/europe/About_RSA_Conference_Europe_2008.aspx	

Description: The RSA Conference offers enterprise and technical professionals one-stop learning at its events, with targeted classroom sessions, innovative and interactive programs, and provocative keynotes for hundreds of information security professionals. More than 1,300 attendees including virtually every profession involved in information security – 33% team leaders/project managers, 11% VP/directors, 10% technology executives (CIOs, CTOs, CSOs, CISOs), and 8% top executives (CEOs, CFOs, CXOs, presidents, senior VPs).	
Infosecurity Europe 2009	
Responsible Organization: InfoSecurity	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Security Professionals	
Weblink: http://www.infosec.co.uk/	
Description: Targeted at security professionals	
IA Industry Forum 2009	
Responsible Organization: UK Information Assurance Community (IAUK)	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks	
Target Groups: Government Institutions, Security Professionals	
Weblink: http://www.iauk.org.uk/Events/IA-Industry-Forum/	
Description: The government's national information assurance event, hosted by the CESG. This event provides the opportunity for information assurance specialists, department security officers, IT security officers, and communications specialists across HMG to see a live demonstration of the latest in secure wireless communications technology and to understand how this capability will be delivered through collaborative government efforts.	
Annual UK Biometrics Exhibition and Conference	
Responsible Organization: Elsevier, publisher of multiple security magazines	Frequency: Annual
ENISA Focus Points: AR, Emerging/Current Risks, e-ID	
Target Groups: Large Enterprises, Security Professionals, SMEs	
Weblink: http://www.biometrics.elsevier.com/	

Description: The annual conferences considers how biometric technology such as fingerprint, facial and iris recognition, is being used to identify individuals – from large-scale government projects such as the national ID card scheme, to law enforcement and border control, to physical and logical access control in the workplace. Sponsored by Intellect.
Intellect Security and Resilience Conference and Dinner 2008
Responsible Organization: Intellect — Frequency: Annual
ENISA Focus Points: Resilience, AR, Emerging/Current Risks
Target Groups: Government Institutions, SMEs, Large Enterprises, Educational and Research Organizations, Security Professionals
Weblink: http://www.intellectuk.org/index.php?option=com_events&task=view_detail&agid=351
Description: Intellect's second annual Security and Resilience conference will examine, from both customer and supplier perspectives, how the wide range of stakeholders in this critical market can better work together.
Intellect Identity and Information Conference 2008
Responsible Organization: Intellect — Frequency: Annual
ENISA Focus Points: Resilience, AR, Emerging/Current Risks, e-ID
Target Groups: Government Institutions, SMEs, Large Enterprises, Educational and Research Organizations, Security Professionals
Weblink: http://www.intellectuk.org
Description: Intellect's sixth annual event, focusing on identity management and information, will provide delegates with the chance to better understand the identity and information assurance environment and the role of information in enabling better public services, and an understanding of how organizations can work more effectively together to deliver enhanced solutions to both government and citizens.

Current Trends in Data Breaches

The fieldwork and data collection phase revealed no NIS trends specific to particular countries; however, some common NIS trends across all countries were identified. The strength of these trends varies in each country, and they are often driven either by the evolution of specific technologies (e.g., increased adoption of mobile devices) or by common policies (e.g. the adoption of EU guidelines).

Nevertheless, inconsistent statistics for most countries analyzed in this study and a lack of a common approach in measuring the specific adoption and evolution of NIS make the evaluation of the abovementioned NIS trends problematic in terms of validation via quantitative data.

For the purposes of this study, one specific NIS trend has been identified and analyzed, namely recent security breaches.

Information security breaches are happening with increasing frequency throughout Europe. Data breaches can happen for numerous reasons, among which are the loss/theft of equipment on which the data is stored, human error, equipment failure, unforeseen disasters (fire, flooding, and other natural calamities), hacking, and – of ever increasing concern – the unauthorized use of data/information (often of a highly sensitive nature) due to inadequate access control.

In the preceding 12 months, there were no fewer than 20 data security breaches in the United Kingdom:

1. In November 2007, HMRC lost two CDs containing the details of 25 million individuals. The CDs are assumed to have been lost while in transit to the National Audit Office. Soon after the loss occurred, it was revealed that sensitive information, such as bank details, was supposed to have been stripped out of the databases on the discs before they were sent to the National Audit Office. It had, however, been left on the discs because of the extra costs that stripping the information would have incurred.

   http://news.zdnet.co.uk/security/0,1000000189,39397478,00.htm

   http://www.mofo.com/news/updates/bulletins/13904.html

   http://news.digitaltrends.com/news-article/14886/massive-uk-data-breach-by-the-government

2. In January 2008, the ICO issued an enforcement notice against Marks & Spencer for its failure to encrypt customer data contained on a company laptop and to notify its customers following the theft of that laptop. The laptop, stolen from the managing director of a pension plan provider, contained data relating to 26,000 pension plan participants.

http://www.mofo.com/news/updates/bulletins/13904.html

3. In June 2008, Virgin Media lost an unencrypted CD containing the bank details of 3,000 customers. Virgin Media, which alerted the Information Commissioner's Office (ICO) to the problem, was ordered by the ICO to encrypt all portable and mobile devices that store and transmit personal information.

   http://www.cio.co.uk/concern/compliance/news/index.cfm?articleid=3202&pagtype=allchandate

4. The Web site of UK retailer Cotton Traders was hacked for credit card details and addresses of thousands of customers. Cotton Traders, which discovered the attack in January, reported the incident to Barclaycard and most cards were stopped. The retailer says all customer credit card data is encrypted on its Web site. The BBC has reported that up to 38,000 customers are affected by the breach, but the retailer dismisses the figure as "widely inaccurate."

   http://www.finextra.com/fullstory.asp?id=18568

5. The Home Office has lost the names, nationalities, passport numbers, and dates of birth of 3,000 seasonal agricultural workers on two CDs in transit to the UK Borders Authority.

   http://news.zdnet.co.uk/leader/0,1000002982,39485540,00.htm

6. The Ministry of Justice reported nine data-breach incidents, affecting around 45,000 people, to the ICO during the last financial year. The incident affecting the most people, reported in the Ministry's 2007-08 resource accounts, took place in June 2007. Discs containing 27,000 supplier records, including supplier names, addresses and, in some cases, bank details, were in the possession of a contractor to the Ministry.

   http://news.zdnet.co.uk/security/0,1000000189,39462444,00.htm

7. In August 2008, Britain's biggest credit card company sent out the wrong account details to thousands of customers. More than 17,000 Barclaycard Goldfish credit card holders received account statements containing personal information relating to other customers. Compromised information included the stranger's name, card number and previous transactions.

   http://www.thisismoney.co.uk/news/article.html?in_article_id=450424&in_page_id=2&in_a_source=&position=moretopstories

8. In August 2008, the personal information on thousands of criminals in England and Wales was lost on a USB drive. Although the data had been encrypted in a database, it was not encrypted when moved to the mobile storage device. The unencrypted details were lost by a private firm, PA Consulting, during what it termed "processing." The data includes information on approximately 10,000 offenders, as well as the names, birth dates and some release information of all 84,000 prisoners in England and Wales – and a further 33,000 records from the police national computer.

   http://www.scmagazineus.com/Every-prisoner-in-UK-victim-of-data breach/article/115796/

9. In August 2008, a server was bought on eBay for just over £35 by Andrew Chapman, an IT manager from Oxford. Chapman told ZDNet.co.uk that the server, a network attached storage (NAS) box, contained unencrypted backups of CDs. The computer had been used by the data archiving firm Graphic Data to store the details on behalf of RBS, of which NatWest is a subsidiary. Details included names, addresses, bank account numbers, telephone numbers, and customer signatures. RBS said on Tuesday that it was in the process of investigating the incident.

   http://news.zdnet.co.uk/security/0,1000000189,39465455,00.htm

10. In September 2008, reports surfaced of a data breach affecting up to 5,000 prison staff, whose details were on a hard disk lost by contractor EDS two months earlier.

    http://news.zdnet.co.uk/leader/0,1000002982,39485540,00.htm

11. On 22 July, payroll details were lost while in transit between the salaries and wages department of Whittington Hospital NHS Trust and the payroll company McKesson, where they were to be stored. The details lost on the 17,990 NHS staff included the names, dates of birth, national insurance numbers, start dates, pay details and sickness dates of all staff members who have worked at Whittington Hospital NHS Trust, Camden Primary Care Trust (PCT), Islington PCT, and Camden and Islington NHS Foundation Trust since April 2001. Included in the lost data relating to the financial year 2007–08 were the addresses of 587 Whittington Hospital NHS Trust staff, 2,303 Camden and Islington NHS Foundation Trust, 1,458 Camden PCT staff, and 1,050 Islington PCT staff.

    http://news.zdnet.co.uk/security/0,1000000189,39489341,00.htm

12. In September 2008, four laptop computers were stolen from the government agency that oversees bankrupt companies. The agency, the Insolvency Service, reported one of the laptops contained personal information about former directors of 122 bankrupt companies, as well as information on creditors and company employees. The laptops were stolen from the Insolvency Service's office in Manchester.

http://www.nytimes.com/2008/09/18/world/europe/18briefs-4GOVERNMENTL_BRF.html

13. In September 2008, names and email addresses on a BBC mailing list were exploited by hackers to send "spam" offering the anti-impotence drugs Viagra and Cialis. Anyone who replied to the sender could have been targeted with scams or computer viruses. The spam email offered the sex drugs at "US$1.49 per pill," but such advertisements are often a front for identity fraudsters attempting to glean financial information from their victims.

    http://www.telegraph.co.uk/news/uknews/3022523/BBC-customers-deluged-by-spam-after-hackers-break-into-mailing-list.html

14. In October 2008, a hard disk drive was lost by the firm EDS that contained sensitive information on approximately 100,000 armed forces personnel, plus 600,000 potential recruits. The Ministry of Defense confirmed to ZDNet.co.uk on Friday that a hard disk had been lost by EDS, but would not confirm that the removable hard disk contained personal information. EDS told ZDNet.co.uk that the disk was being held in a secure location in premises in Hampshire when it went missing, but was unable to say exactly what data was on the drive. Under standard EDS procedures, the disk would not have been encrypted.

    http://news.zdnet.co.uk/security/0,1000000189,39508658,00.htm

15. In October 2008, the *Wall Street Journal* reported that European law-enforcement officials had uncovered a highly sophisticated credit-card fraud ring funneling account data to Pakistan from hundreds of grocery-store card machines across Europe, according to U.S. intelligence officials. Specialists say the theft technology is the most advanced they have seen, and a person close to British law enforcement said it has affected big retailers including a British unit of Wal-Mart Stores Inc. and Tesco Ltd.

    http://www.privacydigest.com/2008/10/11/fraud+ring+funnels+data+cards+pakistan

Definition and Sources

Digital Literacy Indicator: The indicator for Digital Literacy considers the percentage of the entire population which possesses medium or high skills on a defined set of Internet activities such as:

- Using a search engine to find information
- Sending an email with files attached
- Posting a message to chat rooms, newsgroups or online discussion forums
- Using the Internet to make phone calls
- Using peer-to-peer file sharing to exchange multimedia content
- Creating a Web page

People, which are able to perform at least 3 or 4 of the abovementioned activities are considered to have medium Internet skills and the one able to perform on a minimum of 5 or 6 activities are considered possessing high Internet skills.
(Source: Eurostat, Household ICT Survey, 2007)

E-commerce Indicator: represents the percentage of individuals who ordered goods or services, over the Internet, for private use, in the last 3 months
(Source: Eurostat, Eurobarometer e-commerce, 2008)

Broadband penetration Indicator: number of total subscriptions to broadband connections (households, enterprises, public sector) by platform (DSL, all others) divided by the number of inhabitants. 3G subscriptions are not included in the total. *(Source: European Commission ,Preparing Europe's digital future - i2010 Mid-Term Review, April 2008)*

Activities: Only activities with at least a component of the following eight ENISA Focus Points have been taken into account:

- CERT
- Resilience
- Awareness Raising (AR)
- Emerging Risks/Current Risks
- Micro-enterprises
- e-ID
- Development of Security, Technology and Standards Policy
- Implementation of Security, Technology and Standards

Only activities taking place at a national level or of national importance, ongoing or completed recently (in 2008) have been taken into consideration.

Events: Only events with a prime focus or with a major component of at least one of the eight ENISA Focus Points have been taken into account.

One-off Conferences and Workshops are excluded; within this Category only regular events significant at a national level in terms of size or importance have been included, i.e. if the event has already taken place at least twice and will be repeated in the future, or if it has taken place once and the next event has already been planned.