enisa
European Network
and Information
Security Agency

General Report 2007

European Network and Information Security Agency

ENISA – NIS is people

Networks, people and technology

In the 21st century, we take for granted innovations such as mobile phones, computers, the Internet, online banking, e-Health and e-Commerce. The Internet has become indispensable for individuals at work, at home and in doing business. **Network and Information Security (NIS)** is therefore crucial for businesses and home-users alike.

NIS – for Europe's economy

Communication networks and information systems are critical for the European digital economy and business – both today and increasingly for tomorrow. There are millions of e-mails and transactions every day. As networks grow more complex, they also become more vulnerable. Security breaches can generate substantial economic damage. The European Network and Information Security Agency (ENISA) is the European Union (EU)'s response to NIS challenges, especially as they affect the EU's economy.

Expertise and excellence in NIS

ENISA's role is to be an expert body and a Centre of Excellence in NIS. Its mission is to facilitate and support the Members States in enhancing the level of NIS in Europe.

As such, the Agency's role includes:

- Giving **independent, expert advice** to the EU, as the first step towards the drafting of legislation
- **Responding to request**s from Member States and the EU
- **Collecting and analysing** data on security incidents and emerging risks
- Promoting **best practices in e.g. risk assessment & risk management, awareness raising and computer security incident response**

General Report 2007
European Network and Information Security Agency

ISSN: 1830-981X

Europe Direct is a service to help you find answers to your questions about the European Union

***Freephone number:**

00 800 6 7 8 9 10 11

*Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

Editing and design by Kingston Public Relations Ltd., UK (+44 1482 876229) www.kingstonpr.com
Published in July 2008

Luxembourg: Office for Official Publications of the European Communities, 2008

ISBN: 978-92-9204-004-8

ISSN: 1830-981X

Catalogue no.: TP-AB-08-001-EN-C

© European Communities and ENISA, 2008
Reproduction is authorised provided the source is acknowledged.

PRINTED ON WHITE CHLORINE-FREE PAPER

ENISA General Report 2007

Table of Contents

CHAPTER 1
Introduction

- Executive Summary
- A Message from the Executive Director

Executive Summary

2007 posed considerable challenges for Europe with regard to network and information security (NIS). In particular, the cyber attack on Estonia in June generated public and media attention, but several other countries, including Sweden, France and Germany, also suffered major NIS incidents which were widely publicised. The attention which these NIS attacks have attracted has pushed NIS up on the political agenda. ENISA's mission and operations, facilitating co-operation and offering support and advice to the European Union (EU) Member States in their efforts to build protective fences and to implement countermeasures, have become more widely recognised.

In the 21st century, virtually all aspects of everyday life are dominated by information systems, in the form of practical devices and services such as mobile phones, computers, online banking, e-Health and e-Commerce. The Internet has become indispensable for industry and individuals, at work and at home. The European economy, be it corporations or individuals, is highly reliant on NIS for the proper functioning of the Internal Market. Information systems and secure networks in the Information Society have, in that sense, become omnipresent. ENISA's mission in NIS is therefore one of considerable importance for the economy of Europe.

ENISA is an EU Agency, which assists and facilitates the EU and its Member States in their efforts to make networks and information systems more secure. By acting as a forum for the exchange of information for all stakeholders, and by increasing co-operation in NIS, the Agency supports the functioning of the Internal Market. ENISA acts to bridge NIS gaps, for example between policy-makers and technical communities, both in the public and the private sectors. To this purpose, the Agency supports a public-private dialogue regarding responsibilities, roles, problems and solutions to NIS risks and threats. The major NIS challenges facing Europe are common to NIS policy-makers globally. ENISA therefore aims to support Europe's policy-makers in giving Europe a leading role internationally in NIS issues. Consequently, European NIS policy-makers are increasingly convinced of the need for enhanced NIS co-operation in Europe.

The ENISA Work Programme for 2007 focused on the following five priorities, to match and optimise the Agency's available resources:

- Raising awareness and building confidence
- Facilitating the working of the Internal Market for e-Communication
- Mastering emerging technology and services
- Bridging security gaps in Europe in electronic identification (eID), authentication languages, Computer Emergency Response Teams (CERTs)
- Increasing communication and outreach activities.

In 2007 ENISA published a number of important Position Papers on topics that have been identified as significant emerging risks or key security components, notably Social Networking, Botnets and Reputation Based Systems. These reports provide an introduction to security issues in specific areas, highlight the most important threats and make recommendations for action and best practices to reduce the security risks to users. They have received high level, general media attention.

Activities in pursuit of the five goals in the Work Programme were numerous but highlights include a report on the effectiveness of awareness raising campaigns with the aim of identifying best practice, together with a workshop to disseminate the results, a survey of measures taken by Electronic Communication Service Providers to combat spam, the updating of ENISA's inventory of risk assessment and risk management methods and an analysis of the various types of home-users and their perceptions of the Internet and IT security, in order to better target them with NIS information.

The Agency is committed to being the leading European body for the provision of NIS data, reports, information and knowledge to NIS policy-makers, in short, a Centre of Excellence, and completed all the reports and projects laid down in its Work Programme. ENISA has also been well recognised for its advisory role, demonstrated by the number of requests for assistance or advice that it received from the Commission, Member States and EU bodies. In 2007 examples included major studies into the feasibility of a European Information Sharing and Alert System (EISAS) and the establishment of a Data Collection Framework. These requests are in themselves a recognition of the value which the Agency adds.

Throughout 2007 ENISA's Experts spread the word about its operations and findings around Europe through seminars, conferences and workshops, and international media have reported the Agency's activities and achievements. ENISA has also enhanced its outreach and communication, for example by upgrading its website, co-organising and participating in conferences and events all over Europe, and through its *ENISA Quarterly* magazine which provides a forum for European debate on NIS. By drawing on policy effectiveness studies and best practices across Europe, member countries can more swiftly take advantage of lessons learned in implementing NIS policies. ENISA thus acts as a 'clearing house' to disseminate the shared knowledge of Europe.

During 2007, a new process was established for drawing up the Agency's Work Programme, based on a closer consultation process and involving all stakeholders to jointly identify the priorities for ENISA's operations. In this way, the Agency is ensuring that its activities directly meet the needs of users.

As ENISA nears the end of its first mandate period in 2009, it will of course undergo changes. A 'stocktaking' evaluation of the Agency's activities featured as an important process in 2007, with strategic discussions regarding future development. In its first three years of operation, ENISA has carved out a crucial position for itself in European NIS and it is now well placed to respond to the challenges to come.

A Message from the Executive Director

Ambition and change

If 2006 was a year of consolidation, 2007 has been dominated by the need to meet a number of ambitious challenges. The Agency has further stepped up its operations and is functioning effectively as a Centre of Excellence in the field of Network and Information Security (NIS).

The main focus of this General Report is to briefly present the operational tasks and activities undertaken by ENISA in 2007. I am delighted to invite you to take a closer look on the following pages at the activities, reports and studies undertaken, all of which were completed within the deadlines set out in the Work Programme for 2007.

José Manuel Barroso

To sum up this year, ENISA is becoming an increasingly recognised European partner and an important player in NIS. As such, we have now established relations with all major European NIS stakeholders, in this way better positioning ENISA at their service, as a 'think tank' and 'broker' in NIS. ENISA is well established in Heraklion, Crete, which is in line with the EU's ambition to have Agencies distributed throughout the Member States, in the words of EU President Barroso, "from Stockholm to Crete and from Lisbon to Warsaw".

The need for NIS is moving more and more into the media limelight, and thus is also becoming better understood by ordinary citizens and businesses in Europe. The interconnected information networks touch upon fundamental areas of the economy and society. As a result, publication of the ENISA Position Papers was noted not only in specialist NIS media, but also in prominent general publications such as *Le Monde*, the *International Herald Tribune*, *Der Spiegel* and *Fokus*, to mention just a few.

Europe is now confronting a series of NIS issues that require actions across a number of sectors, and co-operation between both private actors and governments. The European capacity in and approach to NIS has traditionally been fragmented, suffering from a diversity of, for example, systems, organisation, system architecture and technical implementations. This annual report shows that the approach of ENISA, Member States and the European Commission which supports closer co-operation, collaboration and co-ordination, while at the same time respecting the fundamental national differences, is vital for more secure information systems and networks across Europe.

New developments

A notable development since the beginning of the year was the welcoming of new members to the European NIS family and to the Management Board, with Romania and Bulgaria smoothly joining the European Union on 1 January 2007.

Looking ahead, ENISA's Work Programme for 2008 sets the compass direction for the Agency's continued operations. The Agency will concentrate its operational activities on a few Multi-annual Thematic Programmes (MTPs), which focus on:

1. Improving resilience in public European e-Communication networks

2. Developing and maintaining co-operation models

3. Identifying emerging risks for creating trust

and finally entails a 'Preparatory Action' regarding the NIS needs and expectations of micro-enterprises.

By applying these MTPs, our goal is to build on synergies and increase our impact in the Member States.

With these priorities set and NIS increasingly being highlighted on the public agenda, the Agency anticipates that the need for NIS will be a decisive political and economic factor for the EU and its Member States in the foreseeable future.

Our valued supporters

ENISA could not fulfil its role as the leading European body committed to providing NIS information to policy-makers in the public and private sectors without the active support and collaboration of the Member States, the EU institutions, industry, research/ academia and consumer/user organisations.

Therefore, as Executive Director, it has been a pleasure to witness the Member States' endorsement of the Agency by their actions. ENISA is dependent on a close dialogue and partnership with all the key players to function as a Centre of Excellence in NIS. The contributions from within the Member States and close partnership with them is thus crucial for our mission. I would therefore like to express my deep appreciation to all our stakeholders, in particular the European Commission, the European Parliament, ENISA's Management Board, our Permanent Stakeholders' Group, members of our Working Groups, the National Liaison Officers, the Greek government and the local authorities in Crete and, last but not least, FORTH, the research centre in Crete that hosts and supports ENISA.

Finally, I would like to thank the ENISA staff for their excellent execution of the Agency's Work Programme.

Please enjoy this General Report, which provides a concise overview of ENISA's work in 2007 and our role and responsibility in network and information security for Europe.

Andrea Pirotti
Executive Director

CHAPTER 2
The 2007 Work Programme: Key Security Themes

- Raising awareness and building confidence
- Facilitating the working of the Internal Market for e-Communication
- Mastering emerging technology and services
- Bridging security gaps in Europe

The 2007 Work Programme: Key Security Themes

The Agency's work in 2007 built on results obtained in 2005 and 2006, categorised into four themes derived directly from the seminal joint workshop discussions between ENISA's Permanent Stakeholders' Group (PSG) and the Management Board in London in June 2006. These themes represent crucial network and information security (NIS) objectives for the whole of Europe:

- **Raising awareness and building confidence** – This area of work is mainly user-oriented, with the aim of improving the safety of network and information security by encouraging the use of appropriate tools and behaviour. In this way, the Agency helps to build the trust that is essential for the acceptance of new technology and the growth of the digital economy.

- **Facilitating the working of the Internal Market for e-Communication** – This objective is oriented mainly towards the needs of business and includes the identification of obstacles to the growth of e-Commerce and assisting the EU to decide on an appropriate mix of regulation and other measures in response to NIS risks. It is in line with the aims of the European Commission's (EC's) i2010 initiative. ENISA's expertise and advice on these matters is considered crucial in achieving the goals laid down in the initiative.

- **Mastering emerging technology and services** – This technology-oriented task includes not only assessing the impact that emerging technology and services have on security and privacy but also enabling Europe as a competitive supplier of network and information products and services.

- **Bridging security gaps in Europe** – Bridging the gaps in the design and implementation of security tools and procedures throughout Europe remains a strong policy-oriented challenge. More precise Europe-wide capacity to measure the current NIS status will be needed. ENISA will help to analyse such gaps, propose ways to reduce them and will monitor their evolution.

ENISA's expertise and knowledge are constantly enhanced and adapted in order to achieve its goals in the most effective way.

Raising Awareness and Building Confidence

Raising awareness and building the confidence of users of electronic communications is widely recognised as a key element for improving the level of information security in Europe. In 2007, ENISA continued its work promoting awareness raising methods and content, disseminating best practices and promoting security certification schemes. There was a particular focus on countermeasures to combat the threat of spam as an important tool in raising users' confidence.

During 2007 the Awareness Raising section analysed security awareness practices and the metrics that are available to measure awareness, drawing on experiences in the Member States and focusing on case studies of local government and Internet Service Providers (ISPs). In doing this, ENISA is contributing to the development of a culture of network and information security.

Recent work in this area has focussed, among other things, on what governments and private companies are currently doing to assess the impact and success of awareness raising activities, on how these metrics and indicators can benefit organisations, and on how information security awareness programmes have been undertaken by government (national and/or local) in an effort to reach out to ISPs within the Member countries.

Identifying and Promoting Key Performance Indicators (KPIs) for Awareness Raising Campaigns

At the end of 2005, a review of some aspects of the effectiveness of awareness raising initiatives highlighted a need for a more strategic approach to ensure that campaign results are properly measured and evaluated. Until now, this had received only minimal attention in most European countries, which has limited the effectiveness of campaign planning. In 2007 ENISA aimed to improve the effectiveness and efficiency of awareness raising initiatives and, more specifically, to promote the importance of using metrics and indicators.

The challenge for the Member States is to ensure that the effectiveness of any initiative intended to raise information security awareness is assessed. ENISA helps the Member States to understand the importance of using metrics and key performance indicators, illustrating the benefits of such activity.

During 2007, ENISA's Awareness Raising Section undertook a study to explore the methods used (both qualitative and quantitative) to measure the performance and success of awareness raising campaigns. The work involved an analysis of case studies, particularly of practices adopted in local government and by Internet Service Providers (ISPs).

The results were published in July 2007, as *Information Security Awareness Initiatives: Current Practice and the Measurement of Success* – the first major report offering a perspective on what governments and private companies are doing currently to assess the impact and success of awareness raising activities. This report is intended for professionals within organisations and public bodies who are responsible for the planning, organisation and delivery of information security awareness initiatives.

The publication focuses on cultural change, the benefits offered by sets of metrics and key performance indicators, and how the assessment of qualitative and quantitative methods can contribute to the development of a wider culture of security. By gathering information on the current practices of a number of European government departments and companies, ENISA has been able to:

- Provide an outline analysis of recommended security awareness practice and metrics to measure awareness
- Provide an outline of key metrics that can be used to effectively assess awareness, as well as some high level metrics
- Provide an overview of current practices with regard to information security awareness
- Provide case studies of good practice for awareness raising and the measurement of its effectiveness, highlighting the benefits thereof, and
- Contribute to the development of an information security culture in Member States by encouraging organisations to act responsibly and thus operate more securely.

The publication is now available in all official languages of the European Union.

Information security awareness initiatives:
Current practice and the measurement of success
July 2007

enisa
European Network and Information Security Agency

The research was carried out from May to July 2007 using a structured questionnaire. This was made available on a self-select basis to people responsible for information security in European government departments and companies. In total, 67 organisations headquartered in nine different European countries responded. This report, therefore, gives a comprehensive overview of what European organisations are doing currently to measure and improve information security awareness. Case studies based on interviews conducted with 12 organisations are included in the report.

Identifying Best Practices, Current Trends and Progress in Awareness Raising – Local Government and Internet Service Providers

Since its inception, ENISA has produced several documents providing details of information security awareness raising initiatives conducted in the Member States. These offer insight into the types of problems being faced by different kinds of users, as well as guidelines and possible solutions. In 2007, the Agency gathered new information on current trends and progress in this area, including a detailed inventory of initiatives focusing on additional target groups: local governments and ISPs.

ENISA examined the information security initiatives undertaken by governments (national and/or local) with an outreach to ISPs. Data were gathered on good practices, techniques, strategies and lessons learned, and the results were published as *Information Security Awareness: Local Government and Internet Service Providers.*

This report:

- Analyses and helps monitor the progress made in national approaches to awareness raising
- Provides an inventory of good practices from the Member States and other organisations
- Provides good practice guidelines that can be customised and presented to the Member States to help facilitate their work on awareness raising
- Identifies and promotes the exchange of good practices and fosters synergy between public and private sector initiatives
- Contributes to the development of an information security culture in the Member States.

The publication also contains good practice guidelines, comprising recommendations, checklists and a roadmap, that can be customised in the Member States to facilitate their work on awareness raising.

The study found that local government and ISPs regard information security as a high priority, as their level of knowledge of the subject is generally either limited or low. It also highlighted the fact that most of the organisations and public bodies plan, organise and deliver information security awareness initiatives for a period of at least 12 months. In particular, within local government organisations, information security awareness raising activities are often part of a larger Information and Communication Technologies (ICT) campaign. Furthermore, training is considered the most effective technique for awareness raising: setting out comprehensive computer-based training plans and communication tools can help employees to ensure the effectiveness of security programmes. Finally, the analysis of European initiatives found that public-private partnerships can be a highly effective means of delivering campaigns, especially if each organisation involved uses its respective strengths and mobilises appropriate resources.

It was also clear from the findings that ENISA, the Member States and stakeholder organisations must continue their efforts to influence the public's behaviour towards information security in a positive way, changing the mindset of the human element in order to achieve greater self-awareness.

This publication is now available in all official languages of the European Union.

Dissemination – a Key Factor in Raising Awareness

Disseminating its findings and facilitating discussions and the exchange of knowledge and good practice are crucial aspects of ENISA's work. A dissemination strategy was developed in 2007. As a result, and in order to allow ENISA to promote its material faster and more effectively, supporting citizens with the skills needed in the Information Society, an important step in 2007 was the release in different languages of ENISA's widely read publication, *A Users' Guide: How to Raise Information Security Awareness.* More than 2000 copies of awareness publications were given out. A survey assessing the quality and impact of reports was also distributed.

The Awareness Raising Section is strengthening its relationship with the Member States through collaborative efforts, regular dialogue and the exchange of good practices. The Section organised monthly conference calls in 2007 to promote regular discussion and knowledge-sharing among experts working on raising information security awareness.

In the course of the year, the Awareness Raising Section released a unique edition containing all of its 2006 publications and incorporating its main findings.

The 3rd Awareness Raising Dissemination Workshop

Finally, ENISA sought to disseminate its findings by organising a workshop. The 3rd Awareness Raising Dissemination Workshop, held in Lisbon in September 2007 under the aegis of the Portuguese Management Board members, brought together professionals responsible for or involved in awareness raising activities in different countries. Through a combination of presentations, case studies and panel debates, participants explored cutting-edge topics, key issues and emerging good practices in awareness raising. Particular attention was paid to private-public partnerships, recent and successful initiatives of ISPs, mobile operators and banks. Participants also identified key next steps.

The Agency will track progress on these issues in 2008 and beyond.

Knowledgebase

In 2006, ENISA collected, analysed, stored and made available a number of best practices on information security, particularly information security policies, through its 'Knowledgebase'. This was made available to all kinds of users to disseminate best practices to the widest possible extent, thus strengthening confidence in ICT systems. The database is stored centrally, but can be shared and reused by others. In 2007 ENISA sought to extend this work by customising the database for more specific audiences.

The Agency has tested several commercial policy management tools and assessed their functionality. A dynamic area with several new products coming onto the market, policy management tools enable organisations to define complex policies and, in certain cases, to deploy or enforce them remotely. However, most of these tools are comparatively expensive and therefore unsuitable for small or medium-sized enterprises.

To enable a broader range of organisations to employ such a tool, ENISA had transformed a document management tool into a simple security policy management tool. The tool was tested in 2007 by a medium-sized organisation for its functionality, and improvements were made. ENISA now intends to make this tool available over the Internet to a wider audience. This will enable organisations to insert security policies into the tool, combine existing policies and develop new, complex ones. A simple user manual and a series of examples will help users to deploy the tool quickly.

Assessment of Information Security Certification

The availability of accreditation and certification schemes can contribute to the trustworthiness of electronic products and services by raising the level of security. Certification is an important factor in creating confidence in users of electronic communication tools, and the use of certificates is often a good indicator of the level of security achieved. In an effort to improve the knowledge, skills and confidence of users, especially non-experts, the Agency has been working to promote certification schemes.

ENISA has made an assessment of the need to facilitate the functioning and accessibility of accreditation and certification schemes and how this could be done in co-operation with the relevant standardisation bodies. This work included consideration of management system certification as well as product certification and the certification of an individual's IT security knowledge. The Agency brought together organisations that are active in the field of information security certifications to present and discuss their schemes, and identified the commonalities and differences between them. This was achieved through a mailing list and online collaboration platform, about a dozen position papers, a questionnaire-based survey collecting answers from 30 certification experts and finally a workshop held in November 2006 with more than 20 contributions.

The findings were analysed during 2007. The results demonstrate that certification schemes can actually improve the ability of organisations to address the security of IT systems, products, services and networks. Certified companies are not immune to NIS risks and threats. However, they seem to be fully aware of the problems and quite well prepared to address them. Certified organisations have developed a systematic approach to deal with risks and have established the necessary processes to manage possible NIS breaches. Their personnel are well trained and informed about what needs to be done during a period of NIS breach. Another important factor is management's engagement and commitment. Prevention pays, and certification is actually a way to ensure that organisations employ appropriate prevention mechanisms.

Other findings of this analysis concentrated on the use of certain NIS-related standards and certification schemes, such as the Common Criteria and ISO 27001. Both standards are quite widely accepted and used extensively by the certification industry and other organisations. Despite criticisms that they are rather generic, such schemes have proved suitable for the needs of organisations and professionals. If Common Criteria become mandatory in different Member States, then it would be worth analysing the mutual recognition of Common Criteria in all Member States. A mutually agreed scheme might contribute significantly to the widespread adoption of the scheme by the market and organisations.

Finally, strengthening accreditation schemes related to people's IT security certification, as well as more systematic reference to recognised standards, might significantly improve the ability of professionals to deal with NIS-related issues. Pan European IT certification schemes (such as the European Computer Driving Licence, ECDL) should pay more attention to NIS issues and develop specialised courses for IT professionals. Additionally, it was suggested that European academic institutions and research bodies should co-operate to reinforce the bridges between education (schools and universities) and the certification industry (private training and certificate providers).

Surveying Electronic Communication Security Measures

Security and Anti-Spam Measures of Electronic Communication Service Providers

Providers of electronic communication services are a vital element of the security chain when individual users and enterprises connect to the Internet. In 2007 ENISA conducted a study into the measures service providers take to secure their services and to combat spam. This was the second year that ENISA had conducted such a survey[1]. The study was based on 30 very detailed replies to a questionnaire circulated to providers in 19 different countries, mainly in Europe. The observations, facts, trends analysis and comments produced as a result of these replies have been grouped under two main themes: security measures and anti-spam measures. These themes have then been subdivided into organisational and technical aspects.

[1] The previous studies can be downloaded from: www.enisa.europa.eu/pages/spam/index.htm

Some of the findings of this study include an increase in training or awareness campaigns by providers, more efforts on Business Contingency (BC) and/or Disaster Recovery plans (DR) and the wide adoption of ingress filtering. Regarding anti-spam measures, providers deploy more than five different anti-spam best practice methods.

Findings of the study

Security

Organisational aspects: Nowadays almost every provider publishes contact details to report security violations and e-mail abuse. Nearly half of the providers who responded provide training or awareness campaigns. Two-thirds of the providers have either a BC or a DR. Implementation of these measures has increased since 2006. There are two interesting changes from last year's study results as to how Internet Service Providers (ISPs) ensure an appropriate level of security. Firstly, there has been a huge increase (from 38% to 65%) in the extent to which providers follow the guidance contained in national legislation. This has been paralleled by a notable reduction in the percentage which follow the guidance laid down in international standards, which has dropped from 46% to 35%. ENISA encourages providers to be involved in information-sharing by joining providers' associations or working groups and by attending and presenting at security conferences so that they become better informed about new trends and best practices.

Technical aspects: Basic ingress filtering is applied by every provider. Basic egress filtering is now widely deployed, with nearly 90% of providers saying they deploy it. This has nearly doubled since 2006, when it was only used by 46% of the providers. ENISA welcomes this development which illustrates that providers are investing resources in the interest of the whole community. Last year, providers relied mainly on complaints from customers or other providers to detect anomalies. It was a reactive process. This year the decrease in tracking complaints and the increase in monitoring traffic peaks could be seen as a move from purely reactive behaviour to integrate more proactive initiatives.

Anti-spam

Organisational aspects: About 73% of all providers process abuse reports manually. Almost half of the providers contact an ISP directly when receiving spam from that network. Different laws, time zones and languages make communications complex for providers seeking to combat spam. ENISA supports the SpotSpam project which aims to collect and share information about spam and helps mitigate the problem by acting as an intermediary.

Technical aspects: On average, providers combine five different anti-spam methods. Although the best practice recommended by all providers' associations is to manage port 25, only 50% of the providers do so. ENISA is convinced that applying best practices will significantly reduce the amount of spam both sent and received, and therefore encourages providers to implement e-mail management best practices.

Recommendations

Based on its analysis of facts and trends from the study, ENISA has made a series of recommendations to providers, the EC, Member States and standardisation bodies. In addition, for its own part, ENISA will examine specifically the status of DNSSEC (Domain Name System (DNS) Security Extensions), which has been designed to protect the Internet from attacks such as DNS cache poisoning. It will also follow the developments of the SpotSpam project and Signal Spam which provides best practices for users, bulk e-mail senders and service providers in order to reduce spam).

Based on the findings of the study, ENISA also organised a workshop on anti-spam measures as part of the Inbox-Outbox event held in London in November 2007. The aim of the workshop was to bring together key European stakeholders to debate the effectiveness of current and future anti-spam measures and their compatibility with existing privacy regulations. More specifically, the workshop addressed filtering methods, emerging anti-spam approaches, spamming trends and the privacy of users. Invited speakers represented the European Commission, regulators, ISP providers, anti-spam software vendors, research institutes and privacy experts. ENISA's session attracted more than 160 attendees. The contributions during panel debates and questions following the presentations will provide input for next year's tasks.

Facilitating the Working of the Internal Market for e-Communication

Secure electronic communication systems are a major factor governing the development of the Internal Market and ENISA has a key role to play in improving the general level of e-Communication security. The Agency's tasks include identifying obstacles (technical, organisational and cultural) to secure e-Communication and ways to overcome them.

Analysing barriers – a price tag on NIS?

On 10 December 2007, the Agency organised a workshop in Brussels on "Barriers and Incentives for Network and Information Security (NIS) in the Internal Market for e-Communication". About 100 stakeholders from industry, consumer organisations, EU institutions and Member States attended the Workshop and discussed the obstacles that hinder the drive for NIS in the Internal Market for e-Communication and the incentives which encourage good practice.

The workshop sought to launch a discussion among relevant stakeholders to collect their input for a report commissioned by ENISA which is aimed at making the economics of security and NIS more visible on the political agenda by putting a 'price tag' on the value of ensuring NIS. One of the leading scholars on Security Economics, Professor Ross Anderson (University of Cambridge, UK), outlined the main objectives of the report he is preparing and gave some thought-provoking examples. The OECD's work on NIS economics added an international perspective to NIS security economics.

The Workshop achieved the following results:

- Identification of existing economic barriers to addressing NIS issues in a single, open and competitive Internal Market for e-Communication
- Assessment of the potential impact of these barriers on the smooth functioning of the Internal Market for e-Communication
- Identification and analysis of incentives (regulatory, non-regulatory, technical, educational etc.) for lifting these barriers
- Recommended policy options, possible follow-up actions and initiatives.

Assessing and Managing Current ICT Risks

ENISA's work on Network and Information Security (NIS) addresses both current and emerging risks. Current risks refer to the management of contemporary risks that have to be managed by using existing Risk Management/Risk Assessment (RM/RA) methods and tools. In this domain ENISA continued the work initiated in 2006 by updating its inventory of RM/RA methods, by looking at additional kinds of current risks in the area of business continuity and by examining the possible integration of RM/RA with other relevant disciplines in the area of technology and governance processes.

Update of the RM/RA methods inventory and demonstrators: ENISA implemented a process for updating the existing inventory of RM/RA methods and tools, based on a submission process that involves sets of templates for organisations to submit new methods and tools. During 2007, the availability of this material led to the submission of three new methods and three new tools. As further submissions are added, the inventory will become increasingly complete and accurate and ever more helpful to external users.

As part of this task, ENISA addressed possible approaches to the integration of RM/RA with overall business processes by generating demonstrators for the deployment of RM/RA in real-life situations. This work has demonstrated how de facto standard processes (e.g. project management, application development, configuration management, incident management etc.) are connected to Risk Management. It has also led to the establishment of good practices which will help users to integrate their Risk Management strategies with the existing operational processes related to their IT systems. ENISA focused on the completeness of the interface definitions (e.g. input part, output part and the conditions or events that would lead to an activation of the interface, as well as the parts played by different members of the organisation and the exchange of data). This material will serve as a solid basis for professional users to support them in the configuration of their Risk Management processes.

Inventory of business continuity risk analysis methods: From the security point of view, Business Continuity involves the availability and integrity requirements for assets connected to the major operations of an organisation. Based on such requirements, continuity risks are identified by means of Risk Assessments that cover the most critical operations. The most critical operations, in turn, are usually identified by means of a Business Impact Analysis (BIA). Risk Management/Risk Assessment thus performs a crucial role within the establishment and the management of a Business Continuity Plan (BCP). While important for many organisations, business continuity is vital for the resilience of IT systems and their components. ENISA has initiated a series of activities in the area of Business Continuity for the years to come which will contribute to the generation of a publicly available information base in this area with inventories, good practices and applicability guides. The work is aimed at providing solutions to the following general problems encountered in the area of Continuity Management in Europe:

- No overview of the contents and structure of methods, tools and good practices
- The absence of a 'common language' for IT Continuity Management to facilitate communication between stakeholders and
- A lack of surveys on existing methods, tools and good practices.

In addition, ENISA will help establish a dialogue among the relevant stakeholders to exchange experiences in Business Continuity and generate momentum for synergies.

Integration of RM/RA with business governance: ENISA is also looking at possibilities for integration between Operational Risks and IT Risks. The management of Operational Risks includes information, system and computer risks. Thus integrating Operational Risks with IT Risks also involves security (both IT and physical) as well as the development and maintenance of information systems. However, the integration of Operational Risks and IT Risks in organisations still causes problems for Chief Information Security Officers (CISOs). The contributions from different sectors of the organisation and the nature of their involvement with Operational Risks must be clarified.

ENISA's work will generate material suggesting various possible integration dimensions of IT Risk Management/Risk Assessment with Operational Risks. This will be demonstrated by means of process interfaces, an analysis of the parts played by different members of the organisation, input/output information and, if relevant, various conditions related to the particular context under which the interfaces will be used. If the timeframe allows, statements concerning the possible integration of the underlying IT services will also be delivered.

Besides serving as a good practice guide for integration, the results produced should assist organisations participating in supply chains, where suppliers may be forced to comply with risk management requirements imposed by their customers. The material delivered will serve as the basis for measuring compliance with existing Operational Risks and Corporate Governance frameworks (e.g. to fulfil SAS70 requirements).

RM/RA methods for SMEs: In addition to the tasks laid out in the Work Programme 2007, ENISA supported the adoption of its 2006 results in the area of Risk Management for SMEs by the UK-based International Association of Accountants Innovation and Technology Consultants (IAAITC). IAAITC has used ENISA's results to generate a comprehensive guide for training and usage by their members (accountants and small businesses). The work has been supported by the Micro Enterprise Acceleration Institute (MAE-I) and has led to the deployment of ENISA's findings to a wide community of users. Building on this work, in 2008 ENISA will run a number of pilot projects to further validate the results generated in small businesses.

Mastering Emerging Technologies and Services

The challenge for Europe is not only to reduce current weaknesses in NIS but also to anticipate future difficulties, both in evolving technology and new applications. Throughout 2007, ENISA continued to identify emerging risks, to analyse the R&D capabilities in Europe and to map them with the new technology and service trends. A number of Position Papers were provided on current security issues, which make recommendations to reduce the security risks to users.

Tackling Emerging and Future ICT Risks

In years to come, new application scenarios and technologies are expected to emerge within the European Union. These are likely to generate new risk factors for IT assets and dependent processes, systems, products and services. An early and accurate identification of such risk factors will increase our capability to reduce and control their impact. However, the majority of Risk Management/Risk Assessment (RM/RA) methods and tools are designed to tackle risks within the timeframe of contemporary risks. RM/RA experts have to use variations of existing methods as well as mixed or new approaches to identify and calculate impacts and mitigate emerging and future risks (EFR).

Methods for Emerging and Future Risks: In order to deal with this development, ENISA has initiated a project to develop an appropriate understanding of the requirements for tackling emerging and future risk and to evaluate current risk assessment and management methods for their suitability. A comprehensive set of evaluation criteria has been developed using Soft Systems Methodology. The criteria were used to assess 18 existing methods for risk assessment and management. Based on the results of this assessment, a detailed requirements definition document has been produced that establishes the foundation for the extension and development of current or new methods to deal with emerging and future risks.

In a further step, a possible scenario-based extension of existing methods for emerging and future risks has been formulated. To provide maximum flexibility and to facilitate its integration into existing methods, a modular approach was taken which outlines clearly defined stages and interfaces. The approach has been tested with a specimen future risk scenario to demonstrate its validity and its suitability for the extension of existing risk assessment and management methods.

Workflow/Process model for assessing emerging and future risks: Expanding on this work and based on the findings of its earlier study, ENISA is developing a workflow/process model for the assessment and management of emerging and future risks. In this way, the Agency will support the proactive and prospective information security activities of its stakeholders. The results will also be used to identify further action required to assess and manage emerging and future risks.

Dissemination of information on emerging risks: In co-operation with the Spanish Institute INTECO, ENISA organised a major event on Risk Management in Barcelona in November 2007. Entitled "Risk Management: Why Business Needs It?", the event included presentations on the different approaches to Risk Management/Risk Assessment adopted by various business sectors from five European countries. The event provided ENISA with valuable input for future developments in the area of Risk Management, especially concerning the deployment of methods and tools for SMEs.

Security Trends in Emerging Technologies and Applications

Analysing trends and developments in NIS

Observing and analysing trends and developments in NIS continued throughout 2007. Important developments in standardisation and research were followed, particularly in the area of NIS technologies, security tools and strategies, as well as emerging information and communication technologies and applications, with a view to identifying the security challenges they present and the solutions they require. The resulting Report, which updated an earlier one issued by ENISA in 2006, is now available in web format. The ENISA website offers easy access to the Agency's activities in Security Technologies and also provides a window on external information and events.

Technology Cabinet

The Technology Cabinet was established to serve as a platform to gain hands-on experience with systems relevant to security (such as software, hardware, devices, services etc.). Administered by the Risk Management section, it also provides a means of demonstrating existing technologies, methods and good practices to interested stakeholders. In particular, the demonstration capacity built into the Technology Cabinet is expected to have a significant impact.

In the second half of 2007, the Technology Cabinet was boosted by the appointment of a new staff member and it was agreed that its design and implementation should be based on Virtualisation Technology. After the design phase, several procurements (hardware and software) were completed to enable it to serve the operational departments of ENISA with a hands-on IT infrastructure: security policy, tools, methodology, vendor and visitors demonstrations...

A functional platform was deployed with all necessary primary functions: virtualisation facility, Internet access, firewall, WLAN, security policies and administration/maintenance tools. By the end of the year, the implementation of the Technology Cabinet reached a beta version.

Many requests have already been made to the service; for example, testing environments have been set up, demonstrations of vendors have been performed for the Security Policy Section, and technical support has been provided for the Knowledgebase.

ICT Security Standards Roadmap

The monitoring of NIS standardisation also continued, building on previous work. ENISA has combined forces with the ITU Telecommunication Standardization Sector (ITU-T) and the Network and Information Security Steering Group (NISSG), to produce an ICT Security Standards Roadmap, a new portal giving Europe a single access point for IT security standards. The site offers a repository for recent activities in NIS standardisation, and contains an extensive list of key standardisation organisations with their descriptions and the standards they have published (also available according to a topical categorisation). One of the objectives of this security standards portal is to provide a central tracking facility for NIS standards. It facilitates the identification of standards and standardisation activities, as well as co-ordination among standardisation bodies, the reduction of duplicate work and easier identification of gaps.

Position Papers on Specific Emerging Security Issues

Virtual Groups of Experts

ENISA has engaged its stakeholders in 'Virtual Groups of Experts', working through wiki, mailing lists and telephone conferences to collect together expert opinion on topics it considers important emerging risks or key security components.

The topics covered in 2007 were Social Networking, Botnets and Reputation Systems, and three Position Papers have been published. The virtual groups have achieved considerable impact for ENISA since they lend weight and independence to the opinions expressed and the conclusions reached.

These papers (www.enisa.europa.eu/pages/position_papers.htm) provide an in-depth analysis of technology-related risks and threats to emerging applications, and each has generated considerable interest in the media. The Position Paper on Botnets led to direct questions in Parliament being put to the Swedish Prime Minister[2]. Further to the two Papers on Online Reputation and Social Networking, ENISA has been invited to present at the European Parliament and to chair a session at Infosec 2008 alongside Facebook and LinkedIn.

Open consultations have also been initiated to collect the views of ENISA's stakeholders in response to these papers.

[2] See: www.riksdagen.se/webbnav/index.aspx?nid=101&bet=2007/08:38

Security Issues and Recommendations for Online Social Networks

Social Networking Sites (SNSs) are expanding at a dramatic rate. This position paper starts from the premise that Social Networking is a positive social phenomenon, provides an introduction to security issues in the area of Social Networking, highlights the most important threats and makes recommendations for action and best practices to reduce the security risks to users. In the light of recent security alerts on the privacy issues related to Social Networks, this paper has attracted considerable press interest.

> *On 12 November 2007, my group and another US NGO wrote to the chair of the US Federal Trade Commission asking for an investigation into the recently announced expanded data collection and targeting systems of both Facebook and MySpace.*
>
> *I just read with great interest – and appreciation – your thoughtful analysis from October (as well as the June conference proceedings). It did a very excellent job raising the range of concerns, placing these networks in the proper intellectual context (as identity systems). Yesterday, I sent off your report to the FTC (Federal Trade Commission) and a number of news outlets.*
>
> Extract from a letter of appreciation from a non-governmental organisation (NGO) in the US

Threats: The commercial success of the multi-billion euro SNS industry depends heavily on the number of users it attracts. Combined with the strong human desire to connect, this encourages design and online behaviour where security and privacy are not always the first priority. Users are often not aware of the size of the audience accessing their content. The sense of intimacy created by being among digital 'friends' often leads to inappropriate or damaging disclosures. Social Networking may be seen as a 'digital cocktail party'. However, compared with a real-world cocktail party, SNS members broadcast information much more widely and sometimes unadvisedly, either by choice or unwittingly.

Some of the main threats that have been identified are digital dossiers, face recognition and social engineering attacks on enterprises using SNS. Other SNS threats include spear phishing using SNSs, reputation damage through ID theft, stalking and cyber-bullying.

Recommendations: This paper makes 19 recommendations – some of the most important ones include:

- Review and reinterpret the regulatory framework
- Increase transparency of data handling practices
- Awareness raising & education
- Discourage the banning of SNSs in schools
- Promote portable networks

The paper also recognises that important emerging trends in convergence with virtual worlds and 3D representation, misuse by criminal groups and the development of online presence deserve further research.

Reputation-based Systems

Reputation-based systems are used by an increasing number of applications as risk management mechanisms to facilitate trust. Electronic reputation is becoming as valuable an asset as traditional offline reputation. As new applications embrace reputation-based systems, the value of online reputation is increasing – and is becoming the target of attacks. Reputation allows users to form an expectation of behaviour based on the judgements of others, bringing the significant economic and social benefits of being able to trust people (or systems) not directly known to the user.

This paper provides an introduction to the concept of reputation-based systems, cites cases where they are used successfully, identifies a number of possible threats and attacks to them and the security requirements they should fulfil, and provides recommendations for action and best practices to reduce the security risks to users.

Four use-cases for reputation are described in this paper: online markets (such as eBay), peer-to-peer networks (for example for bandwidth management), anti-spam techniques and public key authentication (web-of-trust). From these, the main threats and attacks against reputation systems have been derived. The most important threats described are:

- Whitewash attack
- Sybil attack (i.e. pseudospoofing)
- Impersonation and reputation theft
- Denial-of-reputation
- Privacy threats for voters and for reputation owners
- Threats to ratings

The analysis of threats has led to a set of core recommendations for best practice to counter them, including:

- Develop reputation systems which respect privacy requirements
- Provide open descriptions of metrics
- Differentiate by attribute and individualisation as to how the reputation is presented
- Encourage research into:
  a. Common solutions to threats against reputation-based systems
  b. The management of global reputation
  c. Use of weightings in reputation metrics
- Research into and standardisation of portable reputation systems
- The importance of automated reputation systems for e-Government

Botnets – the Silent Threat

With the support of a consultant, a third position paper was written, on botnets. The paper describes the roles and structures of criminal organisations in creating and controlling botnets, and identifies trends in this type of cyber crime. The paper also identifies online tools to identify and counter malicious code.

Typically botnets are used for identity theft, unsolicited commercial e-mail, scams, Distributed Denial of Service (DDoS) attacks and other frauds. It is estimated that more than six million infected computers worldwide are connected to a botnet. Most owners of infected computers do not even know that their machines have been compromised.

The criminal organisations behind the implementation of this new online threat are well organised. They employ software developers, they buy and sell infrastructure for their criminal activities and they recruit people (mules) for money laundering to hide their identities. They have the technical resources to continually improve their attacks – conditions that make online frauds more successful than offline ones. Lack of user security awareness combined with the common habit of using old (sometimes pirated) and unpatched operating systems increase the success of criminal exploitation.

Botnets represent a steadily growing problem threatening governments, industries, companies and individual users with devastating consequences that must be avoided. Urgent preventive measures must be given the highest priority if this criminal activity is to be defeated. Otherwise the effect on the basic worldwide network infrastructures could be disastrous.

This paper makes a number of recommendations to deal with the non-technical problems:

- Government involvement
- Better co-operation between law enforcement agencies and private companies
- User awareness

Technical solutions to the problem of botnets have been identified, including:

- Secure operating systems and software applications
- ISP co-operation
- Give law enforcement agencies the capability to clean botnets

Bridging Security Gaps in Europe

Throughout 2007, ENISA was engaged in activities to bridge the security gaps in Europe, making network and information security policies more efficient and effective at the national as well as European level. The Agency's work involved facilitating the exchange of knowledge about incidents and consumer confidence, the exchange of best practices between Member States, the interoperability of electronic authentication systems and gaps in the provision of Computer Emergency Response Teams (CERTs) and similar facilities.

The NIS Brokerage

Exchanging experiences with others helps extend the overall capability of Europe to address security issues.

ENISA's network of National Liaison Officers (NLOs) and other national experts in NIS from Member States met on 22 February 2007 in Brussels, where ENISA, in co-operation with the German EU Presidency, organised a Kick-off Workshop on a "European Network and Information Security (NIS) Good Practice Brokerage".

This NIS Brokerage provides a structured approach, bringing supply and demand together. In this way, in accordance with the requirements of its Work Programme 2007, ENISA facilitates a European NIS 'market place' by acting as a 'broker' between those Member States that have developed good practices and are willing to share them and those which can learn from the experience of others.

For example, in 2007 ENISA supported the establishment of a co-operation initiative between Hungary and Bulgaria whereby, following a request from Bulgaria, ENISA is facilitating the transfer of Hungarian hands-on experience to Bulgaria in establishing a governmental CERT.

With the support of the NLOs, ENISA is well placed to identify and facilitate different types of co-operation (exchange of views, meetings, topical exchange groups, traineeships, site visits, dispatch of experts...). The work of the Brokerage involves:

- Developing models to spread newly gained knowledge
- Providing a central repository for good practices (including links to useful documents and outlines on how particular problems were tackled)
- Compiling a list of projects and funding (e.g. information about COM-initiatives etc.)
- Promoting existing EU initiatives as well as non-EU ideas within the EU
- Making a sustainable long-term commitment
- Helping bridge the language gap

There already exists a certain degree of co-operation, primarily in the fields of:

- CERTs (information exchange, quarterly meetings, annual fora)
- Awareness Raising (information exchange, formal and informal meetings, preparation of national campaigns)
- Spam (contact network of spam authorities, sharing of information and best practices)
- Electronic Signatures (fora, exchange of experience, expert groups).

Despite all this, there is still considerable scope to increase cross-border co-operation, as what currently exists is limited to a few countries. Significant improvements in efficiency and synergy, together with reduced costs, are therefore likely to be found by extending co-operation beyond national boundaries.

During 2007, a platform was developed to support the Good Practice Brokerage by making available online general information about the various co-operation models and the activities that have been carried out, together with other useful related information. The Brokerage will go online, as a pilot project initially, in 2008.

Who is Who Directory on NIS

A major tool for the interested NIS community is the annually produced *Who is Who Directory on NIS* – now in its third edition[3]. This was updated in 2007 with assistance from the National Liaison Officers (NLOs) and extended this year with the addition of contacts in the European Institutions, industry and international organisations. The directory serves as the 'Yellow Pages' of Network and Information Security in Europe.

[3] www.enisa.europa.eu/doc/pdf/deliverables/who_is_who_dr_20080121.pdf

Towards a Common Authentication System Taxonomy

To ensure a common understanding of what is offered by various authentication systems and to provide a basis for EU-wide harmonisation and alignment of authentication system requirements, a taxonomy for authentication systems is needed to classify methods on the basis of their characteristics. In 2007 ENISA continued to promote the establishment of compatible and interoperable authentication methods through presentations, the publication of papers, a workshop and the creation of an eID directory.

Workshop on Authentication Interoperability

In June 2007 ENISA organised a workshop on Authentication Interoperability as part of the ENISA/EEMA European eIdentity conference, which was held in Paris, France, and attended by over 100 delegates. During the workshop, a number of conclusions were reached which are now guiding ENISA's work in this area.

The workshop concluded that, although many models exist for interoperability, within national and commercial infrastructures, these can be divided into three main areas:

- Government issued credentials (e.g. national ID cards, passports)
- Commercial and banking systems' credentials (e.g. Identrust, SEPA – the Single European Payment Area)
- Tokens conforming to international standards (e.g. European Citizen Card).

The most successful interoperability models in all areas have the following features:

- A central authority collecting specifications and mandating certain features (i.e. essentially a standardisation body)
- A body which is willing to accept liability for acts of certification and testing interoperability.

The workshop concluded that interoperability at the legal, policy and technical levels should be jointly analysed and considered. On the legal level, mutual recognition, transparency of issuance processes and privacy were recognised as significant factors. It is also important to take into account the influence of competition on interoperability (it often works against it). Solutions should be found which retain brand differentiation.

All critical components of an authentication system (including middleware) should be included in certification processes. Banking (in particular SEPA) and the 2006 e-Services directive are major drivers which require international interoperability. Standards issued for authentication interoperability should be free of charge at least to not-for-profit developers.

eIDs

ENISA chaired a panel at the pan European eID conference in Leuven, Belgium, and collaborated with the ITU Focus Group on Identity Management to produce a directory of identity management standards, legislation and projects which will be made public, hosted on ENISA servers from 2008. ENISA will continue its work in this area in 2008.

As part of its contribution to the review of IDABC's eID Interoperability specifications, ENISA has written a proposal for work on extensions/updates to SAML[4] Authentication Context, based on a set of use-cases gathered from an Interest Group run by ENISA. This is being reviewed within the SAML SSTC[5].

[4] Security Assertion Markup Language

[5] Security Services Technical Committee of the standards organisation, OASIS (the Organization for the Advancement of Structured Information Standards)

Computer Emergency Response Teams (CERTs)

Know Your User – A Study

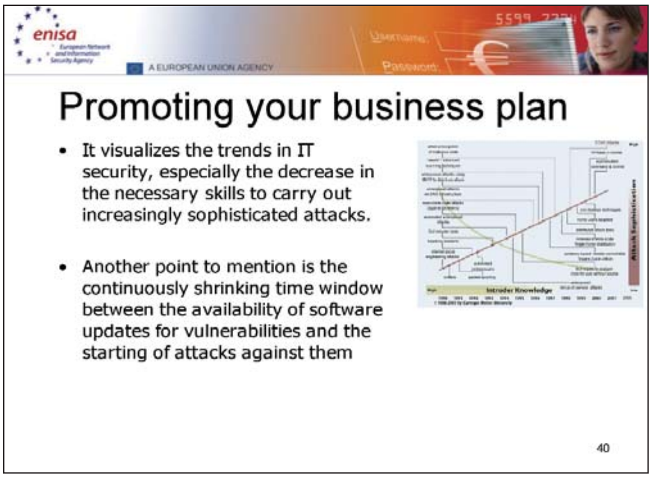
As everyday life is increasingly conducted online, information and the security of information systems are increasingly becoming a focus of concern for the public at large. Information system security has always been an important issue in military and corporate settings. Now home-users are becoming concerned too. Networked computer systems have become critical not only for conventional commercial and financial transactions, but also for ad hoc informal, social interactions.

There is a pressing need to address the question of how best to approach home-users with NIS information and other means of IT security both to reach out to this target group with (CERT) security services and to achieve real impact by changing their behaviour. ENISA has begun to address this problem by initiating a study into the various types of home-users and their perception of the Internet in general and IT security in particular.

The issue can be simplified into questions about how people experience security as part of their daily lives, how they routinely decide "is this system secure enough for what I want to do?", and about how to make the relevant features of security situations visible to users so that they can make informed decisions about potential security problems and the potential implications of their actions.

Facilitating the setting up of CERTs

To reduce areas of weakness in incident response in Europe, ENISA encourages the setting up of CERTs. In 2007, the Agency extended the impact of last year's "CERT setting-up guide" by preparing a set of presentation slides. In a lecture of two-three hours, this presentation provides an introduction to the whole process of establishing a national response team in the Member States.



Promoting your business plan

- It visualizes the trends in IT security, especially the decrease in the necessary skills to carry out increasingly sophisticated attacks.
- Another point to mention is the continuously shrinking time window between the availability of software updates for vulnerabilities and the starting of attacks against them

40

The CERT setting-up guide was used in a number of CERT projects in the EU Member States and was instrumental, for example, in the establishment of the Spanish governmental CERT (CCN-CERT).

CERT certification – a way for enhanced trust building?

Quality assurance is an important issue for CERTs, and one which ENISA supports in helping to enhance the general level of CERT performance in Europe.

During 2007, the Agency conducted a preparatory study on how certification of CERTs could act as a mechanism for building trust among the teams. A more enhanced level of trust among CERTs would stimulate communication between them – in particular the exchange of information about incidents.

But what is trust? What makes a CERT trustworthy? Where does trust come from?

For the establishment of trust, the following requirements – listed here in no particular order – play an important role:

- Availability of a CERT – to know that a CERT is still operating
- Sound business practices – in particular Incident Management processes
- Security of the CERT's operational systems – especially protection against unauthorised access, system and information integrity and secure communications
- The CERT's Information Security Management Systems – including risk management and contingency planning
- Expert knowledge and experience of the CERT's staff

A mechanism for trust building will include a definition of trust building criteria, the kind of assessment to be undertaken (self-assessment or external assessment) and the anticipated assessment result (self-attestation, certification, accreditation or trust seal). Some mechanisms for trust building among CERTs already exist, and an enhanced trust mechanism should build upon these; existing trust building mechanisms are analysed in ENISA's pre-study.

The pre-study defines trust as a set of trust building criteria which must be fulfilled in order to promote trust in communication and co-operation with a CERT.

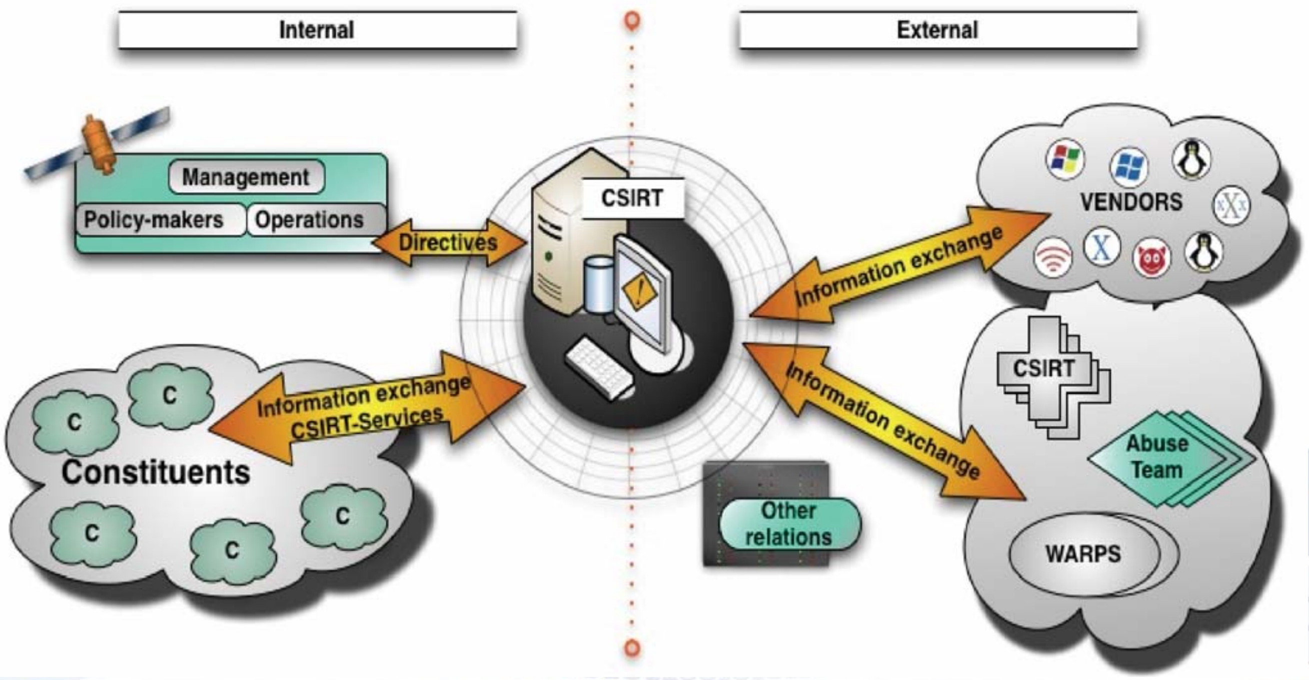
A catalogue is therefore needed which contains the major security controls: the management, operational and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. The pre-study identifies existing applicable standards containing security controls which may be (re)used as trust building criteria for a CERT. All security controls of the existing applicable standards are extracted and mapped as far as possible to one single set of security controls.

Promoting best practices for CERTs

- **Be prepared – CERT exercises**

  The concept of CERTs and their services has been evolving for more than twelve years. However, each team seems to have its own distinct set of services provided and levels at which it provides them to their constituencies. As a consequence, co-operation between CERTs relies mostly on informal relations acquired through various forums and meetings. The level of help that can be obtained from a team with which there has been no previous contact is therefore often unpredictable.

  By establishing a more or less standard set of exercises, it is hoped that staff in different CERTs can be trained in similar ways so that they begin to implement the same mechanisms in their everyday work. This would pave the way for close co-operation in an emergency situation, which requires established and tested communication channels and procedures to enable the mitigation of incidents.



In 2007 ENISA conducted a preparatory study for the compilation of CERT exercises that will be drawn up in 2008.

- **Good practices for running a CERT**
  As a follow-up to the ENISA CERT setting-up guide produced in 2006, in 2007 ENISA prepared a good practice collection on how to run a CERT successfully. This collection provides guidance on what a CERT needs in order to enhance its functions and to deliver the services that progressively meet its constituency's expectations.

  The primary target groups for this collection are governmental and other institutions that have already established a CERT and are ready to take the initial capabilities to the next level as well established teams. The collection focuses especially on the various kinds of connections and communication channels a CERT has externally, outside its management and its constituency, and internally among its team members, and demonstrates methods of coping with various difficult situations.

- **Mitigation of massive cyber attacks – CERTs to the rescue!**
  ENISA organised its 3rd Workshop for CERTs in Europe. This time ENISA's CERT experts teamed up with the most experienced people from the CERT Coordination Centre (CERT/CC) from Carnegie Mellon University in Pittsburgh/Pennsylvania (USA) to discuss the cyber attacks on Estonia earlier in 2007.

  Estonia, with its population of 1.3 million, is one of the smallest, yet one of the most knowledgeable EU Member States with regard to IT, but it was hit by massive, politically motivated Distributed Denial of Service attacks early in 2007. Estonia relies heavily on its Internet infrastructure. Most Estonians use online banking; 85% of all the tax declarations in Estonia in 2006 were submitted online and 94% of declarers received their returns in their bank accounts five working days later. In addition, Estonia runs a number of other eGovernment services that were heavily affected by these attacks. Estonia was fortunate to have established a national level CERT team a year previously to co-ordinate the mitigation of these attacks. Hillar Aarelaid from CERT Estonia summed up the events at the ENISA workshop.

  The workshop gathered together representatives of 25 European countries, including 22 EU Member States with a wide mix of established and new CERTs and CERTs yet-to-be set up. The day was divided into four sessions: "Overview of the threat environment"; "Key players in building a framework for managing cyber activities before, during and after the event"; "Legal issues that prevent or facilitate co-operation"; "Short scenario in responding".

The very positive reaction to this event in 2007 encourages ENISA to continue with its (now almost traditional) workshops in 2008!

ENISA meets the international CERT community
ENISA supported the 19th Annual Forum of Incident Response and Security Teams (FIRST) conference, that took place from 17-22 June in Seville, Spain, as a gold sponsor. At the event, the Executive Director of ENISA, Andrea Pirotti, gave a keynote speech.

FIRST is the premier organisation and recognised global leader in incident response. The Forum brings together a variety of computer security incident response teams from government, commercial and educational organisations, and aims to foster co-operation and co-ordination in incident prevention, to stimulate rapid reaction to incidents and to promote information sharing among members and the community at large.

CHAPTER 3
Relations with ENISA Stakeholders

- Communication and outreach
- External stakeholders, ENISA bodies and groups
- EU and Member State relations
- Other relations with industry and international relations
- Measuring ENISA deliverables

Communication and Outreach

Just as communications has become a policy of its own for the EU, ENISA recognises the strategic value of communications as critical for the achievement of its key operational objectives. Communication and visibility contribute in very real terms to the fulfilment of the Agency's objective to foster a 'culture of network and information security'. Communication and outreach to stakeholders are essential to increase the impact of the Agency's work and meet the goals laid down in its Regulations.

The Press and Communication Section is responsible for the corporate communications of ENISA. At a horizontal level, the Section enhances, advises, guides and supports other sections of the Agency in their outreach and communication activities, be it in stakeholder relations, public conferences or communication planning for projects. The Section's endeavours include the drive for consistency and coherence in all its communication channels (web, press releases, the *ENISA Quarterly*, other publications etc.) to promote the Agency's knowledge and expertise and to strengthen the impact of its reports, studies and operations.

A reorganisation in 2007, bringing the day-to-day operations of corporate communication under the Head of the Co-operation Department, has aligned corporate communications more closely with the operational activities and departments of the Agency. This has enabled the available resources to be optimised and has improved the effectiveness of communications planning.

The Communication Action Plan 2007

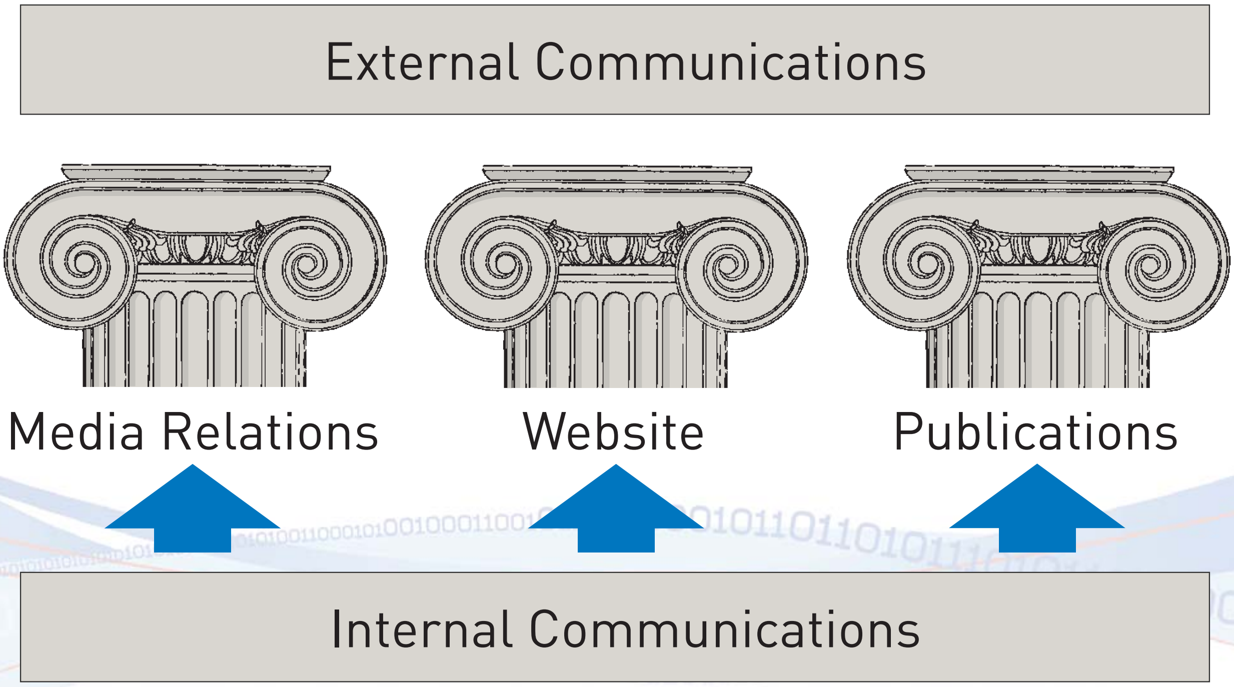
In 2007, ENISA adopted a strategic approach to increase communication planning across all the Agency's operations and a Communication Action Plan was drawn up. This document has clarified roles, responsibilities and tasks, and steered communication activities throughout the year. As a result, communication is considered a vital part of all operational activities – from their inception. This step is proving decisive in achieving results, maintaining the high quality of ENISA's relations with other stakeholders and enhancing both the visibility and impact of the Agency. Advance planning also enables the Agency to integrate better with its stakeholders' information and communication channels, thus increasing general outreach still further.

Implementing the Communication Action Plan – the three pillars

Internal communication is the founding pillar for securing good external communication. In 2007, ENISA's internal communications were strengthened by the development of the Agency's Intranet, alongside staff meetings, departmental meetings and *ENISA Inside*, the Agency's internal newsletter.

The ENISA website, the central pillar for outreach, which remains a top priority and the main external communication channel, was boosted with the recruitment of a Web Developer and a Web Master during the year. Publications and media relations are also being given more emphasis in parallel with other priorities. With additional funding, brand marketing

External Relations and Communication



material and (repetitive) brand recognition advertising have also been commissioned, and pilot event marketing through advertisements was allocated budget to obtain wider visibility for the Agency and its activities, as recommended in the European Commission's mid-term review.

The ENISA website: The website is being developed through restructuring and improving the information available, making it simpler and more efficient. At the same time, it is being expanded and made more accessible with new, thematic portals in order to make it a European 'hub' for NIS information. To increase traffic to the website, the new structure will reflect a more rational division between the areas serving the broad target audience of the website, where non-technical visitors can find information about ENISA's goals and activities easily, and areas where experts can obtain more detailed information quickly. A new element will be a 'Content Management System' (CMS), which will allow authorised staff to publish articles and contribute input easily. In this way, the CMS will make the site easier to maintain and keep published information up to date. In addition, interaction between ENISA and its target audiences should gradually be improved by further developing interactive tools, such as public forums, surveys and polls, and by making online, visual material available.

Publications: The ENISA General Report and four issues per year of the *ENISA Quarterly* are key publications produced during the year. Moreover, corporate materials including Fact Sheets, leaflets, an ENISA brochure, ENISA material folders etc. were produced in order to widen the range of publicly available material and increase the transparency of the Agency's operations. In this way ENISA is using communication not only as a tool for spreading information, but also to influence policy change.

enisa
European Network and Information Security Agency
NIS is people
ENISA Quarterly
Awareness Raising
General Report 2006
The Annual Report of the European Network and Information Security Agency

A general overview of how to improve corporate and sectional publications (the *ENISA Quarterly*, printed reports, the General Report, Fact Sheets, Folders etc.) is being undertaken, aimed at producing guidelines to ensure consistency of style and corporate image and to facilitate production and co-ordination with the European Community's Official Publications Office, OPOCE.

Procurements for other support services were also commissioned, including brand guidelines and brand-building materials, in accordance with ENISA's Communication Plan.

The Media: 18 press releases were issued in 2007 to publicise the Agency's deliverables, in conjunction with web publication of several other Agency news items, feature articles and FAQs presenting its operations. Media is, of course, well recognised as a key component and supreme multiplier to spread knowledge about the Agency's accomplishments and to set NIS on the political agenda. Existing relationships with media contacts were strengthened in 2007, and new steps were taken to increase such contacts, in line with the high priority attached to the media in the Communication Action Plan. ENISA was featured in *Le Monde*, *Der Spiegel*, *Fokus*, the *International Herald Tribune* and other major general media in various countries, as well as in NIS media.

The first modules in a media training programme, introducing media landscape and media relations, were held with most of the operational staff members. This programme is intended to enhance the staff's knowledge of how to increase the visibility and impact of the Agency through consistency and coherency in all communication channels. At the same time, as an EU Agency, it also underpins the EU's policy of increasing and enhancing communication, to raise visibility and explain its operations to the citizens of Europe in a clear language.

Relations with ENISA Stakeholders

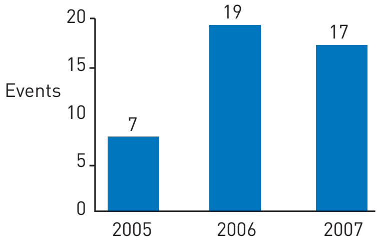
Conferences and (Joint) Events

Building on previous experience, the Agency continued to organise a selection of independent, not-for-profit, high-level European conferences, often in partnership with a third party such as a conference organiser or the EU Presidency. These events allow the Agency to network and promote its work in a cost-effective way, while at the same time keeping track of developments in the field.

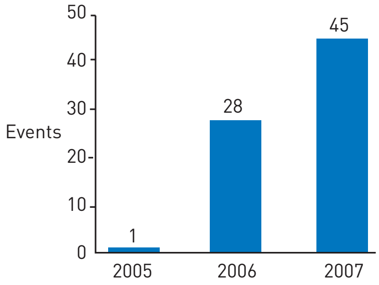
Thematic Workshops

In addition, the Agency organised a number of thematic workshops to discuss Position Papers, the outcome of specific projects or studies etc., or to present opportunities for a first exchange of ideas to raise stakeholder interest before the launch of new Working Groups (see chapter 2).

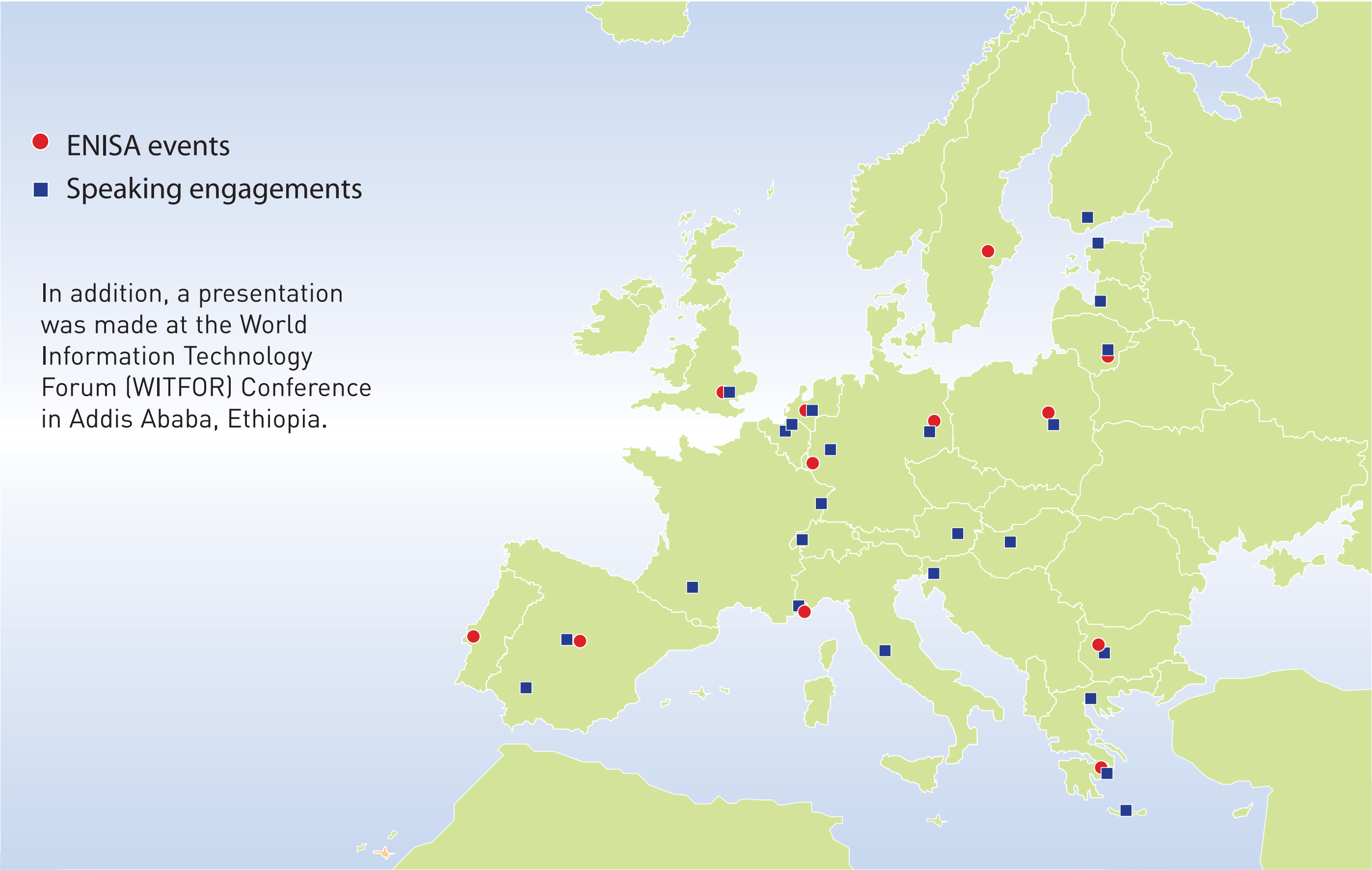
Events supported or co-organised by ENISA 2005-2007



Requests for ENISA speakers at external events



Geographical Distribution of ENISA Events and Speaking Engagements in 2007



In addition, a presentation was made at the World Information Technology Forum (WITFOR) Conference in Addis Ababa, Ethiopia.

During 2007, ENISA participated in or co-ordinated almost 40 events and conferences throughout Europe and further afield. In addition staff attended conferences and other events to fulfil ENISA's role in gathering and disseminating information about Network and Information Security.

External Stakeholders, ENISA Bodies and Groups

Creating a Network of Contacts

ENISA is a centre of Network and Information Security (NIS) expertise. This is required in its mandate, and is essential if the Agency is to effectively fulfil its advisory role.

The communities and activities involved in NIS in Europe are many. ENISA has created a good network of contacts, primarily by participating in key NIS and information society events in Europe and world-wide, liaising with experts in different fields, introducing them to ENISA and its activities, and promoting future collaboration.

Strengthening this network of contacts has two main advantages: firstly, it can help ENISA maintain close contact with NIS stakeholders and is a valuable source of information to keep its knowledge of relevant technologies updated; secondly, it facilitates outreach to the communities with technical expertise and to promote the take-up of products and services.

ENISA's network of contacts includes key people in standardisation bodies, national industry associations and EU-level interest organisations, as well as security experts within the private and public sectors and academia. This network will be further developed during 2008 and groups of experts will be established to write position papers on selected security topics.

The Permanent Stakeholders' Group (PSG)

In 2007, after an open call, the Executive Director appointed the members of the second ENISA Permanent Stakeholders' Group (PSG), for the years 2007-2009. The PSG facilitates the Agency's regular dialogue with the private sector, academia, consumer organisations and other relevant stakeholders. The Group comprises 30 independent experts who are appointed *ad personam*, (i.e. representing neither a country nor a company, but selected for their personal skills), each with proven abilities and expertise in fields relevant to the PSG mandate and with the capacity to contribute to ENISA's activities and to advise the Executive Director.

PSG Members represent a broad range of stakeholders including the Information and Communication Technology industry and research and academia in the field of Network and Information Security, as well as representatives from different user and consumer communities.

In 2007, PSG Members formally met four times, in February, April, September and December. Main items on the agenda of these meetings included advising on drafting the ENISA Work Programme 2008 and providing insights into future and emerging issues in NIS, the selection of topics for ENISA Position Papers and defining the terms of reference for working groups. In addition, the PSG discussed the mid-term review of ENISA commissioned by the European Commission, and provided feedback on the evaluation of the impact of ENISA deliverables. As individuals, PSG Members have contributed to ENISA's operations by writing for the *ENISA Quarterly* and undertaking speaking engagements at different ENISA events.

The PSG, Management Board and the ENISA Strategy 2008-2011

To elaborate the strategic orientation of future ENISA activities, PSG Members and Members of the Management Board, together with ENISA staff, met for an informal workshop in Berlin, Germany, in June 2007. This was a follow-up meeting to last year's successful bringing together of two ENISA bodies that have clearly defined, distinct roles within the overall ENISA structure: the Permanent Stakeholders' Group is the source of input and advice to ENISA's Executive Director, while the Members of the Management Board are the decision-making body of ENISA. The event proved extremely useful both in achieving a common understanding and providing strategic orientation for ENISA. Both groups agreed to continue these informal workshops in the future.

For a list of the members of the PSG, see Appendix 4.

Management Board

In brief, the Management Board's task is to define the general strategic orientation for the operation of ENISA, to ensure consistency between the Agency's work and activities conducted by Member States as well as at Community level, as laid down in the ENISA founding regulation. The Management Board also approves ENISA's Work Programme, ensuring it is in line with the Agency's scope, objectives and tasks, as well as with the Community's legislative and policy priorities for network and information security. It also establishes and oversees the budget.

A key pillar of ENISA, along with the Executive Director and the Permanent Stakeholders' Group (PSG), the Management Board includes one representative of each EU Member State and three representatives appointed by the European Commission. There are also three members, proposed by the Commission and appointed by the Council, without the right to vote, who represent respectively:

- The information and communication technologies industry
- Consumer groups
- Academic experts in network and information security.

Finally, there are also three observers from the European Economic Area (EEA) Member States, Liechtenstein, Norway and Iceland.

In 2007 the Management Board elected Prof. Dr. Reinhard Posch (Austria) as its new Chair. Prof. Posch succeeds Kristiina Pietikäinen (Finland) who served two and a half years as Chair of the Board.

The full Management Board met three times in 2007: in Brussels, Belgium, in Heraklion, Greece, and in Porto, Portugal.

The preparation and subsequent adoption of the Work Programme for 2008 and the (amended 2007) and 2008 budgets were important activities.

However, in 2007 the Management Board received the mid-term evaluation of ENISA and defined the general orientation for the operation of the Agency in the short- and long-term.

On the initiative of the Management Board, changes were also made to the way in which the Work Programme is drawn up. The work programmes are now being set up to accommodate multi-annual programmes, which represent mid- and long-term targets. At the informal joint meeting between the Management Board and the PSG in June 2007 in Berlin, Germany, four main topics were defined and implemented in the Work Programme 2008.

In addition, some key Management Board decisions were taken in 2007, for example, on the setting of minimum standards for the Agency. These standards are based largely on those laid down by the Commission and are required under the ENISA Financial Regulation. These baseline standards reflect the organisational structure and the internal management and control systems and procedures suited for carrying out the duties of the Authorising Officer including, where appropriate, *ex post* verifications.

All minutes and decisions of the Management Board are available on the ENISA website.

For a list of members of the Management Board, see Appendix 3.

EU and Member State Relations

Relations with EU Bodies

Relations with the relevant committees in the European Parliament, in the Council of the EU as well as with the European Commission were further strengthened in 2007. The Agency organised various meetings with different representatives of EU Institutions, and meetings were held between ENISA's Executive Director and Information Society and Media Commissioner Viviane Reding.

As NIS is not only dealt with in the Directorate-General for Information Society and Media (DG INFSO), but also other DGs which have an interest in various NIS-related issues, ENISA arranged meetings and exchanges with representatives of DG Internal Market and Services, DG Enterprise and DG Justice, Freedom and Security. By strengthening its relationships with these major DGs, ENISA has opened up promising opportunities for co-operation.

On 27 March 2007, the Executive Director delivered a presentation to the Committee for Industry, Research and Energy (ITRE) at the European Parliament, where he presented ENISA's role in NIS and introduced specific activities.

Members of ENISA also attended various meetings of the Working Group on Telecommunications at the European Council and are establishing potentially beneficial relationships with the members of this Group.

Relations with ENISA Stakeholders

Relations with Member States

Various meetings were organised in the EU Member States, focussing at the beginning of 2007 on visits to Bulgaria and Romania, the new Member States. These visits provided an opportunity for an exchange of information on NIS with high level representatives and discussions as to how the new Member States might benefit from ENISA's knowledge and expertise. The new Member States have now become active Members of the Management Board as well as in the National Liaison Officers' network.

High Level Dialogue on Information Security

The Portuguese Presidency and ENISA co-organised a high-level dialogue on Information Security (11 October 2007 in Porto) to enable an informal exchange of views on the future activities of the Agency. Topics discussed included ways in which National Competent Bodies, EU institutions and industry could better benefit from ENISA and how ENISA might work with these different stakeholders to enhance the impact of its activities.

The Network of National Liaison Officers

Although not formally based on any ENISA Regulation, the network of National Liaison Officers (NLOs) set up by the Agency is of great value and importance: on the one hand, the NLOs serve as ENISA's primary contact point within the Member States; on the other, they are well placed to reinforce the work of the Agency in the Member States, and to exchange information amongst themselves.

In addition, with input from the Member States through the NLOs' network, ENISA was able to update the 'Country Pages' on its website in 2007, to provide stakeholders with the latest information about contacts and activities in the Member States.

For a list of the NLOs, see Appendix 6.

Other Relations with Industry and International Relations

Industry Relations

In addition to the regular dialogue held with the Members of its Permanent Stakeholders' Group, ENISA has established relationships with relevant national industry associations in EU Member States as well as with a number of pan-European industry representative organisations. These organisations are important partners for ENISA in its drive to foster a culture of NIS in Europe.

Liaison has been maintained with organisations such as the Business Software Alliance (BSA), the European Information & Communications Technology Industry Association (EICTA), the European Telecommunications Network Operators Association (ETNO), the European Internet Service Providers Association (EuroISPA), the Association of European Chambers of Commerce and Industry (EUROCHAMBRES) and CENTR, the Association of Internet Country Code Top-Level Domain Registries.

In addition, ENISA has an 'open door' policy to all relevant stakeholder groups and in 2007 held a number of bilateral discussions with stakeholders at its headquarters in Heraklion, Greece.

During 2007, ENISA extended its relationship-building activity to the national industry multiplier organisations through personal visits and discussions with the vast majority of the EU's 27 Member States as well as EEA countries. Through its 'Road Show' project the Agency presented its role and activities to national organisations, but the campaign also enabled ENISA to learn more about the work carried out at the national level in Member States and to investigate models and platforms for possible co-operation on NIS-related issues. The Road Show will continue in 2008, until all the Member States have been visited. This activity is one way in which the Agency facilitates closer co-operation with its stakeholders, finding opportunities to engage them in partnership in the planning and implementation of future Work Programmes.

International Relations

NIS is a global challenge and does not recognise borders. In its task to foster best European practice, ENISA has regularly participated as a technical expert in different working bodies of international organisations such as the Organisation for the Economic Co-operation and Development's (OECD's) Working Party on Information Security and Privacy (WPISP). ENISA experts have also participated in the meetings and work of the European Council and ITU-T and ITU-D groups by presenting ENISA deliverables for example in the field of awareness raising and CERT co-operation. In addition, in close co-operation under the ITU framework, ENISA experts have engaged in a collaborative effort between the ITU-T and the Network and Information Security Steering Group (NISSG). This resulted in a portal, hosting a roadmap and inventory to vital information security standards.

ENISA experts have continued to meet and discuss global challenges in NIS with representatives from third countries, such as China, Japan and South Africa. In 2008, the Agency will continue building contacts with third countries by co-operating with IDC[6] on joint road show activities targeted at the countries bordering the EU.

EU institutional support

Drawing on its knowledge of appropriate and available expertise, ENISA was able to assist the European Data Protection Supervisor (EDPS) by suggesting a couple of national organisations which might help with a security audit of its EURODAC system (its central system consisting of a central unit, a business continuity system and terminal units at four different locations). The audit team was composed of members of the EDPS, together with representatives from the BSI (the Federal Office for Information Security in Germany) and the DCSSI (Direction centrale de la sécurité des systèmes d'information) in France. ENISA reviewed the quality standards of the report and its advice was taken into account[7].

Speaking engagements of the Executive Director

Speeches were prepared for the Executive Director for a number of high level speaking engagements in various Member States. Among the most prominent of these events were the IT Security Conference Innovation and Responsibility (4–5 June 2007, Berlin, Germany), the 19th Annual FIRST conference (17-22 June 2007, Seville, Spain), the High Level Dialogue on Information Security (11 October 2007, Porto, Portugal), the ISSE conference (25–27 September 2007, Warsaw, Poland) and the Third European Network and Information Security Conference (20-22 November 2007, Vilnius, Lithuania).

The Executive Director speaking in December 2007 at the workshop on 'Barriers and Incentives for NIS in the Internal Market for e-Communication' in Brussels

Measuring ENISA Deliverables

In fulfilling its main objectives, ENISA has produced multiple deliverables. In 2007, the Agency conducted a "Survey to assess the practical usability of ENISA's deliverables" in the Member States. For this deliverable – as laid down in ENISA's Work Programme 2007 – various ENISA stakeholders were questioned. Invitations were sent out to about 1000 stakeholders; respondents were mainly from governments and industry. The focus of the survey was to establish awareness, attitudes, acceptance and action related to the 22 deliverables that ENISA has produced since its inception until September 2007.

Stakeholders assigned ENISA's deliverables high marks in terms of content and approach and the survey suggests that the outreach has not yet reached its full potential. These first findings of the survey were presented at a meeting in January 2008 in Athens, where ENISA's stakeholders were invited. The findings of this survey will enable ENISA to maximise the impact of its contribution to creating a more secure e-environment for Europe.

[6] International Data Consultants: www.idc.com/about/about.jsp

[7] www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-11-09_Eurodac_audit_summary_EN.pdf

CHAPTER 4
Responding to Requests

- Partnership for ICT Security Incident and Consumer Confidence Information Exchange (PISCE)
- EISAS – NIS Information for Home-users and SMEs

Responding to Requests

In 2007, ENISA received five new calls for advice and assistance from:

- The Greek Ministry of Justice concerning the use of voice telephony encryption
- The Austrian Federal Chancellery
  - in the field of risk management
  - in the field of research, development and dissemination with regard to security and risk management in NIS
- The Bulgarian State Agency for Information Technology and Communications for assistance in the establishment of their Gov-CERT
- The Greek Ministry of Development concerning CERTs.

ENISA finalised responses to most of these requests in 2007.

The information requested by the Greek Ministry of Justice was sent in May 2007.

ENISA replied to numerous questions posed by the Austrian Federal Chancellery covering the whole range of IT Risk Management, and a report was delivered in July. Following this, an expert acting as project manager of the Austrian project visited ENISA for a few days in September to discuss additional and more detailed aspects of Risk Management and, as a result, ENISA prepared and delivered supplementary information on existing methods to the Austrian project team.

ENISA was unable to respond positively to the other request from Austria (the work requested was outside the Agency's remit).

In response to the Bulgarian request, the Agency held meetings with representatives from the Bulgarian Gov-CERT and CERT-Hungary and initiated a training programme in which ENISA will offer its expertise to the Bulgarians, and CERT-Hungary will contribute its hand-on experience in the establishment of a governmental CERT.

In addition to these new requests for advice and assistance, throughout 2007 ENISA worked on its response to a two-part request received in 2006 from the European Commission. This involved preparation of a report on "Developing a trusted partnership for a data collection framework", and a feasibility study into an EU-wide information sharing and alert system.

enisa
European Network and Information Security Agency

Examining the Feasibility of a Data Collection Framework

Author: Carsten Casper (ENISA)

November 2007

enisa
European Network and Information Security Agency

EISAS – European Information Sharing and Alert System

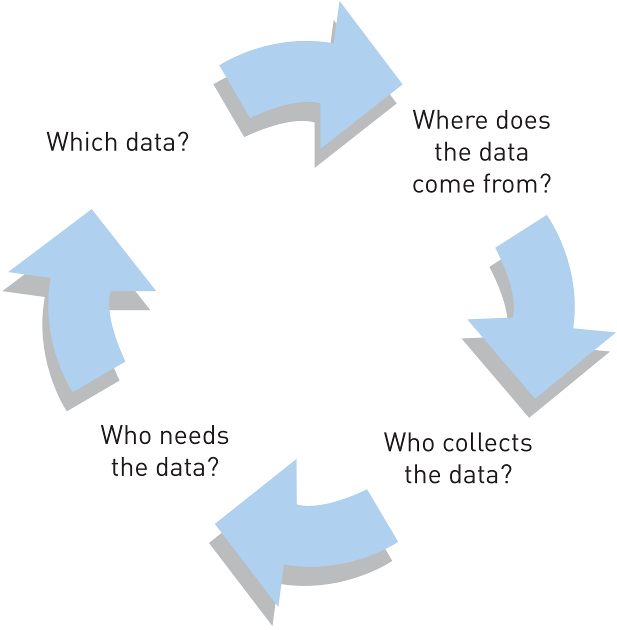
A Feasibility Study

2006/2007

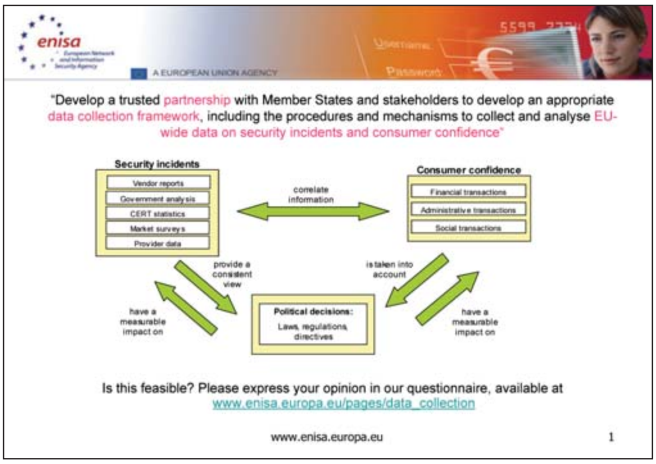
Partnership for ICT Security Incident and Consumer Confidence Information Exchange (PISCE)

ENISA was asked by the European Commission to examine whether it would be feasible to create a data collection framework for security incidents and consumer confidence. The objective would be to create a partnership of public and private entities, which would benefit from or contribute to a data-sharing initiative. This partnership would establish a concrete framework for data-sharing activities. Data shared within this framework would relate to security incidents and consumer confidence. Such data would allow public and private, European and national organisations to base their decisions with respect to information security and consumer confidence on detailed knowledge of the risk situation, to combine various aspects to obtain a 'big picture', to harmonise different data collection approaches and finally to measure the success of previously implemented legal, regulatory, organisational and technical measures.

In 2007 ENISA presented this idea in various forums and publications and gathered feedback over several months. The concept of a data collection partnership and framework is complex, because it touches on four related dimensions, namely the partners, the data owners, the data users and data collection mechanisms. All four aspects depend on each other, so ENISA decided to address them together in several consecutive iterations.



First, ENISA conducted a comprehensive survey, followed by a number of presentations and discussions. It complemented the results of this survey with extensive web research. Finally the work was completed with a workshop, where ENISA invited potential partners, presented the results of the feasibility study and initiated a partnership for data-sharing.


enisa
European Network and Information Security Agency
A EUROPEAN UNION AGENCY
Security incidents
Vendor reports
Government analysis
CERT statistics
Market surveys
Provider data
correlate information
Consumer confidence
Financial transactions
Administrative transactions
Social transactions
provide a consistent view
is taken into account
have a measurable impact on
Political decisions:
Laws, regulations, directives
have a measurable impact on

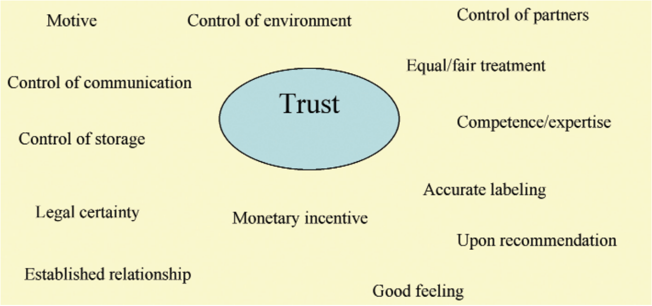
"Develop a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence"

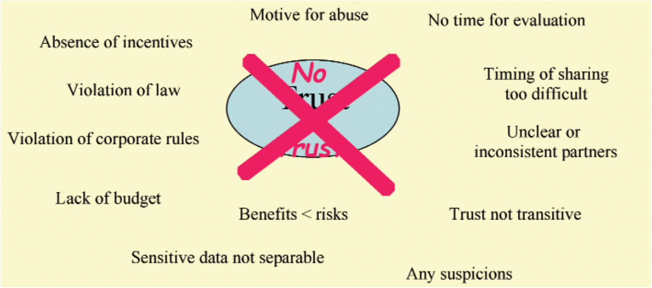
Is this feasible? Please express your opinion in our questionnaire, available at www.enisa.europa.eu/pages/data_collection

www.enisa.europa.eu 1

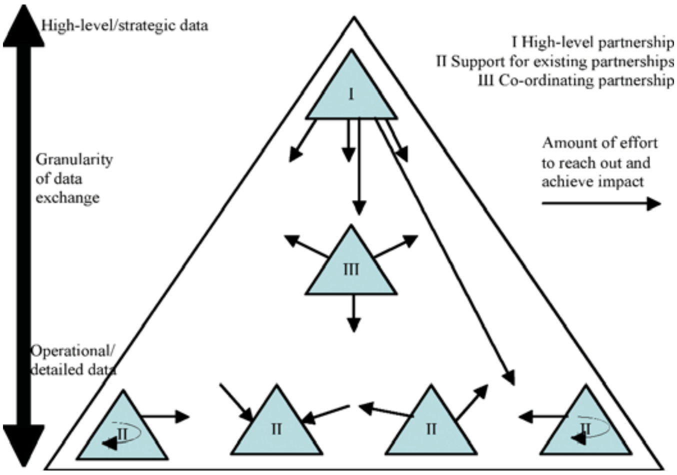
ENISA solicited information from all European parties who potentially have something to contribute, most notably Managed Security Service Providers, Computer Emergency Response Teams, national security organisations, statistics offices (e.g. Eurostat), IT security vendors, communication service providers and universities and other researchers.

The Agency also identified several indicators used in these data collections, surveys and reports, the conditions for sharing – or not sharing – sensitive data, the motivations for doing so (for example when reporting of incidents is required by law) and the contributions that partners might be willing to offer.





With these results, and given the scope of the problem, it is clear that one partnership for data collection (a 'one-size-fits-all' approach) is not feasible. It will be necessary to create new (or promote existing) partnerships of different kinds and on different levels. An additional co-ordinating partnership could tie together specific existing or new partnerships by supporting information and data exchange, harmonising collection methodologies or mediating trust.



ENISA organised a workshop in November 2007, bringing together many potential partners to kick off a general partnership which could then evaluate and decide subsequent activities. Participants in this workshop had the opportunity to decide in which way they would like to support data collection activities in the future: by pursuing a high-level, non-operational data-sharing partnership; by supporting existing and encouraging new operational data collection initiatives, or by initiating a co-ordinating partnership. Workshop participants finally opted for a phased approach, where a high-level partnership between those present along with some additional participants would start immediately. This would then evolve over time to support existing data collection initiatives. Since trust is an important element of such a partnership and can best be established and maintained face-to-face (which is more difficult for overseas partners), the workshop agreed that the partnership should be restricted mostly to European participants.

This initiative is now called 'Partnership for ICT Security Incident and Consumer Confidence Information Exchange (PISCE)'. Its purpose is to create an information exchange on IT security and consumer confidence trend data. A primary goal of this partnership is to encourage the involvement of policy- and decision-makers. This assumes their current need is to deal with emerging threats to the resilience of and confidence in ICT in Europe.

The partnership will evolve in several steps:

- Increase visibility of existing data collections and mediate supply and demand (implemented with a wiki at http://wiki.enisa.europa.eu)
- Categorise reports, e.g. by developing a useful template, including sample size, source, time of collection (presented at a later stage in the wiki)
- Facilitate an understanding of reports, without revealing details unless in a separate trusted partnership (with a closed list and ideally with a conference)
- Develop summary reports for decision-makers (if/when/where resources allow)
- Enlarge and deepen this partnership.

The partnership was supported initially by ENISA in a minimal way until the end of 2007, with the provision of a public wiki and the hosting of a closed mailing list.

EISAS – NIS Information for Home-users and SMEs

Several publications point out that, for various reasons, the computers of home-users and SMEs are the most popular victims of targeted attacks. It is comparatively easy to incorporate these users' computers into botnets, use them as obfuscated paths for launching attacks by hackers, as proxies to send spam or to enrol them as repositories for spreading viruses and worms. At the same time SMEs are important to Europe's economic growth. However, due to their size, SMEs rarely employ dedicated security personnel so the protection of their information assets is often left to non-security experts.

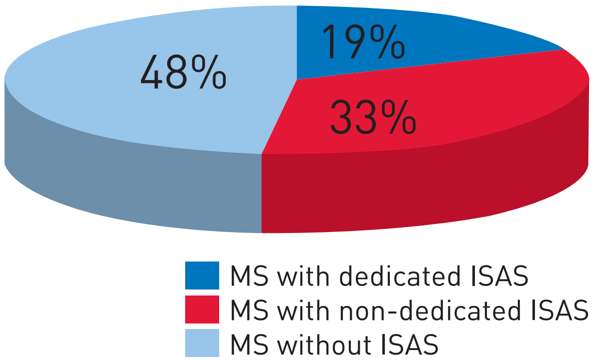
In its Communication to the Council, Parliament, the Economic and Social Committee and the Committee of the Regions (COM(2006) 251)[8], the European Commission emphasised that public authorities in Member States and at EU-level have a key role to play in keeping home-users properly informed so that they can contribute to their own safety and security.

NIS information for citizens and SMEs is important
There is already a lot going on in the Member States, but ...

... what?
BÜRGERCERT
CASES LUXEMBOURG
... who?
[...]
CASES contact network
... are there gaps?
... where?
WAARSCHUWINGSDIENST.NL
ITsafe
... how?
... where are the gaps?
BSI für Bürger
And finally: what can the EU do?

Systems and initiatives already exist in Europe and in the EU Member States which target home-users and SMEs with NIS-related, appropriate and timely information on vulnerabilities, threats, risks and alerts, as well as good practices. However it is clear that not all Member States take advantage of such mechanisms, and that gaps exist in the overall coverage. So the European Commission asked ENISA to *"examine the feasibility of a European information sharing and alert system (EISAS)"*, highlighting the Agency's role in fostering a culture of network and information security in Europe. ENISA thus embarked on a study into the feasibility of an EISAS.

- **Setting the scene**
  In order to provide thorough and responsible advice to the European Commission, ENISA first conducted an analysis of the current state of play in both public and private sectors in all EU Member States, and identified possible sources of security information which could potentially contribute to an EISAS. The findings of this analysis led to the development of a scenario to address both the lack of available NIS information in some Member States and provide a (yet-to-be determined) added value to existing information sharing systems in other Member States. Ideally such an EISAS would also build on these existing systems, firstly to avoid the duplication of effort and competition and secondly to benefit from the lessons learned and the good practices that these (national) systems can provide.



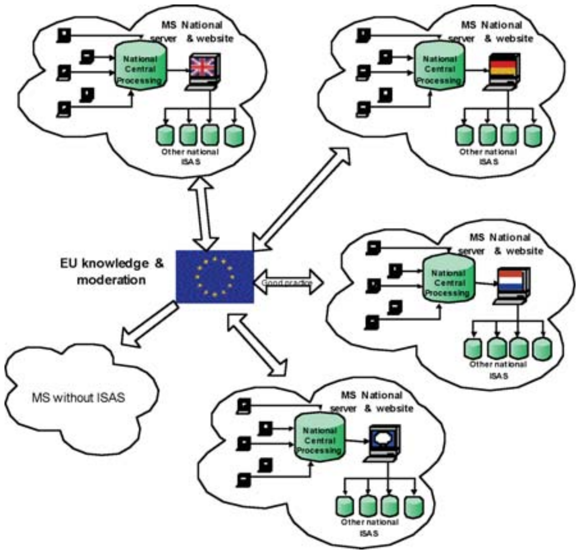
48% of the EU Member States do not have any information sharing activity for home-users and SMEs.

[8] COM (251)2006 – http://ec.europa.eu/information_society/doc/com2006251.pdf

- **Feasible or not?**
  The study focused on the technical feasibility of an EISAS and also adopted a broader approach to ensure acceptance of such a system by EU Member States. Last but not least, the target audiences were considered. Thus, the study examined the question of feasibility from three angles:
  - **Technical/organisational aspect:** the technical/organisational feasibility of an EISAS, including components and workflows etc.
  - **Political aspect:** the political feasibility of an EISAS, i.e. will Member States accept and support the proposed solution?
  - **Social/cultural aspect:** the feasibility of achieving real impact by successfully, effectively and sustainably raising NIS awareness among home-users and SMEs. This is the most crucial consideration, as the intended target groups have special perceptions and needs (e.g. language), most importantly the fact that in most cases they are not security experts.

- **Results**
  A centralised Europe-wide Information Sharing System is not encouraged by the findings of the study as the most feasible scenario. Instead the European Union should use its position and build on existing resources to foster the establishment of information sharing systems at the national level in Member States. The study concludes with four recommendations for a potential role for the European Union:
  - Act as a clearing house for good practice for national Information Sharing and Alert Systems (ISASs)
  - Support new national ISASs
  - Foster dialogue among existing national ISASs
  - Analyse and review practice, components and processes to optimise information sharing for existing ISASs.

- **But what about the user?**
  The feasibility study provided some interesting insight into the problems of how to adequately address home-users in order to achieve real impact. These problems have not yet been solved completely.


MS National server & website
National Central Processing
Other national ISAS
MS National server & website
National Central Processing
Other national ISAS
EU knowledge & moderation
Good practice
MS National server & website
National Central Processing
Other national ISAS
MS without ISAS
MS National server & website
National Central Processing
Other national ISAS

Act as a clearing house for good practice and support information sharing in the Member States

Some of the findings of the study are listed below:
- End-users and SMEs should be addressed in their native language.
- Messages (warnings, good practice documents etc.) should be phrased semantically in an understandable way (addressing the non-expert).
- The method of information dissemination should be thoroughly planned (i.e. other ways besides web pages and mailing lists should be examined such as podcasts, RSS feeds, traditional media etc.) to make it as convenient as possible for the end-user/SME to obtain information.
- Information overflow should be avoided; what and when to publish should be thoroughly planned.
- Information disseminated to end-users/SMEs must be trusted by the recipients if it is to be accepted (on average, end-users and SMEs already trust national governments).
- To be accepted, information should be disseminated as close as possible to end-users/SMEs.

ENISA followed up these results with a study into User Needs for CERT Services (see page 24).

CHAPTER 5
Change and the Perspectives for 2008

- Future Perspectives

Future Perspectives

Looking at 2008, ENISA's work programme is full of continued activities in NIS. The Agency also anticipates that 2008 will shed more light on ENISA's future role, mandate and potential changes. We look forward to these developments as a means of equipping the Agency for new NIS challenges, and we will follow any process in the European Parliament and Council closely throughout 2008.

Our main focus, however, will be on the Work Programme 2008, where the Agency is driving for greater impact through our new Multi-Annual Thematic Programmes (MTPs). These MTPs will run for the next three years (2008-2010).

- **MTP 1 'Improving resilience in European e-Communication networks'** focuses on the identification of current best practices, gap analysis, analysing Internet integrity technologies, and the stability of networks. This MTP will support the review of the EU Electronic Communication Directives.
- **MTP 2 will develop and maintain co-operation models**, in order to use and enhance the existing networks of actors in NIS. In 2008 this MTP will be devoted to:
  a) the identification of Europe-wide security competence circles in Awareness Raising & Incident Response
  b) co-operation on the interoperability of pan European eID and
  c) the European NIS good practice Brokerage.
- **MTP 3 will identify emerging risks for creating trust and confidence.** The Agency will develop a 'proof of concept' of a European capacity for the evaluation of emerging risks, linked to a Multi-Stakeholder Dialogue Forum for public and private sector decision-makers.

Finally, the Agency will undertake a **'Preparatory Action'**, which includes a feasibility study into the needs of and expectations for NIS in micro-enterprises.

The Agency is confident that the importance of NIS for the economy and for the citizens of Europe will become increasingly apparent in the coming years. Therefore, it is with considerable optimism that we anticipate the development of ENISA and the approach to NIS in the European context.

APPENDICES

Appendix 1
Acronyms and Abbreviations

BC	Business Contingency
BSA	Business Software Alliance
CERT	Computer Emergency Response Teams. 'CERT' is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security. (see also: CSIRT)
CERT/CC	Computer Emergency Response Team Coordination Center (USA)
CSIRT	CSIRT (Computer Security and Incident Response Team). Over time, the CERTs (see above) extended their services from being a reaction force to a more complete security service provider, including preventative services such as alerting, advisory and security management. Therefore, the term 'CERT' was not considered to be sufficient. As a result, the new term 'CSIRT' was established at the end of the '90s. Currently, both terms (CERT and CSIRT) are used in a synonymous manner, with CSIRT being the more precise term.
Contract Agent	Staff assigned to a post which is not included in the list of posts appended to the section of the budget relating to each EU institution (as opposed to a Temporary Agent, which is included in the list)
DCSSI	Direction centrale de la sécurité des systèmes d'information
DR	Disaster Recovery
EDPS	European Data Protection Supervisor
EEMA	European Association for e-Identity and Security
EFTA	European Free Trade Association
eID	Electronic Identification
EISAS	European Information Sharing and Alert System
FIRST	Forum of Incident Response and Security Teams – a global CERT organisation
FORTH	Foundation for Research and Technology – Hellas
ICT	Information and Communication Technology
IDABC	Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens (http://europa.eu.int/idabc/)
ISAS	Information Sharing and Alert System
ISP	Internet Service Provider
ISSE	Information Security Solutions Europe – Europe's only independent, interdisciplinary security conference and exhibition
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-T	ITU Telecommunication Standardization Sector
KPI	Key Performance Indicator
MTP	Multi-Annual Thematic Programme
NIS	Network and Information Security
NLO	National Liaison Officer
OECD	Organisation for Economic Co-operation and Development
PSG	Permanent Stakeholders' Group
RM/RA	Risk Management/Risk Assessment
RSS	RSS (Really Simple Syndication) is a family of web feed formats used to publish frequently updated content such as blog entries, news headlines or podcasts.
SEPA	Single European Payment Area
SME	Small and Medium Enterprise
SNS	Social Networking Site
WG	Working Group, ENISA Ad hoc Working Group on specific technical issue.

Appendix 2
Work Programme 2007 Priorities

The following tasks were stipulated in the Work Programme for 2007 – all the deliverables were completed.

Ref.	Deliverable	Output achieved	New activity for ENISA
2.1.1	Awareness Raising Information package 2007	Inventory of good practice for local government and ISP awareness initiatives published. Recommendations made.	No
2.1.2	Written report on KPIs for awareness raising	Survey and case studies undertaken, report published with inventory of current practice and measurement of success. Metrics of KPIs produced.	Yes
2.1.3	Dissemination workshop on awareness raising	One-day thematic workshop for 80 delegates.	No
2.1.4	Operational Knowledgebase accessible to the public	Knowledgebase made available to the public.	No
2.1.5	Presentations, papers and other contributions to promote security certificates	Presentations at conferences and workshops, papers published, and publication via online and print media.	No
2.1.6	Yearly report on electronic communication security measures	Publication of yearly report, detailing measures implemented.	No
2.2.1	Report on barriers and incentives for NIS in the internal market for e-Communication	Report produced.	Yes
2.2.2	Workshop on barriers and incentives for NIS in the internal market for e-Communication	Workshop held – 'Analysing barriers: a price Tag on NIS?'	Yes
2.2.3	Report on demonstrations of RM/RA methods and feasibility of integration in overall business process	Report produced.	Yes
2.2.4	Report on business continuity risk analysis methods for SMEs	Report produced.	No
2.2.5	Report on how to integrate risk assessment and risk management into business governance	Report produced.	Yes
2.3.1	List of information material, methods and tools needed to perform analysis of emerging risks	List produced.	Yes
2.3.2	Report on mechanisms to process and disseminate information on emerging risks	Report produced, including identification of relevant stakeholders and their roles.	Yes
2.3.3	Report on technological developments and trends	Report produced.	No
2.3.4	Workshop on technological developments and trends	Workshop held.	No
2.3.5	Position papers on specific emerging applications and recent technologies	Publication of 3 Position Papers: on Social Networking, Reputation-based Systems and Botnets.	Yes

Appendix 2
Work Programme 2007 Priorities

2.4.1	Establishment of a European NIS good practice Brokerage	NIS good practice Brokerage established.	Yes
2.4.2	Online platform for knowledge exchange on European NIS good practice Brokerage	Online platform established.	Yes
2.4.3	New printed version of the Who is Who Directory	New printed version published.	No
2.4.4	Presentations, papers and other contributions to promote a common authentication system taxonomy	Workshop on authentication interoperability held; presentations at conferences; papers to be published; contributions to online and print media.	No
2.4.5	eID Directory	Report 'Towards a Common Authentication System Taxonomy' published. eID Directory produced with overview of relevant players in Europe.	Yes
2.4.6	Workshop on eID	Workshop held.	Yes
2.4.7	Report on user needs for security services ("CERT services")	Report produced.	Yes
2.4.8	Reviewed and updated report and checklist for setting up of CERTs and similar facilities	Report reviewed and updated, with checklist for setting up a CERT and similar facilities.	No
2.4.9	Collection of best practices for quality assurance for CERTs and similar facilities	Collection completed; report produced.	Yes
2.4.10	Workshop on CERTs	Third workshop on CERTs in Europe held; 'Be prepared' CERT exercises prepared; good practices for running a CERT compiled.	No
3.1.1	Communication Action Plan 2007	Plan produced.	No
3.1.2	Up-to-date ENISA website	Website updated.	No
3.1.3	Four issues of the *ENISA Quarterly*	4 issues produced.	No
3.1.4	Annual report on ENISA activities 2007	Annual Report published.	No
3.1.5	Other deliverables to implement the Communication Action Plan 2007	Procurements of brand guidelines, updated Communication Strategy, brand material etc	No
3.1.6	Increased outreach through Member States' information channels	Continuous	No
3.2.1	Conferences and (joint) events	ENISA supported or co-organised 17 events	No
3.3.1	Thematic workshops	Half a dozen workshops organised.	No
	Feasibility study on a data collection framework	Feasibility study produced.	n.a.
	Feasibility study on an EU-wide information sharing and alert system	Feasibility study produced.	n.a.

Appendix 3
Members of the Management Board

At 10 January 2008

European Commission representatives

Representative	Alternate
Fabio COLASANTI Director General Information Society and Media DG	Michael NIEBEL Head of Unit Information Society and Media DG – "Internet; Network and Information Security"
Gregory PAULGER Director Information Society and Media DG – "Audiovisual, Media, Internet"	Lotte KNUDSEN Head of Unit "Fight against Economic, Financial and Cyber Crime" Acting Director, Internal Security and Criminal Justice DG Justice, Freedom and Security
Francisco GARCIA MORÁN Director General Informatics DG	Marcel JORTAY Head of Unit Informatics DG – "Telecommunications and Networks"

Member States' representatives

Member State	Representative	Alternate
Austria	Prof. Dr. Reinhard POSCH CHAIR OF ENISA MANAGEMENT BOARD Chief Information Officer	Herbert LEITOLD Institute for Applied Information Processing and Communication
Belgium	Georges DENEF Membre du Conseil de l'IBPT	Rudi SMET Ingénieur-Conseiller IBPT
Bulgaria	Stoicho STOIKOV Deputy Chairman of the State Agency for Information Technologies and Communications (SAITC)	Slavcho MANOLOV Advisor to the Chairman of the State Agency for Information Technologies and Communications (SAITC)
Cyprus	Antonis ANTONIADES Senior Officer of Electronic Communications and Postal Regulation	Markellos POTAMITIS Officer of Electronic Communications and Postal Regulation
Czech Republic	David KOTRIS Acting Deputy Minister of the eGovernment Section, Ministry of Informatics of the Czech Republic	Marie SVOBODOVÁ Senior Counsellor Communication Infrastructure Department, Ministry of Interior of the Czech Republic
Denmark	Flemming FABER Head of the IT-Security Division National IT and Telecom Agency	
Estonia	Mait HEIDELBERG IT-Counsellor of the Ministry of Economic Affairs and Communications of Estonia	Jaak TEPANDI Head of the Chair of Knowledge-Based Systems, Department of Informatics, Tallinn University of Technology

Appendix 3
Members of the Management Board

Finland	Mari HERRANEN Ministerial Adviser Ministry of Transport and Communications	Mikael KIVINIEMI Ministry of Finance
France	Patrick PAILLOUX Central Director of Information Systems' Security Prime Minister/General Secretariat of National Defence/DCSSI	Isabelle VALENTINI Central Directorate of Information Systems' Security Prime Minister/General Secretariat of National Defence/DCSSI
Germany	Michael HANGE Vice President of the Federal Office for Information Security (BSI)	Jörn-Uwe HEYDER Federal Office for Information Security (BSI) International Relations
Greece	Nikolaos VLASSOPOULOS Hellenic Telecommunications and Post Commission	Prof. Constantine STEPHANIDIS Director Institute of Computer Science, Foundation for Research and Technology (FORTH)
Hungary	Dr. Ferenc SUBA VICE-CHAIR OF ENISA MANAGEMENT BOARD General Manager of CERT-Hungary	András GERENCSÉR Deputy Head of Department Ministry of Informatics and Communications of the Republic of Hungary
Ireland	Aidan RYAN Telecommunications Adviser Department of Communications	
Italy	Prof. Giandonato CAGGIANO Legal Adviser of the Ministry of Communications	Ciro ESPOSITO Head of Department for Innovation and Technology of the Italian Presidency of the Council
Latvia	Raimonds BERGMANIS Director, Department of Communications	Ingrida GAILUME Head of General and International Issues Division Department of Communications Ministry of Transport
Lithuania	Valdemaras SALAUSKAS Secretary of Ministry of Transport and Communications	Tomas BARAKAUSKAS Director of Communication Regulation Authority
Luxembourg	François THILL Accréditation, notification et surveillance des PSC	Pascal STEICHEN Ministère de l'Economie et du Commerce extérieur, Direction des Communications CASES
Malta	Joseph N. TABONE Chairman Malta Communications Authority	Colin CAMILLERI Chief Technical Officer Malta Communications Authority

Appendix 3
Members of the Management Board

The Netherlands	Edgar R. DE LANGE Ministry of Economic Affairs Director-General for Energy and Telecommunications	Ronald M. VAN DER LUIT Senior Policy Adviser Ministry of Economic Affairs
Poland	Krzysztof SILICKI Technical Director Research and Academic Computer Network (NASK)	Edward SELIGA Ministry of Interior and Administration Information Department Information Society Division
Portugal	Pedro Manuel BARBOSA VEIGA Presidente da Fundação para a Computação Cientifica Nacional (FCCN)	Manuel Filipe PEDROSA DE BARROS Director de Tecnologias e Equipamentos da Autoridade Nacional das Comunicações (ANACOM)
Romania	Liviu NICOLESCU Director General for Information Technology within the Ministry of Communications and Information Technology	Cristina STAN Chief of Department Ministry of Communications and Information Technology
Slovakia	Peter BIRO Information Society Division Ministry of Finance of the Slovak Republic	Ján HOCHMANN Information Society Division Ministry of Finance of the Slovak Republic
Slovenia	Gorazd BOZIC Head ARNES SI-CERT	Marko BONAC Director ARNES SI-CERT
Spain	Salvador SORIANO MALDONADO Deputy Director – Information Society Services Secretariat of State for Telecommunications and Information Society	Antonio ALCOLEA MUÑOZ Senior Officer – Information Society Services Secretariat of State for Telecommunications and Information Society
Sweden	Pernilla SKANTZE Head of Section Ministry of Enterprise, Energy and Communications	Anders JOHANSON National Post and Telecom Agency Director of the Network Security Department
United Kingdom	Geoff SMITH Head of Information Security Policy Information Security Policy Team	Peter BURNETT Corporate Strategy and Policy Centre for the Protection of National Infrastructure (CPNI)

Appendix 3
Members of the Management Board

Stakeholders' representatives

Group	Representative	Alternate
Information and Communication Technologies industry	Mark MACGANN Director General, European ICT & Consumer Electronics Industry (EICTA)	Berit SVENDSEN Executive Vice President Technology/ CTO of Telenor ASA and Chairman of Telenor R&D
Consumer groups	Markus BAUTSCH Stiftung Warentest, Deputy Head of Department	Jim MURRAY BEUC, Director
Academic experts in network and information security	Kai RANNENBERG T-Mobile Chair of Mobile Commerce & Multilateral Security, Department of Information and Communication Systems, Goethe University Frankfurt, (CEPIS)	Niko SCHLAMBERGER Statistical Office of the Republic of Slovenia, Secretary

EEA-country representatives (observers)

Iceland	Björn GEIRSSON Legal Counsel Post and Telecom Administration in Iceland	
Liechtenstein	Kurt BÜHLER Director Office for Communications	
Norway	Jörn RINGLUND Deputy Director General Ministry of Transport and Communications Department of Civil Aviation Postal Services and Telecommunications	Eivind JAHREN Deputy Director General Department of IT Policy Ministry of Modernisation

Appendix 4
Members of the Permanent Stakeholders' Group

Charles BROOKSON	British	DTI
Ilias CHANTZOS	Greek	Symantec/Business Software Alliance (BSA)
James CLARKE	Irish	WIT
Nick COLEMAN	British	IBM Europe
Andrew CORMACK	British	JANET/UKERNA/Terena
Roger DEAN	British	EEMA
Paul DOREY	British	BP
Philippe DULUC	French	France Telecom
Andreas EBERT	Austrian	Microsoft
Kurt EINZINGER	Austrian	ISPA Austria
Alfred EISNER	Dutch	ABM Consultancy
Giusella FINOCCHIARO	Italian	University of Bologna
Wim HAFKAMP	Dutch	Rabobank
Jaap-Henk HOEPMAN	Dutch	Radboud University Nijmegen/TNO
Urho ILMONEN	Finnish	Nokia
Gajewski JACEK	Polish	Consultant for NATO Public Diplomacy Division
Paul KING	British	Cisco
Cornelia KUTTERER	German	BEUC
Antonio LIOY	Italian	Politecnico di Torino
Evangelos MARKATOS	Greek	FORTH Institute
Vilma MISIUKONIENE	Lithuanian	Infobald Association
Magnus NYSTROM	Swedish	RSA Security
Jan ORUAAS	Estonian	Estonian Information Technology Society, Gelsenkirchen
Olivier PARIDEANS	Belgian	Alcatel
Sachar PAULUS	German	University of Brandenburg/SAP
Norbert POHLMANN	German	University of Applied Sciences
Yves LE ROUX	French	Computer Associates
Howard SCHMIDT	US	RH Consultancy
Jacques STERN	French	ENS
Claire VISHIK	US	Intel

Appendix 5
Members of the Ad Hoc Working Groups

Ad Hoc Working Group on Privacy and Technology

Mema ROUSSOPOULOS (Chair)	Greece	FORTH
Laurent BESLAY		European Data Protection Supervisor (EDPS)
Caspar BOWDEN	UK	Microsoft
Giusella FINOCCHIARO	Italy	University of Bologna
Marit HANSEN	Germany	ULD Kiel
Marc LANGHEINRICH	Switzerland	ETH Zurich
Gwendal LE GRAND	France	CNIL
Katerina TSAKONA	Greece	FORTH

Ad Hoc Working Group on Risk Assessment and Risk Management

Luigi CARROZZI	Italy	DG Public Contracts Observatory
Alain DE GREVE	Belgium	Fortis
Serge LEBEL	France	Premier Ministre, Direction, Centrale de la Sécurité des Systèmes d'information
Aljosa PASIC	Spain	Atos Origin
Reijo SAVOLA	Finland	VTT Technical Research Centre of Finland
Dr. Ingrid SCHAUMULLER-BICHL	Austria	Univ.-Doz. University of Applied Sciences, Hagenberg
Marcel SPRUIT	The Netherlands	Haagse Hogeschool
Dr. Lydia TSINTSIFA	Germany	Federal Office for Information Security (BSI)
Dr. Jeremy WARD (Chair)	UK	Symantec
Andrew WILSON (Observer)	UK	Information Security Forum (ISF)

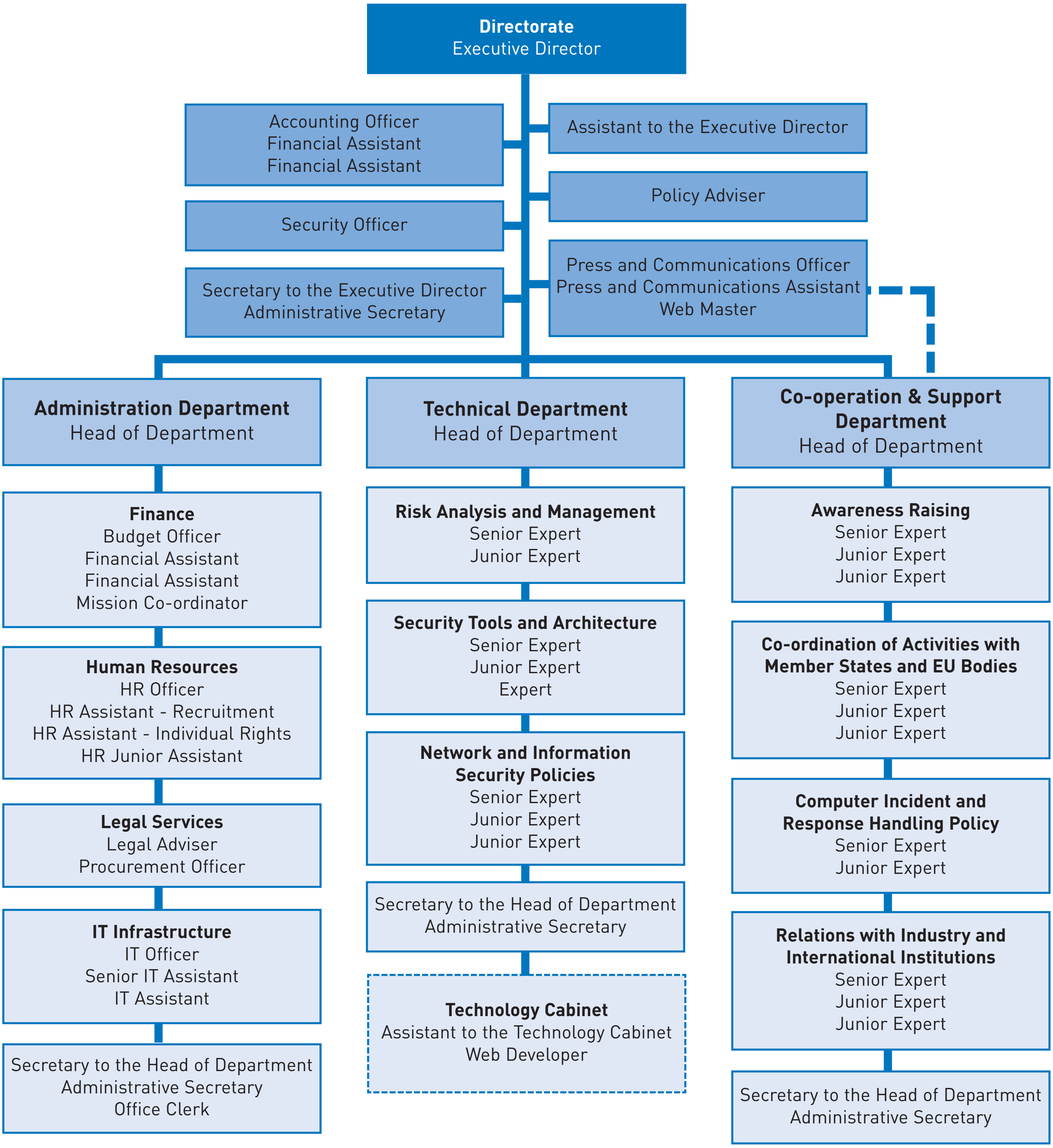
Appendix 6
National Liaison Officers

At 5 December 2007

Austria	Gerald TROST Bundeskanzleramt, Büro der Informationssicherheitskommission
Belgium	Rudi SMET Belgian Institute for Postal Services and Telecommunications
Bulgaria	Vasil GRANCHAROV Director of Crisis Management and Defence and Mobilisation Preparation Directorate, SAITC
Cyprus	Neophytos PAPADOPOULOS Director of the Commissioner's Office for the Control of the Telecommunications and Postal Services
	Antonis ANTONIADES Senior Officer of the Commissioner's Office for the Control of the Telecommunications and Postal Services
Czech Republic	Marie SVOBODOVÁ Communication Infrastructure Department, Ministry of the Interior of the Czech Republic
Denmark	Charlotte JACOBY IT-og Telestyrelsen National IT and Telecom Agency
Estonia	Toomas VIIRA Estonian Informatics Centre
Finland	Mari HERRANEN Ministry of Transport and Communications
France	Benedicte SUZAN Central Directorate for Information Systems' Security, General Secretariat of National Defence
Germany	Jörn-Uwe HEYDER Bundesamt für Sicherheit in der Informationstechnik
Greece	Georgios DROSSOS Hellenic Ministry of Transport and Communications, General Directorate of Communications, Directorate of Radio Frequency Management
Hungary	Ferenc SUBA Head of Department, Ministry of Informatics and Communications
Ireland	Aiden RYAN Telecommunications Adviser Department of Communications
Iceland	Björn GEIRSSON Legal Counsel
Italy	Giandonato CAGGIANO Legal Adviser of the Ministry of Communications
Latvia	Ingrida GAILUME Head of General and International Issues Division, Department of Communications, Ministry of Transport
Liechtenstein	Kurt BUEHLER Director, Office for Communications
Lithuania	Rytis RAINYS Head of Network and Information Security Division Communications Regulatory Authority
Luxembourg	Pascal STEICHEN Ministère de l'Economie et du Commerce extérieur, Direction des Communications Commerce électronique
Malta	Joanna BORG Senior Technical Specialist Malta Communications Authority
The Netherlands	Edgar DE LANGE Ministry of Economic Affairs Director-General for Energy and Telecommunications
Norway	Heidi KARLSEN Adviser, Ministry of Transport and Communications
Poland	Miroslaw MAJ NASK/CERT Team Manager Research and Academic Computer Network, CERT Polska
Portugal	Paulo FERREIRA Fundação para a Computação Científica Nacional
Romania	Liviu NICOLESCU Director General for Information Technology, Ministry of Communications and IT
Slovakia	Rastislav MACHEL CISSP
Slovenia	Radovan PAJNTAR Ministry of Higher Education, Science and Technology, Directorate Information Society, Directorate Trg
Spain	Salvador SORIANO MALDONADO Subdirector General de Servicios de la Sociedad de la Información
Sweden	Björn SCHARIN Adviser, National Post and Telecom Agency, Network Security Department
United Kingdom	Alice REEVES Assistant Director, Communications Security and Resilience, Department for Business, Enterprise and Regulatory Reform

Appendix 7
Administration

Organisation chart for 2007



Directorate
Executive Director

Accounting Officer
Financial Assistant
Financial Assistant

Security Officer

Secretary to the Executive Director
Administrative Secretary

Assistant to the Executive Director

Policy Adviser

Press and Communications Officer
Press and Communications Assistant
Web Master

Administration Department
Head of Department

Finance
Budget Officer
Financial Assistant
Financial Assistant
Mission Co-ordinator

Human Resources
HR Officer
HR Assistant - Recruitment
HR Assistant - Individual Rights
HR Junior Assistant

Legal Services
Legal Adviser
Procurement Officer

IT Infrastructure
IT Officer
Senior IT Assistant
IT Assistant

Secretary to the Head of Department
Administrative Secretary
Office Clerk

Technical Department
Head of Department

Risk Analysis and Management
Senior Expert
Junior Expert

Security Tools and Architecture
Senior Expert
Junior Expert
Expert

Network and Information Security Policies
Senior Expert
Junior Expert
Junior Expert

Secretary to the Head of Department
Administrative Secretary

Technology Cabinet
Assistant to the Technology Cabinet
Web Developer

Co-operation & Support Department
Head of Department

Awareness Raising
Senior Expert
Junior Expert
Junior Expert

Co-ordination of Activities with Member States and EU Bodies
Senior Expert
Junior Expert
Junior Expert

Computer Incident and Response Handling Policy
Senior Expert
Junior Expert

Relations with Industry and International Institutions
Senior Expert
Junior Expert
Junior Expert

Secretary to the Head of Department
Administrative Secretary

Appendix 7
Administration

General Administration, Legal Advice and Procurement

In 2007 the goal of the Administration Department was twofold: complying with the requirements for European Agencies and simplifying administrative procedures where necessary.

In the first of these tasks, ENISA built on the excellent groundwork carried out during the initial set-up phase of the Agency over the previous two years. In 2007 ENISA focused on the feedback that had been received through statutory audits. To date, all the requirements of the Internal Audit Service of the Commission have been met in full, and the Agency has maintained a clean record with the Court of Auditors and in reporting to the European Data Protection Supervisor (EDPS).

In terms of simplifying administrative procedures, the Administration Department focused on reducing unnecessary red tape where appropriate, by reviewing transaction work flows. As a result, although the annual budget of the Agency increased by about 21%, the total number of transactions completed remained almost unchanged.

In terms of budget execution, the overall target for 2007 was to exceed 95% of the significantly higher budget available (the actual figure achieved was 97,76%). Budget execution was channelled through 47 procurement projects. Additionally the Agency signed 63 agreements for services, supplies and co-operation with third parties.

In 2007, the Department carried out its tasks in full, keeping its original headcount unchanged. In other words, the same administrative resources now service an Agency that has increased its overall staff from 47 in 2006 to 59 occupied posts in 2007.

Highlights of the year include the 100% execution of the establishment plan in early 2007, continuous vigilance to respond to staff turnover and the temporary needs of the operational departments, and providing an average of about 10 hours of training for each staff member during the year.

The priorities of 2007 – striving for a lean administration, optimising the work flow and adopting electronic working tools and working methods – will be carried forward into 2008.

Internal Control Co-ordination

As a small Agency, ENISA only operates with an Internal Control Co-ordination function that ensures the needs of the service are met in terms of compliance with internal control standards and though the outsourcing of tasks. In 2007 ENISA joined the Framework Agreement on Internal Control which will allow it to enhance its level of compliance in years to come.

In 2007 the Report of the European Commission's Internal Audit Service assessed the adequacy, effectiveness and efficiency of ENISA's internal control system. Of the 14 comments received in 2006, 11 were closed in 2007; and the remaining 3 are planned to close by Q3 in 2008 when the risk assessment of the Agency by an external firm will have been concluded.

Audits

In 2007 the Agency underwent a scheduled internal audit. Carried out by the European Commission's Internal Audit Service, the audit focused on the organisational and compliance background against which the Agency operates. A scheduled external audit was carried out by the Court of Auditors to obtain reasonable assurance that the Agency's accounts are reliable and that the underlying transactions are legal and regular. The recommendations of both audits also addressed aspects of compliance raised in 2006. The audits mark a positive trend in improving the organisational basis of the Agency, as well as its commitment to compliance with applicable rules. Activities for 2008 include establishing a panel to handle reported irregularities and to move towards an integrated accounting system (ABAC).

Appendix 7 Administration

Physical Infrastructure

Many things that we take for granted are absolutely vital to keeping an Agency running. To mention but a few examples: procuring security services, general maintenance and office fixtures and fittings, moving walls to accommodate new staff, purchasing fuel and new equipment, tools, furniture, office supplies, plants, procuring travel agency services for all the staff's missions, providing electricity and installing sound/smoke isolation systems, installing fire safety systems, and meeting working conditions and safety standards for the staff.

One significant achievement this year was preparing the new wing of the building for the Agency, which was taken into use to accommodate new staff, requiring several new fittings and practical arrangements.

These general services are indispensable to optimise the operations of the Agency, to allow it to function and at the same time to ensure the best possible working environment for its staff. It also requires a substantial amount of administrative work, practical effort and cross-departmental meetings to make the building, the Agency and its staff 'run'.

Technical Infrastructure

In the first half of 2007 a Listserv service was installed. To date, several many-to-many distribution lists have been set up for user communities. In addition a one-to-many distribution list was set up for the automated distribution of the *ENISA Quarterly*. This also allows users to subscribe and un-subscribe themselves.

To increase the efficiency and quality of meetings involving external parties, the services of Genesys Meeting Centre were selected. This service gives users an online tool which is integrated into their e-mail client for setting up and conducting meetings; it has proved very efficient.

The second half of the year saw the arrival of the third member of the IT Section. This allowed for the implementation of 'Intra-ENISA', the Intranet of ENISA. In the first phase of development, general documents have been made available, as well as an events calendar, announcements list, news pages and a site for recreational activities for staff. A site for the IT Section was also launched, offering users a user-friendly interface to obtain IT help and support. Another new system, Centurio, was put into pilot phase. This system will allow the Human Resources Section to manage staff leave and allow staff to view their leave-related data online.

Apart from the usual ongoing maintenance and support services, the IT Section implemented a centralised network monitoring tool which gives a 'global' view of the various services offered and early warning of any potential problems. In addition, the installation of an Uninterrupted Power Supply (UPS) dedicated to the server room, as well as a fire extinguishing system, were completed.

Appendix 7 Administration

Human Resources

In 2007 ENISA faced a number of challenges in terms of Human Resources (HR) management. Substantial resources were allocated to the recruitment and induction of new staff due to personnel turnover as well as to training activities that grew considerably in comparison with 2006 (mainly for management and organisational training). Particular emphasis was also placed on staff performance appraisal, payroll and staffing costs. As a consequence of the integration of the HR and budget liaison office into the HR Section, the monthly management of salaries and allowances became an integral part of the management tasks of Human Resources.

Recruitment

In 2007 several recruitment procedures were carried out both for statutory staff (temporary agents and contract agents) and non-statutory staff (seconded national experts and trainees) in order to ensure the full functioning of all departments. Out of 18 recruitment procedures launched in Quarters one and three of 2007, 80% were successfully completed and suitable candidates were consequently appointed. A limited number of procedures will be completed at the beginning of 2008.

Statutory staff: A total of 441 applications were received for all advertised statutory positions. Candidates from all over Europe showed their interest in working for ENISA. The highest number of applications arrived from the old EU countries such as Greece, Italy, Germany and France. An increasing interest for assistant positions was shown by candidates from the new Member States such as Romania, Bulgaria and Poland. The gender balance was almost equal with a consistent majority of male applicants for technical posts and female applicants for secretarial and assistant jobs. The age indicator presented in the graphs below shows that the Agency continues to attract relatively young professionals aged between 31 and 40 years, which reflects the dynamic environment of NIS.

Non-statutory staff: In 2007 two procedures were carried out for the selection of five National Experts to be seconded to the Agency's operational departments. The national administrations continued to demonstrate an encouraging degree of co-operation with ENISA and facilitated the secondment of highly qualified professional experts.

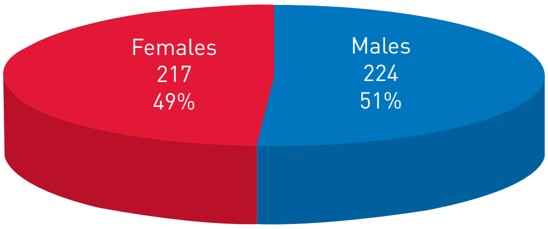
Two additional selection procedures were concluded in order to offer 5-month traineeship grants to young university graduates in the field of network and information security. Thanks to the implementation of its second and third traineeship programme, ENISA welcomed four young trainees from Austria, Greece, Lithuania and Italy, and benefited from their up-to-date academic knowledge and professional enthusiasm.

The HR team also completed the selection of a local employment agency to enable ENISA to hire appropriate support staff to meet short-term need.

With regard to the recruitment procedures completed in 2007, the following graphs show statistics about the applicants, based on the following indicators:

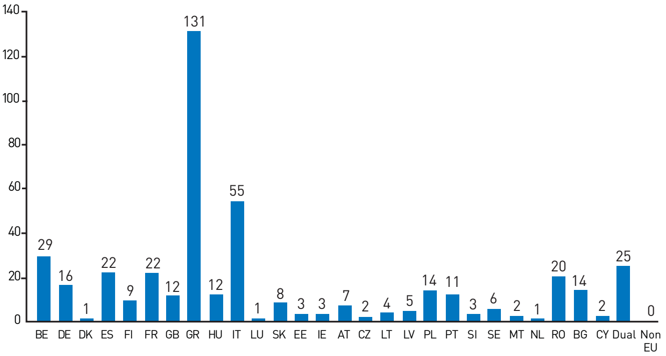
1) Gender: In comparison with 2006, the number of female applicants has slightly diminished; the fact that the majority of advertised vacancies in 2007 was for technical posts may have been a factor in this.

Applicants by Gender



2) Nationality: ENISA has continued to attract female and male applicants from the older and more southern Member States, in particular from Greece, Italy, Belgium, Spain and France. The number of applicants from the countries which have joined the EU recently has increased considerably (particularly from Romania and Bulgaria).

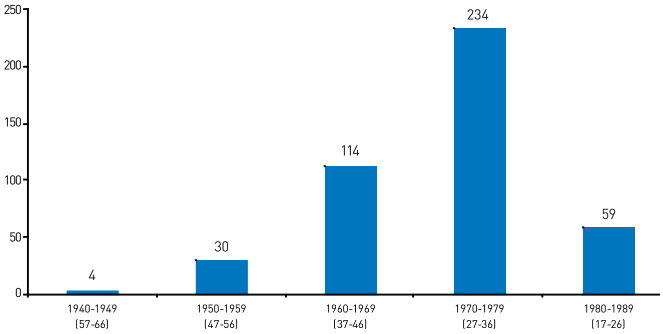
Applicants by Nationality



Appendix 7
Administration

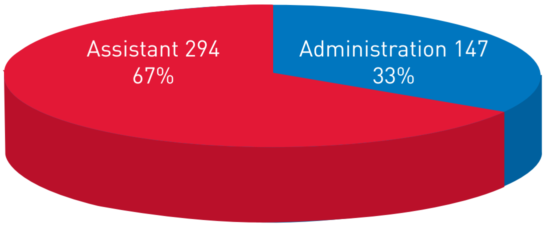
3) Age: The Agency continues to attract young professionals aged between 30 and 40 years.

Applicants by Age



4) Function group: The percentage of applicants for the assistants' function group has increased by 10% compared with 2006. This shows a new tendency, indicating the difficulties which the Agency is experiencing in attracting highly experienced staff for administrators' posts.

Applicants by Function Group



Staff Members

At 31 December 2007

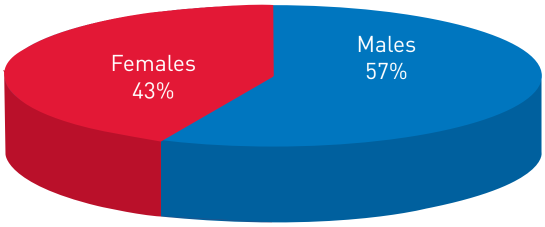
In 2007 73% of the posts foreseen in the establishment plan were filled. The number of new staff appointed remained quite high. However, in comparison with 2006, the high rate was not due to an increase in the number of posts but to the re-publication of vacancies and staff departures. The HR team welcomed 15 new staff members and ensured their smooth relocation into their new working and living environment.

By the end of 2007 the Agency's staff comprised 53 statutory staff members (made up of 42 temporary agents and 11 contract agents) compared with the target anticipated in the Agency's budget of 56 statutory positions.

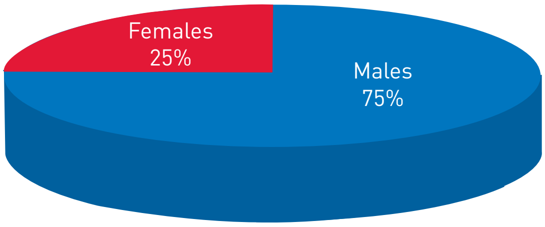
An analysis of the ENISA staff, looking at four main indicators (gender, nationality, age and function group) produces the following conclusions:

1) Gender: The separation between males and females remains balanced, as in 2006. There is a slight increase in female staff; however male staff continue to make up the majority, with a high percentage of males in the administrators' function group.

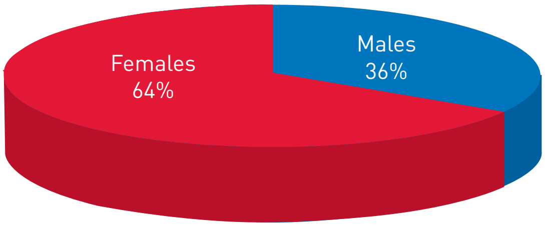
Staff Members by Gender



Administration Staff Members by Gender

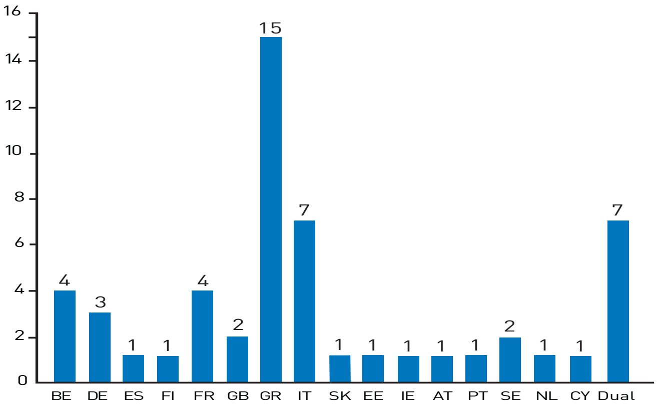


Assistant Staff Members by Gender



2) Nationality: 16 out of 27 nationalities of the European Union are represented with a high percentage from the 'old' Member States (Greece, Italy, Belgium, France and Germany).

Staff Members by Nationality

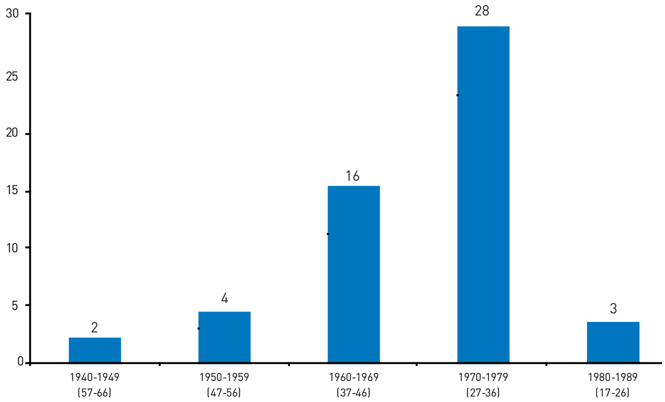


Appendix 7
Administration

3) Age: The majority of staff continues to be aged between 31 and 40 years. Since its establishment, the Agency has attracted mainly young professionals oriented to achieving objectives and increasing their performance.

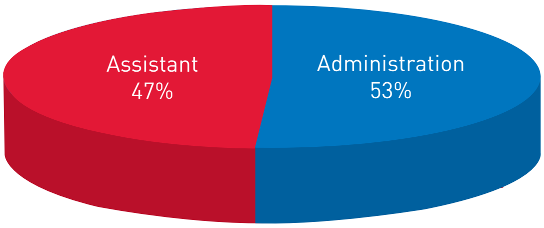
The Agency's location and the grading of the advertised posts have a direct impact on the age of the applicants and the composition of the Agency's staff.

Staff Members by Age



4) Function group: The majority of staff members occupy posts at administrator level with a high percentage of male staff. The majority of female staff occupies assistants' positions.

Staff Members by Function Group
Administration-Assistant



Recruitment policy: All calls for expression of interest in ENISA posts were published on the Agency's website as well as on the website of the European Personnel Selection Office. Technical posts were also advertised in the specialised press.

ENISA takes great care in its recruitment procedures to avoid any form of discrimination based on age, race, political, philosophical or religious conviction, gender or sexual orientation, disabilities, marital status or family situation. The Agency strictly applies the rules of the Staff Regulations of the European Communities in respect of the principles of equal treatment, transparency and objectivity.

Training

In 2007 enhanced emphasis was put on the training activities that have increased considerably since the Agency was set up. ENISA considers training an integral part of its human resources policy. Training expands and improves individuals' competencies so that each staff member can contribute optimally towards achieving the Agency's goals and can reflect its core values of excellence, professionalism and service.

Language courses in Greek, English, French and German continued to be delivered throughout the year. This training is aimed at facilitating the integration of the staff into the local environment and improving communication skills. Additional training in organisational and personal development, as well as management training, were successfully delivered on the Agency's premises by highly experienced trainers.

In 2007 ENISA reached the overall objective of providing an average of 10 days of training per person per year, in accordance with the guidelines set by the Commission's Learning and Development Framework.

Additionally HR supported the staff in their participation in individual training courses at specialised training centres outside Heraklion. These training courses, organised through individual initiative, enable the staff to enhance their professional knowledge.

Other HR Developments

A number of HR policies were also introduced to improve the working conditions of ENISA's staff such as the code of conduct and the appraisal system. With specific attention to the latter, the first yearly career development report (CDR) exercise was launched in 2007 and contributed to the performance assessment of the entire staff. Career objectives and training paths were also set for the professional development of each staff member. The overall appraisal evaluation confirmed the high level of ability, efficiency and integrity of the Agency's staff.

HR worked in close co-operation with ENISA's Staff Committee in order to establish and maintain an open and constructive bilateral dialogue between staff and management. Among its activities, the Staff Committee was involved in recruitment procedures and nominated a full member of the selection interviews for all interviews organised for temporary and contract agents. The Staff Committee was also consulted on the finalisation of the implementing rules of the Staff Regulations and on any relevant matter related to staff welfare.

The HR team also dealt with general HR activities that entail recurrent daily tasks, such as leave and absence management, financial operations, the follow up of specific budget lines linked to training, medical visits, expenses for interviewing candidates and hiring of interim staff.

Appendix 7
Administration

Finance and Accounting

The Finance and Accounting Sections carry out functions associated with the management of the Agency's Budget, the preparation of the Financial Statements in line with its Financial Regulation and the Audits conducted by the Court of Auditors.

Specific activities of the two sections include:

- Implementation of the approved budget
- Establishment of Internal Controls, as appropriate, in order to address possible financial risks
- Reporting on the Annual Budget, including budget status reports and providing an analysis of key aspects
- Budget revision and execution of budgetary transfers
- Planning of the Budget and presentation to the Management Board and the Budgetary Authority for adoption, as appropriate
- Ensuring adherence to the accounting rules
- Validation of the new systems put in place and continuous checking of existing ones
- Keeping the Accounts
- Preparation of the Annual Financial Statements
- Preparation of the Reporting Package for consolidation purposes with the European Commission's Accounts
- Regular financial reporting to the European Commission and the Court of Auditors

Budget Execution

The Budget 2007, as amended on 25 September 2007, reached €8.416.928, which represents an increase of 21% compared with 2006 (€6.940.080). Appropriations were committed at a rate of 97,76% (compared with 90% committed in 2006) to honour obligations related to the operational costs of the Agency and the activities required under the Work Programme 2007. Payments reached the level of 73,51% of the total appropriations managed. This is an indication of very positive performance, showing an upward trend in the capacity of the Agency to use the budget with which it is entrusted. This was achieved in conditions of increased efficiency, as the total number of transactions required has remained relatively unchanged since 2006 and, at the same time, 17,5% of the budget was only made available in the fourth quarter of the year. This explains the high rate of appropriations carried over and the relatively low rate of appropriations paid in 2007.

The Agency's budget is divided into three parts or 'titles':

- **Title 1 – Staff expenditure:** Staff expenditure was as foreseen, with 97,41% of appropriations committed at the end of the year. The respective rate of payments was 94,34%. The management of Title 1 funds improved when compared with 2006, where the respective rates demonstrated commitments of 92,54% and payments of 87,75% on appropriations.

- **Title 2 – Administrative expenditure (Functioning of the Agency):** The funds allocated to administrative expenditure were used as planned, with 97,22% of appropriations being committed by the end of the year, and 77,82% paid. The respective figures for 2006 were 92% and 77,11%.

- **Title 3 – Operating Expenditure:** 98,42% of the funds allocated to the operating expenditure of the Agency, i.e. the funds directed to the core business of the Agency according to the 2007 Work Programme, were committed, with the total rate of paid appropriations reaching 43,71%. The respective figures for 2006 were 82,80% and 53.63%.

Financial Reporting

According to Article 82 of the Financial Regulation, the Agency's Accounting Officer sent to the Commission's Accounting Officer the Provisional Accounts, together with the Report on Budgetary and Financial Management. Subsequently the Commission sent the Provisional Accounts to the Court of Auditors.

Based on the observations of the Court of Auditors, the Executive Director sent the Final Accounts to the Management Board which gave its opinion on them. Finally the Executive Director submitted Final Accounts along with the opinion of the Management Board to the Commission, the Budgetary Authority and the Court of Auditors.

The Final Annual Accounts will be published in the Official Journal of the European Communities together with the statement of assurance which will be given by the Court of Auditors.

The Financial Statements included in the Annual Accounts are the following:

Appendix 7 Administration

Balance Sheet

	31.12.2007	31.12.2006
I. Non Current Assets	**373.352**	**344.932**
Intangible fixed assets	36.176	32.564
Tangible fixed assets	337.176	312.368
II. Current Assets	**2.480.483**	**2.575.036**
Short-term receivables	101.357	55.843
Cash and cash equivalents	2.379.126	2.519.193
Total Assets	**2.853.835**	**2.919.968**
III. Non Current Liabilities		
IV. Current Liabilities	**1.410.260**	**2.289.543**
EC pre-financing received	328.971	1.124.138
EC interest payable	125.560	88.829
Accounts payable	113.977	432.531
Accrued liabilities	686.535	578.173
Provisions	155.216	65.872
Total Liabilities	**1.410.260**	**2.289.543**
V. Net Assets	**1.443.575**	**630.425**
Accumulated result	1.443.575	630.425
Total Net Assets	**1.443.575**	**630.425**

Economic Out-turn Account

	2007	2006
Revenue from the Community Subsidy	7.987.957	5.475.862
Other revenue	202.642	12.309
Total Operating Revenue	**8.190.599**	**5.488.171**
Administrative expenses	-5.176.051	-4.717.893
Staff expenses	-3.572.833	-3.100.024
Fixed asset related expenses	-125.837	-103.279
Other administrative expenses	-1.477.381	-1.514.590
Operational expenses	-2.198.765	-1.236.173
Total Operating Expenses	**-7.374.816**	**-5.954.066**
Surplus/(deficit) from operating activities	**815.783**	**-465.895**
Financial expenses	-2.633	-1.932
Surplus/(deficit) from ordinary activities	**813.151**	**-467.827**
Economic Result for the Year	**813.151**	**-467.827**

Cash Flow Statement

	2007	2006
Surplus/(deficit) from ordinary activities	**813.151**	**-467.827**
Operating activities		
Amortisation (intangible fixed assets)	12.516	9.392
Depreciation (tangible fixed assets)	113.322	93.887
Increase in provisions for liabilities	89.344	0
Increase in short term receivables	-27.361	-42.566
Decrease in accounts payable	-121.991	-606.436
Increase in liabilities to consolidated entities	-864.790	1.126.736
Net cash flow from operating activities	**14.190**	**113.186**
Cash flows from investing activities		
Purchase of tangible and intangible fixed assets	-154.257	-104.043
Net cash flow from investing activities	**-154.257**	**-104.043**
Net increase in cash and cash equivalents	-140.067	9.143
Cash at the beginning of the period	2.519.193	2.510.050
Cash at the end of the period	**2.379.126**	**2.519.193**

Statement of Changes in Capital

	Reserves	Accumulated Surplus/ Deficit	Economic result of the year	Capital
Balance as of 1 January 2007	**0**	**1.098.252**	**-467.827**	**630.425**
Allocation of the Economic Result of Previous Year		-467.827	467.827	0
Economic result of the year			813.151	813.151
Balance as of 31 December 2007	**0**	**630.425**	**813.151**	**1.443.575**

European Commission

General Report 2007
European Network and Information Security Agency

Luxembourg: Office for Official Publications of the European Communities

2008 – 64 pp. – 21cm x 29.7cm

ISBN: 978-92-9204-004-8
ISSN: 1830-981X
Catalogue no.: TP-AB-08-001-EN-C

The report is also available on mini disk:

ISBN: 978-92-9204-005-5
ISSN: 1830-9828
Catalogue no.: TP-AB-08-001-EN-Z

How to obtain EU publications

Priced publications are available from the EU Bookshop
(http://bookshop.europa.eu/), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.
You can obtain their contact details by sending a fax to (352) 29 29-42758.

ENISA General Report 2007

TP-AB-08-001-EN-C

enisa
European Network and Information Security Agency

ENISA – European Network and Information Security Agency
PO Box 1309, 710 01, Heraklion, Greece
Tel: +30 2810 39 12 80, Fax: +30 2801 39 14 10
www.enisa.europa.eu

Publications Office
Publications.europa.eu

ISBN 978-92-9204-004-8

01/07_08