enisa
European Network and Information Security Agency

Securing Europe's Information Society

General Report 2009

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 2010

Luxembourg: Publications Office of the European Union, 2010
ISBN: 978-92-9204-037-6
ISSN: 1830-981X
doi 10.2824/15669

Securing Europe's Information Society
A Message from the Executive Director

2009 has been a very interesting and challenging experience for me, stepping aboard as the Executive Director of ENISA in the latter part of the year. Naturally, this has involved a learning process; as well injecting new direction and energy to the Agency, I have been able to look at ENISA through fresh eyes. I have been impressed by the professionalism and dedication of the staff. It has been a pleasure to get to know them and to work with them, and I look forward to many more productive years working together. We have embarked on a journey that will see the Agency become even better. We will improve its procedures and increase efficiency – and its effects will be demonstrated in the results we produce. The future indeed looks full of promise.

A Vision for the Agency's Future

My vision for ENISA is based on active trust with the Member States. Through this trust, we can promote co-operation between governments, industry and non-governmental organisations (NGOs) to the benefit of all citizens. At the same time, ENISA works for Europe, and gains its credibility by being an independent body of expertise. We provide advice on security matters to the European Commission and the European Parliament, making a lasting impact on the laws and regulations of the Commission and the Member States. In this way, the Agency can act as a 'pace-setter' for the political security agenda. We engage in dialogue, listen and carefully consider our stakeholders' views and translate them into action in our work. This means we have to analyse current technological, economic and societal developments so that we can respond adequately to current security threats, and act as a broker of security knowledge in the EU.

One of my main goals is to work towards a permanent mandate for ENISA – beyond the present 2012 'sunset' clause. A clear and permanent mandate is necessary to manage the increasing, fundamental role of security in economic and financial matters. Internally, an unlimited mandate helps ensure the seamless, smooth and stable functioning of the Agency and its operation.

Security is crucial for businesses and consumers alike – it transcends technology. Ultimately, the economy of Europe is at stake if we do not manage security properly. At the same time, we should promote the benefits of security to citizens, to increase their trust in the advantages of information and communication technology in the realisation that they can safely enjoy life in cyber-space.

To take just one example, our good work in assisting in the setting up of the so called 'digital fire brigades' (CERTs, Computer Emergency Response Teams) to mitigate massive cyber-attacks is aimed at ensuring that, in the near future, all Member States have a national/governmental CERT.

New Strategy Development

A new short-medium strategy for ENISA is being developed, in line with my vision for the Agency and the trust bestowed in me, and in dialogue with our stakeholders. This strategy will define the roadmap for the way ahead, clarify our strategic goals and role, and the mechanisms needed to achieve those goals.

New Political Environment

This development is taking place in a rapidly changing policy context. EU President Barroso has announced the policy priorities for the new European Commission, including a major initiative to boost network security as part of the overall Digital Agenda. Mrs. Neelie Kroes has been appointed as Vice President of the Commission with this Digital Agenda portfolio. A number of recent events, including the Malmö eGovernment Conference, highlighted the importance of Network and Information Security (NIS) and influenced the Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security. The Resolution builds on a number of EU strategies and instruments developed in recent years and provides political direction for how the Member States, the Commission, ENISA and stakeholders can each play their part in enhancing the level of network security in Europe. The Council Resolution should also be considered as a contribution to the ongoing debate, including the relevant public consultation, on the future of ENISA and its role in Critical Information Infrastructure Protection (CIIP).

With these major changes and policy initiatives, it is clear that security is heating up on the political agenda. ENISA will use this political momentum to reinforce its efforts to increase IT-security in Europe. This means, for example, tackling emerging issues such as the Future Internet, interoperable eID and the Internet of Things, and assisting with the first pan-European security exercises for CIIP.

Ultimately, security is about the economy of a modern society. This translates into jobs for ordinary people. Businesses, governments and citizens will only go online if they are confident that electronic services are correctly secured. Therefore, trust – in particular on the Internet – is key to success. Consequently, the privacy and security of digital identities are of the greatest importance.

How well is ENISA fulfilling its role in achieving this security? The results of our work in 2009 speak for themselves; they are impressive. In all modesty, the following pages provide an unparalleled, unique, independent overview of the state of security in Europe.

Enjoy reading.

Udo Helmbrecht
Executive Director of ENISA

Contents

ENISA –
for Europe's People, its Infrastructures and its Economy

Every day we live the Information Society – at home, at work, at play. Interconnected networks touch our everyday lives. They offer great benefits – but they bring with them enormous risks if they are not managed securely.

NIS – for Europe's people
New technology offers huge potential for education, entertainment and communications – but it must be used safely, especially by our children. New applications offer convenience, economies and progress in healthcare and government, but the data handled must be kept private.

NIS – for Europe's infrastructure
As networks grow more complex, they also become more vulnerable. Security breaches can generate substantial economic damage and can jeopardise a country's critical infrastructures – its power, water, transport and communications.

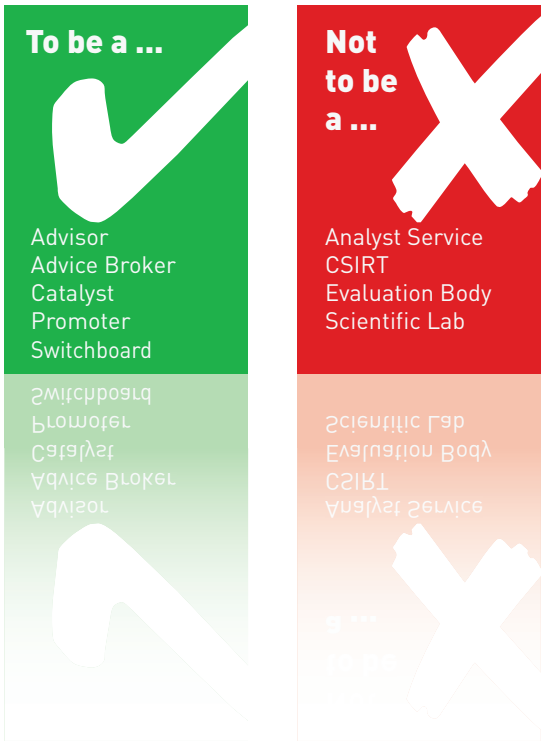
NIS – for Europe's economy
The safe and effective functioning of computers, mobile phones, banking and the Internet are crucial to support Europe's digital economy. They are indispensable to business and commerce and the successful operation of the market economy.

Security breaches can also cost individual businesses heavily. Recently a British bank was fined £3m (over €3.3m) for the loss of non-encrypted data.

Network and Information Security is critical to the progress of society in this digital age. THAT is why ENISA was created.

What does ENISA do?

ENISA's scope of activity



ENISA was set up to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to Network and Information Security (NIS) issues.

ENISA is a Centre of Expertise in Network and Information Security. Its mission is to

- Raise awareness
- Assess risks
- Stress the importance of NIS to all users
- Position NIS high on the political agenda

ENISA as an Advice Broker

ENISA bridges the gap between industry and governments. ENISA gathers and analyses data from the Member States, and recommends action to combat threats. It acts as a broker for advice, providing suitable contacts in the Member States or the EU institutions who will share their expertise and experience. It points towards good practices on key topics such as risk assessment & risk management, awareness raising and computer security incident response.

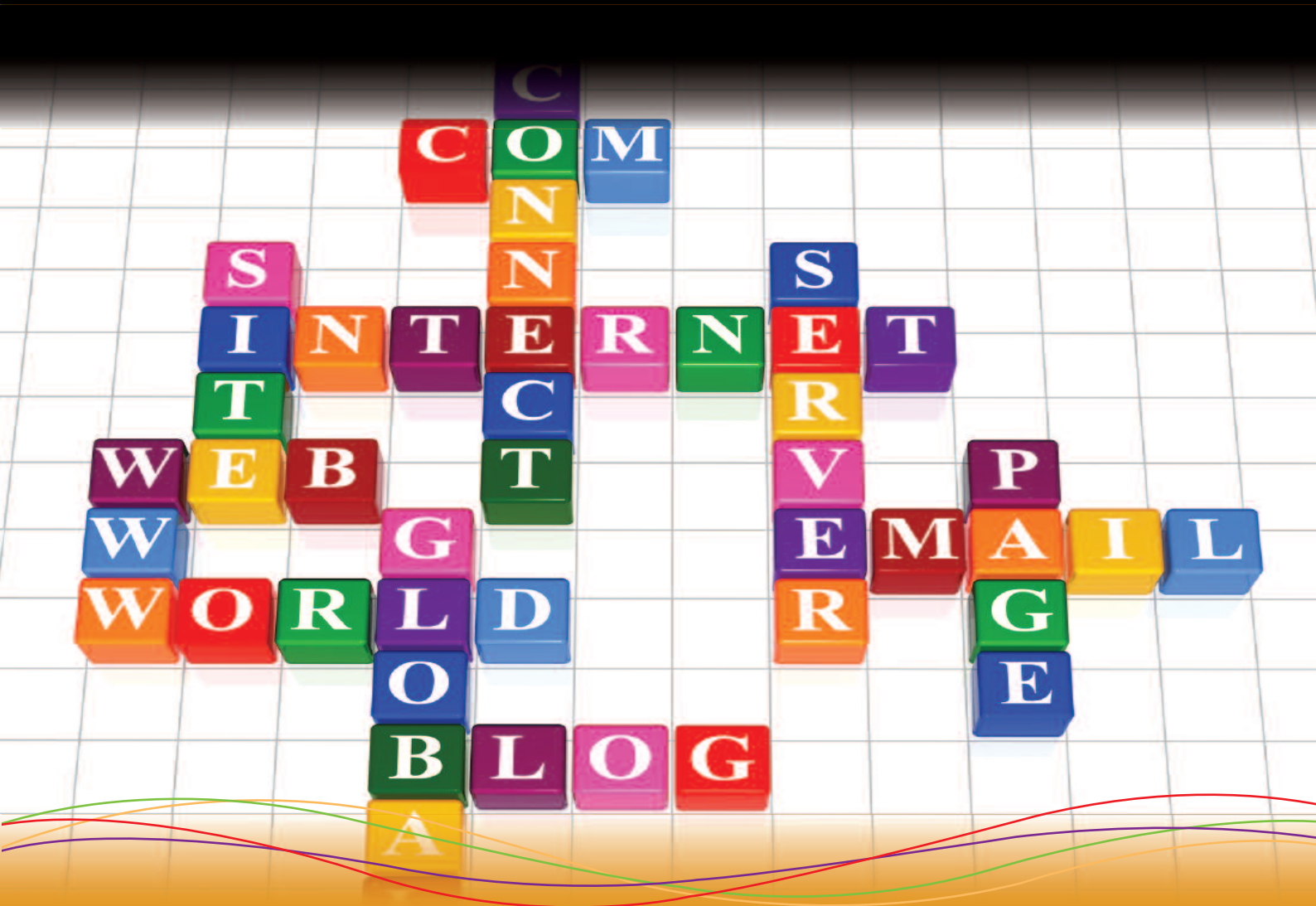
The Agency is uniquely positioned, with a comprehensive overview of the NIS situation within the EU. Its advice is independent, well informed and objective. ENISA advises the European Commission and the European Parliament on security matters, making a lasting impact on laws and regulations, and can act as a 'pace-setter' for the political security agenda.

In the international context, ENISA is the European spokesman on good practice in NIS to the outside world.

CHAPTER 1

Introduction

- NIS in Europe – the Challenges
- Executive Summary – ENISA in 2009
- ENISA – Looking to the Future



NIS in Europe – **the Challenges**

The pace of technological development over the last few years is unprecedented. Even the Industrial Revolution, which changed the way we live and work so dramatically, did not move this fast. Today we are surrounded by Information and Communications Technologies (ICTs). They have become essential tools in human, social and economic interaction, and there is no denying that they offer marvellous benefits to mankind.

But they can also bring with them enormous risks which could jeopardise the security of our society and our economy. 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, endangering both potential economic growth and society's development. It is now widely accepted that the availability, reliability and security of networks and information systems should be of the highest concern.

The European Context

Under the umbrella of the Lisbon Strategy, the European Commission Communication "i2010 – A European Information Society for growth and employment"[1], highlighted the importance of Network and Information Security (NIS) for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and society.

To a large extent, the current EU policy approach builds on the Commission Communication of 31 May 2006, "A Strategy for a Secure Information Society"[2]. This strategy, which responds to an earlier invitation by the Council, is based on an open and inclusive multi-stakeholder debate to foster a structured multi-stakeholder dialogue and establish partnership aimed at greater awareness and a better understanding of the challenges involved. It is also based on empowerment to create commitment by all the relevant stakeholders. It takes into account the role of ENISA, which was established in 2004 as the EU's centre of expertise in Network and Information Security.

A European Council Directive in December 2008 provided a framework for the "identification and designation of European critical infrastructures and the assessment of the need to improve their protection"[3]. As an important milestone in the implementation of the strategy for a Secure Information Society, in March 2009 the Commission then launched a policy initiative for Critical Information Infrastructure (CII) protection[4] – a 'CIIP Action Plan'. This Communication fully acknowledges ENISA's role in supporting the Commission and the Member States in implementing this strategy in a number of ways, including by facilitating collaboration between Member States.

The CIIP Action Plan received a high level of support from the Member States. The Presidency Conclusions of the Ministerial Conference on CIIP, held in April 2009 in Tallinn, state that "there is an urgent need for Member States and all stakeholders [including ENISA] to commit themselves to swift action in order to enhance the level of preparedness, security and resilience of CIIs throughout the European Union". It also states that "the Communication by the European Commission on CIIP furnishes a solid basis for taking such urgent action as is necessary".

The recently adopted review of the EU electronic communications regulatory framework also impacts on network security, in particular, the new provisions of articles 13a and 13b of the Framework Directive[5] and article 4 of the e-Privacy Directive[6]. These provisions aim at strengthening obligations for operators to ensure the security and integrity of their networks and services, and to notify any breaches of security, integrity

1 COM (2005) 229, 01.06.2005
2 COM (2006) 251, 31.05.2006
3 Council Directive 2008/114/EC
4 COM (2009)149
5 Directive 2009/140/EC
6 Directive 2002/58/EC

and personal data to competent national authorities. ENISA will support the Commission by providing its expertise in developing appropriate measures to implement these safeguards.

The Council Resolution of 18 December 2009 on a collaborative European approach on Network and Information Security builds on a number of EU strategies and instruments developed in recent years. It provides political direction on how the Member States, the Commission, ENISA and stakeholders can each play their part in enhancing the level of network security in Europe. The Council Resolution should also be considered as a contribution to the ongoing debate, including the relevant public consultation, on the future of ENISA and its role in Critical Information Infrastructure Protection (CIIP).

On 3 September 2009, EU President Barroso announced his policy priorities for the new European Commission, including a new Digital Agenda as the Commission's post i-2010 initiative. This agenda – and its accompanying targeted legislative programme – aims to tackle the main obstacles within a genuine digital single market, promoting investment in high-speed Internet and averting an unacceptable digital divide. Due to the increasing dependence of our economies and societies on the Internet, a major initiative to boost network security will also be proposed. The Digital Agenda is put into a longer-term perspective by the "eu 2020" strategy (revised Lisbon Strategy). The long-term 'Visby Agenda' for an eUnion 2015 and the Malmö eGovernment conference conclusions also point towards the digital future.

The Treaty of Lisbon, which came into force on 1 December 2009, embodies a strategy for taking Europe into the 21st century. It provides the EU with modern institutions and optimised working methods to tackle today's challenges efficiently and effectively. In a rapidly changing world, it includes security as one of the top priorities for the future of society and for economic development.

Establishing a Culture of Security

Each of us has a role to play in Network and Information Security:

- **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, and 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.

Any attempt to define and implement an appropriate approach to NIS must take place against a backdrop of rapidly changing technological developments. New applications and technologies such as Radio Frequency ID (RFID), the Internet of Things and the Future Internet must be addressed. At the same time existing challenges such as financially motivated organised cyber-crime and politically motivated cyber-attacks must not be ignored; national/governmental CERTs must be established in every Member State.

Whilst the technical challenge of securing new technological advances remains, the number one priority for the immediate future concerns the establishment of a proactive security culture. The creation of such a culture must consider the multi-stakeholder environment, educational gaps, non-optimised business models, the imbalance in Member States' capabilities, the approximation of laws and the global scope of NIS issues. This can only be tackled through dialogue, partnership and empowerment. It is a huge challenge – and ENISA has responded to the call.

Executive Summary –
ENISA in 2009

Achieving a coherent response to the evolving NIS threat landscape – in which all actors contribute to define and implement a global approach to securing infrastructures and reacting to incidents – remains the number one challenge in modern information security.

In 2009, to maximise the effect of its limited resources and increase its impact on key areas, ENISA continued to focus its efforts on a number of strategic priorities. The Work Programme 2009 comprised three Multi-annual Thematic Programmes (MTPs):

- Improving Resilience in European eCommunication Networks (MTP 1)
- Developing and Maintaining Co-operation Models (MTP 2)
- Identifying Emerging Risks for Creating Trust and Confidence (MTP 3)

In some cases, the Agency went the extra mile, tackling additional aspects that were not originally requested in the Work Programme, for example in co-organising the NIS Summer School in Heraklion in September, producing 'Briefings', conducting a survey of Internet service providers' anti-spam measures or producing the new Business Continuity guide tailored specifically for the needs of small and medium-sized enterprises (SMEs).

Improving Resilience in European eCommunication Networks (MTP 1)

Availability, integrity and the continuity of public communication networks are of major importance in a converging environment of fixed and mobile infrastructures. A totally interconnected and networked environment promises significant opportunities but also creates additional security risks. As interdependencies become complex, a disruption in one infrastructure can easily propagate into other infrastructures – and have a devastating impact on a European scale.

Experience proves that neither single providers nor a country alone can effectively detect, prevent and respond to such threats. The situation across Europe as regards the obligations and requirements to ensure and enhance the security and resilience of eCommunications networks is highly fragmented. The smooth functioning of the Internal Market and the demands of global players call for common requirements, rules and practices across the EU.

The recent European Commission communication, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149), recognises the importance of critical communication networks and asks ENISA to play an active role in ensuring that they are adequately protected. The Communication proposes a number of actions to develop an integrated EU approach to enhance the security and resilience of critical communication networks by complementing and adding value to national programmes as well as to other bilateral and multilateral co-operation schemes between Member States. For each of these activities, strong engagement with both the public and private sectors is considered to be a key success factor.

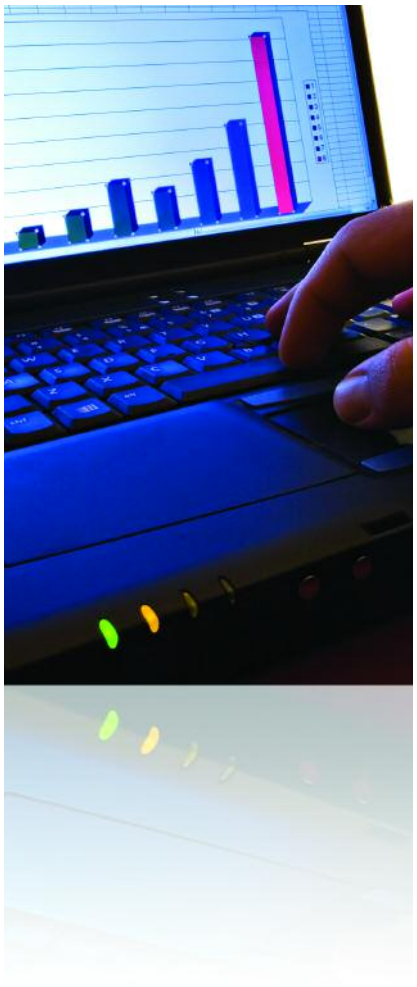
Tackling the problem
Under MTP 1, ENISA has supported the Member States and the European Commission in their efforts to improve resilience by "collectively evaluating and improving security and resilience in mobile and fixed public eCommunications networks and services in Europe".

In 2008 ENISA performed a series of stocktaking exercises of regulatory and policy environments, of providers' measures, and of existing technologies and standards.

In 2009 ENISA analysed the findings of this stocktaking, identified the gaps between the current and the target situation and worked together with stakeholders (using, for example, workshops and working groups of experts) to propose good practice guidelines to bridge gaps.

Good Practices of Regulatory and Policy Issues

Good Practice Guide on Information Sharing
Information sharing among both private and public stakeholders is necessary to better understand a constantly changing environment such as communication networks. Partnerships among private and public stakeholders are key to the identification of risks, threats and vulnerabilities. They represent a good model for developing and testing preparedness measures. Such partnerships are sometimes referred to as 'Network Security Information Exchanges' (NSIEs).



Today there are only a few Information Sharing Exchanges in Europe. Although it takes time and considerable effort to establish and run an NSIE, Europe should capitalise on such partnerships and develop national as well as pan-European Information Sharing Schemes.

In 2009 ENISA published a good practice guide on how to establish and manage national NSIEs. There are currently only a few Information Sharing Exchanges in Europe. This guide will help Member States to develop knowledge and expertise in this area and to establish their own information sharing platforms.

Good Practice Guide on Reporting Security Incidents
Reporting security incidents plays a pivotal role in ensuring the resilience of networks. In 2009, ENISA developed a good practice guide on reporting security incidents. The guide presents a systematic life-cycle on how to design, implement and evaluate Incident Reporting schemes at a national level. It not only aims to support public authorities that do not have significant experience but also to enhance the capabilities of those Member States with established incident reporting schemes.

Good Practice Guide on National Exercises
Exercises are particularly useful for training staff on procedures they should follow in the event of a future emergency and thus form an integral part of many organisations' business continuity planning. Exercises ensure that staff members are fully prepared and capable of responding effectively to incidents.

In its efforts to support EU Member State authorities in their attempts to enhance the resilience of critical information infrastructures, ENISA has developed a good practices guide on planning and conducting national exercises.

Analysing the Measures Deployed by Operators

Network and communication operators play a critical role in the continuous development of Europe's information society. The resilience of their networks is therefore of primary concern for European institutions, national governments, the private sector and civil society as a whole. However, there are currently significant differences in the approaches, methods, measures and strategies deployed by network operators and service providers across Europe.

In 2009, ENISA co-ordinated a group of resilience experts from major European providers. Together they identified the main resilience challenges and proposed a list of measures for each. In parallel, desktop research was conducted in order to identify guidelines in resilience activities in the following areas: organisational, business continuity and risk management. The output of this work was presented at a public workshop organised in October in Paris, France.

The combined analysis of various sources has identified applicable international good practices and, as a result, ENISA has been able to put together strategic guidance aimed at operators seeking to improve their resilience measures. Issues tackled include legal and policy barriers prohibiting providers from sharing information on sensitive matters, means of measuring resilience and providers' levels of security, and effective policies on combating botnets.

Innovative Actions to Improve Resilience

DNSSEC

In 2009 ENISA extended its work on the Domain Name System (DNS) by conducting a study on the cost of implementing Domain Name System Security Extensions (DNSSEC) in terms of both CAPEX and OPEX, as well as the anticipated business benefit. Interestingly, the study showed that the investment cost of new deployments is decreasing.

As a result of this work, ENISA has developed good practices guidelines for deploying DNSSEC. These cover the main considerations for providers deploying the technology and list the items that should be included in policy and practices statements for Trust Anchor Repositories. ENISA intends to promote these recommendations widely, particularly to EU and national policy-makers, in an effort to accelerate the take-up of the most promising innovative actions, and in 2010 the recommendations will be tested in real working environments. The work will also create input for ENISA's awareness raising activities in the preparation of an information campaign targeting users or specific user groups on the risks of DNS and DNSSEC in casual web-browsing applications such as banking, shopping etc.

Tracking standardisation activities

In 2009 ENISA assessed current standardisation developments that relate to the resilience of communication networks. The work involved a gap analysis of standardisation activities while at the same time drawing conclusions on the direction of future standardisation activities in this area.

The work included:

- An investigation of the definition applied to resilience in the context of standardisation
- Identification of the major activities undertaken in the standardisation organisations in either security or architecture that focus on resilience
- Identification of the areas where standardisation activity is required in either security or architecture, where a positive impact on the resilience of networks is expected.

As a result, ENISA has made the following recommendations for future standardisation activities:

- Work items should be actively promoted in the standardisation organisations (e.g. through a standardisation mandate) for the specification of metrics and supporting test and validation criteria to be used in the assessment of resilience (derived, where possible, from existing metrics used in the assessment of reliability and failure analysis)
- Work items should be actively promoted in the standardisation organisations (e.g through a standardisation mandate) to support the development of a taxonomy for resilience.

Priorities of Research on Current & Emerging Network Technologies (PROCENT)

During 2009, ENISA examined the impact of technological evolution and the latest trends in networking technologies (for example, mesh architectures, p2p networking etc.) in terms of the resilience of the communications infrastructure, measured both by its security and its availability.

This work was supported by an 'Expert Group on Priorities of Research on Current & Emerging Network Technologies (PROCENT)' composed of widely renowned specialists from both academia and industry. Both the selection of the areas addressed as well as the composition and the formation of the expert group were carried out in a workshop organised by ENISA in March 2009.

The PROCENT Expert Group addressed the following areas:

- Cloud computing
- Real-Time Detection and Diagnosis Systems
- Future wireless networks
- Sensor networks
- Integrity of supply chain

For each of the networking trends identified, the group considered:

- Ways that the networking technologies identified affect network resilience
- The possible benefits in terms of improving networking resilience that some of the network technologies identified might introduce
- Maintaining an outlook over the next 3-5 years on the R&D challenges relevant to the networking technologies identified
- The possible future role of ENISA in the topics/areas identified.

The findings of the expert group are expected to contribute to the preparation of the Framework Programmes of EU funded R&D. This is just one example of the ways in which ENISA is able to advise the European Commission "on research in the area of network and information security as well as on the effective use of risk prevention technologies".

The Fight Against Spam

Travelling another 'extra mile' to deliver more than was outlined in the Work Programme for the year, ENISA also conducted a survey of anti-spam measures implemented by European Internet service providers (ISPs). The resulting report includes an examination of spam budgets, and an assessment of the impact of spam and spam management. This is the third report on this subject produced by ENISA and unfortunately it records no significant progress in the fight against spam.

Spam remains an unnecessary, time consuming and costly burden for Europe. It is hoped that these new findings will encourage email providers to improve their spam monitoring systems and enable them to better identify its source. ENISA recommends that policy-makers and regulatory authorities should clarify the conflicts between spam-filtering, privacy and the obligation to deliver. In 2010, the Agency plans to study the root causes of spam and produce a report on botnets.

Developing and Maintaining Co-operation Models (MTP 2)

The challenges facing Network and Information Security (NIS) today cannot be addressed successfully with a piecemeal approach. They require a systematic, coherent and integrated strategy that involves all concerned stakeholders and decision-makers and is based on dialogue, partnership and empowerment.

Many Member States need to increase their capabilities in various fields of Network and Information Security (NIS). Some do already co-operate by sharing information on best practices, but this does not happen on a structured basis. As a result, opportunities are probably missed to create synergies at the European level and improve efficiency and effectiveness.

ENISA has a crucial role in Europe as a facilitator, a centre of expertise and an advice broker. The Agency is therefore building on previous work to develop various models of co-operation in predefined areas (such as awareness raising, incident response and building NIS capacity for micro-enterprises). In addition, ENISA operates the European NIS Good Practice Brokerage, including supporting tools such as the Who-is-Who Directory and Country Reports of activities in the Member States. Highlights of 2009 included the various thematic workshops designed to foster relationships with existing NIS communities or to encourage the development of new communities with common interests in specific NIS topics (such as Awareness Raising). To achieve this, the Agency has leveraged on its existing contacts and networks, including the network of National Liaison Officers.

Awareness Raising

During 2009 ENISA focused particularly on enhancing the information security awareness community and offering a perspective of what public institutions and private companies can do to enhance users' information security awareness.

The Awareness Raising Community

Launched in 2008, the awareness raising (AR) community is subscription-free and open to experts who have an interest in raising information security awareness within their organisations. The community is designed to help foster a culture of information security in Europe and is already proving very successful. In a very short time, it has grown to forty-six nations, comprising 325 members. All EU and European Economic Area (EEA) countries are represented and members are welcome from any country, whether within or outside Europe. In 2009, members of the AR community participated in a number of ENISA virtual working groups which produced white papers on ATM crime, information security awareness in financial organisations and the use of social networks through mobile phones.

ATM crime

With the rise in the number of ATMs in Europe there has also been a significant increase in the total number of reported ATM crimes. As a result, the ATM industry has made the safety of users and protection against fraud a high priority. In response, ENISA has published a paper on 'ATM crime: overview of the European situation and golden rules on how to avoid it'. The paper contains a set of recommendations to raise user awareness about the different types of risks faced when using an ATM, along with advice on how to counter them.

Information security awareness in financial organisations

Data security is a key risk for financial organisations; they generally hold significant amounts of personal and financial data, the safety of which is a crucial responsibility. In 2009, ENISA reviewed its previous work on awareness raising in financial organisations in the light of new research and analysis. A revised document, 'Information security awareness in financial organisations', has been produced which contains new case studies as well as recommendations and practical advice.

AR Conference
In June 2009, ENISA organised a conference on 'The growing requirement for information security awareness across public and private organisations', which was hosted by Thomson Reuters at their London offices. Key issues discussed included the effect of the financial crisis on information security and recent leaks of sensitive information.

Spreading the message to organisations
ENISA created awareness raising material tailored for specific organisations, to ensure that employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources, and to assist organisations in keeping their computers and networks safe. The material prepared for British Airways was runner-up in the 2009 IT Real Awards.

Protecting Children
ENISA also created material to raise the awareness of parents about the safety of children using virtual world sites.

In addition, the Agency supported the Child Online Protection (COP) Initiative, established by the International Telecommunication Union (ITU) to provide guidance on safe online behaviour. ENISA contributed to the preparation of Guidelines targeting children, parents, guardians and educators, industry and policy-makers. These Guidelines have been developed with the aim of establishing the foundations for a safe and secure cyber-world not only for today's youth but also for future generations. In recognition of ENISA's dedication to the COP Initiative, ITU Secretary-General Hamadoun Touré presented the Agency with a certificate of appreciation at ITU Telecom World in Geneva, Switzerland in October.

Incident Response

Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every country that is connected to the Internet should have the capability to respond effectively and efficiently to information security incidents. But CERTs must do much more: they must act as primary security service providers for governments and citizens, and be awareness raisers and educators.

However, not every country connected to the Internet possesses CERT capabilities, and the level of maturity among those which do varies dramatically. It is ENISA's mission to fill the gaps on the CERT world map by facilitating the setting up, training and exercising of CERTs.

ENISA's role as good practice knowledgebase and contact broker is supported by the high quality material it has already produced. Following consultation with CERTs in the Member States, the good practice collection was extended in 2009 to cover the special role that national and/or governmental CSIRTs play in their countries' national incident response capability. The Agency also continued to support the very successful TRANSITS training for CERT staff which takes place at least twice a year.

CERT exercise pilots – preparedness is key!
Exercises are an indispensable tool for emergency and crisis preparedness for CERTs. Currently, only a few teams perform crisis management and co-operation exercises in a constructive way that really enhances preparedness. Most teams limit themselves to small, ad hoc exercises with limited scope and coverage.

In 2008 ENISA produced a 'CSIRT exercises collection', which includes exercises and a handbook for trainers and is intended to enable a CERT to train its staff to deal with new or unanticipated situations. The exercises were successfully piloted in 2009, in June in Chisinau, Moldova Republic, and in Kyoto, Japan.

Baseline capabilities of national/governmental CERTs
In 2009 ENISA took the first step towards indentifying a minimum set of (baseline) capabilities for national and governmental CERTs. This is a prerequisite if they are to contribute in Europe-wide co-operation and information sharing, not only for incident response during crisis situations but also in the sharing of operational data and good practice on a day-to-day basis.

The first draft of a document was published at the end of 2009. It will be subject to review in the light of other relevant work in the field and adjusted and discussed with the relevant stakeholders in the CERT communities, the European Commission and the Member States.

European NIS Good Practice Brokerage

Since 2007, ENISA has been facilitating co-operative projects among EU Member States through its European NIS Good Practice Brokerage. In order to enhance the overall level of NIS in Europe, much improved co-operation among both Member States and the private sector is essential.

In 2009, the Agency supported several co-operative projects among the Member States, by acting as a good practice broker in the European NIS 'marketplace', and updated its supporting tools: the Who-is-Who Directory on NIS, the Country Reports and its Online Platform.

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. Awareness, risk assessment and risk management are prerequisites for the establishment of security measures.

ENISA therefore undertook a project in 2009 to increase knowledge and competence on how to build NIS capacity among both micro-enterprise intermediaries and multiplier organisations and their constituencies or members. The work involved developing a tailor-made toolkit by customising existing ENISA Risk Assessment/Risk Management and Awareness Raising deliverables.

In addition, as part of the validation process, the newly developed tool was presented in Brussels, Belgium, in November 2009 to a high-level audience which included the Secretary of State for European Affairs of Hessen, EU decision-makers and numerous Brussels-based multiplier organisations. Following the presentation, a key multiplier stakeholder organisation initiated the evaluation and analysis required prior to integration of the online tool with their website. After a positive assessment, the online tool will be translated into French and Dutch, in addition to the existing German and English versions.

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

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. But ENISA is also working to identify emerging risks, and is establishing an Emerging Risks (ER) Framework that will enable decision-makers to better understand and assess the new risks arising from new technologies and new applications. This will enable better informed decision-making, which in turn will contribute to the growth of stakeholders' trust and confidence.

During 2009, ENISA's work on EFR was used to improve and adapt the Framework. When the updating of the handbook and process is complete, the EFR Framework will provide a method of delivering emerging risk assessments in a standardised way with appropriate quality assurance. The updated version of the EFR handbook is expected to be published on the ENISA website in February 2010.

Analysis of Specific Scenarios

ENISA's work also provides analysis of specific EFR scenarios. This includes the publication of risk assessment reports on new applications and technology areas.

European eID Cards

In 2009 ENISA produced a Risk Assessment Report on 'Security Privacy and Security Risks when authenticating in the Internet with European eID Cards'. The report looks at different use-cases, and identifies relevant security risks, gives an opinion about their relevance and importance and presents mechanisms that could mitigate these risks. The report focuses on authentication using smart cards and compares this approach with other common means of authentication.

The paper is aimed at political decision-makers and NIS stakeholders in Europe. Its main purpose is to help define a comprehensive list of requirements for national ID cards in order to ensure that they are as flexible and as multi-purpose as possible.

Cloud Computing

Cloud computing was identified by ENISA's experts and by its Permanent Stakeholders' Group as one of the emerging applications which is likely to have a significant impact on European businesses and governments in the near future. In 2009 the Agency assembled a group of experts, who worked together over a period of eight months to examine the benefits and risks of cloud computing. Their report is the first to take an independent, in-depth look at the security and privacy issues of moving into the cloud.

The main target audience of the report is businesses, especially small and medium-sized enterprises (SMEs), because they are the largest customers of cloud computing. The report provides a checklist for assessing the maturity of cloud providers' security measures, recommendations for future research and a specific set of recommendations drawn up by legal specialists detailing what to look for in a cloud computing contract.

The Internet of Things/RFID
During 2009, ENISA set out to identify the emerging and future risks involved in the Internet of Things and to make recommendations to address them appropriately. A scenario based on IoT/Radio Frequency Identification (RFID) technologies in future air travel was taken as an example. The work supports EU policy initiatives on RFID and the Internet of Things. Among the technologies in this scenario are smart phones, netbooks, RFID and location-based services (LBS), but the power of these technologies is greatly leveraged by their convergence. This scenario will serve as a test bed to illustrate the convergence of these IoT technologies and the issues that arise as a result of such convergence. The assessment highlights the major assets, vulnerabilities, threats and finally risks in the use of these technologies in air travel. The final report is expected to be published in February 2010.

Cyber-bullying and online grooming
Given current concern about Internet usage and in particular child protection issues, ENISA initiated a risk assessment within the Emerging and Future Risks Framework in the area of cyber-bullying and online grooming. The Agency worked with a group of experts on the subject. Their report makes recommendations for strategies to mitigate the risks.

Other Activities

To both underpin and enable its work, ENISA also continued its ongoing activities – communication and outreach, and relations with its various external stakeholders such as the EU bodies, the Member States, industry, academia, consumers, international institutions and Third Countries.

ENISA's role

ENISA is ideally placed to facilitate the necessary dialogue, to offer advice and assistance and to enable the exchange of information as part of the overall goal of creating a culture of security. The Agency supports an open multi-stakeholder dialogue and, for that reason, maintains close relations with industry, the academic sector and users. It has also developed contacts with a network of national representatives (National Liaison Officers, NLOs), and with individual experts through ad hoc Working Groups, virtual expert groups and platforms. In this way. ENISA is able to gather and disseminate expert recommendations and to facilitate information exchange with and between public and private sector parties.

In addition, the capacity to provide prompt, independent and high quality responses to requests received from EU Institutions and Member States gives the Agency a bridging role between EU and national institutions. This role is specific to ENISA and currently it is unique in the world.

A closer participation in the worldwide dialogue is also being developed through continuously expanding contacts with Third Countries on all continents as well as with international institutions. The expected impact is a better integration of important foreign players' views and a promotion of European approaches.

ENISA –
Looking to the Future

New applications and technologies bring new threats and new risks. To ensure an adequate level of NIS in the EU, all relevant stakeholders must work together in defining appropriate priorities and countermeasures. The fact that the highly dynamic environment of our digital world is continually expanding and providing new services for business and government makes this need even more pressing. Innovations such as Radio Frequency ID (RFID), the Internet of Things and the Future Internet must be addressed. At the same time we must not lose sight of other important trends and challenges such as financially motivated organised cyber-crime and politically motivated cyber-attacks; there are still some Member States that do not have national/governmental CERTs and ENISA can help in their establishment. The Agency also has a key role to play in the first pan-European security exercises for Critical Information Infrastructure Protection (CIIP).

Although the technical challenge of securing new technological advances often dominates, the top priority must be the establishment of a proactive security culture.

ENISA, is uniquely positioned to provide advice and assistance to Member States in enhancing their NIS capabilities. Due to its independent position, the Agency can provide well-informed, objective advice and play a significant role in supporting the European Commission and Member States by facilitating the exchange of good practices and information between all stakeholders at the European level.

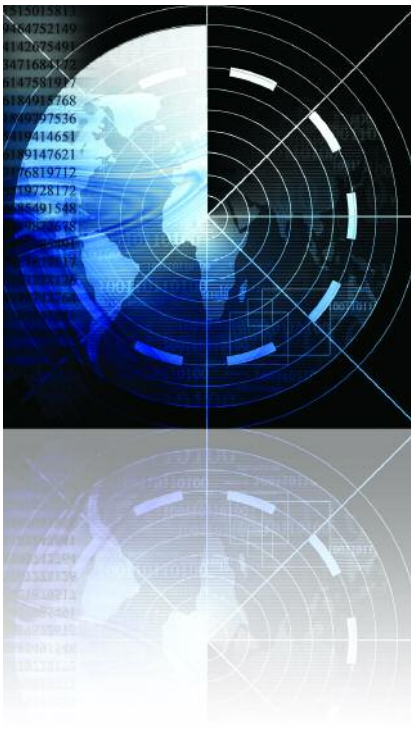
In 2010, ENISA will continue working on its three existing Multi-annual Thematic Programmes (MTPs), while introducing two new Preparatory Actions (PAs, activities lasting one year to investigate the possibility of initiating new MTPs).

In particular, there will be greater prioritisation of work on the resilience of eCommunication networks (MTP 1), in response to the recent communication on Critical Information Infrastructure Protection (CIIP) released by the European Commission in March 2009, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149). There will also be an increased focus in MTP 3 on enhancing national risk management preparedness in order to further support the CIIP action plan.

MTP 1: Improving resilience in European eCommunication networks – In 2010, the main effort will be to support the actions described in Communication COM(2009)149. Activities will be aimed at underpinning stakeholders' efforts to deploy ENISA's information sharing and incident reporting good practice guides, helping providers to enhance the resilience of their networks, investigating innovative actions, and assisting stakeholders towards conducting the first pan-European training exercise.

MTP 2: Developing and maintaining co-operation models – in order to use and enhance the existing networks of actors in NIS. In 2010, ENISA will continue to collaborate with the awareness raising community and the security competence circle for CERTs, and facilitate co-operative initiatives through the European NIS Good Practice Brokerage. The aim will be to improve the capabilities of all Members States and increase the overall coherence of the approach to NIS at the pan-European level. The Agency will co-operate closely with Commission services in order to make best use of its resources and to maximise results.

MTP 3: Identifying emerging risks for creating trust and confidence – ENISA will continue to develop its Emerging Risks Framework. When implemented, this Framework will enable decision-makers to better understand and assess the risks arising from new technologies and new applications, thereby strengthening stakeholders' trust and confidence. In so doing, the Agency will provide an early warning function for decision-makers in Europe and possibly beyond. Work in 2010 will focus on the analysis of specific scenarios, the maintenance of the Framework and enhancing national risk management preparedness. The proof of concept, which was tested and developed in 2009, will be deployed with Member States in 2010, and the Agency will continue preparing Risk Assessment reports on emerging risks.



In addition, ENISA will embark on two Preparatory Actions:

PA1: Identity, accountability and trust in the future Internet – Following recent developments on the Internet, in parallel with real life, individuals now have the opportunity of 'living' additional lives in the virtual world. A trend observed over the last few years, first in the research community, but now also in commercial offerings, is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet. A parallel development is the so-called Internet of Things (IoT) which, as an evolution of today's RFID technology, consists of networks of actuators and sensor nodes that interact with objects bearing tags. As a response to these developments, in 2010 ENISA will undertake activities aimed at achieving a high level of security in Europe and ensuring that both users and industry maintain their confidence in the ICT infrastructure and its services, while at the same time limiting the threats to civil liberties and privacy. This work will involve stocktaking of authentication and privacy mechanisms and of models supporting electronic services.

PA2: Identifying drivers and frameworks for EU sectoral NIS co-operation – As intangible assets become increasingly valuable to a company, traditional forms of protection are no longer enough to prevent intruders from entering and either stealing or damaging key assets. A more proactive approach is needed. This approach must encompass an overall framework of organisational differentiation between public and private actors and along organisational supply chains; it must be based on a realistic assessment of the various parties' ability to tackle NIS challenges, and it should take into account their legitimate commercial or public service responsibilities and capabilities. This PA will examine methods of obtaining commitment from relevant actors to participate in collective action to address NIS challenges at a pan-European level. The work will look at incentives and responsibility requirements for multi-stakeholder NIS governance frameworks in ICT supplier and user communities.

Finally, ENISA will also continue providing advice and assistance when called upon.

CHAPTER 2

Building Synergies, Achieving Impact – the Work Programme 2009:

- Improving Resilience in European eCommunication Networks (MTP 1)
- Developing and Maintaining Co-operation Models (MTP 2)
- Identifying Emerging Risks for Creating Trust and Confidence (MTP 3)

Building Synergies, Achieving Impact – the Work Programme 2009

Multi-annual Planning

In 2009, ENISA continued with its strategy of concentrating its resources to achieve increased impact in key areas. By building on existing national and EU activities, the Agency is avoiding the duplication of effort and maximising results. By working closely with initiatives such as the IST-FP6 Research for Critical Information Infrastructure Protection (CIIP), the Competitiveness and Innovation Programme (CIP), the ICT priority in the 7th Research Framework Programme and the IDABC (Interoperable Delivery of European eGovernment services to public Administrations, Business and Citizens) programme, ENISA can capitalise on their results, interact with their constituencies and engage them in ENISA's work. This co-operation was a key feature of the Work Programme 2009.

To achieve the desired impact and build on synergies, the Agency follows a multi-annual work plan, concentrating its efforts on a limited set of strategic priorities, called Multi-annual Thematic Programmes (MTPs), while at the same time following the high-level direction provided by the ENISA Management Board.

These high-level goals – which guide ENISA's overall strategy – are:

- Building confidence in the information society through increasing the level of NIS in the 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 the dialogue between the various stakeholders in the EU on NIS
- Increasing co-operation between Member States in order to reduce the difference between the capability of various Member States in this area
- Assisting and responding to requests for assistance from the Member States.

The MTPs define the work of the Agency for a number of years. A set of SMART[7] goals is defined for each programme. These goals are related to the desired outcomes and impacts and can be assessed and monitored during the duration of the programme via Key Performance Indicators. Each thematic programme consists of several Work Packages (WPK), that implement the SMART goals of the MTP. Each Work Package defines the tasks, the stakeholders concerned, the desired impact and the resources needed.

The Work Programme 2009

In 2008, ENISA began with three MTPs and one Preparatory Action (PA, a one-year project designed to ascertain the potential of a possible future activity). In 2009, the focus was consolidated around the existing MTPs, while integrating the follow-up of the PA as WPKs in one of the MTPs:

MTP 1: Improving resilience in European eCommunication networks – In 2008, this MTP focused on stocktaking, identifying best practices and analysing gaps in measures deployed by both National Regulatory Authorities (NRAs) and network operators and service providers. ENISA also analysed the suitability of currently deployed backbone Internet technologies in ensuring the integrity and stability of networks. In 2009, MTP 1 compared the findings of its work in 2008 with similar international experiences and results, issued guidelines and, after broad consultation with concerned stakeholders, formulated consensus-based recommendations. The recommendations are now being widely promoted to appropriate policy- and decision-makers.

[7] SMART is an acronym for Specific, Measurable, Agreed, Realistic and Time bound.

MTP 2: Developing and maintaining co-operation models – in order to use and enhance the existing networks of actors in NIS. In 2008 this MTP aimed to identify Europe-wide security competence circles in topics such as Awareness Raising and Incident Response and to develop the European NIS Good Practice Brokerage. This work was further developed in 2009 with the aim of improving the capabilities of all Members States and increasing overall coherence and levels of interoperability. ENISA also added work aimed at NIS capacity building for micro-enterprises.

MTP 3: Identifying emerging risks for creating trust and confidence – ENISA is developing an Emerging Risks Framework. When implemented, this Framework will enable decision-makers to better understand and assess the 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. In 2009, the proof of concept of a European capacity for the evaluation of risks that may emerge in two to three years' time, which was developed in 2008, was tested and developed further, with the aim of deploying it with Member States in 2010. The Agency also continued to prepare Risk Assessment reports on emerging risks.

In some cases, the Agency went the extra mile, tackling additional projects that were not outlined in the original Work Programme, for example by co-organising the NIS Summer School in Heraklion, Greece, in September and the forthcoming ENISA-ANACOM Event on 'Risk and Innovation', producing 'Briefings', conducting a survey of Internet service providers' anti-spam measures, or producing the new Business Continuity guide tailored specifically for the needs of small and medium-sized enterprises (SMEs).

In addition to its specific tasks, the Agency continued with its regular activities – including communication and outreach, and relations with its various external stakeholders such as the EU bodies, the Member States, industry, academia, consumers, international institutions and Third Countries. The Agency also 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 2009, see Appendix 2.

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[8] 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 2009 has the ultimate objective of evaluating and improving the resilience of public eCommunications in Europe.

The situation across Europe as regards the obligations and requirements to ensure and enhance the security and resilience of eCommunications networks is highly fragmented. The smooth functioning of the Internal Market and the demands of global players call for common requirements, rules and practices across the EU.

In 2008, ENISA's stocktaking exercises had 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.

ENISA addressed 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

In 2009 ENISA compared its findings with other studies. Then, after wide consultation with relevant stakeholders, it issued various sets of good practice guidelines, and formulated consensus-based recommendations to improve the resiliency of public eCommunications in Europe. These recommendations are now being widely promoted to appropriate policy- and decision-makers.

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

Good Practices of Regulatory and Policy Issues

Good Practice Guide on Information Sharing

Information sharing among both private and public stakeholders is necessary to better understand a constantly changing environment such as communication networks. ENISA's stocktaking and analysis, performed in 2008, revealed the importance and strategic value of information sharing.

Partnerships among private and public stakeholders are key to the identification of risks, threats and vulnerabilities. They represent a good model for developing and testing preparedness measures. Such partnerships are sometimes referred to as 'Network Security Information Exchanges' (NSIEs) although alternative names are also used.

In 2009 ENISA collected different national practices and performed a state of the art analysis. Through stocktaking and with contributions from experts, the Agency identified good practice on partnerships modes, stakeholders' roles, available services and products, trust models, incentives, confidentiality and privacy and other important issues.

The result was the publication of a good practice guide[9] on how to establish and manage national NSIEs. The guide will help Member States to develop knowledge and expertise in this area and to establish their own information sharing platforms.

Today there are only a few Information Sharing Exchanges in Europe. Although the time and effort involved in establishing and running an NSIE is not inconsiderable, Europe should take advantage of these partnerships and develop national as well as pan-European Information Sharing Schemes.

In 2010, ENISA will continue to support Member States' efforts to deploy NSIEs in Europe. The Agency will also investigate the possibility of establishing a pan-European Information Sharing platform based on existing national platforms.

Good Practice Guide on Reporting Security Incidents

In recent years, the use of communication networks has expanded rapidly to encompass a far wider range of services and applications. Continued transformation constantly opens up new challenges for those aiming to secure the networks and ensure their resilience against all threats.

Reporting security incidents plays a pivotal role. Effective reporting ensures that all those who need to know about an incident learn about it quickly. Timely reporting can also enable a co-ordinated response and give those responding access to a wide pool of expertise about such incidents. Incident Reporting ensures that national authorities can follow up with network operators in a regulatory capacity, if necessary. Reporting can enable the collection of data about incidents, threats and prior experiences to be used for analysis and the identification of good practices in responding to specific kinds of incidents.

In consultation with its constituency and wider stocktaking, ENISA has developed a good practice guide[10] on reporting security incidents. The guide addresses security and resilience related incidents but not privacy-related events.

This guide presents a systematic life-cycle on how to design, implement and evaluate incident reporting schemes at a national level. It not only aims to support public authorities that do not have significant experience but also to enhance the capabilities of those Member States with established incident reporting schemes.

[9] www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/information-sharing-exchange

[10] www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms

One of the key findings is that the usage of incident reporting schemes across the EU varies widely; some Member States have very extensive systems, while others have yet to launch one. And those that do exist often have significantly different objectives and procedures, deal with different types of incidents and participants and produce different results.

The recently adopted reform of the Telecommunication Package (article 13) mandates competent national authorities to establish and manage national incident reporting schemes. In 2010 ENISA will continue working with Member States and the Commission on the design and implementation of effective incident reporting mechanisms.

Good Practice Guide on National Exercises

Exercises have been widely used in various sectors for a long time. They are now commonly deployed by many players in the ICT sector, particularly by telecommunication network operators and Computer Emergency Response Teams (CERTs).

Exercises are particularly useful for training staff on procedures they should follow in the event of a future emergency and thus form an integral part of many organisations' business continuity planning. Exercises ensure that staff members are fully prepared and capable of responding to incidents by efficiently following existing preparedness measures (e.g. business continuity and disaster recovery procedures).

Planning and executing a national exercise effectively is a challenging task. In its efforts to support EU Member State authorities in their attempts to enhance the resilience of critical information infrastructure, ENISA has developed a good practices guide[11] on planning and conducting national exercises.

The guide was prepared by surveying and interviewing relevant stakeholders (e.g. public authorities, network operators, IT industry players and network security experts). ENISA also performed secondary research to identify good practices. As a result, the guide represents a broad consensus of the experiences of a wide selection of public and private sector experts.

This good practice guide presents a systematic life-cycle on how to design, plan, implement and evaluate a national exercise. The guide aims to support authorities that do not have significant experience in planning and executing exercises. It also helps authorities to identify and develop the skills needed to select measures and processes to be tested, to plan, execute and evaluate interdependencies-focused exercises themselves and to use the experience gained by other stakeholders to improve their own measures and processes.

In 2010 ENISA will facilitate Member States' effort to establish, run and monitor the first pan-European exercise.

11 www.enisa.europa.eu/act/res/policies/good-practices-1/exercises

Analysing the Measures Deployed by Operators

Network and communication operators play a critical role in the continuous development of Europe's information society. The resilience of their networks is therefore of primary concern for European institutions, national governments, the private sector and civil society as a whole. However, there are currently significant differences in the approaches, methods, measures and strategies deployed by network operators and service providers across Europe.

In 2009, ENISA co-ordinated a group of resilience experts from major European providers. Together they identified the main resilience challenges[12] and proposed a list of measures for each. In parallel, desktop research was conducted in order to identify guidelines in resilience activities[13] in the following areas: organisational, business continuity and risk management. The output of this work was presented at a public workshop organised in October in Paris, France.

ENISA used a variety of sources representing industry or sector-specific good practices, including telecommunications operations guidance, internationally accepted standards for business continuity and risk management guidance, advice from national authorities and the results of relevant research.

The combined analysis of these various sources has identified applicable international good practices and concludes with strategic guidance for operators seeking to improve their resilience measures. Issues tackled include legal and policy barriers prohibiting providers from sharing information on sensitive matters, means of measuring resilience and providers' levels of security, and effective policies on combating botnets.

In 2010, ENISA will work to promote the guidelines and the new measures proposed. The results of this work will serve as background knowledge for the analysis of new areas such as security and resilience metrics.

Innovative Actions to Improve Resilience

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.

In 2008, ENISA analysed a number of technologies, protocols and architectures currently available to improve the resilience of public communication networks; at the suggestion of stakeholders, the Agency focused on three: MPLS (Multiprotocol Label Switching), Domain Name System Security Extensions (DNSSEC) and IPv6.

In 2009, ENISA continued to investigate possible ways of enhancing the resilience of public eCommunication networks, not limiting itself to technologies, architectures and protocols. The Agency looked at incentives and market and/or policy-related aspects with a view to identifying their impact on business practices and to developing recommendations addressed mainly to EU and national policy-makers. The results of these investigations have led to the definition of guidelines on innovative actions to enhance the resilience of public eCommunication networks.

12 www.enisa.europa.eu/act/res/providers-measures/vwg-2009

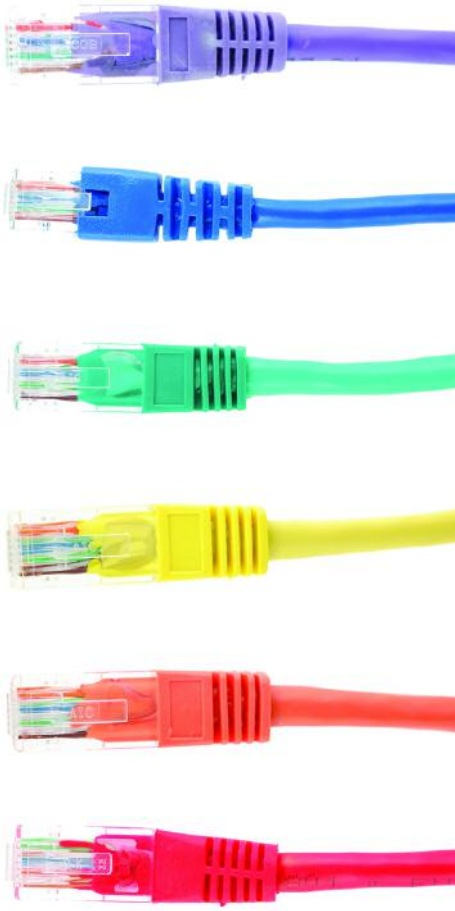
13 www.enisa.europa.eu/act/res/providers-measures/files/resilience-good-practices

DNSSEC

In 2009 ENISA extended its work on the Domain Name System (DNS). At the beginning of 2009, the Agency organised a workshop on 'Improving the resilience of DNS'. As a result of this event, an expert group was formed comprising well known key experts in DNS, and a list of actions that could be addressed by ENISA in collaboration with the members of the expert group was drawn up.

One of the actions adopted was to study the costs of deploying DNSSEC, a technology that, according to ENISA's 2008 stocktaking findings, has significant potential to improve the resilience of communications networks. However, deploying a new technology requires investment in software and hardware as well as human resources. Uncertainty as to the costs involved may hinder deployment. In 2009, ENISA therefore conducted a study through targeted stocktaking and by interviewing twenty organisations with different roles in DNS administration and operation – all the organisations interviewed had operational experience of the subject. The study assessed the costs that might be expected to be incurred for deployment in terms of both CAPEX and OPEX and the anticipated business benefit. Interestingly, the study showed that the investment cost of new deployments is decreasing.

As a result of this work, ENISA has developed good practices guidelines for deploying DNSSEC. These cover the main considerations for providers deploying the technology and list the items that should be included in policy and practices statements for Trust Anchor Repositories. ENISA intends to promote these recommendations widely, particularly to EU and national policy-makers, in an effort to accelerate the take-up of the most promising innovative actions, and in 2010 the recommendations will be tested in real working environments. The work will also create input for ENISA's awareness raising activities in the preparation of an information campaign targeting users or specific user groups on the risks of DNS and DNSSEC in casual web-browsing applications such as banking, shopping etc.



Tracking standardisation activities

In 2009 ENISA assessed current standardisation developments that relate to the resilience of communication networks. The work involved a gap analysis of standardisation activities while at the same time drawing conclusions on the direction of future standardisation activities in this area.

The work included:

- An investigation of the definition applied to resilience in the context of standardisation
- Identification of the major activities undertaken in the standardisation organisations in either security or architecture that focus on resilience
- Identification of the areas where standardisation activity is required in either security or architecture, where a positive impact on the resilience of networks is expected.

As a result, ENISA has made the following recommendations for future standardisation activities:

- Work items should be actively promoted in the standardisation organisations (e.g. through a standardisation mandate) for the specification of metrics and supporting test and validation criteria to be used in the assessment of resilience (derived, where possible, from existing metrics used in the assessment of reliability and failure analysis)
- Work items should be actively promoted in the standardisation organisations (e.g. through a standardisation mandate) to support the development of a taxonomy for resilience.

Priorities of Research on Current & Emerging Network Technologies (PROCENT)
During 2009, ENISA examined the impact of technological evolution and the latest trends in networking technologies (for example, mesh architectures, p2p networking etc.) in terms of the resilience of the communications infrastructure, measured both by its security and its availability.

This work was supported by an 'Expert Group on Priorities of Research on Current & Emerging Network Technologies (PROCENT)' composed of widely renowned specialists from both academia and industry. Both the selection of the areas addressed as well as the composition and the formation of the expert group were carried out in a workshop organised by ENISA in March 2009.

The PROCENT Expert Group addressed the following areas:
- Cloud computing
- Real-Time Detection and Diagnosis Systems
- Future wireless networks
- Sensor networks
- Integrity of supply chain

For each of the networking trends identified, the group considered:
- Ways that the networking technologies identified affect network resilience
- The possible benefits in terms of improving networking resilience that some of the network technologies identified might introduce
- Maintaining an outlook over the next 3-5 years on the R&D challenges relevant to the networking technologies identified
- The possible future role of ENISA in the topics/areas identified.

The findings of the expert group are expected to contribute to the preparation of the Framework Programmes of EU funded R&D. This is just one example of the ways in which ENISA is able to advise the European Commission "on research in the area of network and information security as well as on the effective use of risk prevention technologies".

The Fight Against Spam

Travelling another 'extra mile' to deliver more than was outlined in the Work Programme for the year, ENISA conducted a survey of anti-spam measures implemented by European Internet service providers (ISPs). The resulting report includes an examination of spam budgets, and an assessment of the impact of spam and spam management. This is the third report on this subject produced by ENISA and unfortunately it records no significant progress in the fight against spam.

The survey targeted email service providers of different types and sizes, and received replies from 100 respondents from 30 different countries throughout the Member States.

Spam remains an unnecessary, time consuming and costly burden for Europe. It is hoped that these new findings will encourage email providers to improve their spam monitoring systems and enable them to better identify its source. ENISA recommends that policy-makers and regulatory authorities should clarify the conflicts between spam-filtering, privacy and the obligation to deliver.

In 2010, the Agency plans to study the root causes of spam and produce a report on botnets.

Key findings:
- Less than 5% of all email traffic is delivered to mailboxes, which means that the main bulk of mails, 95%, is spam. This compares with 6% in earlier ENISA reports.
- 70% of respondents consider spam extremely significant or significant for their security operations.
- Over 25% of respondents received spam, and spam accounted for more than 10% of helpdesk calls.
- Among very small providers, 25% of respondents allocate anti-spam budgets of over €10,000 per year; 33% of very large providers dedicate over €1 million/year to fight spam.
- ISPs are using various kinds of measures: technical, awareness, policies and legal framework. Blacklists are the most commonly used anti-spam tool.
- ISPs consider spam prevention as a competitive advantage to attract and retain customers.

Developing and Maintaining Co-operation Models

A Co-operation Platform for the Awareness Raising Community

During 2009 ENISA focused particularly on enhancing the information security awareness community and offering a perspective of what public institutions and private companies can do to enhance users' information security awareness. To this end, ENISA worked to identify relevant information security experts and activities with which it could be involved, along with security topics which may be relevant for raising information security awareness.

The Awareness Raising Community

The awareness raising (AR) community is subscription-free and open to experts who have an interest in engaging in raising information security awareness within their organisations. The AR community was launched in February 2008 and is designed to work with ENISA in fulfilling its mission to foster a culture of information security.

The AR community sees different people and cultures as an asset in promoting a culture of information security. In a very short time, the community has grown to 46 nations, comprising 325 members. All EU and European Economic Area (EEA) countries are represented and members are welcome from any country, within or outside Europe.

The AR community now serves as an effective point of contact for matters related to information security awareness. 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 of the exchange of information security good practices.

The AR community's work increased in 2009 through a combination of activities supported by the continuous involvement of members of the community. *ARNews* and a calendar of events were prepared using inputs received by experts and were then distributed to community members. Alongside this, the AR community offers the chance to participate in presentations at events. To enhance its capacity, and promote knowledge sharing and dialogue within Member States and stakeholders, a new way of coming together and sharing information was established with regular conference calls to exchange emerging good practices and to discuss cutting-edge topics and key issues in the information security field.

In addition, a number of AR community members have participated in virtual working groups which have enabled the preparation of white papers on ATM crime, information security awareness in financial organisations and the use of social networks through mobile phones (to be published in 2010).

ATM Crime: Overview of the European Situation and Golden Rules to Avoid it

The number of ATMs in Europe is rising every year. ATMs can be found increasingly in many remote site locations other than banks, such as convenience stores, airports, petrol stations, railway stations, department stores and so on. In 2008, with the rise in the number of ATMs in Europe, there was also a significant rise in the total number of reported ATM crimes. As a result, the ATM industry has made the safety of users and protection against fraud a high priority.

To help these efforts, ENISA published a paper on 'ATM crime: Overview of the European situation and golden rules on how to avoid it', which contains a set of recommendations to raise user awareness about the different types of risks faced when using an ATM, along with advice on how to counter them. The intention was to provide a useful starting point to increase overall users' awareness of the issues they face when using ATMs, both within the European Union and elsewhere in the world, and to help establish data security and industry good practices.

Information Security Awareness in Financial Organisations

In 2009, ENISA reviewed its previous work on awareness raising in financial organisations in the light of the latest research and analysis. As a result, a new publication has been produced which contains additional case studies as well as recommendations and practical advice for financial institutions which are committed to implementing awareness raising programmes.

By the very nature of their business, data security is a key risk for these organisations. They generally hold significant amounts of personal and financial data, the safety of which is a crucial responsibility.

ENISA's new paper, 'Information security awareness in financial organisations', contains a set of twenty recommendations, practical advice and case studies. The document provides a valuable tool to help organisations in this industry sector appreciate the importance of data loss and to prepare awareness raising and training programmes.

AR Conference

On 19 June 2009, ENISA organised a conference on 'The growing requirement for information security awareness across public and private organisations', which was hosted by Thomson Reuters at their London offices. The speakers discussed the investments and technologies that organisations should have at every layer of security, and explored the state of risks, the latest trends and international policy. More importantly in the light of recent global developments, they addressed the effect of the financial crisis on information security.

Recent events associated with significant data losses in both the private and public sectors have raised concerns about leaks of sensitive information. It has been widely recognised that policies and controls are needed to ensure the security of information on networks and to manage data that enter and leave an organisation. While policies and technology are certainly a critical part of any information security programme, in reality these measures alone cannot deliver an adequate level of information security. Awareness of the related risks and safeguards available is the first line of defence on the long road towards security. Employees are the real perimeter of an organisation's network and their behaviour is a vital aspect of the overall security picture.

As a result, organisations have been investing time and money to safeguard personal and financial data while more recently they have shifted towards including the secure management of mobile assets in corporate policy. Clearly there is the expectation of reaping dividends in terms of greater market recognition and compliance with the prevailing regulatory frameworks. For obvious reasons, data security is a particular risk for financial organisations. However, in this tough time of economic downturn managers have been challenged to cut costs without jeopardising the security position of their organisations. Never before has the balancing act between cost and benefit in information security been more critical.

ENISA's Awareness Raising team received the runner-up award in the category 'Security Education Programme' in the Real IT Awards 2009. This category included organisations raising awareness as to correct security policies and procedures in the work environment. British Airways' entry, which included ENISA's posters and videos, was entitled 'Information Security Awareness Workshop'.

Real IT
AWARDS 2009

Protecting Children .... and Organisations

In 2009 ENISA produced material to help raise information security awareness targeted at two different groups: parents and organisations. The first set of material is designed to make parents more aware of what they can do to enhance the safety of children using virtual world sites. ENISA believes that awareness of what children can do online and parental involvement are crucial. 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.

The material created for organisations is intended to ensure that employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources, and to help organisations keep their computers and networks safe. It also draws employees' attention to some golden rules of information security.

All material – posters, illustrations, screensavers and video clips – is available for download for use in any information security training programme, awareness activity or company website. Several organisations asked to have the ENISA material customised to meet their specific needs – ranging from posters advertising the importance of 'locking' your PC while away from the desk, to the production of security awareness videos about the protection of information

Child Online Protection Initiative

The Child Online Protection (COP) Initiative has been established by the International Telecommunication Union (ITU) as an international collaborative network for action to promote the protection of children worldwide by providing guidance on safe online behaviour. It operates in conjunction with other United Nations agencies and partners.

As part of the Initiative, ENISA contributed to the preparation of Guidelines targeting children, parents, guardians and educators, industry and policy-makers. These Guidelines have been developed as part of the ITU's Global Cybersecurity Agenda, with the aim of establishing the foundations for a safe and secure cyber-world, not only for today's youth but also for future generations. The Guidelines are intended to act as a blueprint which can be adapted and used in a way which is consistent with national or local customs and laws.

In recognition of ENISA's dedication to the COP Initiative, ITU Secretary-General Hamadoun Touré presented the Agency with a certificate of appreciation at ITU Telecom World in Geneva, Switzerland in October.

Spreading the Message

To promote its awareness raising findings faster and more effectively, ENISA published a volume, entitled 'The growing requirement for information security awareness', which includes selected 2009 results: 'ENISA's ten security awareness good practices', 'ATM crime: Overview of the European situation and golden rules on how to avoid it', 'The ENISA Awareness Raising Community' and 'Information security awareness in financial organisations – Guidelines and case studies'.

1000 copies of the comparable 2008 volume, 'Raising awareness on information security across public and private organisations', have also been distributed and a survey assessing the quality and impact of reports was undertaken.

Finally, ENISA continues to strengthen its relationship with the Member States through collaborative efforts, regular dialogue and the exchange of good practices. The translation of awareness publications into different languages and the awareness pages of the ENISA website have both helped to create awareness around Europe and to disseminate ENISA's findings.

Security Competence Circle and Good Practice Sharing for CERT Communities

Enhancing Member States' Capabilities in Incident Response
Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the Internet must have the capability to respond effectively and efficiently to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens, and be awareness raisers and educators.

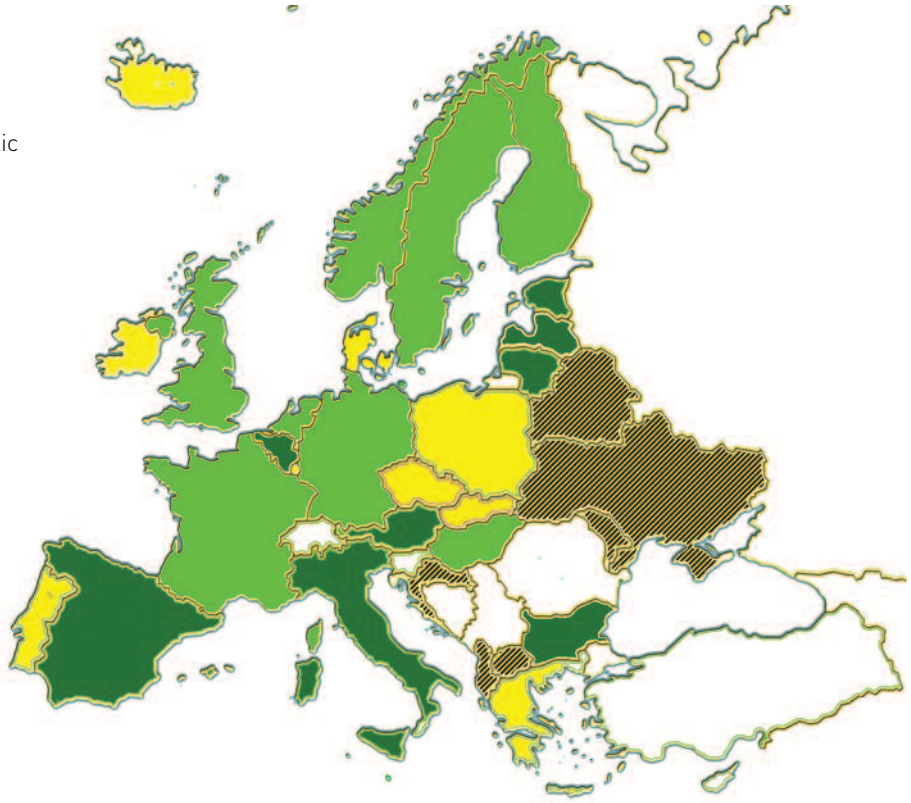
Not every country connected to the Internet possesses CERT capabilities, and the level of maturity among those which do varies dramatically. It is ENISA's mission to clear out the 'white spots' on the CERT world map and to minimise the gaps by facilitating the setting up, training and exercising of CERTs.

Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
UK

PLUS
Austria
Belgium
Bulgaria
Estonia
Italy
Latvia
Lithuania
Spain

PLANNED:
Czech Republic
Cyprus
Iceland
Ireland
Greece
Luxembourg
Poland
Portugal
Slovakia

Outside EU:
Most former Soviet Republics
South Africa



National and Government CERTs in Europe, 2009

ENISA's role as good practice knowledgebase and contact broker is supported by the high quality material it has already prepared (such as its 'Step-by-step guide on how to set up a CSIRT', various operational guides, a co-operation guide and its new CSIRT exercise collection). Following consultation with CERTs in the Member States, the good practice collection was extended in 2009 to cover the special role that national and/or governmental CSIRTs play in their countries' national incident response capability. The Agency also continued to support the very successful TRANSITS training for CERT staff which takes place at least twice a year (March 2009 in Dublin, Ireland, and November 2009 in Vienna, Austria).

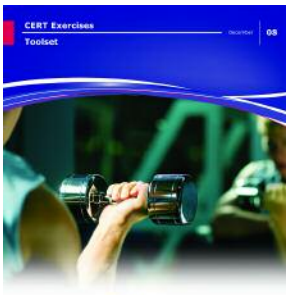
CERT Exercise Pilots – Preparedness is Key!

Exercises are an indispensable tool for emergency and crisis preparedness for CERTs. Currently, only a few teams perform crisis management and co-operation exercises in a constructive way that really enhances preparedness. Most teams limit themselves to small, ad hoc exercises with limited scope and coverage.

In 2009 ENISA's 'CSIRT exercises collection' was piloted. This package, which includes exercises and a handbook for trainers, is intended to enable a CERT to train its staff to deal with new, unknown events. Both everyday changes such as the incorporation of a new team member and highly critical events like massive cyber-attacks against the infrastructure of their clients can be tackled more effectively if the teams are trained to respond appropriately.

Exercise Pilot 1: Large-scale Incident Response – The first pilot was organised on 5 June 2009 in Chisinau, Moldova Republic, in full compliance with the ENISA handbook. In a one-day event, 16 teams from the Eastern part of Europe exercised reaction and workflows in areas including:

- Organised phishing attack against the constituency
- Hunting down the C&C (command and control server) of a newly found botnet
- Reaction to the infection of the corporate network by a Slammer-like worm
- Reaction to massive DDoS (Distributed Denial of Service) attacks from abroad



Under the instruction of seasoned CERT members, the main goal of the exercise, besides validating the ENISA material, was to assess and to enhance the students' capability to act and react in different crisis situations which required excessive co-ordination not only within the team but also in co-operation with other teams worldwide.

Exercise Pilot 2: Network Forensics – The second pilot was organised on 30 June 2009 in Kyoto, Japan, as part of the Network Monitoring Special Interest Group (NM-SIG) meeting that took place during the 21st Annual FIRST Conference. In a five-hour hands-on class, more than 40 students from CERTs worldwide were trained in the analysis of evidence brought by data samples resulting from various kinds of attacks:

- Pcap trace analysis exercise (post-mortem server-side exploit)
- Pcap trace analysis exercise (post-mortem client-side exploit)
- Netflow analysis exercise (ongoing DDoS attack)

The students were equipped with specially crafted Live-DVDs and USB-drives containing disk images of infected computers. The whole exercise was overseen by three very experienced instructors from the CERT community and complemented by comprehensive presentations.

The ENISA CERT exercise material successfully passed its 'baptism of fire' and left behind very satisfied instructors and students. The pilots resulted in a report and were documented in a video, both of which are available at: www.enisa.europa.eu/act/cert.

Baseline Capabilities of National/Governmental CERTs

National and governmental CERTs are the key tool for the protection of national critical information infrastructure in the Member States and for combating massive cyber-attacks through cross-border co-operation with other teams.

The importance of national and governmental CERTs in all Member States having similar capabilities in order to co-operate more effectively and to successfully perform their duties is well acknowledged. In most EU Member States, national or governmental CERTs are established and functional, but their capabilities and maturity vary.

Working with stakeholders from the CERT communities, the European Commission and the Member States, in 2009 ENISA took the first step towards indentifying a minimum set of (baseline) capabilities for national and governmental CERTs. This is necessary if they are to contribute in Europe-wide co-operation and information sharing, not only for incident response during crisis situations but also in the sharing of operational data and good practice on a day-to-day basis.

ENISA's CERT experts approached this task with a survey among all 120 known teams listed in the Inventory of CERT Activities in Europe. More than two-thirds of all teams answered questions about their service portfolio, constituency, plans for the future and especially about requirements for and obstacles to cross-border co-operation with other teams. From this valuable input ENISA filtered out proposals for the definition of baseline capabilities for national and governmental CERTs in four categories:

- **Service portfolio**, including mandatory reactive and proactive services
- **Operational capabilities**, including necessary operational modes and equipment
- **Mandate**, including emphasising the necessity of a clear, official mandate by the relevant government
- **Co-operation capabilities**, including necessary powers and privileges for sustainable cross-border co-operation

The first draft of the document was published at the end of 2009. It will be subject to review in the light of other relevant work in the field, adjusted where necessary and discussed with relevant stakeholders in the CERT communities, the European Commission and the 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. To facilitate co-operation and the exchange of expertise and experience, ENISA has established a European Good Practice Brokerage[14].

In 2009, the Agency supported several co-operative projects among the MSs, by acting as a good practice broker in the European NIS 'marketplace'. For example, ENISA facilitated the organisation of the second European FI-ISAC (Financial Institutions – Information Sharing and Analysis Center) Workshop that took place in Amsterdam, The Netherlands, in April, and the third European FI-ISAC Workshop in Berne, Switzerland, in November.

In addition, the Agency facilitated the meeting with Scandinavian local governments on Information Security in Oslo in May, when representatives of municipalities and regions from Denmark, Norway and Sweden exchanged their NIS good practices – including good practice in Awareness Raising – and discussed possible follow-up activities.

Supporting tools

The European NIS Good Practice Brokerage is supported by a set of tools, which were updated and further enhanced during 2009:

- **The Who-is-Who Directory** on NIS is a compilation of generic addresses of relevant players in NIS in the Member States, in the EEA and EFTA countries, and of EU Institutions and EU bodies, international organisations and other pan-European stakeholder organisations active in NIS.

- **The Country Reports** are an assessment of ongoing and planned NIS activities in Member States. They also include comprehensive information about relevant players and NIS activities.

These two 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.

- **The Online Platform**: information on successful co-operation initiatives and good practice material developed through co-operation initiatives. It provides stakeholders with an easy means of offering and requesting good practice from other stakeholders, as well as tools to identify partners for co-operation initiatives aimed at the exchange and development of good NIS practices.

A case study – the European FI-ISAC Workshops

The FI-ISAC Workshops held in Amsterdam and Berne aimed to create a trusted environment where stakeholders could share freely information about cyber-crime in the financial sector and their experiences of national co-operation. These events brought together banks, law enforcement representatives, Computer Emergency Response Teams and policy-makers from 19 different countries.

The workshops were organised by the Theodore Puskas Foundation and CERT-Hungary, the Dutch Financial Information Sharing and Analysis Center (FI-ISAC)/NICC, MELANI, Switzerland and UK Payments Online (formerly APACS), with the support of ENISA and the Netherlands Bankers Association (NVB).

It became clear during the meetings that international collaboration is greatly facilitated by the Europe-wide use of the same or similar ways of working and structures. Case studies were presented and good practice in the field exchanged.

[14] www.enisa.europa.eu/act/sr/nis-brokerage-1

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. Awareness, risk assessment and risk management are prerequisites for the establishment of security measures. Several Member States have already implemented programmes aimed at changing the information security behaviour of micro-enterprises. However, others still have a need for knowledge, information and support in the field.

Security Toolkit for Micro-enterprises' Multiplier Organisations

ENISA therefore undertook a project in 2009 to help micro-enterprises. The overall aim is to increase knowledge and competence in how to build NIS capacity among both micro-enterprise intermediaries and multiplier organisations and their constituencies or members. The project involved developing a tailor-made toolkit by customising existing ENISA Risk Assessment/Risk Management and Awareness Raising deliverables.

The toolkit includes appropriate NIS capacity building material (a training manual, training package etc.). It was deployed and implemented by multiplier and affiliate organisations in one EU Member State, through peer-to-peer learning and as a training module provided by a dedicated trainer (exploiting the 'train-the-trainer' concept). A beta version of the new online tool was made available in late 2009 at the following web addresses – in German: www.kmu-sicherheit.eu/ and English: www.sme-security.eu/.

In addition, as part of the validation process, the newly developed tool was presented in Brussels, Belgium, in November 2009 to a high-level audience which included the Secretary of State for European Affairs of Hessen, EU decision-makers and numerous Brussels-based multiplier organisations. An English language version of the online tool was provided as an add-on to the original German version.

The Brussels event was a major success. It brought together more than 80 participants and was well received by key multiplier organisations and political decision-makers alike but it also led to a very specific outcome. Following the presentation, a key multiplier stakeholder organisation initiated the evaluation and analysis required prior to integration of the online tool with their website. After a positive assessment, the online tool will be translated into French and Dutch, making two new language versions available to ENISA for further dissemination. In the meantime, further requests have been received to translate and customise the deliverable in other language versions.

ENISA will identify and assess potential follow-up initiatives and activities in 2010, including opportunities to partner with established regional networks and EU decision-makers in the context of existing European Community programmes and projects.

ENISA targets Micro-enterprises – the Real Giants of the EU Economy

On 12 November 2009, Hessen Agentur and the State of Hessen invited stakeholders to spend an evening dedicated to IT security for micro-enterprises at the Brussels representation of the State of Hessen. In her welcome address to more than 80 participants, Secretary of State Nicola Beer thanked ENISA for targeting micro-enterprises, which she described as "the real giants of European economy", and for entrusting Hessen Agentur with the development of the online tool, underlining the importance of Hessen as an ICT region.

Discussions then focussed on ENISA's work on threats and vulnerabilities, the specific needs of micro-enterprises in facing those challenges on a day-to-day basis, and motivating micro-enterprises. The newly developed online tool was introduced. Based on a methodology developed by ENISA as part of its Work Programme 2009, Hessen Agentur has realised a toolkit enabling multipliers such as sectoral associations and regional authorities to address their micro-enterprise constituency easily, using their own, branded security awareness campaign. Presentations were followed by a reception which provided further opportunities for networking among key multiplier organisations and political decision-makers.

Secretary of State Nicola Beer (left) and ENISA's Dr. Ronald De Bruin (centre) with the project team.

Identifying Emerging Risks for Creating Trust and Confidence

The rapid progress in new technology – and its crucial importance to society, business and virtually every aspect of life today – brings with it new risks. There is a pressing need to identify, assess and manage these emerging and future risks (EFR) so that they can be effectively addressed and mitigated.

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. ENISA has initiated a new approach to tackle the challenge of *emerging and future* risks.

ENISA's third Multi-annual Thematic Programme (MTP 3) aims to identify emerging risks for creating trust and confidence. The Agency is establishing a framework that will enable decision-makers to better understand and assess emerging risks arising from new technologies and new applications. This in turn will contribute to the growth of stakeholders' trust and confidence.

ENISA's work also provides analysis of specific EFR scenarios. This includes the publication of risk assessment reports on new applications and technology areas. Based on discussions with its stakeholders and with the Commission services, as well as the dialogue established with the Stakeholder Forum, various topics have been identified as critical and a number of these were tackled in 2009; reports were produced on eID cards, cloud computing, cyber-bullying and online grooming, the Internet of Things/RFID and the security of cross-border authentication. Although only published at the end of 2009, early responses to these reports suggest that ENISA's target of having by 2010 at least 30 stakeholders or stakeholder organisations from at least 15 Member States refer to ENISA as a point of reference for discussing the nature and impact of emerging security challenges in the Information Society has already been exceeded.

A second objective of this work was to test the EFR Framework that ENISA is developing. When finalised, the application of the EFR Framework will provide a method of delivering emerging risk assessments in a standardised way with appropriate quality assurance.

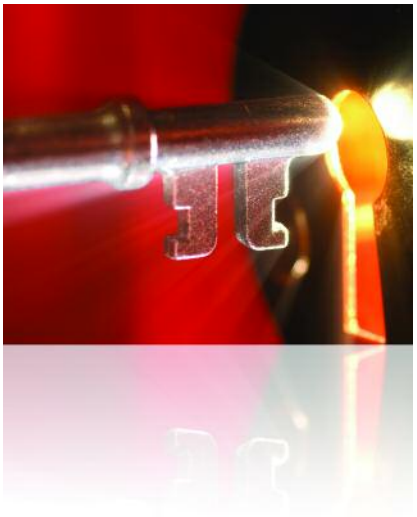
The EFR Framework
ENISA has developed a method for identifying EFR and is building a comprehensive framework for identifying and assessing risks that may emerge in 2-3 years' time. This framework will enable decision-makers to better understand and assess emerging risks arising from new technologies and new applications. It will also help increase stakeholders' trust and confidence.

Once a 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 EFR Stakeholder Forum
ENISA has established an EFR Stakeholder Forum to support the Agency in its 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 also maintains contact and co-operation with similar initiatives, such as the European Commission FP7 FORWARD initiative.

Analysis of Specific Scenarios

European eID Cards



Whenever we use Internet services, the first steps we take are usually identification (we input our names) and authentication (we prove that it is us). How we actually identify and authenticate ourselves depends on the security level of the application. The means used can vary from a simple combination of username and password, through a secret PIN, to a PIN generated by some external device or a smart card using cryptography.

The requirements for differing online applications vary considerably; whereas for some services a high level of security is required, in other areas the protection of the card-holder's privacy is the first priority. Smart cards are being used increasingly for authentication purposes. The new generation of European identity cards, so-called 'electronic identity cards' (eID cards) now contain a smart-card chip, equipped with functionalities for online authentication.

In response to these developments, ENISA has produced a Risk Assessment Report on 'Security Privacy and Security Risks when authenticating in the Internet with European eID Cards'. The report summarises the contributions of an EU expert group made up of representatives of government, industry and academia. The report looks at different use-cases, and identifies relevant security risks, gives an opinion about their relevance and importance and presents mechanisms that could mitigate these risks. The report focuses on authentication using smart cards and compares this approach with other common means of authentication.

The paper is aimed at political decision-makers and NIS stakeholders in Europe. Its main purpose is to help define a comprehensive list of requirements for national ID cards in order to ensure that they are as flexible and as multi-purpose as possible.

Security of Cross-border Electronic Authentication

During the last few years, Member States of the European Union have increasingly been issuing electronically readable identity (eID) documents to their citizens for different purposes and applications. These solutions are designed to be the most efficient and appropriate with respect to national requirements and available or planned infrastructures. The goals of these systems are in general (if not in detail) identical for all Member States: managing identities, improving administrative efficiency, improving accessibility and user-friendliness, reducing abuse and fraud and, above all, reducing costs.

European citizens who move freely through Member States face the problem that their eID documents from their home states do not allow access to the electronic services of another Member State in which they may be present. Administrations have the problem that they cannot provide services to European citizens from other Member States with the same ease and efficiency as to their own citizens.

Improving the interoperability of electronic identification and authentication systems is a European task and a task for all Member States. Considerable efforts have been made in several projects to address the challenges of pan-European interoperability of electronic authentication and to assess the feasibility of differing approaches.

In 2009, ENISA analysed the current situation and assessed the security risks of electronic authentication in cross-border solutions. To visualise these risks, two different projects offering cross-border authentication were taken as examples, examined and evaluated, NETC@RDS and STORK.

The report that has been produced answers a fundamental question: what is the difference between electronic authentication and electronic cross-border authentication, and which new threats arise from it. It is targeted at decision-makers, in order to help them understand the risks of online cross-border authentication, and at others involved in technical or organisational aspects of this issue.

Cloud Computing

Cloud computing was identified by ENISA's experts and by its Permanent Stakeholders' Group as one of the emerging applications which is likely to have a significant impact on European businesses and governments in the near future.

To tackle this issue, ENISA assembled a group of experts from major cloud providers, market leaders in security and IT services and research projects, as well as legal experts and independent security consultants, who worked together over a period of eight months to create a report. This report is the first to take an independent, in-depth look at the security and privacy issues of moving into the cloud.

The main target audience of the report is businesses, especially small and medium-sized enterprises (SMEs), because they are the largest customers of cloud computing.

The most significant outputs of the paper are:

- A security checklist or assurance framework for assessing the maturity of cloud provider security measures. One of the most important issues identified early on is that businesses would like to know what questions to ask when evaluating cloud providers' security. Secondly, cloud providers are overloaded with requests for audit and assurance – this takes up valuable time and can even weaken their security perimeters if it involves access to premises. The checklist is aimed at addressing both these issues.
- A set of recommendations for research directions to advance the state of cloud security including trust, systems engineering and data protection.
- A specific set of recommendations drawn up by legal specialists detailing what to look for in a cloud computing contract.

The security checklist is only the first step. ENISA is now working with a group of interested organisations to produce something more formal in 2010. Together with CSA (Cloud Security Alliance) and ISACA, the global organisation for information governance, control, security and audit professionals, ENISA is also organising a conference dedicated to this topic, to be held in Barcelona, Spain, from 16-17 March 2010.

Along with the report, separate documents containing the assurance framework and the results of a survey on SME attitudes to cloud computing security, which was used to guide the report, are available at: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

Cloud computing is a new way of delivering computing resources, not a new technology. With cloud computing, services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. Since we are in a time of belt-tightening, this new economic model for computing has found fertile ground and is seeing massive global investment. According to IDC's analysis, the worldwide forecast for expenditure on cloud services in 2009 will have been in the order of $17.4bn.

Internet of Things/RFID

During 2009, ENISA set out to identify the emerging and future risks involved in the Internet of Things and to make recommendations to address them appropriately. A scenario based on IoT/Radio Frequency Identification (RFID) technologies in future air travel was taken as an example. Given that we are already seeing the introduction and use of smart technologies in air travel (e.g., RFID-enabled passports, electronic boarding passes sent using SMS and displayed using cell phones etc.), this was considered a representative, realistic, emerging, showcase scenario on which to elaborate as a means of identifying other important risks and challenges posed by IoT technologies. The work also supports EU policy initiatives on RFID. Among the technologies in this scenario are smart phones, netbooks, RFID and location-based services (LBS), but the power of these technologies is greatly leveraged by their convergence. This scenario will serve as a test bed to illustrate the convergence of these IoT technologies and the issues that arise as a result of such convergence.

The 'Internet of Things' (IoT)[15] – sometimes referred to as the ubiquitous network or pervasive computing environment – is a vision where all manufactured things can be IT-enabled and connected to each other via wireless or wired communication networks. The Internet of Things is expected to bring many benefits, but it also poses many challenges and risks.

[15] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

The scenario examined is explorative and is set in the future, approximately five years from now in the year 2015. It follows three passengers, of different citizenships (EU, US, Japan), ages, health status, IT literacy and language skills, flying from European airports. The scenario depicts emerging automated procedures typically used in normal air travel, such as arriving at the airport, check-in and boarding. The scenario and the subsequent risk assessment do not cover national security or border control issues; and the focus is on passengers, without considering aircraft security issues and general aviation maintenance, repair and overhaul (MRO) procedures.

ENISA's work in this scenario will produce:

- A presentation of the risk assessment methodology used in the scenario assessment, which was based on the standard ISO/IEC27005
- Identification of major assets, vulnerabilities, threats and subsequently risks at different risk levels, related to various aspects: policy/organisational, legal, technical, and social/privacy/economic
- Recommendations for further action to be taken respectively by the European Commission and other EU Institutions, Member States, academia and research institutions, industry, and consumer associations and other non-profit institutions.

The final report is expected to be published in February 2010.

Cyber-bullying and Online Grooming

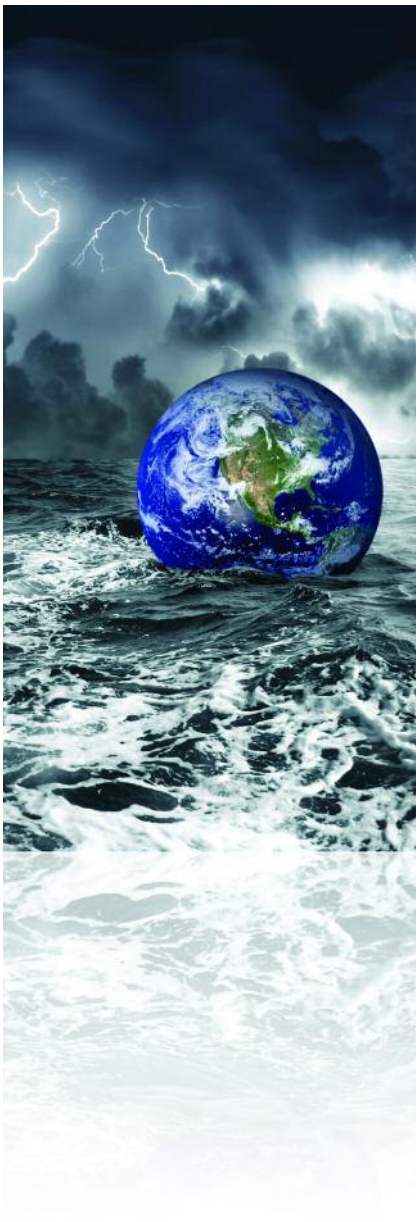
Given current developments in the area of Internet usage and in particular in child protection issues, ENISA initiated a risk assessment within the Emerging and Future Risks Framework to identify, analyse and mitigate relevant risks. The Agency established an expert group to perform this task, which proposed a scenario in the area of cyber-bullying and online grooming – an area which is already the focus of various activities at national (Canada, the UK, the USA), European (Reding, ENISA) and international levels (the International Telecommunication Union (ITU), UNESCO).

Children are the most valuable part of every society, regardless of culture, religion and national origin. They are our future. They depend on the care of their parents, their schools and their social environment. Naturally, parents worry about any of their children's activities that might involve risks, whether from participation in extreme sports or the use of technology. But the latter presents parents with particularly difficult problems, as they often do not feel as confident with technology as their children. Children have fun using technology and gadgets. They use technology intuitively and develop an understanding of the use of technical features very easily. They become familiar with innovations very quickly and use technology as a matter of course when communicating with their friends. All this puts them particularly at risk when going online. The protection of children against such risks is of paramount importance for society and must be viewed as a key responsibility for parents, within education and in the governmental care of minors.

In 2009, ENISA performed a risk assessment on cyber-bullying and online grooming and has published a report which catalogues the major risks involved and makes recommendations for strategies to mitigate them. The activities undertaken complement previous work in this area, by assessing risks and by making recommendations that embrace both technical and societal issues of security and protection. In order to avoid the duplication of effort, ENISA took into account other developments in this area and drew on the knowledge and experience obtained from its expert group and through discussions with other colleagues, both within and outside ENISA.

Development of the EFR Framework

During 2009, ENISA's work on EFR was used to improve and adapt the EFR Framework. The Agency worked with many experts to prepare EFR assessment reports and gained considerable additional experience in EFR. A feedback loop from experiences gained from practical use will be incorporated into the final EFR Framework documentation. The work involves updating of the ER analysis process, a new version of the ER infrastructure, updating of the role definitions involved and revision of the ER handbook. When the updating of the handbook and process is complete, the EFR Framework will provide a method of delivering emerging risk assessments in a standardised way with appropriate quality assurance. The updated version of the EFR handbook is expected to be published on the ENISA website in February 2010.



ENISA's EFR deliverables documenting the EFR Framework:

- **Emerging and Future Risks Workflow:** provides an initial description of the activities, steps, information flow and roles involved in the scenario-based assessment process of Emerging Risk (www.enisa.europa.eu/act/rm/files/deliverables/emerging-and-future-risks-workflow).
- **Emerging and Future Risks Executable Workflow, UML Description:** refines the contents of the Emerging Risk Workflow above and provides details that allow for the implementation (both manual and automated) of the EFR process. It is based on UML specification (www.enisa.europa.eu/act/rm/files/deliverables/emerging-and-future-risks-executable-workflow-uml-description).
- **EFR Framework Handbook:** encompasses the documentation of the EFR Framework which consists of a scenario-based process model developed in order to assess and manage emerging and future risks (www.enisa.europa.eu/act/rm/files/deliverables/efr-framework-handbook).
- **EFR Infrastructure:** consists of a portal implementing functions for the collaboration (i.e. EFR Collaboration Portal) within an assessment (e.g. version management, notification, review etc.), together with a user guide (www.enisa.europa.eu/act/rm/files/deliverables/efr-collaboration-platform).

Extra Miles

ENISA undertook other projects in risk management in addition to the work outlined within its Work Programme for 2009.

Business Continuity Approach for SMEs

The Agency embarked on a project aimed at facilitating a knowledge transfer of key IT security issues to small and medium-sized enterprises (SMEs). This work was in response to the identified need of SMEs for a simplified approach to IT Business Continuity. ENISA has already produced a simplified approach to Risk Management; this new document is thus the second provided to cover the basic IT security needs of SMEs (www.sme-security.eu).

The new document provides a simplified and comprehensive view of IT Continuity/Business Continuity Management (BCM) for use specifically within SMEs. The document has been structured in a modular way; it is made up of various parts each devoted to the particular needs of stakeholders involved in the process of establishing a Business Continuity Plan (BCP) as part of their BCM process.

A full understanding of Business Continuity Management would involve a plunge into the fine details of corresponding measures and technology. But the ideas and approach presented in this guide cover an acceptable level of availability for small organisations with reduced security budgets.

The guide has been generated by anticipating the whole range of skills of different stakeholders involved in continuity management. The proposed BCM process is structured into a simplified four-phase assessment approach. No advanced knowledge of continuity and availability issues on the part of users is assumed. Where this knowledge would be necessary, the guide offers a limited number of comprehensive choices.

ENISA-ANACOM Event on 'Risk and Innovation'

Innovation generates new opportunities for traditional business activities by injecting new ideas that are often oriented towards higher specialisation, making them more knowledge-intensive as a result. In this way innovation contributes to the improvement of competitiveness, fosters a knowledge-based economy and contributes to the overall prosperity of our societies.

However, in order to innovate, organisations need to take risks – there is no innovation without risk. The issue, then, is to find ways for an organisation to judge risks and prepare risk-taking decisions, while mitigating unacceptable risks.

To support decision-makers in managing these risks, new approaches for risk identification with regard to prospective/futuristic scenarios need to be developed. These approaches will require a larger and wider knowledge capacity as part of the assessment, and new categories of threat will have to be taken into account. A vital element will be the validation of the scenarios. In order to achieve this, additional facilities are required, such as research labs and open knowledge communities, and they have to be seen in the light of current and future market trends, and used in novel ways of interaction.

ENISA and ANACOM (the regulatory authority for electronic communications and postal services in Portugal) are together organising a workshop in January 2010 to open up debate between organisations and innovation activities of different sizes and from different sectors.

Briefings on Quantum Key Distribution and Behavioural Biometrics

In 2009 ENISA experimented with a new short format for the results of risk analysis topics, the briefing. ENISA Briefings are short descriptions of emerging issues in security aimed at policy- and decision-makers. They give a brief introduction to the topic, outline areas of debate and propose a reasoned opinion on controversial points. So far, two briefings have been produced: on Quantum Key Distribution and Behavioural Biometrics.

CHAPTER 3

Relations with ENISA Stakeholders

- Communication, Outreach and Impact
- External Stakeholders, ENISA Bodies and Groups
- EU and Member State Relations
- Other Relations with Industry and International Institutions

Relations with ENISA Stakeholders

Communication, Outreach and Impact

The EU has recognised the importance of conveying its work and achievements effectively[16] and communications is now an EU policy issue in its own right. As an EU Agency, ENISA recognises the strategic value of communications; they are critical to attaining the Agency's key operational objectives. They are crucial to make its results known – and thus to change behaviour, to fulfil the requirements of the Agency's founding regulation by "developing a culture of Network and Information Security". Communication is indispensable to achieving visibility for the Agency's results, and thus to achieving impact.

The Tools for Achieving Impact

ENISA's communication activities involve the press and media, the ENISA website, publications and outreach to NIS experts, which is achieved through a variety of means including the *ENISA Quarterly Review*, co-organised events and speaking engagements at conferences, workshops etc.

In November 2009, ENISA created a new team, the Strategy and Public Affairs Department (SPAD), which brings together the development of the Agency's strategy, the management of public affairs, and communication and outreach.

Communication Planning

In order to increase the impact of its reports, studies and operations, ENISA endeavours to achieve consistency and coherence across all its communication channels. Corporate communications are closely aligned with the other operational activities of the Agency, from their inception, to optimise resources and improve the effectiveness of communications planning. This strategy is proving effective in achieving results with tangible impact, maintaining the high quality of ENISA's relations with other stakeholders and enhancing the visibility of the Agency. For this purpose, a Communication Action Plan is regularly updated. Advance planning enables ENISA to integrate better with its stakeholders' information and communication channels, thus increasing the Agency's impact still further.

Widening the Agency's Visibility

Additional brand marketing material was produced in 2009 and repetitive, brand recognition through both print and online advertising was maintained during the year. A standard glossary of NIS terms was also drafted to ensure the accurate translation of material.

The ENISA website underwent a technical overhaul in 2009 to pave the way for the introduction of a new platform. This will enable the Agency to develop new features and innovative online services in the future. A procurement for online advertising to increase website traffic was also undertaken, which will be launched early in 2010.

The impact of ENISA's press releases was maximised through the finalisation of two complementary contracts, greatly increasing the Agency's outreach. To overcome the most common and difficult communications barrier in Europe – language – press releases are translated. ENISA now follows Commission best practice with the inclusion of FAQs to accompany press releases, and more web content such as focus articles and interviews has been produced, presenting the Agency's work in an attractive way.

16 http://ec.europa.eu/commission_barroso/wallstrom/communicating/policy/index_en.htm#apr2008

Visual communication was strengthened through a three-pronged approach:

- The Brand Manual was updated with toolkits tailored specifically to the needs of designers and ENISA Experts, and the logo was amended to ensure the consistent application of the ENISA visual identity
- The Agency subscribed to a new library of about 7 million professional images, which is being widely used within the Agency (for example for the website, presentations, studies and reports)
- A number of corporate videoclips were produced, using modern communication tools and new, social media, to enhance the audiovisual content of the website and to present results in a different, more accessible package

Publications

The *ENISA General Report* and the *ENISA Quarterly Review (EQR)* are the key publications produced during the year. The *General Report* is published both as a hard copy and on CD-ROM to reach out to as many recipients as possible.

EQR is an extremely effective method of outreach to the Agency's various stakeholders. Four issues of the magazine were produced in 2009, covering topics such as:

- Resilience of Communication Networks
- Information Sharing
- CIIP (Critical Information Infrastructure Protection)
- Emerging and Future Risks
- Skills and Certifications
- Awareness and End-user Issues
- Business Risks
- Information Security Management Systems (ISMS)
- Privacy
- Wireless Security

Each edition scores more than 10.000 hits on the website (www.enisa.europa.eu/eq), 3000 hard copies are distributed and the electronic mailing list has over 2500 subscribers[17].

Internal Communication

Regular staff meetings and the Agency's intranet, INTRA ENISA, have ensured a sound and interactive flow of communication internally. In 2009 the wider use of the intranet has offered common ground for all staff to deal with a variety of information sources. Its role will be strengthened even further in 2010.

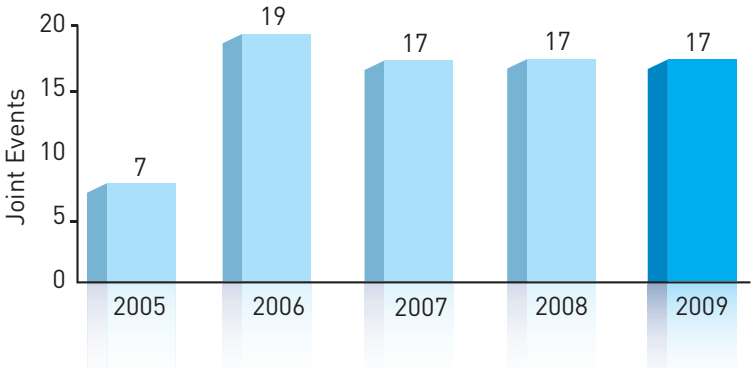
17 Readers may subscribe to EQR at www.enisa.europa.eu/eq.

Conferences, Joint Events and Speaking Engagements

Building on previous experience, ENISA was involved in a selection of high-level European conferences in 2009. Often these conferences are run in partnership with a third party such as a professional conference organiser or a not-for-profit organisation. Such events allow the Agency to network and promote its work in a cost-effective way.

During 2009, ENISA participated in or co-ordinated almost 40 events and conferences throughout Europe and further afield.

Joint Events (i.e. events supported or co-organised by ENISA), 2005-2009:



Highlights of the year included an Awareness Raising event in June, organised by ENISA and hosted by Thomson Reuters in London. The conference, which was entitled 'The growing requirement for information security awareness across public and private organisations', was very well received by the 100 or so delegates who attended.

In addition, ENISA was invited to nearly 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.

Joint EDPS-ENISA Seminar – "Responding to Data Breaches"

On 23 October 2009, in co-operation with the European Data Protection Supervisor (EDPS), ENISA hosted a seminar on "Responding to Data Breaches" at the European Parliament premises in Brussels. The one-day event saw the first public appearance of and key-note speech delivered by the new ENISA Executive Director, Dr. Udo Helmbrecht.

The seminar was devoted to three main objectives corresponding to the "life-cycle of data breach". Its aim was to encourage the sharing and exploring of good practices for preventing and mitigating the occurrence of data breaches from a data controller's perspective, along with an exchange of good practices developed by data protection agencies and institutional and industry stakeholders on how to manage security breaches, including the development of procedures aimed at investigating breaches. Finally, the seminar provided an opportunity to gather experiences on data breach notification management from other sectors and from outside the EU.

The event, which attracted about 80 stakeholders, brought together representatives from EU institutions, national authorities, telecommunication operators and software companies, user and consumer organisations and academics. Discussions highlighted the need for data controllers, in close co-operation with other stakeholders, to adopt proper risk management in order to mitigate the risk of such breaches appropriately. Adequate responses will have to comprise technological solutions as well as organisational measures to ensure that top management take responsibility and adequately support all the individuals concerned.

New Executive Director, Dr. Udo Helmbrecht (right), with the European Data Protection Supervisor, Peter Hustinx (centre), and Commissioner Viviane Reding (left) at the Joint ENISA-EDPS Seminar at European Parliament premises in Brussels on 23 October 2009.

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, five meetings and workshops were organised between January and November 2009 on the Resilience of Public eCommunication Networks:

- First Workshop on the Deployment of DNSSEC
- First Meeting of PROCENT Experts Group
- Workshop on Providers' Resilience Measures and associated Guidelines
- Second Informal Meeting of the European Forum for Member States
- Second Workshop on the establishment of a European Public-Private Partnership for Resilience (EP3R)

Meetings were also organised by ENISA as part of the implementation of the NIS Brokerage activities.

From 14-18 September 2009, the 2nd ENISA-FORTH Summer School in Network and Information Security (NIS'09) took place near Heraklion in Crete, Greece. As in 2008, NIS'09 was jointly organised with the Institute of Computer Science of the Foundation for Research and Technology – Hellas (FORTH-ICS). This year the event took as its theme 'Privacy and Trust in a Networked World'. An exciting programme featured invited lecturers who covered a range of topics extending beyond pure technological areas to encompass economic, policy and legal issues.

The main objective of the Summer School on NIS is to provide a forum for experts in Information Security, policy-makers from EU Member States and EU Institutions, decision-makers from the industry, as well as members of the research and academic community, for interacting on cutting edge and interesting topics in Network and Information Security.

Participants included key policy-makers from EU Member States and EU Institutions, top-level decision-makers from industry and members of the academic and research community. Judging from the positive feedback received, it seems safe to say that the Summer School on NIS is now an established event.

www.nis-summer-school.eu/

External Stakeholders, ENISA Bodies and Groups

ENISA regards its relationships with EU bodies, industry, academic and consumer/user representatives, Third Countries and international institutions as crucial to its ability to perform and deliver. The continuing 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 an important source of information to keep ENISA's knowledge of relevant technologies up-to-date, and enable it to facilitate outreach with technical expertise and promote the take-up of products and services.

By participating in key NIS and information society events in Europe and world-wide, liaising with experts in different fields, introducing them to the Agency and its activities and promoting future collaboration, ENISA has created an excellent network of contacts. These contacts include key people in standardisation bodies, national, European and international interest organisations, as well as security experts within the private and public sectors and academia. ENISA plans to develop this network still further during 2010, and groups of experts will be established to write Position Papers on selected security topics.

New times – Management Board and ENISA staff meeting for the first time, with the new Executive Director

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 2009, providing valuable advice to the Executive Director and input to the implementation of the Work Programme 2009, ENISA's Strategy and the prospective Work Programme 2010.

The PSG met formally twice in 2009, in April and September. An informal meeting was also held with the Management Board in Vienna, Austria, in June to discuss ENISA's Strategy and the Work Programme 2010. A notable achievement was delivery of formal advice to the Executive Director on Network and Information Security issues within the context of the crisis in the financial world. Individual PSG Members also 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.

The Executive Director, Dr. Udo Helmbrecht, and Chairman of the Management Board, Dr. Rienhard Posch

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 twice in 2009: in Athens and in Heraklion, Greece.

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 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 2009 in Vienna, Austria, two new topics were defined and implemented in the Work Programme 2010 – one on Identity, Accountability and Trust in the Future Internet, and the other on Drivers and Barriers for Co-operative Frameworks. In addition, a key Management Board decision was the appointment of a new Executive Director 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.

The inauguration of the new Executive Director – the ENISA staff and Management Board forged new professional networking ties and commemorated a new start for the Agency

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 and the European Commission were further strengthened in 2009. The Agency organised various meetings with different representatives of EU Institutions, and discussions were held between ENISA's incoming Executive Director, the European Parliament and the Information Society and Media Commissioner, Mrs. Viviane Reding.

As NIS is not only dealt with in the Directorate-General for Information Society and Media (DG INFSO), but also other DGs, ENISA held meetings and had exchanges with representatives of other relevant DGs in order to explore opportunities for co-operation.

One of the highlights of the year was a visit by a delegation of Danish MEPs to ENISA's headquarters in Heraklion in June. The MEPs praised the Agency's work and activities in NIS in Europe.

Outgoing Director-General of DG INFSO, Fabio Colasanti, with the Chair of the Management Board, Dr. Reinhard Posch

Relations with Member States

Various meetings were organised in the EU Member States during 2009. These visits provided an opportunity for an exchange of information on NIS with high level representatives and discussions as to how the Member States might benefit from ENISA's knowledge and expertise. Collaboration can always be improved, and ENISA is in contact with representatives of the Member States on an almost daily basis, exchanging information and giving and receiving advice on day-to-day business issues.

Responding to Requests

In 2009, the Agency received a request from Austria to help set up a CERT by organising appropriate training. The Agency was able to assist through the successful programme of TRANSITS training.

By providing prompt, independent and high quality responses to requests received from EU Institutions and Member States, ENISA is fulfilling its appointed task to advise and assist the Member States and EU Institutions, giving 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. Similar requests are expected to emerge in 2010.

The Network of National Liaison Officers

Although not formally based on any ENISA Regulation, the network of National Liaison Officers (NLOs)[18] is very helpful to the Agency: 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 February 2009 ENISA organised the 4th annual NLO meeting in Prague in the Czech Republic, at which representatives from Member States delivered presentations about their NIS activities and exchanged views and information. ENISA presented its recent activities and gave an overview of its Good Practice Brokerage activities. ENISA's Country Reports were also discussed.

For a list of the NLOs, see Appendix 5.

Meeting of the network of National Liaison Officers, February 2009

[18] www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office

Other Relations with Industry and International Institutions

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 2009. In addition, ENISA has an 'open door' policy to relevant stakeholder groups. In 2009 a number of bilateral discussions with stakeholders were held at the Agency's headquarters in Heraklion, Crete.

In 2009, ENISA consolidated its relationship-building activity with national industry multiplier organisations through personal visits and discussions in EU Member States. Building on the 2007-2008 'Road Show' project, the Agency continued to enhance its networks, resulting in almost 1200 personal contacts which were fed into the ENISA Stakeholder database and hence form the basis of its engagement with stakeholders. In addition, structured dialogue meetings have proved an 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, the Agency 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 taken part in meetings and in the work of the Council of the 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 2009, 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 the Japanese Information-Technology Promotion Agency (IPA), the Korean Information Security Agency (KISA) and a Chinese Government delegation comprising representatives from the Ministry of Industry and Information Technology (MIIT) of the People's Republic of China and the China Academy of Telecom Research (CATR).

Speaking Engagements of the Executive Director

After his appointment in October, the new Executive Director began a round of high level speaking engagements in various Member States. Among the most prominent of these events were, in Brussels, Belgium, at the Joint European Data Protection Supervisor (EDPS)-ENISA Seminar in October, when he spoke on 'Responding to Data Breaches'. The speech coincided with Dr. Helmbrecht's first meeting with Commissioner Reding.

The Executive Director also spoke at the Swedish EU Presidency Resilience Conference on 'The Future Challenges of Resilient Electronic Communications' in Stockholm in November, and in December he gave a keynote speech at the official inauguration ceremony of Michael Hange as the new President of the BSI (Bundesamt für Sicherheit in der Informationstechnik, the German Federal Office for Information Security).

Commissioner Viviane Reding and Dr. Udo Helmbrecht

Dr. Helmbrecht, Mr. Hange and the Director General of Agence Nationale de la sécurité des systèms d'information (ANSSI), Mr. Patrick Pailloux, at the BSI.
Image supplied by: Luckhardt / <kes>

The Executive Director with the Director General of the PTS (the Swedish Regulatory Agency), Marianne Treschow, at the Swedish EU Presidency Resilience conference.

CHAPTER 4

Administration

- Organisational Structure
- General Administration
- Legal Advice and Procurement
- Technical Infrastructure
- Physical Infrastructure
- Human Resources
- Finance and Accounting

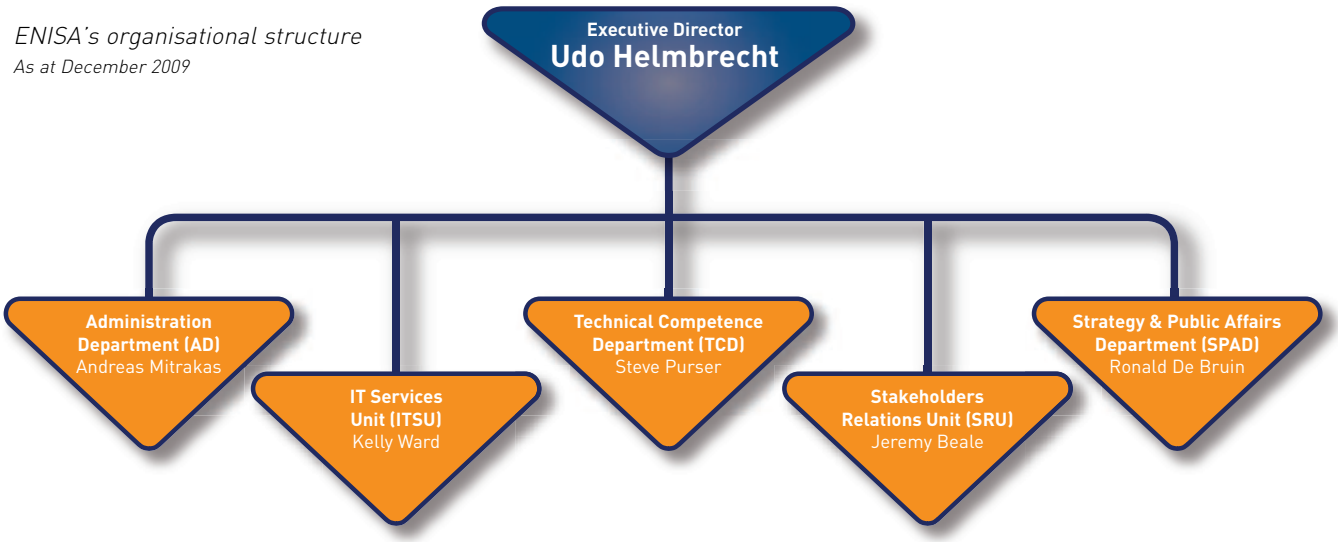
Administration

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.

The core activities of the Administration Department cover finance, human resources, ICT and legal services.

ENISA's Organisational Structure

ENISA's organisational structure
As at December 2009



With the arrival of a new Executive Director in October 2009, the organisational structure of ENISA has evolved to meet the challenges ahead. Initially ENISA's focus was on setting up the structures to perform its designated responsibilities and establishing a presence. Five years on, it is a well established European Agency and has moved into a new phase. The emphasis now is on consistently delivering high quality material in line with stakeholders' expectations.

In addition, the tasks assigned to the Agency when it was first established in 2004 have been extended to reflect the new priorities of its stakeholders. For example, the work being carried out in the area of resilience has been re-structured in order to provide support to the Commission and the Member States in the area of Critical Information Infrastructure Protection. As a result, the Work Programme is strongly aligned with the Commission's CIIP action plan, as defined in Communication COM(2009)149 – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'.

ENISA's capacity to deliver has therefore been increased, without raising the total number of staff employed, to accommodate these new areas of work.

The Council Resolution on a collaborative European approach on Network and Information Security of 18 December 2009 builds on a number of EU strategies and instruments developed in recent years. It provides political direction on how the Member States, the Commission, ENISA and stakeholders can play their part in enhancing the level of network security in Europe. The Council Resolution should also be considered as a contribution to the ongoing debate on the future of ENISA and its role in CIIP.

General Administration

In 2009 the Administration Department remained focused on meeting in full the compliance requirements for European Agencies and providing services within the area of its competence.

The compliance target built upon the groundwork laid over the previous three years. In 2009 the Agency benefited from audits carried out by the European Court of Auditors and the Internal Audit Service of the Commission. Additionally positive input was received by the European Data Protection Supervisor.

In terms of budget execution, the overall expectation for 2009 was to maintain previous standards and exceed the 90% mark. In the event, the Agency achieved 94.4%.

Following the standing guidelines of senior management, the Administration Department maximised the use of available resources, carrying out its tasks in full within the original plan. This was accomplished despite the overall headcount beginning to drop in the second quarter of the year and continuing to fall until the fourth quarter.

The approach taken in late 2009 is likely to impact the plan for forthcoming years, especially in terms of striving for ever leaner administration, with the further optimisation of work flows, assisted by the adoption of appropriate electronic workflow tools and working methods. To this end, during 2009 the Agency began to see the effects of the implementation of the results of the internal control project that was conducted in 2008.

Finally, the Agency began to prepare a concrete business continuity plan.

Legal Advice and Procurement

In 2009, the Agency continued meeting 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 were addressed as appropriate.

The execution of the Agency's budget was channelled through 26 procurement projects linked to 26 contracts for services or supplies, 188 purchase orders and 5 co-operation agreements, as shown in the table below.

Procurement projects launched – 2009							
Open		**Negotiated**		**Request for Offers (< €25.000)**		**Calls for Expression of Interest**	**Service agreements**
service 6	supply 0	service 15	supply 1	service 4	supply 0	1	2
6		**16**		**4**		**1**	**2**

Contracts signed – 2009			
Service **24**	**Supply** **2**	**Co-operation Agreements** **5**	**Purchase Orders** **188**

Technical Infrastructure

In the early part of 2009 the aging ENISA network backbone was renewed. The new network delivers 1GB/second to the desktop and lays the foundation for Voice over Internet Protocol (VoIP)-based services. Shortly after this major overhaul of infrastructure came the replacement of the virtualisation environment as some of the equipment was near the end of its life. This project also increased available capacity, allowing ENISA to run as much as 65% of servers in this virtual environment.

Through a concerted effort by all departments, a new ENISA website was rolled out in 2009. This was achieved in a six-month timeframe and was completely developed in the virtual environment. In addition, a new Content Management System (CMS) was put in place, allowing for the decentralisation of the management of content and better ownership of data.

Following the successful rollout of the new website, IPv6 was implemented for the website – ENISA is the first EU Agency to achieve this.

Work on the ENISA Intranet continued at a faster pace than planned. The main goals are to improve internal communication and leverage on new technologies to replace paper-based workflows with electronic ones, thus simplifying processes and improving transparency and compliance. In addition, a new leave management application was installed to replace the paper and Excel-based system with a fully electronic system. Similarly an application for missions management was tested and installed; it went live operationally on 1 January 2010.

The Listserv/Maestro service (for email distribution/discussion groups) was outsourced and all sites were upgraded to use SSL (Secure Sockets Layer) encryption to secure sensitive user data.

Physical Infrastructure

Work has been initiated on the construction of new Agency premises in Heraklion for the optimal functioning of the Agency in the future. The new building is planned to be able to house more than 100 staff with appropriate logistic services. The work is being financed by the Greek Ministry of Development, which is investing €9.800.000 for a larger and more suitable building. Work is expected to be completed at the latest by 2012.

On 8 October ENISA hosted a Management Team meeting in its new office in Athens, a bureau de passage which is conveniently situated ten minutes' drive from Athens international airport. The office is equipped with meeting rooms and a reception and has been provided by the Greek Ministry of Transport and Communications to assist ENISA in the performance of its work. The venue will facilitate meetings with stakeholders from industry in particular, and other stakeholders, allowing them to travel between Athens and continental Europe in one day.

Human Resources

In 2009 ENISA maintained its staff levels at 44 temporary agents and marginally reduced its contract agent base, to a total of 12. Particular emphasis was placed on the timing of the staff performance appraisal and the introduction of the promotion exercise. The Human Resources (HR) team also dedicated relevant resources to the implementation of the training plan.

Recruitment

Ten recruitment procedures were carried out during the course of the year and suitable candidates were consequently appointed.

Statutory staff: A total of 415 applications were received for all positions advertised. While the highest number of applications arrived from such Member States as Greece, Italy, Germany and France, increasing interest for assistant positions was demonstrated by candidates from Member States such as Romania, Bulgaria and Poland.

Non-statutory staff: 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 a young trainee from Austria.

Recruitment policy: All calls for expression 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 specialised press.

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

Training

Training activities are an integral part of ENISA's human resources policy. The Agency's training programme serves to expand and improve individual competencies and skills so that each staff member can contribute optimally to achieve ENISA's goals and reflect its core values of excellence, professionalism and service.

Language courses in Greek and French continued to be delivered throughout the year. Additional training in organisational, technical and personal development, as well as management training, was successfully delivered. Staff were also encouraged to participate in individual training courses at specialised training centres.

The overall objective of providing an average of 10 days of training per staff member was achieved again in 2009.

Other HR Activities

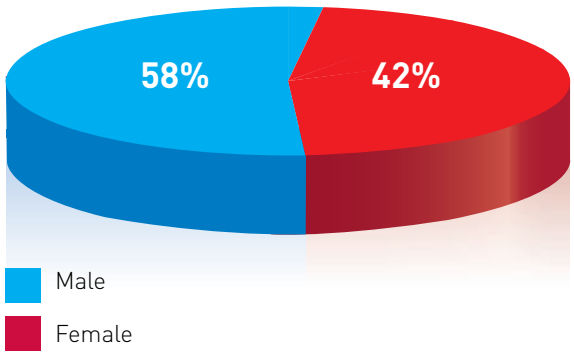
In late 2009, the third yearly career development report exercise was launched and contributed to the performance assessment of staff. Career objectives and training paths were also set, tailored to the professional development of each member of staff. The overall appraisal evaluation confirmed the high level of ability, efficiency and integrity of the Agency's staff.

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

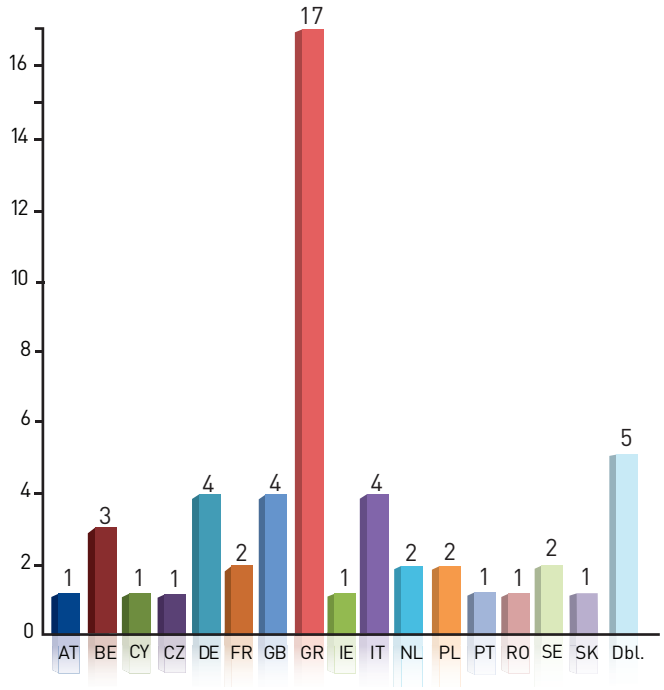
To optimise HR work, the Agency deployed leave management workflow and electronic recruitment tools.

HR Statistics

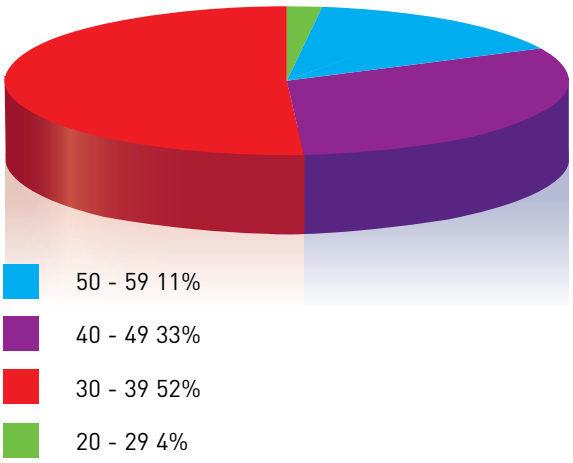
Staff members by gender



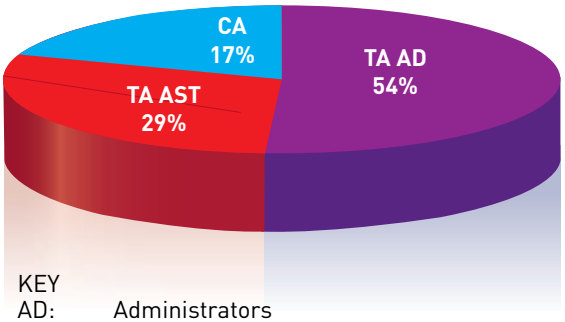
Staff members by nationality



Staff members by age



Staff members by function group or type of employment



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

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 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 2009, as amended in October 2009, reached €8.117.200, which represents a decrease of 2,8% compared with the 2008 figure (€8.355.024). Appropriations were committed at a rate of 94,4% (95,8% committed in 2008) to honour obligations related to the operational costs of the Agency and the activities required under the Work Programme 2009. Payments reached the level of 75,7% (76,2% paid in 2008) of the total appropriations managed. The level of committed appropriations demonstrates that the Agency's capacity to manage its annual budget efficiently has been sustained.

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

- **Title 1 – Staff expenditure:** Staff expenditure was committed at a rate of 94,4% at the end of the year. The respective rate of payments was 87,2%.

- **Title 2 – Administrative expenditure (functioning of the Agency):** The funds allocated to administrative expenditure were used as planned, with 92,9% of appropriations being committed by the end of the year, and 66,6% paid.

- **Title 3 – Operating Expenditure:** 94,7% 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 Work Programme 2009, were committed, with the total rate of paid appropriations reaching 53,6%.

Financial Reporting

According to Article 82 of the Financial Regulation, the Agency's Accounting Officer sends to the Commission's Accounting Officer the Provisional Accounts 2009, together with the Report on Budgetary and Financial Management. Subsequently the Commission sends the Provisional Accounts to the Court of Auditors. Based on the observations of the Court of Auditors, the Executive Director sends the Final Accounts 2009 to the Management Board which gives its opinion on them. Finally the Executive Director submits the 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, together with the statement of assurance which will be given by the Court of Auditors, will be published on the ENISA website and a link to them will be published in the Official Journal of the European Communities. The Financial Statements included in the Annual Accounts are the following:

Balance Sheet

	31.12.2009 €	31.12.2008 €
I. Non Current Assets	**396.580**	**373.124**
Intangible fixed assets	34.138	45.035
Tangible fixed assets	362.442	328.089
II. Current Assets	**3.437.593**	**2.638.207**
Short-term receivables	169.384	201.513
Cash and cash equivalents	3.268.209	2.436.694
Total Assets	**3.834.173**	**3.011.332**
III. Non Current Liabilities	**13.441**	**0**
Long-term provision for risk and charges	13.441	0
IV. Current Liabilities	**2.620.499**	**1.928.333**
EC pre-financing received	1.324.500	641.325
EC interest payable	46.948	143.818
Accounts payable	879.117	415.538
Accrued liabilities	319.934	677.652
Short-term provision for risk and charges	50.000	50.000
Total Liabilities	**2.633.940**	**1.928.333**
V. Net Assets	**1.200.233**	**1.082.999**
Accumulated result	1.082.999	1.443.575
Result for the year	117.234	-360.576
Total Net Assets	**1.200.233**	**1.082.999**

Economic Outturn Account

	2009 €	2008 €
Revenue from the Community Subsidy	7.434.025	7.713.699
Other revenue	54.008	0
Total Operating Revenue	**7.488.033**	**7.713.699**
Administrative expenses	-5.217.390	-5.146.114
Staff expenses	-4.259.042	-4.215.495
Fixed asset related expenses	-196.176	-162.654
Other administrative expenses	-762.172	-767.965
Operational expenses	-2.150.129	-2.925.591
Total Operating Expenses	**-7.367.519**	**-8.071.704**
Surplus/(Deficit) from Operating Activities	**120.514**	**-358.006**
Financial expenses	-2.137	-3.201
Exchange rate loss	-1.143	630
Surplus/(Deficit) from Ordinary Activities	**117.234**	**-360.576**
Economic Result for the Year	**117.234**	**-360.576**

Cash Flow Statement

	2009 €	2008 €
Surplus/(Deficit) from Ordinary Activities	**117.234**	**-360.576**
Operating Activities		
Amortisation (intangible fixed assets)	20.940	19.490
Depreciation (tangible fixed assets)	175.236	143.164
Increase in provisions for liabilities	13.441	0
Increase in short term receivables	-13.071	-100.157
Increase in value reduction for doubtful debts	45.200	0
Increase in accounts payable	692.166	518.073
Gains on sales of property, plant and equipment	-5.975	0
Net Cash Flow from Operating Activities	**1.045.172**	**219.994**
Cash Flows from Investing Activities		
Purchase of tangible and intangible fixed assets	-224.257	-162.427
Proceeds from tangible and intangible assets	10.600	0
Net Cash Flow from Investing Activities	**-213.657**	**-162.427**
Net decrease in cash and cash equivalents	831.515	57.568
Cash at the beginning of the period	2.436.694	2.379.126
Cash at the End of the Period	**3.268.209**	**2.436.694**

Statement of Changes in Capital

	Reserves €	Accumulated Surplus/ Deficit €	Economic result of the year €	Capital €
Balance as of 1 January 2009	**0**	**1.443.575**	**-360.576**	**1.082.999**
Allocation of the Economic Result of Previous Year		-360.576	360.576	0
Economic result of the year			117.234	117.234
Balance as of 31 December 2009	**0**	**1.082.999**	**117.234**	**1.200.233**

CHAPTER 5

Appendices

- Acronyms and Abbreviations
- Work Programme 2009
- Members of the Management Board
- Members of the Permanent Stakeholders' Group
- National Liaison Officers
- ENISA Deliverables 2009

Appendix 1
Acronyms and Abbreviations

AR	Awareness Raising
CAPEX	Capital expenditure
CERT/ CSIRT	Computer Emergency Response Team/Computer Security Incident Response Team. 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. Over time, the CERTs 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. As a result, the new term 'CSIRT' was introduced at the end of the '90s. Currently, both 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
DDoS	Distributed Denial of Service (attack)
DG INFSO	Directorate General Information Society and Media
DNSSEC	Domain Name System Security Extensions
EEA	European Economic Area
EFR	Emerging and Future Risk
EFTA	European Free Trade Association
eID	Electronic Identification
EU	European Union
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/)
ISAC	Information Sharing and Analysis Centre
ITU	International Telecommunication Union
KPI	Key Performance Indicator
MB	ENISA Management Board
MEP	Member of the European Parliament
MPLS	Multiprotocol Label Switching
MS	Member State of the European Union
MTP	ENISA Multi-Annual Thematic Programme
NIS	Network and Information Security
NLO	National Liaison Officer
OECD	Organisation for Economic Co-operation and Development
OPEX	Operating expenditure
PA	ENISA Preparatory Action
PSG	ENISA Permanent Stakeholders' Group
RFID	Radio Frequency Identification
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
VoIP	Voice over Internet Protocol
WG	Working Group, ENISA Ad hoc Working Group on specific technical issue
WP	Work Programme
WPK	ENISA Work Package

Appendix 2
Work Programme 2009

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 2009 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	Good Practice Guide on Network Security Information Sharing (NSIE)	Stocktaking of national information sharing schemes; report published
	Good Practice Guide on Reporting Security Incidents	Stocktaking of national incident reporting schemes; interviews with selected stakeholders; report published
	Good Practice Guide on National Exercises	Stocktaking of national exercises, reporting; interviews with selected stakeholders; report published
WPK 1.2	Resilience Measures – Virtual Group of Experts Report	Analysis of important resilience issues and challenges by a group of experts from operators; report published
	Good Practice Guidelines on Resilience Measures	Extensive analysis of good practices, internationally accepted standards, advice from national authorities and results from research; report published
WPK 1.3	DNSSEC Good Practice Guide	Stocktaking and analysis with experts; report published
	Tracking Standardisation Activities in the area of Resilience	Analysis of issues with the help of group of experts; report published
	Priorities of Research on Current & Emerging Network Technologies (PROCENT)	Analysis of issues with the help of group of experts; report published
MTP 2	**Developing and maintaining co-operation models**	
WPK 2.1	Co-operation platform for awareness raising community	
	1) Awareness raising online portal to be launched beginning of 2010.	N/A
	2) Enhancing AR community	The AR Community now numbers 353 members from all EU and EEA countries; six EU Member States are not represented with at least one representative from academia, industry and government; a welcome pack was sent to all members who registered before November. A welcome pack to the new remaining members will be sent in Q1 2010. Monthly conference calls were run each third Friday and eARNews distributed every 4 weeks except July, August and December
	3) AR Conference	Conference organised on "The growing requirement for information security awareness across public and private organisations"
	4) White Papers	Several White Papers published including "Child online protection", "ATM crime" and "Information security awareness in financial organisations"
WPK 2.2	Security competence circle and good practice sharing for CERT communities	
	1) Update CERT Inventory	Updated as planned (May and September)

	2) Maintain a Europe-wide co-operation activity for financial Information Sharing and Analysis Centres (ISACs)	Successfully maintained
	3) Maintain support of the creation of the South-African national CSIRT by Finland	Support maintained
	4) Pilot CERT exercise material	Two CSIRT exercise pilots successfully executed in Moldova and Kyoto; field report with feedback from the pilots assembled and published on ENISA website
	5) Conduct survey among European CERTS with regards to baseline capabilities, services and other data	Survey conducted among 120+ European CERTS (80+ teams answered); first draft of "Baseline capabilities for national/governmental CERTs" assembled, discussed with the teams and published on ENISA website (work to be continued in 2010)
WPK 2.3	European NIS Good Practice Brokerage	
	1) Successful partnerships	Facilitation of the organisation of the second European FI-ISAC (Financial Institutions – Information Sharing and Analysis Center) Workshop in Amsterdam, The Netherlands, in April, and the third European FI-ISAC Workshop in Berne, Switzerland, in November; facilitation of the meeting with Scandinavian local governments on Information Security in Oslo in May. Preparatory work for potential co-operation in 2010.
	2) Web-based online platform	Pilot phase
	3) Who-is-Who Directory	Updated; electronic and printed version expected to be published online and distributed January-February 2010.
	4) Country Reports	Finalised, ready to be published online
	5) Evaluation report	Finalised (internal document in PDF)
WPK 2.4	Building information confidence in the area of micro enterprises through capacity building and enhanced co-operation with multipliers	
	New online Security Toolkit to enhance capacity building amongst the micro-enterprises	Toolkit developed, tailor-made for intermediaries and/or multiplier organisations, by customising existing ENISA material (currently available in German and English); toolkit deployed and validated using road show concept and 3 interactive training sessions; validation of concept and toolkit at event in Brussels for European multiplier and umbrella organisations; report produced on Lessons Learned including Dissemination Strategy
MTP 3	**Identifying emerging risks for creating trust and confidence**	
WPK 3.1	Framework for assessing and discussing emerging risks – Analysis of specific scenarios	Five reports delivered on: • European eID cards • Security of cross-border electronic authentication • Cloud computing • Internet of Things/RFID Air Travel • Data Mining/Profiling
WPK 3.2	Framework for assessing and discussing emerging risks – Documentation & maintenance	Improved and updated EFR Framework, taking into consideration stakeholders' feedback

Measuring Progress

A set of SMART[19] 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 2009. 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
Commission using ENISA recommendations	YES	**Yes, through EU's COM on CIIP**
% Member States using ENISA recommendations	50%	**Too early to assess**
# users covered by service providers using ENISA recommendations	50 million	**Yes**

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 50% of Member States participate in the open consultation process for each good practice

SMART goal: at least 3 Member States express interest in piloting good practices for each area

KPI	Required	Achieved by end 2009
% Member States covered by the analysis	50%	**60% (information sharing); 78% (exercises); 82% (incident reporting)**
% Member States participated in the open consultation	50%	**60% (information sharing); 78% (exercises); 82% (incident reporting)**
# Member States express interest in piloting good practices for each area	3	**1 on information sharing (too early to assess)**

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

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

SMART goal: At least 50% of Member States participate in the open consultation process

KPI	Required	Achieved by end 2009
% Member States taking part in the analysis	50%	**60%**
% participated in the open consultation process	50%	**Too early**

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

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

SMART goal: ENISA's recommendations of innovative actions are applied in at least ten Member States by 2010

SMART goal: To make contributions to at least one research priority for the next revision of the ICT WP of the FP7 of EU funded R&D.

KPI		Achieved by end 2009
# Member States adopting ENISA recommendations	10	Too early
# contributions to work programmes of FP7 on relevant topics	1	Too early

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 2009
# Member States involved in co-operation models	10	27 plus 3 EEA and 10 Third Countries
# Co-operation models	3	5

WPK 2.1: Co-operation platform for Awareness Raising (AR) Community

SMART goal: By 4Q 2009, have all EU Member States represented in the AR Community with at least 1 representative from the following sectors: industry, academia and government

SMART goal: By 2009, have 50 downloads of good practice material shared within the AR Community from the AR portal, 1500 visits per month to the AR portal and 10 explicit requests for not-downloadable deliverables

SMART goal: By Q2 2009, organise a conference with at least 80 participants from 10 different EU Member States

KPI	Required	Achieved by end 2009
# EU Member States represented in the AR Community	All Member States, with at least one from each of the following sectors: industry, academia, government	All EU & EEA countries are represented. There is no representative for the following sectors/countries: Industry: 2 (Hungary and Liechtenstein); Academia: 3 (Finland, Iceland, Malta); Government: 1 (Slovak Republic)
# experts signed up to the AR Community through AR portal and receiving the welcome pack		N/A as portal not available[20]
# downloads of good practice material shared within the AR Community from the AR portal	50	N/A as portal not available
# visits to AR portal per month	1500	N/A as portal not available
# requests for non-downloadable deliverables from portal	10	N/A as portal not available
# participants in conference	80	93
# EU Member States represented at conference	10	11

[20] The Awareness Raising portal will be delivered and operational beginning of 2010.

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

SMART goal: By Q4 2009, at least 3 presentations given about ENISA's work in the CERT field at the CERT/CSIRT community events

SMART goal: By Q4 2009, 80% of updates in CERT inventory are confirmed

SMART goal: By Q4 at least two TRANSITS trainings have been organised with support by ENISA

SMART goal: By Q4 2009, at least 50 downloads of ENISA CSIRT good practice collection materials that have been produced or updated in 2009

SMART goal: "ENISA CSIRT exercise collection" piloted at least between 2 CSIRT teams

Extra mile: publish additional CERT exercise material

KPI	Required	Achieved by end 2009
# of presentations	3	> 10
% confirmed updates	80%	100%
# of trainings supported	2	2
# of downloads	2	Too early (report published end of December 2009)
# of exercise pilots	1 pilot, 2 teams	2 pilots, > 16 teams (other exercises planned)
	None	3 Live DVD ISO images created and published

WPK 2.3: European NIS Good Practice Brokerage

SMART goal: By Q4 2009, at least 4 Member States are engaged in at least 2 new co-operations, facilitated through the European NIS good practice Brokerage.

SMART goal: By Q4 2009, the Online Platform is visited by all Member States

SMART goal: By Q4 2009, all Member States are covered by the Who-is-Who Directory

SMART goal: By Q4 2009, all updates in Who-is-Who Directory are confirmed

SMART goal: By Q4 2009, the Country Reports will be updated for all the Member States and they will contain at least 1 thematic section on a specific NIS related topic

KPI	Required	Achieved by end 2009
# Member States engaged in co-operation	4	18
# New co-operations	2	3
# Member States stated to have visited the Online Platform	27	0[21]
# Member States covered by Who-is-Who Directory	27	31 (incl. EEA & EFTA)
% Confirmed updates in Who-is-Who Directory	100%	100%
# Member States covered by updated Country Report	27	30 (incl. EEA)
Thematic section contained in the updated Country Reports	1	> 5

[21] The online platform will be introduced beginning of 2010.

WPK 2.4: Building information confidence of micro-enterprises through capacity building and enhanced co-operation with multipliers

SMART goal: By end of 2009, at least 1 multiplier organisation from at least 1 different Member States has been trained to use the customised ENISA security toolkit to build information confidence with micro-enterprises.

KPI	Required	Achieved by end 2009
# Multiplier organisation	1	1
# Member States	1	1

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 security challenges in the Information Society.

KPI	Required	Achieved by end 2009
# Stakeholders referring to ENISA as point of reference	30	**Too early. Most deliverables only published at the end of 2009. However, responses received so far suggest that the target has been exceeded.**
# Member States of stakeholders referring to ENISA as point of reference	15	**Too early (see above)**

Appendix 3
Members of the Management Board
At 12 December 2009

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).

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	Pavel **TYKAL** Head of Unit Department of eGovernance Project and Service Development Ministry of Interior 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
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	Sylvain **LEROY** Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information
Germany	Michael **HANGE** Vice President of the Federal Office for Information Security (BSI)	Roland **HARTMANN** Head of International Relations Federal Office for Information Security (BSI)
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	
Ireland	Aidan **RYAN** Telecommunications Adviser Department of Communications	Paul **CONWAY** Head of Compliance and Operations Commission for Communications Regulation
Italy	Rita **FORSI** Director General Ministry of Economic Development	Alessandro **RIZZI** Audiovisual and Telecommunications Permanent Representation of Italy to the EU
Latvia	Ugis **SARMA** Director of Communications Department Ministry of Transport and Communications	Maris **ANDZANS** Head of Transport and Communications Security Division Ministry of Transport and Communications
Lithuania	Valdas **KISONAS** Director of the ICT Department Ministry of Transport and Communications of the Republic of Lithuania	Tomas **BARAKAUSKAS** Director of the National Regulatory Authority of the Republic of Lithuania
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)	
Portugal	Pedro Manuel **BARBOSA VEIGA** Presidente da Fundação para a Computação Cientifica Nacional (FCCN)	Manuel Filipe **PEDROSA DE BARROS** Director de Tecnologias e Equipamentos da Autoridade Nacional das Comunicações (ANACOM)

Romania	Toma **CIMPEANU** Vice-President Agentia pentru Serviciile Societatii Informationale (ASSI)	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	
Sweden	Lena **CARLSSON** Special Adviser, Ministry of Enterprise, Energy and Communications Division for Information Technology Policy	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** Office of Cyber Security (OCS) Cabinet Office

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	
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** Secretary, Statistical Office of the Republic of Slovenia

EEA-country representatives (observers)

Group	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

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

Appendix 5
National Liaison Officers

At 9 December 2009

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	Mirka **MERES-WUORI** - Ministry of Transport and Communications
France	Sylvain **LEROY** - Central Directorate for Information Systems' Security, General Secretariat of National Defence
Germany	Martin **BIERWIRTH** - Federal Office for Information Security (BSI), International Relations
Greece	Panagiotis **PAPASPILIOPOULOS** - General Directorate of Communications, Ministry of Transport and Communications
Hungary	Ferenc **SUBA** - Chairman of the Board of CERT-Hungary
Ireland	John **MOORE** - Communications Business & Technology Division, Department of Communications
Italy	Rita **FORSI** - Director General, Ministry of Economic Development
Latvia	Maris **ANDZANS** - Head of Transport and Communications Security Division, Ministry of Transport and Communications
Lithuania	Rytis **RAINYS** - Head of Network and Information Security Division, Communications Regulatory Authority
Luxembourg	Manuel **SILVOSO** - Ministry of the Economy and Foreign Trade, Department for eCommerce and Information Security
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	Lino **SANTOS** - Director of Security and Users Services, CERT.PT/FCCN
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	Oscar **MARTINEZ DE LA TORRE** - Head of Unit for eSignature & eSecurity, Directorate for Information Society Services Ministry for Industry, Tourism and Commerce
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, Innovation & Skills

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

Appendix 6
ENISA Deliverables 2009

Directories:

1. Who-is-Who in Network and Information Security, 5th Edition 2010
   www.enisa.europa.eu/act/sr/files/deliverables/who-is-who-directory-on-nis-ed.-2009

2. Updated Country Reports
   www.enisa.europa.eu/act/sr/country-reports

Periodicals:

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

Improving Resilience in eCommunication Networks (MTP 1):

1. Information Sharing Good Practice Guide
   www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange

2. Incident Reporting Good Practice Guide
   www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms

3. National Exercises Good Practice Guide
   www.enisa.europa.eu/act/res/policies/good-practices-1/exercises

4. Guidelines on Providers' Resilience Measures
   www.enisa.europa.eu/act/res/providers-measures

5. Report of Virtual Working Group on Providers' Resilience Measures
   www.enisa.europa.eu/act/res/providers-measures/vwg-2009

6. Study on the Costs of DNSSEC Deployment
   www.enisa.europa.eu/act/res/technologies/tech/dnsseccosts

7. Priorities of Research on Current & Emerging Network Technologies (PROCENT)
   www.enisa.europa.eu/act/res/technologies/procent

8. Gap analysis of standardisation activities in the area of resilience
   www.enisa.europa.eu/act/res/technologies/std

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

1. Key facts and figures about the awareness raising community and its members
   www.enisa.europa.eu/doc/pdf/other/awareness/ar_comm_key_facts_may_09.pdf

2. ENISA's ten security awareness good practices
   www.enisa.europa.eu/act/ar/deliverables/2009/ar-security-practices-en

3. ATM crime – Overview of the European situation and golden rules on how to avoid it
   https://www.enisa.europa.eu/act/ar/deliverables/2009/atmcrime/at_download/fullReport

4. The ENISA awareness raising community
   www.enisa.europa.eu/act/ar/deliverables/2009/ar-community-en

5. Information security awareness in financial organisations – Guidelines and case studies
   www.enisa.europa.eu/act/ar/deliverables/2009/is-in-financial-organisations-09

6. The growing requirement for information security awareness
   www.enisa.europa.eu/act/ar/deliverables/2009/ar-book09

7. Field report from the two CSIRT exercise pilots
   www.enisa.europa.eu/act/cert/support/exercise/files/field-report-pilots

8. First draft of the definition of "Baseline capabilities for national/governmental CERTs"
   www.enisa.europa.eu/act/cert/support/baseline-capabilities

9. ISO images for the CSIRT exercises
   www.enisa.europa.eu/act/cert/support/exercise

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

1. Position Paper – Privacy and Security Risks when Authenticating on the Internet with European eID Cards
   www.enisa.europa.eu/act/it/eid/eid-online-banking

2. Cloud Computing – benefits, risks and recommendations
   www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

3. Cloud Computing SME Survey
   www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey

4. Cloud Computing – Information Assurance Framework
   www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

5. Briefing – Quantum Key Distribution
   www.enisa.europa.eu/act/rm/files/deliverables/briefing-quantum-key-distribution

European Commission

General Report 2009
European Network and Information Security Agency

Luxembourg: Publications Office of the European Union

2010 – 80 pp. – 21cm x 29.7cm

ISBN: 978-92-9204-037-6
ISSN: 1830-981X
Catalogue no.: TP-AB-10-001-EN-C
doi 10.2824/15669

The report is also available on DVD:

ISBN: 978-92-9204-038-3
ISSN: 1830-9828
doi 10.2824/15907

Editing and design by Kingston Public Relations Ltd., UK (+44 1482 876229) www.kingstonpr.com
Published in July 2010

TP-AB-10-001-EN-C

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

Publications Office

doi 10.2824/15669
ISBN 978-92-9204-037-6

01/07_10