enisa
European Network and Information Security Agency

General Report 2008

European Network and Information Security Agency

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 2009

Luxembourg: Office for Official Publications of the European Communities, 2009
ISBN: 978-92-9204-021-5
ISSN: 1830-981X
doi 10.2824/10051

Printed in Belgium
PRINTED ON WHITE CHLORINE-FREE PAPER

Clear Targets, Tangible Results
A Message from the Executive Director

Every year, the European Network and Information Security Agency delivers a presentation of its task and activities. I am pleased to invite you to read through the following pages to better understand the mission and work of this European Agency. ENISA, which is now entering its fourth year of operation, is now fully living up to expectations. The Work Programme 2008 was implemented as foreseen and all departments of the Agency worked well and delivered impressive results. A full list of the deliverables published in 2008 is included in Appendix 7.

In addition, some extra miles were achieved in 2008. The NIS Summer School, for example, initiated by our hosting Institute in Crete, FORTH, was particularly successful. It attracted 100 participants, as well as speakers from all over Europe and Third Countries, and will be repeated in September 2009.

Another highlight for ENISA was the press conference held in the Berlaymont Press Room in Brussels in May 2008, under the auspices of DG COMM. It was a golden opportunity to explain to the international press, as well as our colleagues in Brussels, the tangible risks of a 'digital 9/11' and to send out a request to combat cyber-crime worldwide, while at the same time proudly demonstrating the Agency's many achievements. This event generated enormous positive media impact in the written press and on television, which in turn reverberated among our key stakeholders.

2008 was a year in which we saw the flourishing results of the seeds we have been sowing since the Agency began operating, back in 2005. NIS is an ever-growing concern in everyday life, and our mission is to spread awareness, assess risks and to raise the profile of NIS with the general public, thus influencing the political agenda.

The NIS environment is rapidly changing and ENISA has always responded to demand. For example, the Agency facilitated the establishment of a CERT in the Baltic States, which helped equip Estonia to tackle the massive cyber-attack it suffered in 2008. Our efforts, however, have not been limited to the European borders. In 2008 we had the chance to participate in international fora (for example, the OECD and the ITU) and we worked alongside our valued counterparts and stakeholders in countries such as Japan, P.R. China, the USA, South Africa and Israel, thus raising our profile at the global level. For example, ENISA acted as a matchmaker between the CERT-FI, Finland, and the CSIR/MERAKA, South Africa, to facilitate the exchange of good practice and the establishment of a South African CSIRT.

However, our aim to consolidate ENISA as the European hub of Network and Information Security, and indeed a Centre of Expertise in the field, was temporarily challenged in 2008. There were proposals to merge ENISA into a new agency. We received a visit by a European Parliament delegation on 30 April with a view to preparing their position on this proposal and the role of ENISA. The Agency demonstrated the value of its contribution to the challenges in European NIS convincingly and, the following week, the ITRE Committee publicly praised ENISA's work and the quality and dedication of our people in Parliament, resulting in a three-year extension of the Agency's Mandate until March 2012.

NIS is increasingly critical for the European and global economies. The need for secure networks, systems and services will certainly not suddenly disappear in 2012. Following the EU parliamentary elections in 2009 and the establishment of a new European Commission, this extension of our Mandate allows time to plan for ENISA's role beyond 2012. In a landscape of ever-evolving threats, the importance of Network and Information Security needs constant reinforcement. The fact that NIS touches both the economy of Europe and the daily lives of its citizens means that we cannot afford to neglect it for a moment.

Clear Targets, Tangible Results
A Message from the Executive Director

The need for NIS is now appearing regularly both on the political agendas of Member States and in the international media. This new visibility gives European citizens a better insight into and understanding of the daily threats they face at home and at work. Whether it be the dangers in social networks, the concern for child protection online or privacy and data protection challenges, ENISA is tackling the problem. This annual report shows the ever closer co-operation between our Agency, the European Commission and the Member States in a joint effort towards strengthening NIS.

ENISA could not fulfil its commitment to provide 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. So, as Executive Director, it has been a professional fulfilment for me to witness the Member States' support of the Agency by their direct actions. I would therefore like to express my sincere gratitude 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 local authorities and FORTH, the research centre that hosts and supports ENISA.

As further evidence of its support, and to assist ENISA in the performance of its work, the Greek Ministry of Transport and Communications has approved funding to provide the Agency with an office in Athens. This will facilitate meetings with stakeholders from the EU, EFTA and Third Countries. The inauguration of this branch office will take place in 2009.

In addition, the host Member State signed a contract in December 2008 for the construction of new premises for the Agency in Heraklion to accommodate possible further expansion of the Agency. The new building will be able to house more than 100 staff with appropriate logistics services.

Looking to the future, 2009 will be my last year in command of the ENISA ship. I started this voyage in October 2004. Today ENISA is a well established Agency with a reputation as a reliable centre of expertise for NIS. For this, thanks are due to the staff of ENISA and to all those who have supported us over the years. I feel proud that I will be able to hand over to my successor an Agency that is implementing its ambitious programmes competently and successfully and that is well regarded by the European Community institutions and its stakeholders.

Andrea Pirotti
Executive Director

Contents

ENISA – NIS is people

Networks, people and technology

In the 21st century, we take for granted innovations such as mobile phones, personal computers, online banking, eHealth and eCommerce. 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 Expertise in NIS. Its mission is to enhance the level of NIS in Europe by:

- Giving **independent, expert advice** to the EU
- Promoting **good practices in, for example, risk assessment & risk management, awareness raising and computer security incident response**

ENISA is **bridging the gap** between industry and governments, acting as a knowledge **broker** of information and good practices for EU Member States. ENISA is uniquely positioned to be a 'matchmaker' of knowledge, because of its comprehensive overview of the NIS situation within the EU. In the international context, ENISA is the European spokesman on good practice in NIS to the outside world.

A recent resolution of the European Council recognises that

> **"the establishment of ENISA has been a major step forward in the EU's efforts to respond to the challenges relating to network and information security".**

CHAPTER 1
Introduction

- NIS in Europe – 2008 and Beyond
- Executive Summary – ENISA in 2008
- 2009 and Beyond

NIS in Europe – 2008 and Beyond

We live in an information-centred society, where the use of Information and Communications Technologies (ICTs) has rapidly accelerated. ICTs have become essential tools in human, social and economic interaction. It is now widely accepted that the availability, reliability and security of networks and information systems are central to the success of our economies and of society. This can only be achieved through a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment.

Network and Information Security is a challenge for everybody:

- **Public administrations** need to make informed policy decisions and to address the security of their own systems, not just to protect public sector information, but also to serve as an example of good practice for other players.
- **Enterprises** increasingly see NIS as a critical element in their success or failure, but also as an element of competitive advantage rather than as a 'negative cost'. They need to be given the tools to exploit ICTs securely.
- **Individual users** are the targets of malware and extortion through botnets, and suffer real economic and emotional damage as a result of poor NIS practices. Users must be made aware of how they can protect themselves and the security of the network as a whole.

ENISA was created to provide a focal point for information, co-operation and facilitation in Network and Information Security (NIS). Its activities support the European Commission's drive for a secure Information Society based on enhanced NIS and a widespread culture of security. A recent Council resolution recognises that "the establishment of ENISA has been a major step forward in the EU's efforts to respond to the challenges relating to network and information security".

NIS in Europe – 2008 and Beyond

Key Challenges

- **Interconnectivity** – New services such as Social Networking, Federated Identity and VoIP depend heavily on complex, interdependent networks. As interdependencies increase, a disruption in one infrastructure can easily propagate into other infrastructures creating a Europe-wide domino effect. Global interconnectivity brings with it the disappearance of national network boundaries and injects an international dimension to what may previously have been only a localised incident. The vulnerabilities increase if any of the network operators, service providers, equipment suppliers, and networks operating across Member States' boundaries are using immature technologies.
- **Mobile communications** – Striking a balance between backward compatibility requirements and the need to explore new architectures to build future Internet, mobile, broadband and associated service infrastructures poses a major security challenge. The increasing deployment of mobile devices and mobile-based network services opens up new risks. Mobile communication devices could eventually prove to be a more common route for attacks than personal computers, due to their increased complexity and interoperability with more open networks.

- **Failure to build security into product development** – The liberalisation of the telecommunications markets has increased competitive pressures on service providers, leading them towards more cost-effective infrastructure investments with a direct impact on the quality of software and hardware components. This sometimes means that the security of network components is not always given the highest priority throughout the entire product lifecycle (e.g. through design, development, deployment, support).
- **Outsourcing of network infrastructure management** – Several service providers have outsourced the management of their network infrastructures without the appropriate quality and security measures being fully provided.
- **Growing fraud** – Increasingly attacks on information systems are motivated by profit, rather than by the desire to create disruption for its own sake. Data are illegally mined, often without the user's knowledge.
- **New technologies need stronger authentication mechanisms** – With the explosion of Web 2.0 technologies and multiple interlinked data-sources, many people are unwittingly exposing highly sensitive personal information without appropriate privacy protection. The lack of strong, interoperable authentication mechanisms makes controlling appropriate access to data and services very costly and often ineffective.

Strengthening trust in the use of networks, software and services for governments, businesses and consumers remains a major task. A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is concern that security problems may discourage users and lead to a lower take-up of ICT, jeopardising both potential economic growth and society's development.

CHAPTER 1 – Introduction
Executive Summary – ENISA in 2008

To maximise the effect of its limited resources and increase its impact on key areas, ENISA focussed its efforts in 2008 on a number of strategic priorities. A new Work Programme approach was adopted, with a series of Multi-annual Thematic Programmes (MTP), which define the work of the Agency for the coming years. The Work Programme also includes 'Preparatory Actions' (PAs) – activities lasting one year to investigate the possibility of initiating new MTPs.

The tasks outlined in the Work Programme were carried out according to plan. In some cases, the Agency went the extra mile, taking the work further than originally requested.

In 2008, ENISA focussed on three MTPs and one PA.

Improving Resilience in European eCommunication Networks (MTP 1)

Reliable communications networks and services are now critical to public welfare and economic stability. Public institutions, citizens and businesses all demand an acceptable level of service in the networks, with resilience to faults and disruption of their normal operation. As real-time applications become more popular with the widespread use of innovations such as Voice over Internet Protocol (VoIP), instant messaging and IP-based desktop video, 21st century man is now so reliant on Information and Communication Technologies (ICT) that life grinds to a standstill with any network outage.

Physical phenomena, software and hardware failures, human mistakes or intentional attacks can all affect the proper functioning of public eCommunication networks. The first step in improving resiliency – and the focus of ENISA's work in this area in 2008 – is to take stock of Member States' existing policy and regulatory frameworks related to the resilience of public eCommunication networks.

ENISA is thus addressing three key strands:

- National policies and regulations
- Measures deployed by operators
- The use of existing technologies such as Domain Name System Security Extensions (DNSSEC) and other advanced technologies to enhance resilience

The stocktaking exercise was successfully completed in 2008 and ENISA is now analysing the results to identify common measures and good practices deployed in the different Member States – as well as gaps and inconsistencies. After further consultations, ENISA will then be able to recommend action to the different categories of stakeholder.

To complement its analysis of the measures deployed by operators, in 2008 ENISA also addressed Business Continuity, undertaking a survey into availability and continuity issues to assess the current state of play among providers of eCommunication infrastructures (mainly telecommunication companies and Internet Service Providers). The results reinforced the importance of continuity to telecommunication providers. An inventory of Business Continuity methods and tools was also produced to help users understand their needs and to acquire information about existing approaches to Business Continuity.

Developing and Maintaining Co-operation between Member States (MTP 2)

Addressing the challenges facing NIS in 2008 and beyond requires a systematic, coherent and integrated strategy that involves all concerned stakeholders and decision-makers and is based on dialogue, partnership and empowerment. To expand and improve the opportunities for Member States to share information on good practices, ENISA is developing various models of co-operation in predefined areas, such as awareness raising, incident response and eID. In addition, the Agency is further developing its European NIS Good Practice Brokerage, with supporting tools such as the Online Platform, the Who-is-Who Directory and 'Country Reports' of activities in the Member States.

CHAPTER 1 – Introduction
Executive Summary – ENISA in 2008

Highlights of the year in this respect include the various thematic workshops that help foster a relationship with existing NIS communities (such as Computer Emergency Response Teams (CERTs)) or build up new communities which share common interests in specific NIS topics (for example, Awareness Raising and eID). The Agency has further developed its existing contacts and networks throughout the year, including the network of National Liaison Officers (NLOs) and National Competent Bodies.

A Co-operation Platform for the Awareness Raising Community

In February 2008, ENISA launched the Awareness Raising (AR) community, a subscription-free community open to experts who have an interest in raising information security awareness within their organisations. It is designed to help foster a culture of information security and to serve as a point of contact for matters related to information security awareness. The community now embraces some 40 nations and comprises 167 members; all European Union (EU) and European Economic Area (EEA) countries are represented with the exception of Liechtenstein. Membership applications have also been welcomed from outside Europe.

ENISA reviewed its 'Users' guide: How to raise information security awareness' in the light of new research and analysis and published a revised version in 2008. A White Paper on 'Obtaining support and funding from senior management' was also produced to help raise awareness among senior management about the importance of endorsing information security awareness within an organisation. A more in-depth analysis of financial organisations led to an additional publication specifically for that sector.

Two topical papers were released on the security of corporate data. One addresses the inherent risks for business assets if secure printing policies are not in place. Unintended disclosure of sensitive information, such as invoices, employee records and customer details, may jeopardise crucial company assets and confidential data. In the second paper, ENISA advises on the threats from accidental loss or theft of confidential corporate data on unsecured USB flash drives. These reports highlight potential risks and list good practice guidelines to help readers overcome obstacles within their organisations.

With every passing day, a new social networking website seems to spring up, and entertainment companies are rushing to exploit the latest new market – the younger generation. Children are on the Internet at an earlier age than ever before and, according to research conducted by EMarketer Inc, around 20 million children and tweens will visit virtual worlds by 2011 – up from 8.2 million in 2007. Inevitably, this raises enormous safety concerns. ENISA has therefore produced a White Paper, 'Children on virtual

worlds: what parents should know', to provide clear and comprehensive information about virtual worlds, the risks children can encounter and what parents can do to protect their children and help them understand how to behave in virtual worlds to reap the many potential benefits whilst minimising the dangers.

Other awareness raising projects in 2008 included a White Paper explaining the threat of social engineering, a survey into how various Scandinavian regions and municipalities are currently working on information security management, and the production of a set of quiz templates for parents, end-users and executive managers of small and medium-sized enterprises (SMEs) to test their level of security awareness.

Sharing Good Practice in CERT Communities

The number of EU Member States with their own governmental or national CERT is growing (due in no insignificant part to the efforts of ENISA), but coverage can still be improved. ENISA continues to help establish new CERTs – even beyond the borders of Europe: in 2008, ENISA and Finland together supported the setting up of a national CERT capability in South Africa, proving just how far ENISA's reputation has advanced! This project is an excellent example of the work of ENISA's Good Practice Brokerage in action.

CHAPTER 1 – Introduction
Executive Summary – ENISA in 2008

The annual ENISA Workshop on CERTs in Europe took place in May 2008 in Athens, providing an opportunity for CERTs new and old to extend their network of contacts, thus enhancing their ability to react quickly and effectively to cyber-incidents and increasing the overall robustness of information networks.

The lack of a common good practice approach for CSIRT exercises poses one of the greatest obstacles for teams trying to run cross-border exercises and develop common knowledge. In December 2008 ENISA published a collection of 'Good practices for CSIRT exercises', aimed at enhancing the operational capabilities of incident response teams at various levels. The two books (one for students, the other for teachers) are accompanied by various LiveDVDs with material for the exercises.

Supporting the Faster Take-up of Interoperable eIDs in Europe

Electronic Identity (eID) is part of the EC's i2010 initiative and eGovernment plans for Europe; the objective is to have efficient, effective and interoperable eGovernment systems in Europe by 2010. The slow take-up of pan-European electronic identification (eID) services is significantly influenced by the lack of a consistent, interoperable eID infrastructure. Despite the efforts made by some Member States, there is still fragmentation, not only on technical but also on legal and regulatory issues. Interoperability work and the identification of good practices would help accelerate the uptake of secure pan-European services.

ENISA has therefore joined forces with leading pan-European initiatives and interoperability frameworks. In particular, in 2008 the Agency conducted a study into current policy and implementation issues for electronic identity in Europe. The Agency has produced a Position Paper containing an overview of existing European eID specifications and explaining the privacy-enhancing technologies – 'Privacy Features' – which can be found in existing technical specifications and European standards.

Mobile devices, such as smart phones and PDAs, play an increasingly important role in the digital environment. Besides their primary use, these devices offer the possibility of electronically authenticating their owner to a service. This, of course, also brings new security and privacy risks. An ENISA Position Paper on 'Security Issues of Mobile Electronic Identity (Authentication)' summarises the contributions of an international expert group from Europe, the USA and Asia. By looking at different use-cases such as NFC payment and trustworthy viewing, ENISA has identified the security risks which need to be overcome, and offers an opinion both about their relevance and existing mechanisms that might help mitigate these risks.

One of the concepts of eID interoperability is the idea of Authentication Assurance Levels; four such levels have been defined to foster interoperability by providing a common policy language for describing authentication assurance strength. In 2008 ENISA mapped these authentication levels to a machine readable format using the OASIS SAML standard, making them widely accessible. At the same time, the Agency has produced a gap analysis with documented technical information and guidance on how to implement these authentication levels in eGovernment applications using SAML context classes.

CHAPTER 1 – Introduction
Executive Summary – ENISA in 2008

European NIS Good Practice Brokerage

The exchange of good practices between EU Member States (MSs) is essential to enhance the level of Network and Information Security on a pan-European scale. Several MSs already share their experience but, to fully develop the EU's NIS capabilities, it is crucial that a more structured approach is applied to the exchange of NIS good practices. To facilitate co-operation and the sharing of expertise and experience, ENISA has established a European Good Practice Brokerage. By acting as a good practice broker in the European NIS 'marketplace', the Agency facilitated several co-operative projects among the MSs in 2008 and helped Member States make real progress in NIS.

ENISA was able to assist Bulgaria in the establishment of a governmental Computer Emergency Response Team (CERT), offering its own expertise and facilitating the transfer of hands-on experience from CERT-Hungary. The Agency also brought together CERT-FI, Finland, and CSIR/MERAKA in South Africa to enable the exchange of good practice aimed at the establishment of a South African Computer Security Incident Response Team (CSIRT).

In the context of the European NIS Good Practice Brokerage, a closed workshop on structured cyber-crime-related information exchange between the financial sector and the government was organised in November 2008 by the Dutch Financial Information Sharing and Analysis Centre (FIISAC)/NICC, the Theodore Puskas Foundation/CERT-Hungary and the Security Working Group of the Hungarian Banking Association, with the support of the Netherlands Bankers' Association (NVB). ENISA facilitated this co-operation by helping to identify participants from other MSs, supporting their participation, and by contributing to the drafting of the agenda and during the workshop's preparation and discussion.

Identifying Emerging Risks for Creating Trust and Confidence (MTP 3)

The speed with which new technologies and applications are being introduced brings new risks on an almost daily basis. There is a pressing need to identify, assess and manage these emerging and future risks (EFR) so that they may be effectively addressed and mitigated.

In addition, decision-makers in both the public and private sectors need a clear insight into the nature and impact of emerging Network and Information Security challenges if they are to make informed decisions.

Supported by the establishment of an EFR Stakeholder Forum, ENISA has developed a comprehensive framework for identifying and assessing risks that may emerge in 2-3 years' time. To provide a 'proof-of-concept' of this EFR Framework, a successful pilot test of Remote Health Monitoring and Treatment was performed to evaluate risks.

In a separate but related initiative, a new Ad Hoc Working Group was established to address the issues of Privacy and Technology. The Group has identified major gaps and challenges in privacy and data protection induced by technology, and made 13 specific recommendations targeted at various stakeholders.

Position Papers on Specific Emerging Security Issues

In 2008, ENISA analysed two specific emerging technology threats and produced Position Papers on Virtual Worlds and Web 2.0.

Virtual Worlds, Real Money – 2007 was the year of online gaming fraud, with malicious programmes that specifically target online games and virtual worlds increasing by 145%, and the emergence of over 30,000 new programmes aimed at stealing online game passwords. Such malware is invariably aimed at the theft of virtual property accumulated in a user's account and its sale for real money. At the same time, online gaming offers a significant risk in the disclosure of private data. This paper describes these risks and others, before making a number of recommendations on how to remedy them.

Web 2.0 Security and Privacy – Web 2.0 (user-generated content, rich user interfaces and co-operative, dynamic services) has brought with it a new and extremely virulent breed of 'Malware 2.0'. A key motivation for ENISA's study into this subject was the link between Web 2.0 and the increase in 'drive-by' malware infections requiring no intervention or awareness on the part of the user. To give some idea of the threat posed, a Scansafe report analysing malware trends confirms that risks from compromised websites increased 407% in the year to May 2008. This Position Paper analyses the vulnerabilities and makes a series of wide-ranging recommendations.

CHAPTER 1 – Introduction
Executive Summary – ENISA in 2008

Building Information Confidence with Micro-enterprises (PA 1)

The digital information age continues to provide many opportunities for businesses, especially for micro-enterprises (1-10 people). These businesses tend to rely on ICT services but information security guidelines for micro-enterprises, particularly related to the understanding and implementation of risk management processes, are not always adequate. ENISA undertook a 'Preparatory Action' in 2008, gathering and assessing the needs and expectations of micro-enterprises in this field, conducting a gap analysis and exercises and piloting the Agency's risk management/risk assessment approach. The results achieved demonstrated the need for the seamless integration of security services through outsourcing and the use of external experts. The projects clearly validated the feasibility of a 'light' approach to security, tailored specifically to the needs and resources of smaller businesses.

Other Activities

In addition to the tasks outlined in its Multi-annual Thematic Programmes, the Agency continued with its horizontal activities – communication and outreach, relations with its various external stakeholders such as the EU Bodies, the Member States, industry, academia, consumers, international institutions and Third Countries, and measuring the uptake of its deliverables. The Agency provided advice and assistance to the European Union and the Member States when called upon.

Growing Recognition

ENISA's contribution to enhancing NIS was recognised in 2008 when the Council and the European Parliament extended the ENISA Mandate until March 2012, recognising the importance of the Agency's role in the development of Network and Information Security.

ENISA's reputation has also reached wider international levels – witnessed by the participation of organisations from outside Europe in the Agency's activities and ENISA's participation in international fora (such as the OECD and the ITU). ENISA is now widely perceived not just within Europe, but worldwide, as *the* Centre of Expertise in Network and Information Security for Europe. Attacks on NIS do not observe national boundaries; to ensure security for all end-users within the rapidly changing world of technology, all players must be united at a global level, and large scale co-operation and support must be encouraged; facilitating co-operation and the sharing of expertise is a key part of ENISA's role – and one which it has performed with particular success in 2008.

CHAPTER 1 – Introduction
2009 and Beyond

Work in 2009 will continue on our three-year rolling programme of activities in the Multi-annual Thematic Programmes (MTPs), with which the Agency is striving for greater impact.

These MTPs started in 2008 and will continue until 2010:

- **MTP 1 'Improving resilience in European eCommunication networks'** focuses on the identification of current best practices, gap analysis of policy and providers' measures and investigation of innovative actions.
- **MTP 2 will develop and maintain co-operation models,** in order to use and enhance the existing networks of actors in NIS. In 2009 this MTP will be devoted to further developing the awareness raising community and a security competence circle for CERTs, building information confidence in the area of micro-enterprises, as well as facilitating co-operation initiatives through the European NIS Good Practice Brokerage.
- **MTP 3 will identify emerging risks for creating trust and confidence.** The Agency is establishing an Emerging Risks framework that will enable decision-makers to better understand and assess emerging risks arising from new technologies and new applications, thereby strengthening stakeholders' trust and confidence. In doing so, the Agency will provide an early warning function for decision-makers in Europe and possibly beyond.

The importance of NIS for the economy and for the citizens of Europe has become increasingly evident in recent years. NIS is now highlighted on the public agenda, and 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. ENISA is well placed to meet the evolving challenges in NIS and, in no small part as a result of its work, the Member States are becoming increasingly equipped to meet them.

With its priorities set and a clear plan in place for coming years, ENISA is confident that 2009 will confirm its role, Mandate and position in the long term. We look forward to developments as a means of equipping the Agency to meet new challenges in Network and Information Security.

CHAPTER 2
Building Synergies, Achieving Impact – the 2008 Work Programme

- Improving Resilience in European eCommunication Networks (MTP 1)
- Developing and Maintaining Co-operation between Member States (MTP 2)
- Identifying Emerging Risks for Creating Trust and Confidence (MTP 3)
- Building Information Confidence with Micro-enterprises (PA 1)
- Working Group Activities

Building Synergies, Achieving Impact – the 2008 Work Programme

The 2008 Work Programme was the result of a new approach, designed to fulfil the following high-level goals:

- Building confidence in the information age through increasing the level of Network and Information Security (NIS) in the European Union (EU)
- Facilitating the Internal Market for eCommunication by assisting the institutions to decide the appropriate mix of regulation and other measures (noting in particular, the important contribution the Agency can make to the Framework Directive)
- Increasing co-operation between Member States (MSs) in order to reduce the variance between the capability of different MSs in this area
- Increasing the dialogue between the various stakeholders in the EU on NIS
- Assisting and responding to requests for assistance from the MSs.

To make the best use of available resources and maximise its impact on crucial areas, ENISA's efforts in 2008 were concentrated on a number of strategic priorities – a set of Multi-annual Thematic Programmes (MTPs) and work packages. By leveraging existing national and EU activities, the Agency was able to avoid the duplication of effort and maximise results.

These MTPs define the work of the Agency for the coming years. A set of SMART (Specific, Measurable, Agreed, Realistic and Time bound) goals are defined for each programme. These goals were related to the desired outcomes and impacts and can be assessed and monitored during the duration of the programme via Key Performance Indicators.

In addition, the Work Programme includes Preparatory Actions (PAs) – activities lasting one year to investigate under what conditions a new Multi-annual Thematic Programme might be initiated.

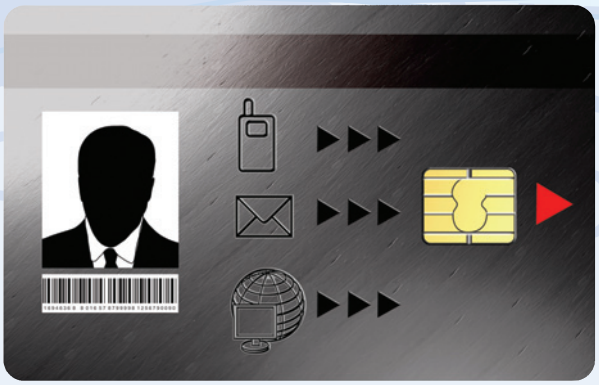
Each thematic programme consists of several Work Packages (WPKs) that implement the SMART goals of the MTP. Each Work Package defines the tasks, the stakeholders concerned, the desired impact and the resources needed.

CHAPTER 2 – Building Synergies, Achieving Impact

In 2008, the Agency focussed on three MTPs and one PA:

- **MTP 1: Improving resilience in European eCommunication networks**
  This involves stocktaking, the identification of good practices and the analysis of gaps in measures deployed by both National Regulatory Authorities (NRAs) and network operators and service providers. This programme also includes an analysis of the suitability of currently deployed backbone Internet technologies regarding integrity and the stability of the network. In 2009, ENISA will compare its findings with similar international experiences and results, issue guidelines and, after broad consultation with concerned stakeholders, finally formulate recommendations. Work will follow and support, as appropriate, the reviewing and updating of the EU Electronic Communication Directives.

- **MTP 2: Developing and maintaining co-operation between Member States**
  In 2008 the initial phase of this MTP was devoted to:
  a) the identification of Europe-wide security competence circles on topics such as Awareness Raising and Incident Response
  b) building on ENISA's previous work on a common language to improve eID interoperability, co-operation on the interoperability of pan-European eID
  c) the European NIS Good Practice Brokerage.
  From 2009 to 2010, ENISA will work towards increasing co-operation among Member States with the aim of improving the capabilities of all Members States and strengthening overall coherence and interoperability levels.



- **MTP 3: Identifying emerging risks for creating trust and confidence**
  In 2008, the Agency developed a framework that will enable decision-makers to better understand and assess emerging risks arising from new technologies and new applications. This will contribute to stakeholders' trust and confidence. To this end, the Agency developed a proof of concept of a European capacity for the evaluation of risks that may emerge in 2 to 3 years' time, linked to a Stakeholder Forum for multi-stakeholder dialogue with public and private sector decision-makers. In addition, the Agency prepared position papers to express its view on risks arising from new technologies and new applications. In this way, ENISA acts as an antenna for decision-makers in Europe and possibly beyond, pointing out and helping them to prepare for the issues to come.

- **PA 1: Building information confidence with micro-enterprises**
  This Preparatory Action involved an evaluation of the feasibility of enhancing information confidence with micro-enterprises, focussing on their needs and expectations. Pilot actions were performed on risk assessment.

The tasks outlined in the Work Programme were carried out according to plan. In some cases, the Agency went the extra mile, taking the work further than originally requested, for example in co-organising the NIS Summer School in Heraklion in September.

In addition to these specific tasks, the Agency continued with its regular activities – including communication and outreach, relations with its various external stakeholders such as the EU Bodies, the Member States, industry, academia, consumers, international institutions and Third Countries, and measuring the uptake of its deliverables. The Agency provided advice and assistance to the European Union and the Member States when called upon.

For a summary of the various tasks which comprised the Work Programme 2008, see Appendix 2.

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.). It also provides a means of demonstrating existing technologies, methods and good practices to interested stakeholders.

Following its full implementation at the beginning of 2008, the Technology Cabinet provided support in particular to work being undertaken in MTP 1, MTP 3 and PA 1, for example with the deployment of DNSSEC systems, the hosting of risk assessment tools and a web development platform for the assessment methodology tool of micro-enterprises.

The Cabinet also contributed to internal projects such as Identity Management 2.0 and the enhancement of ENISA's wiki, and collaborated closely with core IT activities.

CHAPTER 2 – Building Synergies, Achieving Impact
Improving Resilience in European eCommunication Networks

The Resilience of Public eCommunication Networks

Reliable communications networks and services are now critical to public welfare and economic stability. Disruptions due to physical phenomena, software and hardware failures, human mistakes or intentional attacks on networks and services all affect the proper functioning of public eCommunication networks. Such disruptions reveal the increased dependency of our society on these networks and their services. Experience proves that neither single providers nor a country alone can effectively detect, prevent and respond to such threats.

Recent European Commission Communications[1] have highlighted the importance of Network and Information Security and resilience for the creation of a single European Information Space. They stress the importance of dialogue, partnership and empowerment of all stakeholders to properly address these threats. The existing and recently proposed updates of Regulatory Framework Directives include regulatory provisions for the improvement of the security and resiliency of public eCommunications.

A **Public eCommunication network** means every electronic communications network that is used for the provision of publicly available electronic communications services. It includes Internet access and backbone networks, fixed line and mobile voice networks.

Resilience characterises those networks that provide and maintain an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) which affect their normal operation. The main aim of resilience is for faults to be invisible to users.

Tackling the problem

The first Multi-annual Thematic Programme (MTP 1) in ENISA's Work Programme 2008 has the ultimate objective of evaluating and improving the resilience of public eCommunications in Europe.

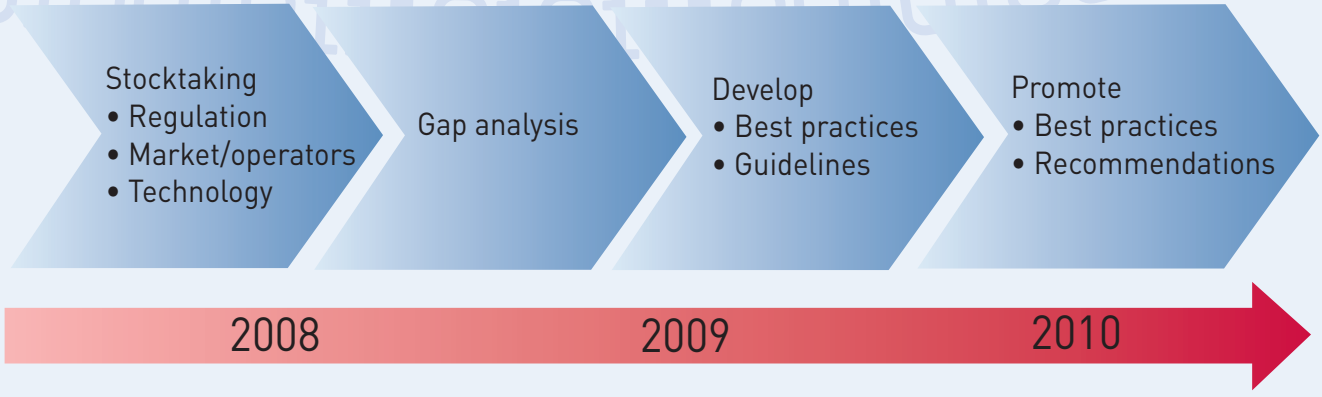
The initial step in reaching this goal – and the focus of work in 2008 – is to take stock of Member States' existing policy and regulatory frameworks related to the resilience of public eCommunication networks. This will help the Agency to identify common measures and good practices deployed in the different Member States as well as gaps and inconsistencies. The Agency intends to analyse the findings of this stocktaking and compare them with trends and recommendations and guidelines proposed by other national, European and global initiatives. After extensive consultation with all relevant stakeholders, ENISA will then be able to suggest new guidelines that could improve the resiliency of public eCommunications in Europe.

ENISA is addressing three key strands:

- National policies and regulations
- Measures deployed by operators on the resilience of public communication networks
- Existing technologies enhancing the resilience of public communication networks

MTP 1 – Improving Resilience in European eCommunication networks

Collectively evaluate and improve resilience in Europe eCommunication networks



By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy-making process

[1] 'i2010 – A European Information Society for growth and employment' and 'A Strategy for a Secure Information Society'

CHAPTER 2 – Building Synergies, Achieving Impact
Improving Resilience in European eCommunication Networks

Stocktaking and Analysis of National Policies and Regulations

The stocktaking exercise was conducted in 2008 and has provided an inventory of national policies, regulations and initiatives deployed by Member States. Particular importance was paid to the way that Member States implement these policies.

More specifically, the stocktaking identified at a national level all the relevant authorities (stakeholders) as well as their tasks, existing policy initiatives and regulatory provisions, the exchange of information between authorities and providers, national risk management processes, how prepared they are to deal with incidents and their recovery measures.

The survey was performed through targeted interviews with small groups of stakeholders in each Member State, using a questionnaire. The topics covered had been identified in wide consultation[2] with relevant stakeholders. The interviews were conducted in telephone conferences between July and September 2008. Participating stakeholders were given enough time to prepare their answers and the option to reply in writing.

25 countries participated in the exercise (23 Member States and 2 EFTA countries). The report reveals a significant variety in the strategies deployed, policies, approaches and regulatory provisions. Despite these differences, a number of common good practices emerged:

- Developing a national strategy, a solid policy and/or regulatory environment and concrete preparedness measures; defining clear roles and the responsibilities of involved public agencies; encouraging intra-agency collaboration and information sharing
- Encouraging voluntary collaboration between public and private stakeholders and supporting the development of commonly agreed good practices and guidelines by capitalising on the knowledge of experts from both industry and public authorities
- Focusing on positive practical progress and fostering continuous learning by developing the appropriate mechanisms (e.g. exercises, audits, on-site visits)
- Reacting promptly to reported incidents and analysing them within a trusted group of experts from public and private sector stakeholders
- Recognising that achieving greater dependability and resilience of public eCommunication networks is a journey not a destination; having started yesterday with small but frequent steps is more effective than failing to shore up resources now

By consulting this inventory of policies, strategies and mechanisms, individual Member States' authorities and other institutional stakeholders will be able to confirm the appropriateness of their own measures and activities and take inspiration from the initiatives of other Member States.

ENISA is currently analysing the findings of its stocktaking. The intention of the analysis is neither to assess how well a country is doing nor to benchmark Member States against each other. Instead the work will concentrate on identifying good practices, interesting initiatives, innovative operational methods and practices, effective methods of preparation for an incident and recovery measures. The analysis will also try to draw conclusions and recommend action by different categories of stakeholders.

[2] www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf

CHAPTER 2 – Building Synergies, Achieving Impact
Improving Resilience in European eCommunication Networks

Analysis of Measures Deployed by Operators on the Resilience of Public Communication Networks

Surveying Network Operators

The availability and integrity of networks and services and business continuity is of major concern to network operators and service providers across Europe. As the number of disruptions increases, network operators and service providers put measures in place to ensure security and the resilience of public communication networks.

However, there are currently significant differences in the approaches, methods, measures and strategies deployed by network operators and service providers across Europe. To examine these differences, ENISA conducted a survey of network operators across the EU. Over two months in September and October 2008, close to 300 network operators in all EU Member States were contacted.

The survey addressed several topics relevant to the management of network resiliency including:

- Threats to the network
- Organisational factors in managing resiliency
- Maturity of network management processes
- Business Continuity planning
- Managing third-party dependencies
- Risk management

Because of the wide range of topics included in the survey and the great variety of types of operators, multiple approaches were taken in conducting the survey. A total of 54 responses were obtained, representing a wide variety of telecommunications operators. They were distributed across 17 of the 27 EU Member States, with wide geographic distribution and variation in terms of size of company, number of countries of operation, services offered and networks operated.

The results of the survey indicate that network operators take network resiliency very seriously, and there were some very positive findings. However, the survey did reveal areas of weakness:

- A small percentage of respondents reported having no formal business continuity or risk management processes in place.
- Though management processes tend to be mature, a small percentage of respondents reported relatively immature processes. Policy-makers and industry players may want to focus on strengthening processes in these remaining operators.

The less mature processes tended to be among alternative fixed-line operators, which raises some key conclusions:

- Some alternative operators may not be taking resiliency seriously enough, or addressing it appropriately.
- On the other hand, alternative operators vary widely and are often very small. As such, it may be the case that recommendations on resiliency may not always apply to them if, for example, they do not operate infrastructure critical to public welfare.
- This ambiguity would suggest caution on the part of policy-makers when trying to develop industry standards and recommendations. It may be that such efforts should be optional, or limited to those operating infrastructure critical to public welfare.

Overall, an industry approach to good practices, standards and recommendations is probably advisable.

Business Continuity

Given the increasing IT support within service provision, service continuity is becoming an important factor. As a result, Business Continuity is currently enjoying significant attention both in public and private organisations. In the international arena, many players (standardisation bodies, industry, national agencies etc.) are setting standards or requirements for continuity that can be used by businesses of all kinds and in all sectors.

To complement its analysis of measures deployed by operators in the resilience of public communication networks, in 2008 ENISA circulated a questionnaire on availability and continuity issues to assess the current state of play among providers of eCommunication infrastructures, mainly telecommunication companies and Internet Service Providers (ISPs). The results reinforced the importance of continuity to telecommunication providers.

In parallel, in response to the rapid growth of interest in Business Continuity methods and tools and the dynamic evolution of standards and good practices, the Agency produced an inventory of Business Continuity methods and tools. This is intended to help users to understand their needs and to acquire information about existing approaches to Business Continuity. ENISA examined 15 available continuity standards/good practices and 8 available tools. The inventory offers information on issues such as purpose, content supported and vendor information.

CHAPTER 2 – Building Synergies, Achieving Impact
Improving Resilience in European eCommunication Networks

Analysis of Existing Technologies Enhancing the Resilience of Public Communication Networks

The provision of value added services requires stable, scalable and available infrastructures and technologies. The interdependencies of technologies, the interoperation among them and the rapid deployment of emerging technologies pose challenges to the integrity and availability of networks.

Recently a vulnerability in the Domain Name System (DNS) attracted considerable media attention when a flaw in the DNS threatened to bring chaos to the Internet by poisoning the servers that translate domain names into Internet protocol addresses. ENISA is investigating the use of Domain Name System Security Extensions (DNSSEC) and other advanced technologies for improving the resilience of public communication networks.

At the suggestion of stakeholders, ENISA focused its analysis on three of the technologies currently available to improve the resilience of public communication networks: MPLS (Multiprotocol Label Switching), DNSSEC and IPv6.

To assess their effectiveness and identify potential problems or gaps that could compromise the availability of networks and services, the Agency has interviewed a number of network operators in the EU. The collected input has been analysed, in consultation with all leading stakeholders, and was presented at an Agency workshop, 'Resilience of Public eCommunication Networks', in Brussels in November 2008. A report on 'Resiliency Features of IPv6, DNSSEC and MPLS, and Deployment Scenarios' was published in 2008. Another report, 'Stock Taking on the Technologies Enhancing Resilience of Public Communication Networks in the EU Member States', together with related guidelines, is now being finalised in wide consultation with technology providers, network operators, standardisation bodies and the R&D community, in an effort to build consensus and develop concrete recommendations.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

Addressing the challenges facing Network and Information Security (NIS) in 2008 and beyond requires a systematic, coherent and integrated strategy that involves all concerned stakeholders and decision-makers and is based on dialogue, partnership and empowerment.

As an independent Europe-wide platform, ENISA is uniquely placed to provide advice and assistance to Member States in enhancing their Network and Information Security capabilities, and has an established reputation for its valuable work in important areas such as awareness raising, risk assessment, computer incident response and spam protection. It is also able to play a co-ordinating role within the EU to facilitate the exchange of good practices and information between all stakeholders at the European level, thus maximising results and impact.

ENISA supports an open multi-stakeholder dialogue and, for that reason, maintains close relations with industry, the academic sector and users. It also sets and develops contacts with a network of national representatives (National Liaison Officers – NLOs) and with major individual experts through Ad Hoc Working Groups. Less formal but equally efficient interactions are in progress through virtual expert groups and platforms to gather and disseminate expert recommendations and to facilitate information exchange with and between public and private sector parties.

Many Member States need to increase their capabilities in various fields of Network and Information Security. Several Member States already co-operate by sharing information on good practices – but this does not happen on a structured basis. As a result, opportunities are probably missed to create synergies and improve efficiency and effectiveness. The Agency is therefore building on previous work to develop various models of co-operation in predefined areas (awareness raising, incident response and eID). In addition, ENISA operates the European NIS Good Practice Brokerage, including supporting tools such as the Online Platform to support the dialogue, the Who-is-Who Directory and 'Country Reports' of activities in the Member States.

Among many highlights of the year in this area were the various thematic workshops that help foster the relationship with existing NIS communities (such as Computer Emergency Response Teams (CERTs)) or build up new communities which share common interests in specific NIS topics (for example, awareness raising and eID).

The capacity to provide prompt, independent and high quality responses to requests received from EU Institutions and within Member States gives the Agency a bridging role between the EU and national institutions. This role is specific to ENISA and currently it is unique in the world. A number of new requests for assistance were received in 2008. For details, see p35.

A Co-operation Platform for the Awareness Raising Community

During 2008 ENISA focused on creating a recognised and established information security awareness community and offering a perspective on what public institutions and private companies could do to enhance users' information security awareness. To this end, the Agency worked to identify relevant activities and information security experts who might become involved in the awareness raising (AR) community, together with security topics which might be useful in raising information security awareness. Recent events, surveys and research suggested that ENISA should focus on corporate data security and on the latest Internet phenomena – virtual worlds for children.

The Awareness Raising Community

The Awareness Raising community is a subscription-free community open to experts who have an interest in raising information security awareness within their organisations. Launched in February 2008 as the culmination of an initiative begun in late 2006, it is designed to help foster a culture of information security. It also serves as a point of contact for matters related to information security awareness. A booklet has been published containing key facts and figures about the AR community and its members.

To enhance the capacity of the community, promote knowledge sharing and a dialogue within Member States and with stakeholders, a new way of coming together and sharing information has been initiated, with monthly conference calls to share emerging good practices and to discuss cutting-edge topics and key issues in the information security field.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

Members of the AR Community

Joined in February 2008:
Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Ireland, Italy, Malta, the Netherlands, Norway, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States, Vietnam

Joined in April 2008:
Egypt, Luxembourg, Morocco, New Zealand, Turkey

Joined in May 2008:
Australia, Latvia, Cyprus

Joined in June 2008:
Lithuania and Poland

Joined in July 2008:
Bulgaria, the Czech Republic, Sierra Leone

The AR community sees different people and cultures as an asset in promoting a culture of information security and has grown to forty nations, comprising 167 members. All European Union (EU) and European Economic Area (EEA) countries are represented with the exception of Liechtenstein. In addition, membership applications have been welcomed from outside Europe.

Though members have a diverse range of skills and knowledge of ICTs, and differing interests and levels of expertise and priorities, they are united in helping the AR community become the intellectual backbone for the exchange of information security good practices. In this way the establishment of the AR community is a significant step not only in promoting the sharing but also in the analysis of information security good practices across Europe.

The AR community went from strength to strength in 2008, with members becoming increasingly involved in activities. 'ARNews' and a calendar of events were prepared and distributed to community members. The AR community also offered members the opportunity to participate in presentations at events, for example the INFOSEK 2008 conference in Nova Gorica, Slovenia, in June 2008. Some members took part in virtual working groups for the preparation of the ENISA White Papers on obtaining support and funding from senior management while planning an awareness programme and organising awareness programmes in financial organisations.

How to Raise Information Security Awareness

ENISA reviewed its 'Users' guide: How to raise information security awareness', published in 2006, in the light of new research and analysis. A revised version was published in 2008 containing a new process modelling, new activities and tasks, key performance indicators and case studies. The guide also points out obstacles to success and provides practical advice on how to overcome them during the planning and implementation phases of programmes. In addition, it describes the main factors governing the success of any information security initiative.

Providing information security is a challenge in itself; awareness raising among select target audiences is an important first step towards meeting that challenge. Obtaining management support and sponsorship for an awareness programme is probably the most crucial aspect of the entire initiative. Even though many managers express their desire to support security initiatives, putting it into action is sometimes another story. With contributions from a virtual working group, ENISA published a White Paper on 'Obtaining support and funding from senior management while planning an awareness initiative'.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

Safeguarding Corporate Data

Recent events have raised concerns about leaks of sensitive corporate information. It is now widely recognised that policies and controls are needed to ensure the security of information on the network and to manage the data which enter and leave the company. While policies and technology are certainly a critical part of any information security programme, in practice these measures alone cannot deliver sufficient information security. Awareness of the related risks and available safeguards is the first line of defence for security. Employees are the real perimeter of an organisation's network and their behaviour is a vital aspect of the total security picture.

In recent years, corporate end-users have increasingly needed to be fully mobile and connected, taking work home or out of the office to maintain their productivity. The use of mobile devices such as laptops, universal serial bus (USB) flash drives, personal digital assistants (PDAs) and other sophisticated devices such as multi-function printers has therefore proliferated. These devices are usually lacking in security, control and management tools. In most cases their use is not covered by a corporate policy foreseeing audit, backup, encryption or asset management.

To raise awareness about these issues, in 2008 ENISA provided an outline of the data which is susceptible to security breaches and incidents while using devices such as USB flash drives and multi-function printers, and published two White Papers: 'Secure printing' and 'Secure USB flash drives'. These highlight potential risks and list good practice guidelines to help readers overcome obstacles within their organisations.

An in-depth analysis was also conducted for the financial services industry, including retail and wholesale banks, investment firms and insurance companies. Owing to the nature of their business, these firms hold large amounts of personal and financial data, and data security is a significant risk area. With contributions from a virtual working group, ENISA published a White Paper, 'Information security awareness in financial organisations', which contains a set of twenty recommendations.

Children on Virtual Worlds

New social networking websites seem to spring up almost on a daily basis. Online users are spoilt for choice – from Facebook to Bebo, MySpace and Second Life to the business-oriented LinkedIn. But there is a growing new online phenomenon – aimed at the younger generation.

Entertainment companies are rushing into this latest Internet phenomena to attract big crowds. Children are on the Internet at a younger age than ever before and they are more comfortable in an online environment than their parents. According to research conducted by EMarketer Inc, around 20 million children and tweens will visit virtual worlds by 2011 – up from 8.2 million in 2007. In America, children are already seasoned social networkers via sites such as Club Penguin, a playful virtual world where animated penguin alter egos go sledging and make buddies. While Europe has been slow to catch on, US-based services are attracting both attention and users, and one British company is unleashing a somewhat more fearsome alternative to the sweetness of Club Penguin.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

Recent research conducted by Virtual Worlds Management demonstrated that there are now over 150 virtual worlds either live or in development with a focus on the youth market (18 and under), with 88 of those live or in development aimed at the general tween category (8 to 12) (up from 62 in April 2008), followed by 72 worlds live or in development aimed at children (7 and under) (up from 52 in April 2008). Recent figures confirm that virtual worlds are popular with children; by April 2008, Mattel Inc. had already counted more than 10 million users.

Virtual worlds are not limited to games and, depending on the degree of immediacy presented, can encompass computer conferencing and text-based chat rooms. Parents are naturally concerned about how their children are using and acting in the virtual worlds. The greatest concern about virtual worlds is the online safety of children and how they can be protected from online predators. Adults must assist children to ensure positive experiences in these three-dimensional environments.

ENISA has therefore provided a set of 25 recommendations for raising the awareness of parents about the safety of children using virtual world sites. Parents must be educated, empowered and engaged to ensure truly positive and valuable experiences for their children, while reinforcing safe online habits in the process. ENISA's paper, 'Children on virtual worlds: what parents should know', is intended to provide clear and comprehensive information to parents about virtual worlds, the risks children can encounter and what parents can do to protect their children and help them understand how to behave in the virtual worlds to reap the many potential benefits whilst minimising the dangers.

Social Engineering – Exploiting the Weakest Links

Social engineering – techniques that exploit human weaknesses and manipulate people into breaking normal security procedures, performing atypical actions or divulging confidential information – has become a significant problem in the security domain. Attackers have recognised that it is often easier to exploit the users of a system than the technology itself.

In 2008 ENISA published a White Paper explaining the threat of social engineering. User susceptibility to social engineering is revealed by a series of e-mail-based case studies, and a checklist for users is proposed, containing a list of factors to consider when asked for information. The paper also includes an exclusive interview with Kevin Mitnick.

Security Awareness Management in Local Governments: Approaches in Scandinavia

ENISA undertook a survey and published a report as to how the regions and municipalities in Denmark, Norway and Sweden are currently working on information security management. The focus of the investigation was directed towards issues related to local governments' management of users' knowledge and awareness of information security.

Awareness Raising Quizzes

ENISA produced a set of quiz templates targeting parents, end-users and executive managers of small and medium-sized enterprises (SMEs). These quizzes are not comprehensive self-tests of an individual's current level of awareness and knowledge; rather they provide respondents with an indication as to their level of awareness. The quizzes are intended to serve as a tool to encourage further interest in the values and risks of using computers and utilising online services on the Internet.

Spreading the Message

During 2008, ENISA continued to disseminate its findings in awareness raising. A new dissemination strategy was developed. In an effort to promote its material faster and more effectively, the Agency produced one volume, 'Raising awareness on information security across public and private organisations', containing selected 2008 publications.

A collection of 2007 publications, 'Raising information security awareness across Europe', was prepared for documentation purposes and almost 2,000 copies were circulated. A survey assessing the quality and impact of reports was distributed.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

Security Competence Circle and Good Practice Sharing for CERT Communities

Enhancing Member States' Capabilities in Incident Response

The number of EU Member States with their own governmental or national Computer Emergency Response Team (CERT) is growing (due in no insignificant part to the efforts of ENISA), but the coverage can still be improved. Drawing on its own expertise embodied in its 'Step-by-step guide on how to set up a CSIRT', and in close collaboration with the various CERT communities, in 2008 ENISA continued to help establish new CERTs – and the ENISA CERT Inventory was updated accordingly.

Training was delivered to help Bulgaria establish a governmental CERT, with the assistance of CERT-Hungary and ENISA's own experts. At the request of the Austrian Government and the Internet registry for Austria, NIC.AT, ENISA facilitated the establishment of a national CERT in Austria, and organised TRANSITS training for 40 participants from Austria. The Agency is now dealing with a request from the Government of Cyprus for the setting up of two CERTS, a national one and an academic one. This project is planned to kick off early in 2009. Even beyond Europe, ENISA's expertise is much sought after: in 2008, ENISA and Finland together supported the setting up of a national CERT capability in South Africa! The establishment of new CERTs has been facilitated through the European Good Practice Brokerage, which brings Member States together to share their expertise and experience (see p25).

Bringing the Players Together – The ENISA CERT Workshop

The annual ENISA Workshop on CERTs in Europe took place in May 2008 in Athens. After covering international co-operation to mitigate massive cyber-attacks (such as those against Estonia in 2007), this year's workshop focussed on co-operation among key players in NIS at a national, Member State level, and the role played by CERTs in national incident response plans.

ENISA informed the Member States' representatives about its plans and projects, as well as those of the European Commission and others, in the field of the resilience of public communication networks. Feedback received will be incorporated into a good practice guide on this topic to be produced in 2009. The results of the workshop will also be used to support the EC's policy-making initiatives by identifying good practice and formulating guidance for minimal (baseline) services and functions for national and governmental CERTs.

This annual event is an opportunity for new CERT teams to integrate quickly with the existing communities, and for established CERTs to extend their network of contacts into new areas, thus enhancing the overall capability of European CERTs to react quickly and successfully to cyber-incidents and increasing the general robustness of information networks in Europe and beyond.

The report from the workshop is available at:
www.enisa.europa.eu/pages/04_01_4th_cert_ws_2008.htm

ENISA also collaborates widely with academic organisations and standards bodies, in Europe and further afield.

Exercises: New Additions to ENISA's CERT Library

ENISA's role as good practice knowledgebase and contact broker is supported by the high quality material it produces. In 2008 ENISA enhanced its library of CERT good practice guides with new CERT Exercises books.

Exercises are an indispensable tool for emergency and crisis preparedness for Computer Security Incident Response Teams (CSIRTs). Currently, only a few teams perform crisis management and co-operation exercises in a constructive way that really enhances their preparedness. Most teams limit themselves to small, ad hoc exercises with limited scope and coverage. The lack of a common good practice approach for CSIRT exercises poses one of the greatest obstacles for teams trying to run cross-border exercises and develop common knowledge. In December 2008 ENISA published a collection of 'Good practices for CSIRT exercises', aimed at enhancing the operational capabilities of incident response teams at various levels. The two books (one for students, the other for teachers) are accompanied by various LiveDVDs with material for the exercises.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

Supporting the Faster Take-up of Interoperable eIDs in Europe

The slow take-up of pan-European electronic identification (eID) services is significantly influenced by the lack of a consistent, interoperable eID infrastructure. Despite the efforts made by some Member States, there is still fragmentation, not only on technical but also on legal and regulatory issues. Interoperability work and the identification of good practices will help accelerate the uptake of secure pan-European services.

Throughout 2008, ENISA continued its work in this area, joining forces with leading pan-European initiatives and interoperability frameworks. In particular, the Agency conducted a study into current policy and implementation issues for eID in Europe, revisiting the 'Roadmap for a pan-European eIDM Framework by 2010', drafted by the European Commission in 2006, in the light of developments over the last two years. During this time, a range of activities at European and national levels were undertaken to support the enhancement of pan-European eID interoperability. One such initiative is the STORK project, funded by the ICT Policy Support Programme (ICT PSP) under the Competitiveness and Innovation Programme (CIP). This study is evaluating whether the milestones of the roadmap have been achieved and reassessing major risks and objectives.

Governments all over the world are seeking to introduce electronic national ID Cards. These cards usually contain sensitive information and might therefore infringe the holder's privacy. ENISA has produced a Position Paper which provides an overview of existing European eID specifications and explains the privacy-enhancing technologies – 'Privacy Features' – which can be found in existing technical specifications and European standards. This paper represents work undertaken by ENISA over and above the tasks laid down in the Work Programme for 2008; it is one example of the Agency 'going the extra mile'.

A second Position Paper in this area, 'Security Issues of Mobile Electronic Identity (Authentication)', summarises the contributions of an international expert group from Europe, the USA and Asia. Mobile devices, like smart phones and PDAs, play an increasingly important role in the digital environment. Besides their primary use, these devices offer the possibility of electronically authenticating their owner to a service. However, as is the case with many new technologies, the pervasive use of mobile devices also brings new security and privacy risks. By looking at different use-cases, such as NFC payment and trustworthy viewing, ENISA has identified the security risks which need to be overcome, and offers an opinion both about their relevance and existing mechanisms that might help mitigate these risks.

One of the concepts of eID interoperability is the idea of Authentication Assurance Levels. A report conducted by the IDABC (Interoperable Delivery of European e-Government Services to Public Administrations, Businesses and Citizens), an EC initiative launched in 2004, defines four authentication levels. This is intended for use in developing and setting authentication policies (for example, in government agencies) and aims to foster interoperability by providing a common policy language for describing authentication assurance strength. It aims to provide an overarching model which is compatible with all existing European policy models and thus represents a very important step in providing interoperability for authentication frameworks in Europe and worldwide. ENISA has mapped these authentication levels to a machine readable format using the OASIS SAML standard. At the same time, the Agency has produced a gap analysis with documented technical information and guidance on how to implement the IDABC authentication levels in eGovernment applications using SAML context classes. This work was aimed primarily at corporate and political decision-makers as well as implementers of IDABC Authentication Policy, but it also provides stakeholders with input when making decisions about eGovernment frameworks and applications. To that extent, it serves not only as a means to provide technical guidance to stakeholders involved in IDABC initiatives but also as a tool to support European policy on electronic identity.

CHAPTER 2 – Building Synergies, Achieving Impact
Developing and Maintaining Co-operation between Member States

The European NIS Good Practice Brokerage

The exchange of good practices between EU Member States (MSs) is essential to enhance the level of Network and Information Security on a pan-European scale. Several MSs already share their experience but, to fully develop the EU's NIS capabilities, it is crucial that a more structured approach is applied to the exchange of NIS good practices. To facilitate co-operation and the exchange of expertise and experience, ENISA has established a European Good Practice Brokerage. In 2008, the Agency facilitated several co-operative projects among the MSs, by acting as a good practice broker in the European NIS 'marketplace'.

In the context of the European NIS Good Practice Brokerage, a closed workshop on structured cyber-crime-related information exchange between the financial sector and the government was organised in November 2008 by the Dutch Financial Information Sharing and Analysis Centre (FIISAC)/NICC, the Theodore Puskas Foundation/CERT-Hungary and the Security Working Group of the Hungarian Banking Association, with the support of the Netherlands Bankers' Association (NVB). ENISA facilitated this co-operation by helping to identify participants from other MSs, supporting their participation, and by contributing to the drafting of the agenda and during the workshop's preparation and discussion.

Supporting Tools

The European NIS Good Practice Brokerage is supported by a set of tools, which were updated during the year:

- **The Who-is-Who Directory on NIS**[3] is a compilation of generic addresses of relevant players in NIS.
- **The Country Reports** is an assessment of ongoing and planned NIS activities in Member States. They also include comprehensive information about relevant players and about ENISA activities.

These documents are not intended to constitute an assessment or benchmark of Member States; instead they represent an important tool in increasing understanding of the 'state of the art' in NIS and in keeping up to date with the latest NIS activities in Europe.

Finally, an online survey was prepared to gather data from participants involved in co-operation with other MSs, and an evaluation report of the functioning of the European NIS Good Practice Brokerage was compiled.

Two case studies

When it emerged that Bulgaria wanted to increase its level of Network and Information Security, particularly by establishing a governmental Computer Emergency Response Team (CERT), ENISA and CERT-Hungary immediately offered their assistance. Hungary had expertise in setting up a governmental CERT (Gov-CERT) – gathered from previous co-operation with Germany – and was willing to offer this expertise to Bulgaria. ENISA had knowledge and good practice material on how to establish a CERT. Bulgaria gladly accepted the offer and submitted a request to ENISA to transfer the Agency's expertise and Hungarian hands-on experience in setting up a Gov-CERT.

A two-part training programme was delivered by CERT-Hungary and ENISA experts. The first part took place in April 2008 in Sofia, with an audience which included not only experts from the hosting organisation (SAITC), but also representatives of other interested parties. The second session was held in June 2008 in Budapest. This training programme demonstrates how ENISA's facilitation, through its European NIS Good Practice Brokerage, can help the Member States make real progress in NIS.

Also in 2008 ENISA acted as a matchmaker between CERT-FI, Finland, and the CSIR/MERAKA in South Africa to facilitate the exchange of good practice and the establishment of a South African Computer Security Incident Response Team (CSIRT). ENISA gave the parties involved an opportunity to meet and discuss co-operation. The Agency helped CERT-FI to arrange suitable funding to offer assistance to South Africa, and provided insights into similar initiatives undertaken in the past. The ENISA 'CSIRT step-by-step' guide was used as a common reference during the project.

[3] www.enisa.europa.eu/doc/pdf/deliverables/enisa_who_is_who_2009.pdf

CHAPTER 2 – Building Synergies, Achieving Impact
Identifying Emerging Risks for Creating Trust and Confidence

The accelerated pace of development of new technologies and applications in an increasingly digitally interconnected society, with its growing reliance on computers and networks in almost every aspect of human life, poses significant risks and raises many serious concerns. There is a pressing need to identify, assess and manage these emerging and future risks (EFR) so that they may be effectively addressed and mitigated.

In addition, decision-makers in both the public and private sectors need a clear insight into the nature and impact of emerging Network and Information Security challenges if they are to make informed decisions. This holds true for both new technologies and new application scenarios entering the European market.

Risk Management methods and tools are used to identify risks and possible strategies and controls to address them; however, the majority of Risk Management/Risk Assessment (RM/RA) methods and tools are designed to identify and manage current risks. To tackle the challenge of emerging and future risks, ENISA is taking a different approach.

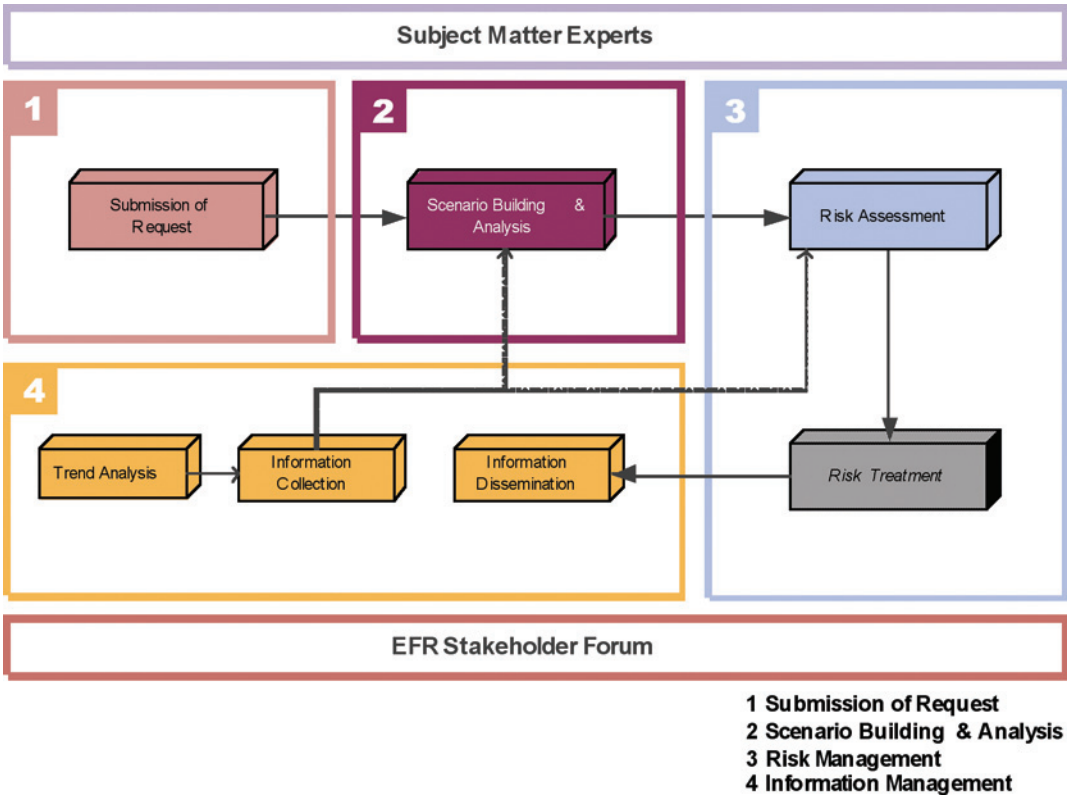
In 2007, ENISA developed a method for identifying EFR and conducted a study into mechanisms to collect, process and disseminate information on emerging risks. In 2008, working with stakeholders, ENISA put this work into practice by conducting a series of activities aimed at developing a more comprehensive framework for identifying and assessing risks that may emerge in 2-3 years' time. This framework will enable decision-makers to better understand and assess emerging risks arising from new technologies and new applications. It will also contribute to stakeholders' trust and confidence.

The EFR Stakeholder Forum

As an initial step, ENISA established an EFR Stakeholder Forum to support the Agency in this work. The Forum consists of stakeholder partners and experts from the industry, the EC and Member States. To achieve better results that will have a greater impact, ENISA has also maintained contact and co-operation with similar initiatives, such as the European Commission FP7 FORWARD initiative.

The EFR Framework

ENISA has developed a scenario-based model as an EFR Framework, i.e. the identification and assessment of the risks is based on a specific scenario. A high level overview of this approach is presented in the following image:



CHAPTER 2 – Building Synergies, Achieving Impact
Identifying Emerging Risks for Creating Trust and Confidence

Once the scenario has been built and analysed, risk assessment begins. The final result is basically a list of possible risks posed by the technology and/or applications under study. In addition, controls may be identified and recommended in order to address those risks.

The First EFR Pilot – 'Being diabetic in 2011'

In order to test and to provide a 'proof-of-concept' of this EFR Framework, a pilot test was performed to evaluate risks. Based on proposals by the EFR Stakeholder Forum, it was decided to address the area of Remote Health Monitoring and Treatment. For the pilot project, an application scenario was developed, based on emerging and near-future technologies and applications for the remote health monitoring and treatment of a diabetic patient. A scenario analysis and risk assessment were then performed to identify the major risks that the use of such technologies and applications could entail in different areas: social, medical, technical, legal, political, ethical, privacy, economic etc. The members of the Stakeholder Forum and other invited external subject experts (for example in the fields of medical informatics and risk management) provided their particular expertise to the assessment.

The exercise was judged extremely successful: valuable results were achieved which can be used in two ways: firstly they highlight some important possible socio-economical, political, ethical, legal and privacy risks in the deployment of emerging health remote and monitoring systems; secondly, they provided feedback on how to optimise the EFR Framework per se.

Position Papers on Specific Emerging Security Issues

During 2008, ENISA analysed emerging technology threats and produced Position Papers, guided by suggestions from the Permanent Stakeholders' Group and other stakeholders. The analysis contained therein is intended to help policy-makers and other decision-makers to better understand the nature of these emerging threats and develop appropriate policies for mitigating them.

The papers were developed with the support of a Virtual Group of Experts using telephone and video conferences, wiki and mailing lists. Each paper provides background, security threat analysis and recommendations to stakeholders.

The topics covered in 2008 were Virtual Worlds and Web 2.0.

Virtual Worlds, Real Money

Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds

2007 was the year of online gaming fraud – with malicious programmes that specifically target online games and virtual worlds increasing by 145%, and the emergence of over 30,000 new programmes aimed at stealing online game passwords. Such malware is invariably aimed at the theft of virtual property accumulated in a user's account and its sale for real money. With nearly 1 billion registered users of MMO/VWs (Massively Multiplayer Online Games and Virtual Worlds) and real-money sales of virtual objects estimated at nearly US$ 2 billion worldwide at the end of 2007, this is a serious issue. The failure to recognise the importance of protecting the real-money value locked up in this grey zone of the economy is leading to an exponential increase in attacks targeting online MMO/VWs.

CHAPTER 2 – Building Synergies, Achieving Impact
Identifying Emerging Risks for Creating Trust and Confidence

Another important area of risk is the disclosure of private data. MMO/VWs are commonly perceived as being completely separate from the real lives of their users and therefore immune to privacy risks. In reality, representing oneself as an avatar is little different from using any other form of online persona. The inclusion of Internet Relay Chat (IRC) and VoIP channels, along with the false sense of security created by MMO/VWs, leads to significantly increased disclosures of private data such as location and personal characteristics – perhaps jeopardising personal safety.

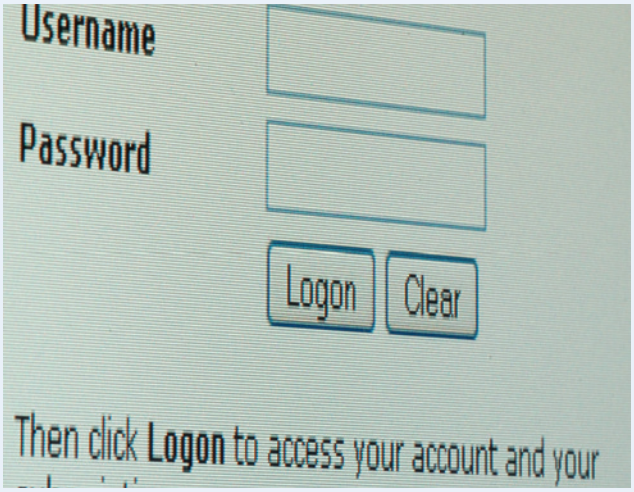
This paper describes in detail these risks and others, including in-game access-control vulnerabilities, scripting vulnerabilities, denial of service, spam and threats to minors, before making a number of recommendations on how to remedy them.

Web 2.0 Security and Privacy

Web 2.0 – user-generated content, rich user interfaces and co-operative, dynamic services – has also brought with it a new and extremely virulent breed of 'Malware 2.0'. A key motivation for ENISA's study into this subject was the link between Web 2.0 and the increase in 'drive-by' malware infections requiring no intervention or awareness on the part of the user. To give some idea of the threat posed, a Scansafe report analysing malware trends confirms that risks from compromised websites increased 407% in the year to May 2008.

One of the most significant sources of vulnerabilities in Web 2.0 is the inadequacy of access and authorisation frameworks used in Web 2.0 environments. In particular, this paper highlights problems in policy frameworks governing the separation of control between web applications. These centre on the 'same-origin' policy, which sandboxes web applications coming from different domains, and the cases where this policy is either deliberately relaxed or circumvented for malicious purposes. Problems in access and authorisation frameworks often stem from the difficulty in finding a balance between allowing enough freedom for Web 2.0 applications to function and providing adequate security.

Web 2.0 has also brought a sea-change in the way knowledge and information is managed. One page



contains content and even executable code from multiple sources including end-users, and information may be syndicated (for example, using RSS) and altered many times from its original source.

This means in particular that:

- The increased opportunities for contributing content also provide more opportunities to inject malicious code leading to many vulnerabilities in the category of cross-site scripting, an important weakness exploited by Malware 2.0. This is exacerbated by very short development cycles and the fact that programmers often have little or no security training.

- Trust in information is more difficult to establish, making it easier to promote fraudulent information for criminal purposes (for example, distortion of stock prices in so-called 'pump and dump' schemes).

The vulnerabilities identified in this paper are extremely important because of the potential damage they cause through identity theft, extortion via botnets, financial loss, loss of privacy and damage to reputation.

Technology can address many of the more immediate problems, but eliminating the more systemic risks requires a comprehensive approach to security involving people, process and technology. The paper concludes with wide-ranging recommendations.

CHAPTER 2 – Building Synergies, Achieving Impact
Building Information Confidence with Micro-enterprises

The digital information age continues to provide many opportunities for businesses, especially for micro-enterprises (1-10 people). These businesses tend to rely on ICT services. Risk assessment and risk management are prerequisites for the establishment of security measures, but in several Member States there is a lack of information security guidelines for micro-enterprises, particularly related to the understanding and implementation of risk management processes.

ENISA therefore undertook a 'Preparatory Action' in 2008, gathering and assessing the needs and expectations of micro-enterprises in this field, conducting a gap analysis and exercises and piloting the Agency's risk management/ risk assessment approach.

Analysing the Needs and Expectations of Micro-enterprises

An ENISA Working Group was created to facilitate discussion on micro-enterprises' requirements. An overview and analysis of existing good practices in NIS for micro-enterprises was produced. Where micro-enterprises obtain security information and what can be done to improve that mechanism was also identified.

Assessing Risk Management Processes for Micro-enterprises

Four multiplier organisations which answered an invitation from ENISA were selected to perform pilot projects with their associated micro-enterprises (and in some cases SMEs).

Three of these projects were completed in 2008:

- in the UK with the International Association of Accountants Innovation & Technology Consultants (IAAITC)
- in Italy with Centro Servizi Informatici dell' Università di Bologna (CESIA)
- in Spain with GMV Soluciones Globales Internet, SA.

The objective was to check how well prepared micro-enterprises are to apply risk assessment and risk management methods, and to receive feedback on the practical use of ENISA's new simplified approach to risk assessment which was developed in 2007 specifically for micro-enterprises and SMEs.

The results of the pilot projects demonstrated the need for the seamless integration of security services through outsourcing and the use of external experts. The projects clearly validated the feasibility of a 'light' approach to security, tailored specifically to the limited resources of smaller businesses, and showed the level of knowledge, investment and quality of the assessment produced.

ENISA will use the results obtained from these pilot studies to further improve its approach for micro-enterprises; others may find the information invaluable in understanding the needs and current security culture of micro-enterprises.

CHAPTER 2 – Building Synergies, Achieving Impact
Working Group Activities

From time to time, according to need, Ad Hoc Working Groups (WGs) are established to address specific scientific and technical matters. Composed of experts in their fields, these WGs allow ENISA to gain access to the most up to date information available and thus to respond to the security challenges posed by a rapidly developing information society.

In 2008, ENISA set up three new Ad Hoc Working Groups:

Assessing the Security Needs of Micro-enterprises

(Ad Hoc WG on Analysing Micro-enterprises' Needs and Expectations in the Area of Information Security)

Micro-enterprises (1-10 people) tend to rely on ICT services, so effective security measures are essential to their success. Risk assessment and risk management should therefore be important activities for such businesses, but in several Member States there are insufficient information security guidelines for micro-enterprises, particularly related to the understanding and implementation of risk management processes.

An Ad Hoc Working Group was created in 2008 to facilitate discussion on micro-enterprises' requirements. An overview and analysis of existing good practices in NIS for micro-enterprises was produced. Where micro-enterprises obtain security information and what can be done to improve that mechanism was also identified.

Sketching a Risk Profile

(Ad Hoc WG on Risk Management and Risk Assessment)

Building on previous work, and through the efforts of its third Working Group on Risk Assessment and Risk Management, ENISA produced a fully developed exposure and impact questionnaire which allows organisations to sketch their risk profile, determining its information risk assessment and management requirements and selecting appropriate methodologies. This profile represents the combination of an organisation's exposure to threats and vulnerabilities, together with the potential impact on its critical information assets (and should not be confused with the result of a fully conducted risk assessment).

The information risk assessment and management requirements that relate to this profile are identified, thus helping non-experts to understand the content – and complexity – of such an activity for their business. Advice about risk assessment and risk management methods that should be considered is also provided.

The risk exposure and risk impact analysis can also be used to generate processes that enable an organisation to consider which risk assessment and management methodologies are best suited to meet its requirements. As a result of this work, ENISA will next produce a tool (the Self Assessed Risk Profiler, SARP) to generate the risk profile for an organisation and automatically deliver the appropriate description of its risk assessment and management objectives and relevant charts.

Inside the Matrix: Privacy and Data Protection Challenges

(Ad Hoc WG on Privacy and Technology)

Privacy and the protection of personal data are serious challenges facing the development of ICT systems and applications. As part of its work to develop a culture of security by ensuring an effective level of Network and Information Security, in 2008 ENISA established an Ad Hoc Working Group on Privacy and Technology.

Throughout the year, the Working Group analysed current and emerging problems that new technologies pose in relation to compliance with privacy regulations and the existing legal framework on personal data protection in Europe.

The Group's final report identified major gaps and challenges in privacy and data protection induced by technology, and makes 13 specific recommendations targeted at various stakeholders (including the EC, industry, academia, Data Protection Authorities, consumer organisations and ENISA itself). These recommendations involve a variety of measures including tax incentives, online subject access at zero cost, comprehensive security breach notification law, and improvements to ensure the effective auditing and certification of data collection. The full report is available at: www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf

For a list of the members of ENISA's Working Groups in 2008, see Appendix 5.

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

Communication and Outreach

The communication and outreach activities of ENISA are pivotal in increasing the impact of the Agency's work. This involves corporate communication channels such as the press and media, the website, the General Report on ENISA activities and other communication material, and outreach to NIS experts, which is achieved through the ENISA Quarterly Review, co-organised events and speaking engagements at conferences and events.

The Tools for Achieving Impact

The EU has recognised the need to convey its activities better[4] and communications is now a policy issue in its own right for the EU. As an EU Agency, ENISA recognises the strategic value of communications; they are critical for the achievement of the Agency's key operational objectives and crucial to its objective to foster a 'culture of Network and Information Security'. Communication is indispensible if change is to be achieved. Dialogue with stakeholders is essential to increase the impact of the Agency's work and meet the goals laid down in its Regulation.

Widening the Agency's visibility

In order to increase the impact of its reports, studies and operations, ENISA endeavours to achieve consistency and coherence across all its communication channels (for example, the website, press releases, publications etc.), and corporate communications are closely aligned with the other operational activities of the Agency to optimise resources and improve the effectiveness of communications planning.

In response to the European Commission's mid-term review, ENISA has successfully sought to obtain wider visibility for the Agency and its activities in 2008. The creation of new Brand Communication Guidelines (BCG) in 2008 has introduced a new and consistent visual identity. The BCG were gradually implemented throughout the Agency's communication channels. The new image reflects the changed roles, responsibilities and position of ENISA following the announcement of the extension of its Mandate to March 2012.

The new visual strategy was strengthened by obtaining access to a professional image bank of 4 million images, which is being widely used within the Agency (for example for presentations, studies and reports). Brand marketing material and repetitive brand recognition advertising for the Agency were also realised.

Communication Planning

ENISA applies a strategic approach towards communication planning across all its operations. 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. For this purpose, a Communication Action Plan is regularly updated. Advance planning also enables the Agency to integrate better with its stakeholders' information and communication channels, thus increasing general outreach still further.

[4] http://ec.europa.eu/commission_barroso/wallstrom/communicating/policy/index_en.htm#apr2008

CHAPTER 3 – Relations with ENISA Stakeholders
Communication and Outreach

Internal Communication

Internal communication is the foundation for securing good external communication. Staff meetings, the Agency's Intranet, the internal newsletter, Inside ENISA, on the Intranet and departmental meetings form the backbone of ENISA's internal communications, but new ways of improving and strengthening internal communications have been explored and will be applied in 2009.

Media

Media is well recognised as a crucial component and the supreme multiplier in spreading knowledge. It is the Agency's key tool for disseminating information about its achievements. Media can also set NIS on the political agenda. Existing relations with media were expanded and strengthened in 2008.

In May 2008, the Agency arranged a highly successful media briefing in Brussels' Berlaymont Press Room, under the auspices of DG COMM[5]. The Executive Director and the Head of the Co-operation and Support Department made presentations on ENISA's activities and Europe's response to security threats. This event made an unprecedented impact in the European Commission's Media Monitoring reports, outclassing the other EU parameters by about 75%. The Agency was featured in major European and international publications, including Euronews, the International Herald Tribune, The Financial Times and der Spiegel, and was relayed through the newswires of Reuters, Associated Press (AP), Ansa, Deutsche Presse Agentur (DPA), Tidningarnas Telegrambyrå (TT) and other key media around the globe.

In 2008, ENISA procured a media database and online publication tool, including translation services and media monitoring. This will further increase the Agency's media outreach and impact in 2009. The Agency also procured External Communication Support Services, for example, for the writing of FAQs and mini-interviews.

In 2008, 23 press releases were issued to the media announcing the Agency's studies, reports and Position Papers. Other activities included publication of Agency news items, feature articles and FAQs on the web, and corporate marketing through repetition advertising in key European media.

The first modules of a media training programme were executed to introduce media landscape and media relations to the Agency's operational staff members, better preparing them for interview situations, article requests and public speaking. Media induction training was also carried out with some of the Agency's Experts. This training underpins the EU's policy of increasing and enhancing communication, by explaining its operations to the citizens of Europe in a clear language.

The ENISA website

The ENISA website was revamped in line with the new visual strategy and with the inclusion of additional images and audiovisual video clips. It is being restructured, making it more efficient and improving the information available. At the same time, the website is being expanded and made more accessible with new, thematic portals, becoming a European 'hub' for specialised NIS information. A 'Content Management System (CMS)' will gradually be introduced to allow authorised staff to publish articles and contribute input easily. Interaction between ENISA and its target audiences may be introduced progressively by developing interactive tools, such as public forums, surveys and polls, and by making online, visual material available.

Publications

The ENISA General Report and the ENISA Quarterly Review (EQR) are the key publications produced during the year. In 2008, for the first time, the General Report was published both as a hard copy and as a minidisc to reach out to a higher number of recipients.

EQR is an extremely effective method of outreach. Four issues of the magazine were produced in 2008, including two special thematic issues: one on 'Resilience of Communication Networks', the other on 'Security and Privacy of eID'. Each edition scores more than 10.000 hits on the website (www.enisa.europa.eu/eq), 3.000 hard copies are distributed and the electronic mailing list has over 2.500 subscribers[6].

Additional corporate materials such as Fact Sheets, leaflets, an ENISA brochure and folders were produced to increase the visibility of the Agency's operations. Translations are foreseen for a selection of key ENISA publications, with the aim of overcoming language barriers and widening the audience. Procurements for other professional support services were also commissioned, including proofreading, design and printing. In this way ENISA is employing communication to spread information, but also to influence change in both policy and behaviour – it is spreading a culture of NIS in practice.

[5] www.enisa.europa.eu/audio/ENISA_briefing_27052008.mp3
[6] Readers may subscribe to EQR at www.enisa.europa.eu/eq

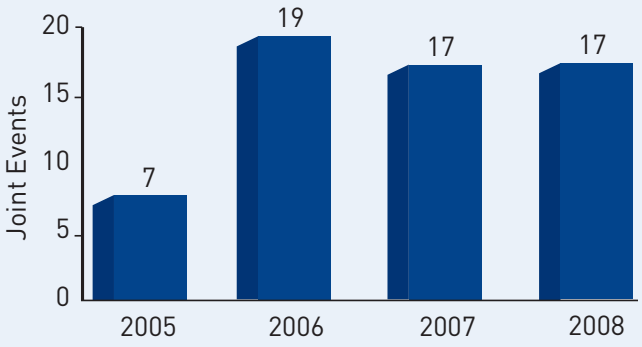
CHAPTER 3 – Relations with ENISA Stakeholders
Communication and Outreach

Conferences, Joint Events and Speaking Engagements

Building on previous experience, ENISA organised a selection of independent, not-for-profit, high-level European conferences in 2008. Often these conferences are run 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.

During 2008, ENISA participated in or co-ordinated almost 50 events and conferences throughout Europe and further afield.

Joint Events (i.e. events supported or co-organised by ENISA), 2005-2008:



Of particular significance was the ENISA-FORTH Summer School in Network and Information Security in September 2008, which was co-organised with the Institute of Computer Science of the Foundation for Research and Technology – Hellas (FORTH-ICS), in Heraklion, Greece. The Summer School brought together experts and key players from all sectors of the information security field.

In addition, the Agency was invited to 30 speaking engagements, and staff attended conferences and other events to fulfil ENISA's role in gathering and disseminating information about Network and Information Security.

Thematic Workshops and Meetings

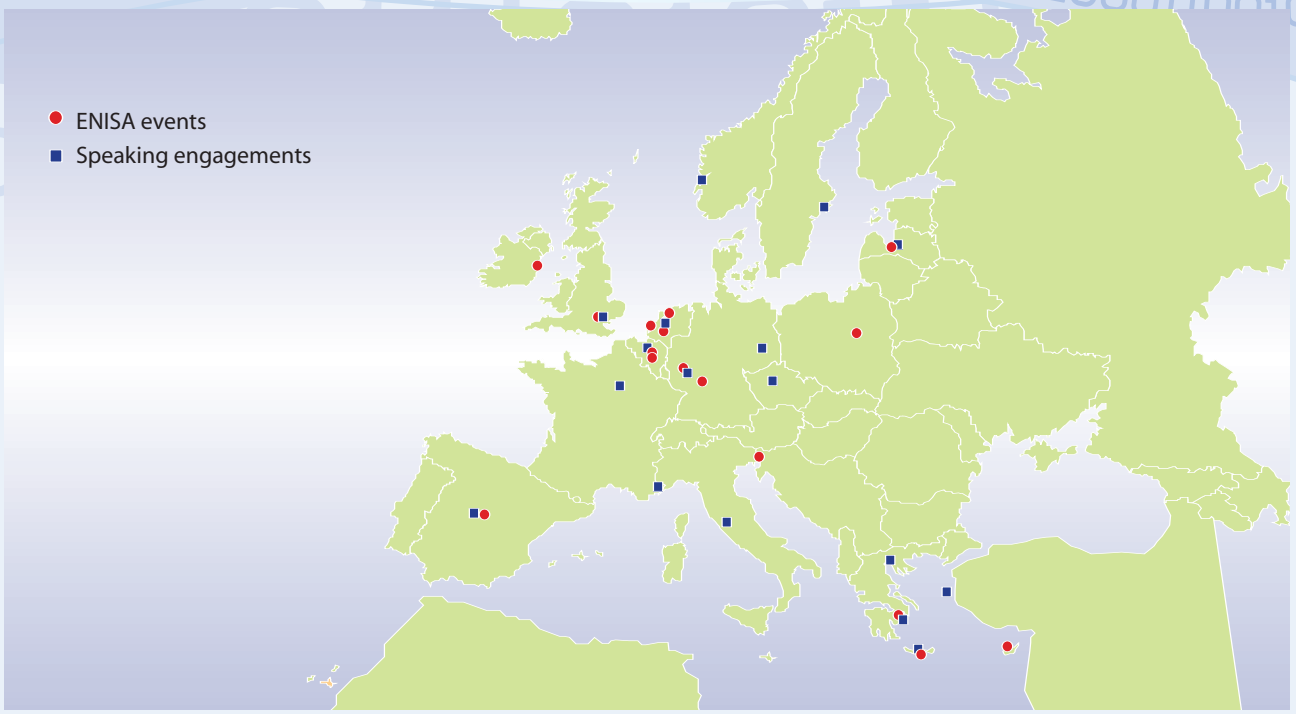
ENISA organised a number of thematic workshops on key issues: to discuss Position Papers, the outcome of specific projects or studies etc., or to present opportunities for a first exchange of ideas to raise stakeholder interest before the launch of new Working Groups.

In particular, three workshops were organised in support of the Agency's stocktaking of the Resilience of Public eCommunication Networks, including one in November in Brussels, Belgium, during which ENISA presented its findings, along with possible directions for the Agency's work during the course of 2009.

Other workshops included the ITU Regional CyberSecurity Forum for Europe and CIS and the 4th annual workshop on CERTs in Europe.

ENISA also gathered its stakeholders at a public meeting in Athens in January 2008 to discuss how its impact in the Member States can best be optimised. The Agency presented the results of the 'Survey to assess the practical usability of ENISA's deliverables' and invited feedback.

Geographical Distribution of ENISA Events and Speaking Engagements in 2008



CHAPTER 3 – Relations with ENISA Stakeholders
External Stakeholders, ENISA Bodies and Groups

ENISA has continued to develop its relationships with EU Bodies, industry, academic and consumer representatives, Third Countries and international institutions. The aim has been to identify common areas of interest and assess the extent to which collaboration with other players in specific activities of the Agency is feasible. In addition, these relationships provide a valuable source of information to keep the Agency's knowledge of relevant technologies updated, and to enable it to facilitate outreach with technical expertise and promote the take-up of products and services.

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. These contacts include 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 2009 and groups of experts will be established to write Position Papers on selected security topics.

Working Groups

From time to time, ENISA establishes Ad Hoc Working Groups (WGs) to provide advice to the Executive Director on specific matters. Members of these groups are usually renowned experts in their field who are able to make recommendations to ENISA, for example on future activities.

Three WGs were active in 2008: the Ad Hoc Working Group on Analysing Micro-enterprises' Needs and Expectations in the Area of Information Security, the Ad Hoc Working Group on Privacy and Technology and the Working Group on Risk Assessment and Risk Management (see p30).

ENISA Permanent Stakeholders' Group

The ENISA Permanent Stakeholders' Group (PSG) facilitates the Agency's regular dialogue with the private sector, academia, consumer organisations and other relevant stakeholders. The second PSG, established in 2007 with a two-and-a-half-year mandate, continued its activities in 2008, providing valuable advice to the Executive Director and input to the implementation of the Work Programme 2008.

The PSG met formally three times in 2008, in February, April and November. Main items on the agenda of these meetings included advising on drafting the ENISA Work Programme 2009 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 advised the Executive Director on the changing regulatory environment and ENISA's role in this context. Individual PSG Members contributed to ENISA's operations by writing for the ENISA Quarterly Review and undertaking speaking engagements at different ENISA events.

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

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 Hersonissos, Crete, in June 2008. This was a follow-up meeting to the successful bringing together in previous years 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 Management Board is 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 as an integral part of the annual Work Programme drafting process.

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 adopts the Agency's budget.

The full Management Board met three times in 2008: in Athens and in Heraklion, Greece, and, at the invitation of the French Presidency, in Paris.

The preparation and subsequent adoption of the Work Programme for 2009 and the (amended) 2008 and 2009 budgets were important activities during the year.

The work programmes of ENISA are 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 Permanent Stakeholders' Group in June 2008 in Heraklion, three main topics were defined and implemented in the Work Programme 2009. In addition, some key Management Board decisions were taken in 2008, for example, on the setting of confidentiality rules for the Agency.

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.

CHAPTER 3 – Relations with ENISA Stakeholders
EU and Member State Relations

Relations with EU Bodies

Relations with the relevant committees and working groups in the European Parliament, in the Council of the EU as well as with the European Commission were further strengthened in 2008. 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 a stake 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.

The highlight of the year came in April 2008, when a delegation of the Committee for Industry, Research and Energy (ITRE) at the European Parliament paid a very successful visit to ENISA at its headquarters in Heraklion. The European Parliament praised the Agency's excellent work and ENISA's Mandate was extended for three years until March 2012, allowing time for a thorough discussion on how to address NIS in Europe in the future. The delegation's visit was a major milestone in ENISA's relations with the European Parliament.

Relations with Member States

Various meetings were organised in the EU Member States during 2008. 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. Collaboration can always be improved, however, and ENISA is in contact with representatives of the Member States on an almost daily basis, exchanging information and giving advice on day-to-day business issues.

Responding to Requests

A major evolution since 2006 has been the receipt by ENISA of Requests for assistance with specific projects. In 2008, the Agency handled requests from four Member States and the European Parliament. Similar requests are also expected to emerge in 2009. In answering requests such as these, ENISA is fulfilling its appointed task to advise and assist the Member States and EU Institutions.

Requests handled in 2008

Requester	Subject	Deliverable
Bulgaria	Facilitating Hungarian-Bulgarian co-operation to set up Bulgarian Government CERT	2 training sessions in Sofia and Budapest
Greece	Creation of CSIRT at FORTH-ICS	CERT workshop
Austria	Assistance in setting-up of CERTs through organising CERT training	TRANSITS training in Vienna
European Parliament	Advice on Internet security matters	Written report
Cyprus	Assistance in setting up a governmental CERT	Review setting up plan

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 the valuable input from the Member States through the NLOs' network, ENISA was able to conduct various surveys and studies in the field.

In January 2008 ENISA organised the annual NLO meeting in Athens. The main topics discussed included the study on the usefulness of the ENISA deliverables, to which the NLOs provided valuable input.

ENISA is very grateful to this network and recognises the time-consuming nature of the work of the National Liaison Officers in co-ordinating the various approaches from ENISA within the Member States.

For a list of the NLOs, see Appendix 6.

CHAPTER 3 – Relations with ENISA Stakeholders
Other Relations with Industry and International Relations

Industry Relations

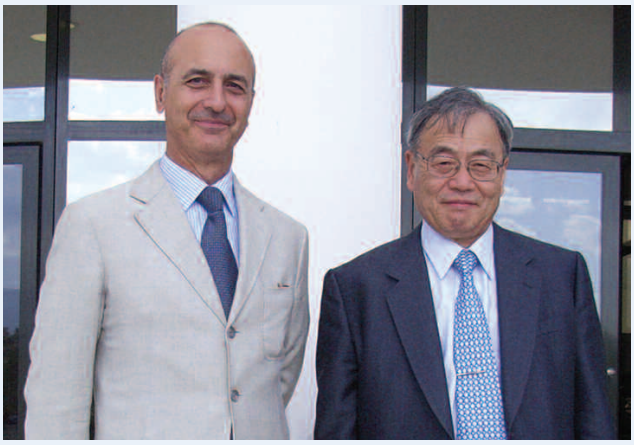
In addition to the regular dialogue held with the members of its Permanent Stakeholders' Group, ENISA has established relationships with relevant national industry associations in all EU Member States as well as with a number of pan-European umbrella organisations representing ICT and software industries, telecommunications network operators and Internet service providers. These organisations are important partners for ENISA in its drive to foster a culture of NIS in Europe. A structured dialogue, with regular meetings between industry representatives and ENISA experts, is maintained with relevant European organisations, which provided input for the implementation of the ENISA Work Programme 2008. In addition, ENISA has an 'open door' policy to all relevant stakeholder groups. In 2008 a number of bilateral discussions with stakeholders were held at the Agency's headquarters in Heraklion, Crete.

In 2008, ENISA consolidated its relationship-building activity with national industry multiplier organisations through personal visits and discussions with all 27 EU Member States as well as EEA countries. Through its 'Road Show' project, the Agency presented its role, tasks and activities, resulting in almost 800 personal contacts which have formed the basis of a new ENISA Stakeholder database. In addition, the campaign enabled the Agency to learn more about NIS activities 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 has proved a highly effective method for the Agency to facilitate closer co-operation with its stakeholders, and to identify opportunities to engage them in partnership in the planning and implementation of current and future ENISA Work Programmes.

International Relations

NIS is a global challenge and does not recognise borders. In its task to foster good European practice, ENISA has regularly participated as a technical expert in different working bodies of international organisations such as the Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP). ENISA experts have also participated in meetings and in the work of the Council of Europe Convention on Cybercrime as well as the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) and Telecommunication Development Sector (ITU-D) groups; the Agency provided technical expertise and presented its activities, for example, in the field of awareness raising and CERT co-operation.

In 2008, ENISA enhanced its relations with non-EU countries. Global challenges in NIS and the means to address them were discussed with representatives from Third Countries. For example, ENISA hosted visits to its headquarters by Japanese industry representatives and a Chinese Government delegation. In co-operation with IDC IT Security Roadshow, network building continued with EU neighbouring countries, specifically Turkey, Croatia and Bosnia Herzegovina. Joint road show activities, targeting in particular the countries bordering the EU, will continue in 2009.



The Executive Director with Mr. Koji Nishigaki, Chairman of the Information-technology Promotion Agency (IPA), Japan

Speaking Engagements of the Executive Director

The Executive Director had a number of high level speaking engagements in various Member States in 2008. Among the most prominent of these events were, in Brussels, Belgium, the Worldwide Security Conference at the East West Institute in February, and the 2nd European Security Awareness Day in April, when he spoke about striking the right balance when regulating Network and Information Security. The Executive Director also addressed BITKOM – 'Forum Public Sector' in Berlin, Germany, in February, with a speech on the borderline between NIS and homeland security and the respective responsibilities of Member States and ENISA following cyber-attacks such as the one which struck Estonia in 2007.

Measuring ENISA Deliverables

ENISA has undertaken a substantial number of activities and produced many deliverables with the goal of enhancing Europe's approach towards information and network security. In 2007, the Agency conducted a 'Survey to assess the practical usability of ENISA's deliverables' in the Member States. Over 800 people were invited to participate, from which 297 responded in whole or in part. The focus of the survey was to establish Awareness, Attitudes, Acceptance and Action related to the 22 deliverables that ENISA produced from its inception until September 2007. The results of the survey were presented to an audience of ENISA stakeholders in Athens in January 2008.

Overall stakeholders assign ENISA deliverables high marks in terms of content and approach but suggestions were made to raise the Agency's profile and enhance the impact of its deliverables.

For a list of ENISA's deliverables in 2008, see Appendix 7.

CHAPTER 4
Administration

- Organisation Chart
- General Administration
- Legal Advice and Procurement
- Technical Infrastructure
- Physical Infrastructure
- Human Resources
- Finance and Accounting

Administration

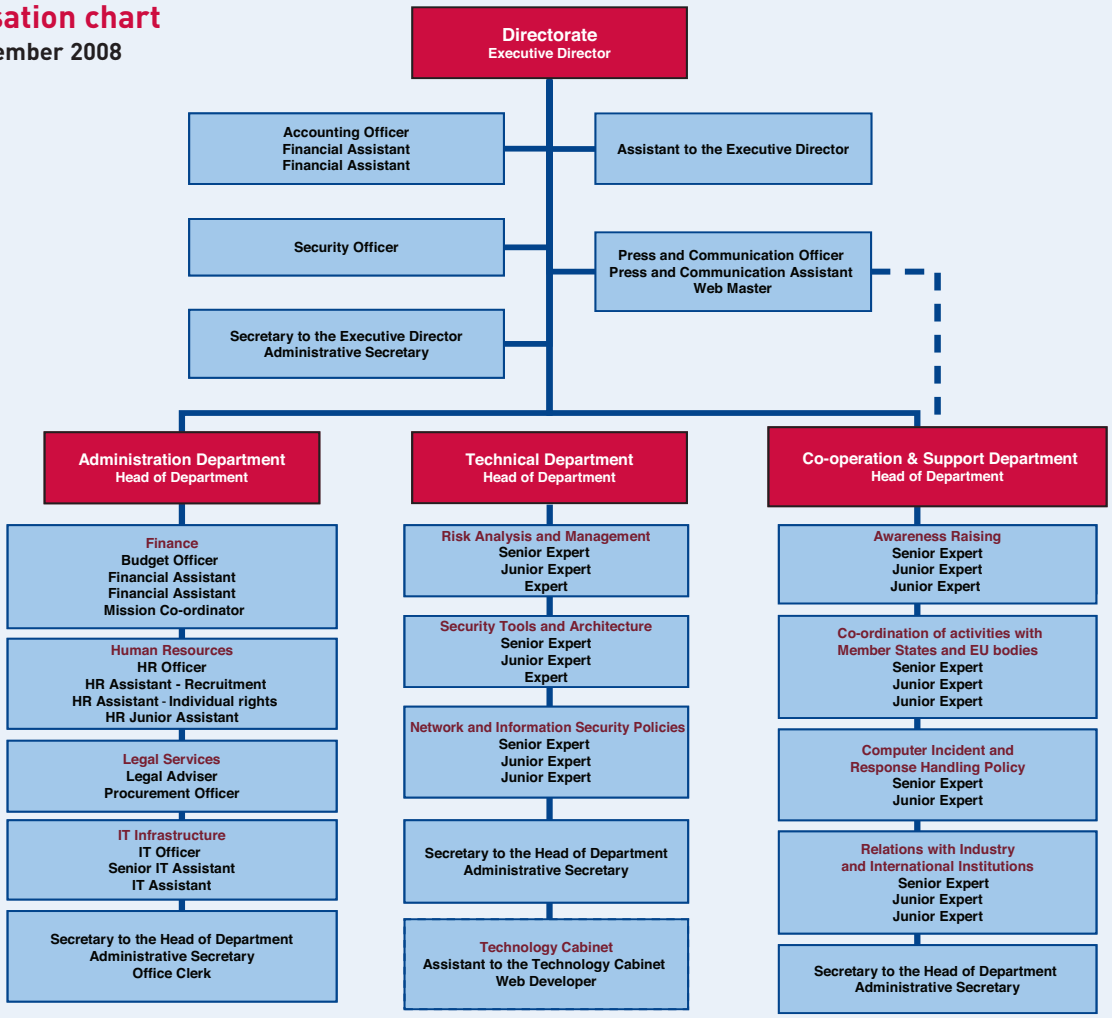
ENISA's Administration Department ensures the legality and integrity of the administrative procedures followed by the Agency in line with the prevailing regulatory framework. The Administration Department also renders certain services to the Agency as a whole and liaises with designated EU organisations as appropriate. In addition, the Administration Department undertakes a secondary role in support of selected operational tasks of the Agency, such as legal support.

In 2008 the goal of the Administration Department was to simplify administrative procedures, specifically to:

- further enhance the established practices and procedures of the past three years
- improve areas in need of administrative attention in line with guidance received through audit
- facilitate the goal of the Agency for a flexible, cross-team organisational scheme of work as appropriate, by ensuring an operation-wise organisation and the close monitoring of appropriations in line with the requirements of sound financial management.

Organisation chart

As at December 2008



CHAPTER 4 – Administration

General Administration

In 2008 the goal of the Administration Department was twofold: to meet in full the compliance requirements for European Agencies and to provide the high level of service expected from users and stakeholders.

The compliance target followed the groundwork completed over the previous three years. In 2008 the Agency welcomed the results of statutory audits carried out by the European Court of Auditors and the Internal Audit Service of the Commission. In addition, positive input was received from the European Data Protection Supervisor (EDPS), with regard to procedures concerning the processing of personal data that falls under the competence of EDPS.

Following standing guidelines from senior management, the Administration Department maximised the utilisation of resources available. In 2008, the Administration Department carried out its tasks in full, within its original plan of activities, maintaining its original headcount while servicing a growing number of staff and stakeholders.

The results of 2008 will eventually impact the plan in forthcoming years, as ENISA strives to achieve a lean administration, optimising workflows and adopting further electronic workflow tools and working methods wherever appropriate.

Internal Control

ENISA's Internal Control Co-ordination function ensures that the Agency complies with internal control standards. In 2008 ENISA adopted an approach towards a Panel for Financial Irregularities that leverages the procedures of the European Commission. The groundwork for the adoption of the new Financial Regulation was also completed in line with the requirements of the Framework Financial Regulation. In 2008 the internal procedures of the Agency were duly rationalised with the support of a professional consultant; 2009 will see their implementation.

In 2008 ENISA underwent a scheduled internal audit of Human Resources, carried out by the European Commission's Internal Audit Service. The results highlight previous efforts in a positive light. A scheduled external audit was also planned in two parts and carried out by the Court of Auditors to check 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 2007. The audit results mark a positive trend in improving the organisational basis of the Agency, and demonstrate its commitment to compliance with applicable rules.

Legal Advice and Procurement

In 2008, the Agency continued to meet the compliance requirements of the European Data Protection Supervisor, completing an inventory and reporting on relevant processing activities. In addition, a small number of appeals based on Staff Regulations was addressed as appropriate.

The execution of the Agency's budget was channelled through 32 procurement projects linked to 28 contracts for supplies or services, 175 purchase orders and 15 co-operation agreements, as shown in the table below.

Procurement projects launched in 2008

Open		Negotiated		Request for Offers (< €25.000)		Service agreements
service	supply	service	supply	service	supply	
3	0	25	1	3	0	2
3		**26**		**3**		**2**

Contracts signed in 2008

Service	Supply	Co-operation Agreements	Purchase Orders
26	2	15	approx. 175

CHAPTER 4 – Administration

Technical Infrastructure

ENISA performed an assessment of continuity risks for its own IT environment which has led to the implementation of a number of measures to increase the availability of internal IT services in cases of failure, error or disaster. In addition, steps were taken to better co-ordinate IT-related resources that are available across the various departments of the Agency.

In an effort to improve service delivery and information sharing, the IT Section implemented an Intranet, which allows the Agency to reduce still further its reliance on paper-based documents. The server virtualisation programme has also led to significant updating of the infrastructure available by adopting contemporary systems. The Agency is leveraging on these developments for the first phase of the implementation of electronic workflows, which relate to employee data management and leave management systems that have been set up and are due for deployment in early 2009. These workflows were developed within the Intranet, thus making it simpler for employees to perform their part in specific administrative tasks and to locate related information. It is expected that the overall cost of these administrative tasks will be cut still further and functionality will be improved since, depending on circumstances, the Intranet is also remotely accessible for busy staff members.

As of August 2008, designated ENISA staff members are able to connect to the ENISA network via a Virtual Private Network (VPN), using their electronic certificate. The implementation has been based on an in-house Public Key Infrastructure (PKI) solution on top of VPN functionality on the firewall. ENISA's workforce is required to be highly mobile and carries a heavy mission payload; remote access has greatly increased the effectiveness of the staff in meeting the Agency's operational goals.

Physical Infrastructure

To assist ENISA in the performance of its work, the Greek Ministry of Transport and Communications has approved funding to provide the Agency with an office in Athens. This will facilitate meetings with stakeholders from the EU, EFTA and Third Countries. The inauguration of this branch office will be in 2009.

In addition, the host Member State signed a contract in December 2008 for the construction of new premises in Heraklion to accommodate possible further expansion of the Agency. The new building will be able to house more than 100 staff with appropriate logistic services. Work has already started and the building is due for completion in 2011.

Human Resources

In 2008 ENISA continued to face challenges in the area of Human Resources (HR) management, mostly associated with the dynamic working environment of ENISA. The Agency maintained its staff levels at 44 temporary agents and reinforced its contract agent base, adding one

additional post to reach 13 in total as it sought to better service its operational needs. Particular emphasis was placed on staff performance appraisal and the introduction of the reclassification (promotions) exercise. A significant amount of resources was also dedicated to the implementation of the training plan.

Recruitment

In 2008 10 recruitment procedures were completed – with a success rate of 95% – and suitable candidates were consequently appointed.

Statutory staff: A total of 430 applications were received for all statutory positions advertised. While the highest number of applications arrived from such Member States as France, Germany, Greece and Italy, increasing interest for assistant positions was demonstrated by candidates from the newer Member States such as Bulgaria, Poland and Romania.

Non-statutory staff: In 2008 one additional selection procedure was carried out in order to offer 5-month traineeship grants to young university graduates in the field of Network and Information Security. As a result, ENISA welcomed four trainees from Austria, Greece, Italy and Lithuania.

The successful selection of an interim agency enabled ENISA to hire appropriate support staff whenever necessary to meet short term needs.

Recruitment policy: To ensure broad communication and transparency, all calls for expressions of interest for 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 specialist press.

In 2008, ENISA reaffirmed its commitment, reflected in its recruitment procedures, to the avoidance of 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.

CHAPTER 4 – Administration

Training

ENISA considers training as an integral part of its human resources policy, and in 2008 considerable emphasis was placed on training activities. The training programme at ENISA serves to expand and improve individual competencies and skills so that each staff member can contribute optimally towards the Agency's goals and reflect its core values of excellence, professionalism and service.

Language courses in Greek, English, French and German continued to be delivered throughout the year. Additional training in organisational and personal development, as well as management training, was successfully delivered.

In 2008 ENISA reached the overall objective of providing an average of 10 days of training per person, in accordance with the guidelines set by the Commission's Learning and Development Framework.

In addition, staff were encouraged to participate on their own initiative in training courses in specialised training centres, which has enabled staff to enhance their professional performance in individual areas.

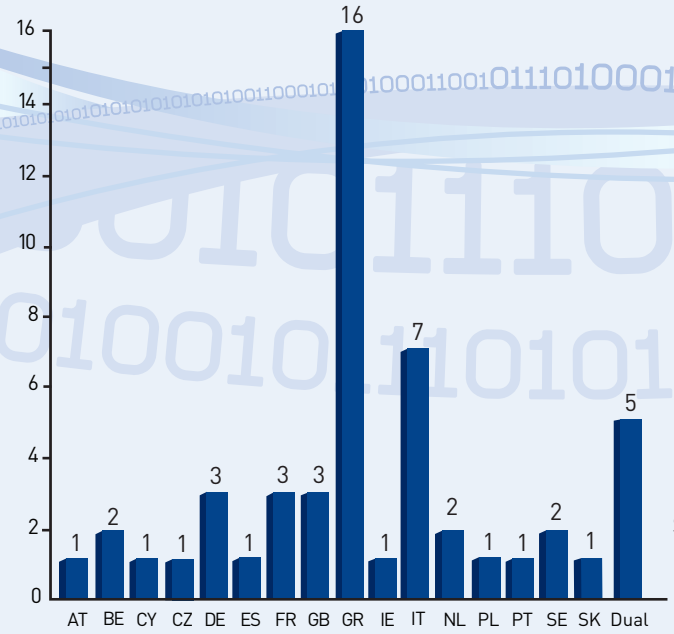
Other HR developments

In 2008, the second yearly career development report exercise was launched and contributed to the performance assessment of staff. To encourage the professional development of each staff member, career objectives and training paths were also set. The overall appraisal evaluation confirmed the high level of ability, efficiency and integrity of ENISA's staff.

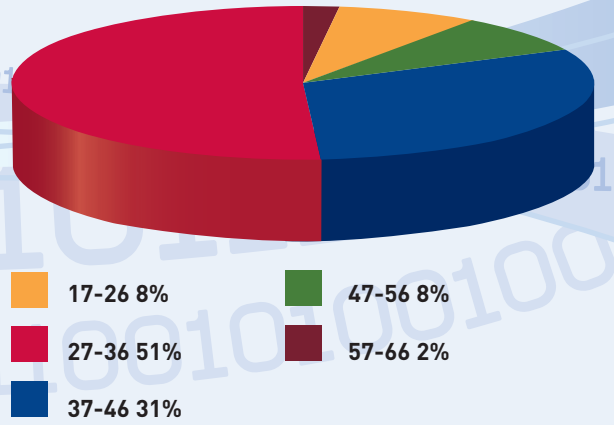
In addition, the HR section worked in close co-operation with ENISA's Staff Committee in order to establish and maintain an open and constructive bilateral dialogue between the Agency's staff and management. The Staff Committee was involved in recruitment procedures and nominated a full member of the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

HR statistics

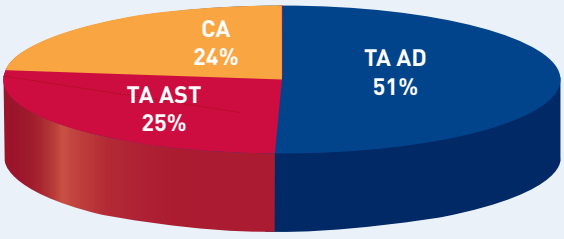
Staff members by nationality



Staff members by age



Staff members by function group or type of employment



KEY

AD: Administrators
AST: Assistants
TA: Temporary Agents
CA: Contract Agents

CHAPTER 4 – 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 European 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 with the European Commission's Accounts
- Regular financial reporting to the European Commission, the Court of Auditors and the Budgetary Authority

Budget Execution Report

The Budget 2008, as amended in October 2008, reached €8.355.024 which represents a decrease of 0,7% compared with the 2007 figure (€8.416.928). Appropriations were committed at a rate of 95,8% (97,6% committed in 2007) to honour obligations related to the operational costs of the Agency and the activities required under the Work Programme 2008. Payments reached the level of 76,2% (73,5% paid in 2007) of the total appropriations managed. The level of committed appropriations demonstrates that the very positive performance of 2007 was sustained in 2008, showing an upward trend in the capacity of the Agency to use the funds with which it is entrusted.

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

- **Title 1 – Staff expenditure:** Staff expenditure was as foreseen, with 97,8% of appropriations committed at the end of the year. The respective rate of payments was 94,8%.

- **Title 2 – Administrative expenditure (functioning of the Agency):** The funds allocated to administrative expenditure were used as planned, with 92% of appropriations being committed by the end of the year, and 51,5% paid.

- **Title 3 – Operating Expenditure:** 93,6% 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 2008 Work Programme, were committed, with the total rate of paid appropriations reaching 53,8%.

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 following are the Financial Statements included in the Provisional Annual Accounts. The Final Accounts will be prepared on 1 July 2009 after the Agency receives feedback from the European Court of Auditors. It is expected that the Final Accounts will not differ materially from the Provisional ones.

CHAPTER 4 – Administration

Balance Sheet

	31.12.2008 €	31.12.2007 €
I. Non Current Assets	**373.124**	**373.352**
Intangible fixed assets	45.035	36.176
Tangible fixed assets	328.089	337.176
II. Current Assets	**2.638.207**	**2.480.483**
Short-term receivables	201.513	101.357
Cash and cash equivalents	2.436.694	2.379.126
Total Assets	**3.011.332**	**2.853.835**
III. Non Current Liabilities		
IV. Current Liabilities	**1.928.333**	**1.410.260**
EC pre-financing received	641.325	328.971
EC interest payable	143.818	125.560
Accounts payable	415.538	113.977
Accrued liabilities	677.652	686.535
Provisions	50.000	155.216
Total Liabilities	**1.928.333**	**1.410.260**
V. Net Assets	1.082.999	**1.443.575**
Accumulated result	1.443.575	630.425
Result for the year	-360.576	813.151
Total Net Assets	**1.082.999**	**1.443.575**

Cash Flow Statement

	2008 €	2007 €
Surplus/(deficit) from Ordinary Activities	**-360.576**	**813.151**
Operating Activities		
Amortisation (intangible fixed assets)	19.490	12.516
Depreciation (tangible fixed assets)	143.164	113.322
Decrease in provisions for liabilities	-105.216	89.344
Increase in short term receivables	-100.157	-27.361
Increase in accounts payable	623.289	-986.782
Net Cash Flow from Operating Activities	**219.994**	**14.190**
Cash Flows from Investing Activities		
Purchase of tangible and intangible fixed assets	-162.427	-154.257
Net Cash Flow from Investing Activities	**-162.427**	**-154.257**
Net decrease in cash and cash equivalents	57.568	-140.067
Cash at the beginning of the period	2.379.126	2.519.193
Cash at the End of the Period	**2.436.694**	**2.379.126**

Economic Outturn Account

	2008 €	2007 €
Revenue from the Community Subsidy	7.713.699	7.987.957
Other revenue	0	202.642
Total Operating Revenue	**7.713.699**	**8.190.599**
Administrative expenses	-5.146.114	-5.176.051
Staff expenses	-3.919.782	-3.572.833
Fixed asset related expenses	-162.654	-125.837
Other administrative expenses	-1.063.678	-1.477.381
Operational expenses	-2.925.591	-2.198.765
Total Operating Expenses	**-8.071.704**	**-7.374.816**
Surplus/(deficit) from Operating Activities	**-358.006**	**815.783**
Financial expenses	-3.201	-2.633
Exchange rate loss	630	
Surplus/(deficit) from Ordinary Activities	**-360.576**	**813.151**
Economic Result for the Year	**-360.576**	**813.151**

Statement of Changes in Capital

	Reserves €	Accumulated Surplus/ Deficit €	Economic result of the year €	Capital €
Balance as of 1 January 2008	**0**	**630.425**	**813.151**	**1.443.575**
Allocation of the Economic Result of Previous Year		813.151	-813.151	0
Economic result of the year			-360.576	-360.576
Balance as of 31 December 2008	**0**	**1.443.576**	**-360.576**	**1.082.999**

APPENDICES

- Acronyms and Abbreviations
- Work Programme 2008
- Members of the Management Board
- Members of the Permanent Stakeholders' Group
- Members of the Ad Hoc Working Groups
- National Liaison Officers
- ENISA Deliverables 2008

Appendix 1 – Acronyms and Abbreviations

AR	Awareness Raising
BCG	ENISA Brand Communication Guidelines
CERT	Computer Emergency Response Teams. A '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 offer other information to help improve computer and network security. (see also: CSIRT)
CSIRT	Computer Security Incident Response Team. Over time, the CERTs (see above) extended their services from being a reactive 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
DG COMM	Directorate General Communication
DNSSEC	Domain Name System Security Extensions
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFR	Emerging and Future Risk
EFTA	European Free Trade Association
eID	Electronic Identification
eIDM	Electronic Identification Management
FAQ	Frequently Asked Question
FIRST	Forum of Incident Response and Security Teams – a global CERT organisation
FORTH	Foundation of 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/)

APPENDICES
Appendix 1 – Acronyms and Abbreviations

ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
ISSE	Information Security Solutions Europe – Europe's only independent, interdisciplinary security conference and exhibition
ITU	International Telecommunication Union
KPI	Key Performance Indicator
MB	ENISA Management Board
MMO/VWs	Massively Multiplayer Online Games and Virtual Worlds
MPLS	Multiprotocol Label Switching
MS	Member State of the European Union
MTP	ENISA Multi-Annual Thematic Programme
NFC	Near Field Communication
NIS	Network and Information Security
NLO	National Liaison Officer
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
PA	ENISA Preparatory Action
PDA	Personal Digital Assistant
PSG	ENISA Permanent Stakeholders' Group
RM/RA	Risk Management/Risk Assessment
SAITC	Bulgarian State Agency for Information Technology and Communications
SAML	Security Assertion Markup Language
SMART	Specific, Measurable, Agreed, Realistic and Time bound, describing the goals defined in ENISA's Work Programme
SME	Small and Medium Enterprise
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.
VoIP	Voice over Internet Protocol
WG	Working Group, ENISA Ad hoc Working Group on specific technical issue
WP	Work Programme
WPK	ENISA Work Package

APPENDICES
Appendix 2 – Work Programme 2008

Output Achieved

The Work Programme is a rolling programme of tasks to be completed over a three-year period from 2008-2010. The following table shows the progress achieved in 2008 towards completion of the full programme by 2010.

Work item Ref.	Deliverable	Output achieved
MTP 1	**Improving resilience in European eCommunication networks**	
WPK 1.1	Stocktaking and analysis of national regimes to ensure security and resilience of public communication networks	Survey completed; report published Analysis due for completion in February 2009
WPK 1.2	Analysis of measures deployed by operators on resilience of public communication networks	Survey and analysis completed, report published
WPK 1.3	Analysis of existing technologies enhancing the resilience of public communication networks	Report on resilience features of IPv6, DNSSEC and MPLS published Recommendations on technologies and standards that enhance the resilience of public communication networks due for completion in Q1 2009
MTP 2	**Developing and maintaining co-operation models**	
WPK 2.1	Co-operation platform for awareness raising community	
	1) Awareness raising online portal	Pending implementation of content management system
	2) Building AR community	The AR Community now numbers 167 members drawn from all EU and EEA countries; a welcome pack was sent to all members who registered before November 2008; other new members will receive theirs in Q1 2009. Monthly conference calls were run every third Friday with the exception of July, August and December; the eARNews was dispatched every 4 weeks.
	3) Translation of AR material	Translation of two documents completed
WPK 2.2	Security competence circle for CERT community	
	1) Update CERT Inventory	Updated as planned (May and September)
	1a) Support Austria, Bulgaria and Cyprus in their plans to establish national CSIRTs	CERT training provided to Austria and Bulgaria, support ongoing; work initiated to support Cyprus.
	1b) Launch a Europe-wide co-operation activity for financial ISACs	Kick-off workshop in Budapest November 2008
	1c) Support for the creation of a South African national CSIRT by Finland	Support initiated and ongoing
	2) 4th ENISA Workshop on CERTs	Held in May 2008 in Athens; report published on ENISA website

APPENDICES
Appendix 2 – Work Programme 2008

	3) CSIRT Exercise Book and additional material	Text finalised, design, printing and distribution progressing
WPK 2.3	Supporting the faster take-up of interoperable eIDs in Europe	
	1) Gap analysis on IDABC authentication levels	Analysis completed and published
	2) Report on eIDM framework	Report completed, to be published January 2009
	3) Position Paper on mobile eID	Paper completed and published
	4) Position Paper on privacy features in eID specifications (extra mile)	Description of PETs for eID completed and published in Elsevier newsletter; Position Paper to be published January 2009
WPK 2.4	European NIS Good Practice Brokerage	
	1) Successful partnerships	HUN-NL-Other MS in the field of structured cyber-crime related information exchange (closed workshop on FI-ISAC took place in Budapest in November 2008); HUN-BUL in field of governmental CERT (concluded in June 2008); FIN-South Africa in the field of CERT (concluded August 2008).
	2) Web-based online platform	Pending implementation of content management system
	3) Who-is-Who Directory	Editing finalised, layout and printing progressing
	4) Country Pages	All updated information received was implemented
	5) Country Reports	Finalised, ready to be published online
	6) Evaluation report	Finalised (internal document in PDF)
MTP 3	**Identifying emerging risks to create trust and confidence**	
WPK 3.1	Framework for assessing and discussing emerging risks	EFR Workflow design: Specification of the EFR Framework completed EFR Framework Handbook prepared EFR Framework first pilot test completed in Remote Health Monitoring and Treatment
WPK 3.2	Position Papers	2 papers produced: Virtual Worlds, Real Money – Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds; and Web 2.0 Security and Privacy
PA 1	**Building information confidence with micro-enterprises**	
WPK 4.1	Analysing micro-enterprises' needs and expectations (Ad Hoc WG)	Report completed
WPK 4.2	Assessing risk management process for micro-enterprises	Feedback report of risk management pilots with SMEs completed

APPENDICES
Appendix 2 – Work Programme 2008

Measuring Progress

A set of SMART[7] goals has been defined for each Multi-Annual Thematic Programme. These are related to the desired outcomes and impacts and can be assessed and monitored during the duration of the programme using Key Performance Indicators (KPIs).

Each thematic programme consists of several Work Packages (WPKs) that implement the SMART goals of the MTP. The WPKs include their own SMART goals and KPIs.

The following summarises the SMART goals set for 2010 and progress made towards achieving them in 2008. In many cases, ENISA's work is ahead of schedule.

MTP 1: Improving Resilience in European eCommunication Networks

SMART goal: By 2010, the Commission and at least 50% of the Member States will have made use of ENISA recommendations in their policy-making processes

SMART goal: By 2010, service providers covering at least 50 million users will be using ENISA recommendations to improve resilience

KPI	Target	Result by end 2008
Commission using ENISA recommendations	Yes	Too Early
% Member States using ENISA recommendations	50%	Too Early
# users covered by service providers using ENISA recommendations	50 million	Too Early

WPK 1.1: Stocktaking and analysis of national security regimes to ensure security resilience of public communication networks

SMART goal: The analysis covers at least 50% of Member States

SMART goal: At least 3 references in official EU publications or peer reviewed papers

SMART goal: At least 5 references to official ENISA recommendations

KPI	Required	Achieved by end 2008
# Member States covered by the analysis	50%	92%
# References (EU Publications, papers)	3	2
# References to ENISA recommendations	5	Too Early

WPK 1.2: Analysis of measures deployed by operators on resilience of public communication networks

SMART goal: In 2008, service providers covering at least 50 million users participate in the survey

SMART goal: In 2008, at least 50% of Member States represented in the survey

SMART goal: By Q4 2008, at least 10 references in official EU publications, peer reviewed papers, websites or mailing lists

KPI	Required	Achieved by end 2008
# Users covered by the service providers participating in the survey	50 Million	> 50 Million 63%
# Member States represented in the survey	50%	
# References in official EU publications, peer reviewed papers, websites or mailing lists	10	Too Early

WPK 1.3: Analysis of existing technologies enhancing resilience of public communication networks

SMART goal: By 2010, service providers covering at least 50 million users adopt ENISA's technical recommendations

SMART goal: At least 50% of Member States adopt ENISA's technical recommendations

SMART goal: At least 5 international organisations adopt or refer to ENISA's technical recommendations

KPI	Required	Achieved by end 2008
# Users covered by service providers adopting ENISA recommendations	50 Million	Too Early
# Member States adopting ENISA recommendations	50%	Too Early
# International organisations adopting or making reference to ENISA recommendations	5	1

[7] Specific, Measurable, Agreed, Realistic and Time bound

APPENDICES
Appendix 2 – Work Programme 2008

MTP 2: Developing and Maintaining Co-operation Models

SMART goal: By 2010, at least 10 Member States have participated in at least 3 different co-operation models.

KPI	Required	Achieved by end 2008
# Member States involved in co-operation models	10	27 plus 3 EEA and 10 Third Countries
# Co-operation models	3	4

WPK2.1: Co-operation platform for Awareness Raising (AR) Community

SMART goal: By Q4 2008, have 40 experts signed up to the AR community list via the awareness raising portal

SMART goal: By 2008, have 10 contributions to the AR portal, 50 downloads of good practice material shared within the AR community from the AR portal, 2.500 visits per month to the AR portal and 10 explicit requests for not-downloadable deliverables

SMART goal: By 2008, have translations of the ENISA AR publications in at least 3 different languages

KPI	Required	Achieved by end 2008
# Experts signed up to the AR Community	40	167
# Contributions to AR portal	10	0[8]
# Downloads from portal	50	0
# AR portal visits per month	2500	0
# Requests for deliverables	10	0
# Translations of AR documents	3	5

WPK 2.2: Security competence circle and good practice sharing for CERT communities

SMART goal: By Q4 2008, 80% of updates in CERT inventory are confirmed

SMART goal: At least 50% of the EU population is represented at the workshop

SMART goal: Workshop participants score the workshop at least as 3 on a scale of 1-5

SMART goal: By Q4 2008, at least 50 downloads of ENISA CSIRT exercise book

SMART goal: By Q4 2008, at least 5 references in peer reviewed papers, websites or mailing lists

KPI	Required	Achieved by end 2008
# Confirmed updates to CERT inventory	80%	100%
% EU population represented at workshop	50%	77%
Average feedback on workshop (1-5 (max))	3	4.3
# Downloads of ENISA CSIRT exercise book	50	Too Early[9]
# References to CSIRT exercise book	5	Too Early[9]

WPK 2.3: Supporting the faster take-up of interoperable eIDs in Europe

SMART goal: By Q4 2008, at least 3 references to position papers in official EU publications or peer reviewed papers

SMART goal: By Q4 2008, at least 5 references to official ENISA recommendations

SMART goal: By Q4 2008, at least 1 cross-border pilot implements ENISA recommendations

[8] The AR portal has not yet been established, pending implementation of a Content Management System due to the unavailability of a Web Master in 2008. The 10 contributions that were created in co-operation with the AR community were published on the main ENISA website.

[9] # downloads and # references still to be measured as the books were only published at the end of 2008.

APPENDICES
Appendix 2 – Work Programme 2008

KPI	Required	Achieved by end 2008
# References to position papers (EU Publications, papers)	3	4
# References to ENISA recommendations	5	> 200
# Cross-Border pilots implementing ENISA recommendations	1	1 Prospect

WPK 2.4: European NIS Good Practice Brokerage

SMART goal: By Q4 2008, at least 2 partners have engaged in a co-operation initiative facilitated through the European NIS Good Practice Brokerage

SMART goal: By Q4 2008, the Online Platform has been visited by at least 15 Member States

SMART goal: By Q4 2008, at least 25 Member States are covered by the Who-is-Who Directory and Country Pages

SMART goal: By Q4 2008, 80% of updates in Who-is-Who Directory and Country Pages are confirmed

SMART goal: By Q4 2008, a Country Report is made on at least 20 Member States

KPI	Required	Achieved by end 2008
# Partnerships facilitated	2	3
# Member States visiting online platform	15	0[10]
# Member States covered by Who-is-Who Directory and Country Pages	25	27
% Confirmed updates in Who-is-Who Directory and Country Pages	80%	100%
# Member States covered by Country Report	20	27

MTP 3: Identifying Emerging Risks for Creating Trust and Confidence

SMART goal: By 2010, at least 30 stakeholders or stakeholder organisations from at least 15 Member States refer to ENISA as point of reference for discussing the nature and impact of emerging Network and Information Security challenges in the Information Society

KPI	Required	Achieved by end 2008
# Stakeholders referring to ENISA as point of reference	30	Too Early
# Member States of stakeholders referring to ENISA as point of reference	15	Too Early

WPK 3.1: Framework for assessing and discussing emerging risks

SMART goal: In 2008, the proof of concept and the Foresight Forum both cover emerging risks in at least 2 new application areas

SMART goal: By Q4 2008, at least one expert or stakeholder organisation from at least 5 different Member States contributes to the 2008 Foresight Forum

SMART goal: By Q4 2008, at least 3 stakeholder organisations from at least 3 different Member States make reference to the report on the proof of concept and 2008 Foresight Forum outcomes

KPI	Required	Achieved by end 2008
# New application areas	2	2
# Contributors to Foresight Forum	5	12
# Member States represented in Foresight Forum	5	8
# Stakeholders making reference to proof of concept	3	Too Early
# Member States of stakeholders making reference to proof of concept	3	Too Early

[10] The online platform has not yet been established, pending implementation of a Content Management System, due to the unavailability of a Web Master in 2008

APPENDICES
Appendix 2 – Work Programme 2008

WPK 3.2: Position Papers

SMART goal: By Q4 2008, above average satisfaction rate (3 on a scale of 1-5, 1=low, 5=max) of position papers received via forms on ENISA website

SMART goal: By Q4 2008, at least 2 papers accepted in a conference that follows a formal peer review evaluation

SMART goal: By Q4 2008, at least 6 references to position papers

KPI	Required	Achieved by end 2008
Satisfaction rate of position papers [1-5 (max)]	> 3	See note[11]
# Position papers accepted in a conference	2	2
# References to position papers	6	>100

PA 1: Building Information Confidence with Micro-enterprises

Follow-up options	MB decision of 17-10-2008
1. MTP	No
2. No follow-up	No
3. 1-year Work Package	Yes

WPK 4.1: Analysing micro-enterprises' needs and expectations (Ad Hoc Working Group)

SMART goal: At least 1 European SME organisation and at least 4 national associations are represented in a Working Group that, according to the ENISA rules of operation, consists of a maximum number of 9 members

SMART goal: At least 70% of the Working Group members endorse the Working Group's findings

KPI	Required	Achieved by end 2008
# European SME organisations in working group	1	1
# National SME organisations in working group	4	4
% Members endorsing findings	70%	100%

WPK 4.2: Assessing risk management process for micro-enterprises

SMART goal: By 2008, at least 2 pilots in at least 2 Member States are deployed that implement ENISA risk assessment material

KPI	Required	Achieved by end 2008
# Pilots	2	3
# Member States	2	3

[11] Tool for measuring satisfaction rate was not available.

APPENDICES
Appendix 3 – Members of the Management Board

A key pillar of ENISA, 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. The Management Board is chaired by Prof. Dr. Reinhard Posch (Austria).

At 31 December 2008
European Commission representatives

Representative	Alternate
Fabio **COLASANTI** Director General Information Society and Media DG	Andrea **SERVIDA** Deputy 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	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 Division of the IT-Security Division National IT and Telecom Agency	Thomas **KRISTMAR** Senior Advisor 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

APPENDICES
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	
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	Prof. Constantine **STEPHANIDIS** Director Institute of Computer Science Foundation of Research and Technology (FORTH)	Theodoros **KAROUBALIS** Hellenic Ministry of Transport and Communications
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	Ivo **TUKRIS** Director Department of Communications Ministry of Transport	Janis **GRAUDINS** Deputy Director 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	Damian **XUEREB** Policy Manager ICT Ministry for Infrastructure, Transport and Communications	Steve **AGIUS** Chief Information Officer Malta Communications Authority
The Netherlands	Edgar R. **DE LANGE** Ministry of Economic Affairs Director-General for Energy and Telecommunications	Peter **HONDEBRINK** Ministry of Economic Affairs Directorate-General for Energy and Telecommunications
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)

APPENDICES
Appendix 3 – Members of the Management Board

Romania	Toma **CIMPEANU** Director General for Information Technology Ministry of Communications and Information Technology	Gheorghe **MURESANU** Head of the Centre of Expertise for Information Security National Institute for Research and Development in Informatics
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	Denis **TRCEK** Head of the Laboratory of e-media Faculty of Computer and Information Science University of Ljubljana
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)

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 Dept. of Information and Communication Systems Goethe University Frankfurt (CEPIS)	Niko **SCHLAMBERGER** Statistical Office of the Republic of Slovenia, Secretary

EEA-country representatives (observers)

Member state	Representative	Alternate
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

APPENDICES

Appendix 4 – Members of the Permanent Stakeholders' Group

The Permanent Stakeholders' Group (PSG) comprises 30 independent experts who are appointed *ad personam* (i.e. selected on personal merit rather than representing either a country or a company), each with proven abilities and expertise in fields relevant to the PSG mandate and with the capacity to contribute to ENISA activities and to advise the Executive Director. PSG Members represent a broad range of stakeholders including the Information and Communication Technology industry, research and academia in the field of Network and Information Security, as well as representatives from different user and consumer communities.

Industry

Howard Schmidt	US
Paul King	British
Kurt Einzinger	Austrian
Alfred Eisner	Dutch
Philippe Duluc	French
Claire Vishik	US
Urho Ilmonen	Finnish
Vilma Misiukoniene	Lithuanian
Roger Dean	British
Magnus Nystrom	Swedish
Nick Coleman	British
Olivier Parideans	Belgian
Ilias Chantzos	Greek
Andreas Ebert	Austrian
Yves le Roux	French

Academia/Research

Jacques Stern	French
Jaan Oruaas	Estonian
Evangelos Markatos	Greek
Norbert Pohlmann	German
Giusella Finocchiaro	Italian
James Clarke	Irish
Antonio Lioy	Italian
Jaap-Henk Hoepman	Dutch
Sachar Paulus	German
Andrew Cormack	British

User/Consumer

Nissim Bar-El	Israel
Wim Hafkamp	Dutch
Gajewski Jacek	Polish
Paul Dorey	British
Charles Brookson	British

APPENDICES
Appendix 5 – Members of Ad Hoc Working Groups

Ad Hoc Working Group on Analysing Micro-enterprises' Needs and Expectations in the Area of Information Security

David **REYNOLDS** (Chair)	UK	International Association of Accountants Innovation & Technology Consultants (IAAITC)
Dr. Werner **DEGERHARDT**	Germany	Faculty of Psychology and Educational Sciences, University of Munich
Prof. Dr. Urs E. **GATTIKER**	Switzerland	CyTRAP Labs
Phillipp **GRAF**	Austria	WKÖ
Dr. Nineta **POLEMI**	Greece	University of Piraeus
Ken **RABEY**	UK	School of Computing and Information Technology, University of Wolverhampton
Claudio **TELMON**	Italy	Associazione Italiana Per la Sicurezza Informatica (CLUSIT)
Philippe **VANERIE**	Belgium	European Business and Innovation Centre Network (EBN)

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	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)

APPENDICES
Appendix 6 – National Liaison Officers

At 13 November 2008

Member State	National Liaison Officer
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	René Risom JOHANSEN – Fuldmægtig, Ministeriet for Videnskab, Teknologi og Udvikling IT- og Telestyrelsen, IT-Sikkerhedskontoret
Estonia	Toomas VIIRA – Estonian Informatics Centre
Finland	Mari HERRANEN – Ministry of Transport and Communications
France	Aymeric SIMON – 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 – Chairman of the Board of CERT-Hungary
Ireland	John MOORE – Communications Business & Technology Division, Department of Communications
Italy	Giandonato CAGGIANO – Legal Adviser of the Ministry of Communications
Latvia	Janis GRAUDINS – Senior Adviser, General and International Issues Division, Department of Communications Ministry of Transport
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	Steve AGIUS – Chief Information Officer, Malta Communications Authority
The Netherlands	Edgar DE LANGE – Ministry of Economic Affairs, Director-General for Energy and Telecommunications
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 Information Technology
Slovakia	Rastislav MACHEL – Machel Consulting
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

APPENDICES
Appendix 6 – National Liaison Officers

EEA	National Liaison Officer
Iceland	Björn GEIRSSON – Legal Counsel
Liechtenstein	Kurt BUEHLER – Director, Office for Communications
Norway	Heidi KARLSEN – Adviser, Ministry of Transport and Communications

European Commission Liaison	
European Commission	Rogier HOLLA – Policy Officer, Policy Developer ENISA

Council Liaison	
Council of the European Union	Anastassios PAPADOPOULOS – Council of the European Union – General Secretariat

APPENDICES
Appendix 7 – ENISA Deliverables 2008

Directories:

1. Who-is-Who in Network and Information Security, 4th Edition 2009
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_who_is_who_2009.pdf

2. Country Reports, 1st Edition 2009
   - http://enisa.europa.eu/pages/country_pages.htm

Periodicals:

1. ENISA Quarterly Review
   - www.enisa.europa.eu/pages/02_02.htm

Improving Resilience in eCommunication Networks (MTP 1):

1. Stocktaking exercise among 25 Member States on resilience of public communication networks (survey on policies and regulation)
   - www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_10_29_strengthen_resilience.html
   - www.enisa.europa.eu/pages/resilience.htm

2 Analysis of stocktaking findings – Policy, Regulations and Initiatives
   - www.enisa.europa.eu/pages/resilience.htm

3. Analysis of measures deployed by operators on resilience of public communication networks
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_network_provider_measures_on_resilience.pdf
   - www.enisa.europa.eu/pages/02_01_press_2009_01_22_network_resilience.html
   - www.enisa.europa.eu/pages/resilience.htm

4. Study: 'Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios'
   - www.enisa.europa.eu/sta/files/resilience_features.pdf
   - www.enisa.europa.eu/pages/02_01_press_2009_01_22_network_resilience.html

5. Workshop: 'Improving Resilience in European e-Communication Networks', Brussels, 7 March 2008
   - www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf
   - www.enisa.europa.eu/doc/pdf/resilience/Workshop/AGENDA.pdf

6. Workshop: Improving Resilience in European e-Communication Networks', Brussels, 12-13 November 2008
   - www.enisa.europa.eu/sta/h_ws08.html

7. Business and IT Continuity: Overview and Implementation Principles (updated version including inventory of methods and tools for BCM)
   - http://enisa.europa.eu/rmra/files/enisa_business_it_continuity_v1.51.pdf

8 ENISA website section on Business Continuity Management & Resilience, with inventory of BCM methods etc.
   - www.enisa.europa.eu/rmra/ic_home.html

Developing and Maintaining Co-operation Models (MTP 2):

1. Report: Key Facts and Figures about the Awareness Raising Community and its members
   - www.enisa.europa.eu/doc/pdf/deliverables/ar_comm_key_facts.pdf

2. Report: 'Information Security Awareness in Financial Organisations'
   - www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_11_26_financial_markets.html

3. The New Users' Guide: How to raise information security awareness
   - www.enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf

4. Report on Security Awareness in Scandinavian Local Governments
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_scandinavian_gov.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_10_31_awareness%20scandinavian%20gov.html

APPENDICES
Appendix 7 – ENISA Deliverables 2008

5. Report: 'Children on Virtual Worlds' including 25 parental safety tips on how to ensure children behave safely in online virtual worlds
   - www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_10_06_children_virtual_worlds.html

6. Report: 'Obtaining Support and Funding from Senior Management'
   - www.enisa.europa.eu/doc/pdf/deliverables/obtaining_support_and_funding_from_senior_management.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_09_26_funding_security_initiatives.html

7. 'Secure USB Flash Drives' – accidental loss and theft of confidential corporate data on unsecured USB flash drivers (in EN/FR/DE)
   - www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf
   - www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_fr.pdf
   - www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_de.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_06_19_USB.html

8. Awareness Raising Quizzes Templates: Targeting Parents, End-users and SMEs
   - www.enisa.europa.eu/doc/pdf/deliverables/awareness_raising_quizzes_templates.pdf

9. 'Secure Printing' (in EN/FR/DE)
   - www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf
   - www.enisa.europa.eu/doc/pdf/ENISA_secure_printing_fr.pdf
   - www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_de.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_06_03_printing.html

10. Report of the Awareness Raising session at INFOSEK 2008 in Slovenia
    - www.enisa.europa.eu/doc/pdf/other/ar_report_slov.pdf

11. Stakeholder survey and evaluation report of responses to Report on 'Security Economics and the Internal Market' on barriers and incentives for Network and Information Security in the Internal Market for eCommunication
    - www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf
    - www.enisa.europa.eu/doc/pdf/deliverables/report_evaluation_stakeholder_replies_2008.pdf
    - www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm

12. White Paper: Social Engineering: Exploiting the Weakest Links
    - www.enisa.europa.eu/doc/pdf/publications/enisa_whitepaper_social_engineering.pdf

13. Proceedings of 4th ENISA Workshop CERTs in Europe: 'The role of CERT teams in National incident response plans'
    - www.enisa.europa.eu/pages/04_01_4th_cert_ws_2008.htm
    - www.enisa.europa.eu/doc/pdf/other/4th_cert_ws/workshop_report.pdf

14. Guide: ENISA CSIRT Exercise Material – Handbook
    - www.enisa.europa.eu/doc/pdf/deliverables/enisa_csirt_exercises_handbook.pdf

15. Guide: ENISA CSIRT Exercise Material – Toolset
    - www.enisa.europa.eu/doc/pdf/deliverables/enisa_csirt_exercises_toolset.pdf

16. Updated ENISA Inventory of CERT activities in Europe
    - www.enisa.europa.eu/cert_inventory/index_inventory.htm

17. Mapping IDABC Authentication Assurance Levels to SAML v2.0
    - www.enisa.europa.eu/doc/pdf/deliverables/enisa_IDABC_SAML.pdf

18. Report on the state of pan-European eIDM initiatives
    - www.enisa.europa.eu/doc/pdf/deliverables/enisa_eID_management.pdf

19. Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID)
    - www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf

20. Privacy features of European eID card specifications
    - www.enisa.europa.eu/doc/pdf/publications/privacy_features_of_eid_cards.pdf
    - www.enisa.europa.eu/pages/02_01_press_2008_11_21_mobile_eid.html

APPENDICES
Appendix 7 – ENISA Deliverables 2008

Identifying Emerging Risks for Creating Trust and Confidence (MTP 3):

1. Report: 'Methods for the Identification of Emerging and Future Risks'
   - www.enisa.europa.eu/doc/pdf/deliverables/EFR_Methods_Identification_200804.pdf

2. Visual Tool to Ensure Regulatory Compliance and Effective Implementation of Corporate Risk Management Requirements
   - www.enisa.europa.eu/rmra/ir_downloads.html
   - www.enisa.europa.eu/pages/02_01_press_2008_05_20_integrated_rmra.html

3. Position Paper: Web 2.0 Security and Privacy
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_web2.pdf

4. End-user survey: Web 2.0 Security and Privacy
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_survey_web2.pdf

5. Position Paper: Security and Privacy in Virtual Worlds and Gaming
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_security_privacy_virtualworlds.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_11_20_online_gaming.html

6. End-user survey: Web 2.0 Security and Privacy (1500 end-users)
   - www.enisa.europa.eu/doc/pdf/other/survey_vw.pdf

7. 'Privacy and Data Protection Challenges' including a grid of policy and legal challenges and 13 recommendations
   - www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf
   - www.enisa.europa.eu/pages/02_01_press_2008_11_14_privacy_challenges.html

Building Information Confidence with Micro-enterprises (PA1)
Piloting ENISA Risk Assessment methodology targeting micro-enterprises:

- Assessing a simplified Information Security approach – Feedback from RA/RM Pilot (main consolidated report)
  http://enisa.europa.eu/doc/pdf/deliverables/sme_rarm_pilot.pdf

- UNIBO (Case study – Italy) – Risk Management Pilot
  http://enisa.europa.eu/doc/pdf/deliverables/cs_UNIBO.pdf

- IAAITC (Case study – UK) – Risk Management Pilot
  http://enisa.europa.eu/doc/pdf/deliverables/cs_IAAITC.pdf

- GMV (Case study – Spain) – Risk Management Pilot
  http://enisa.europa.eu/doc/pdf/deliverables/cs_GMV.pdf

Determining an Organisation's Information Risk Assessment and Management Requirements and Selecting Appropriate Methodologies
(Ad Hoc WG on Risk Management and Risk Assessment)

1. Ad Hoc Working Group on Risk Assessment and Risk Management (WG-RARM):
   - www.enisa.europa.eu/doc/pdf/ad_hoc_wg/wg_2008_deliverable_2.pdf

European Commission

General Report 2008
European Network and Information Security Agency

Luxembourg: Office for Official Publications of the European Communities

2009 – 60 pp. – 21cm x 29.7cm

ISBN: 978-92-9204-021-5
ISSN: 1830-981X
Catalogue no.: TP-AB-09-001-EN-C
doi 10.2824/10051

The report is also available on CD:

ISBN: 978-92-9204-022-2
ISSN: 1830-9828
doi 10.2824/10164

TP-AB-09-001-EN-C

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

doi 10.2824/10051
ISBN 978-92-9204-021-5

01/07_09