



Security, People, and the Economy

Celebrating Five Years of the European Network and Information Security Agency



Per Aspera ad Astra

Security, People, and the Economy

As modern European citizens we have become so accustomed to today's technology that it is now hard to imagine life without mobile phones, personal computers and the Internet. We take the convenience of online banking, eHealth and eCommerce for granted.

Communication networks and information systems provide exciting opportunities for home-users. But they also increase the efficiency and effectiveness of the key services on which society relies such as power, water and communications. The security of these services are also critical for the functioning – and growth – of the European economy.

As networks grow more complex, they also become more vulnerable; new technology brings new risks. Security breaches can generate substantial economic damage. They can cripple the infrastructure of a country – as witnessed by the massive cyber-attack against Estonia in 2007. The security of the networks and data on which new technologies are based – Network and Information Security (NIS) – has therefore become a crucial issue in the 21st century. And it affects us all, businesses and citizens alike.

Set up five years ago, the European Network and Information Security Agency (ENISA) is the European Union (EU)'s response to these new challenges. As a Centre of Expertise in NIS, ENISA has assisted the EU, its Member States and the business community to prevent, address and respond to NIS issues. It is now time to take stock of these successes, and to look towards the future.

Electronic communications are critical to the success of the European economy. In 2007, purchases and sales of electronic networks amounted to 11% of the total turnover of EU companies. 77% of businesses accessed banking services over the Internet and 65% of companies used online public services





This Latin motto that I have chosen for the celebration of our fifth anniversary translates roughly as **'Through hardships to success'**. It seems particularly appropriate for ENISA, which has faced many difficulties since its formation – and has emerged in triumph.

ENISA is now widely recognised as an impartial, independent EU authority in the field of NIS. The Agency has developed numerous good practice guides, given advice, shared knowledge and information. It has facilitated the setting up of Computer Emergency Response Teams (CERTs), helped increase cross-border co-operation and improved the response to large-scale cyber-attacks.

ENISA has created awareness raising material, tailoring it for specific organisations to use in their information security events and training, and has produced guidance to help parents ensure the safety of children using the Internet.

In major work on the resilience of public communication networks, the Agency has examined national policy and regulatory environments and is developing good practices in information sharing, exercises and incident reporting mechanisms. ENISA analyses providers' measures related to resilience and issues guidelines to enhance their preparedness. Following an assessment of a number of technologies, the Agency is now preparing guidelines for deploying DNSSEC to enhance the resilience of communication networks. Inventories of risk assessment and risk management methods and of Business Continuity methods and tools have been produced.

ENISA is also working to identify future threats. With its technical expertise, its central position and its independence, the Agency is well placed to ring the alarm bells on Emerging and Future Risks.

The following pages highlight some of our achievements in our first five years in endeavouring to make the world of ICT a safer place for the people of Europe. ENISA is now firmly established and well prepared to meet the challenges of the next five years and beyond. *Ad majora*¹!

A handwritten signature in blue ink, which appears to read "Andrea Pirotti".

Andrea Pirotti
Executive Director

¹ Ancient Roman greeting wishing success to those setting out on a challenging mission.

ENISA's Role – Expertise and Excellence in NIS

ENISA is an expert body and a Centre of Expertise in Network and Information Security (NIS). Its mission is to enhance the level of NIS in Europe by:

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

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

The challenges facing NIS are vast, multi-faceted and urgent. They affect individual users and, crucially, they affect the economy and infrastructure of Europe. Tackling these challenges requires a systematic, coherent and integrated strategy that involves all concerned stakeholders and decision-makers and is based on dialogue and partnership. Supported by a Permanent Stakeholders' Group of leading experts that advises the Agency on identifying and achieving its strategic goals, ENISA has already had a major impact on NIS in the countries it supports. It has made a significant contribution to reducing obstacles to secure NIS, working to the benefit of individual users of information systems and the whole economy of Europe.

Sharing of information, facts and knowledge

To expand and improve the opportunities for EU Member States to share information, ENISA is developing various models of co-operation in areas such as awareness raising, incident response and electronic identity (eID). With the assistance of its Network of National Liaison Officers, the Agency has established a European NIS Good Practice Brokerage, along with supporting tools such as the Online Platform, the Who-is-Who Directory of Network and information Security and 'Country Reports' of activities in the Member States.



Establishing good practices

ENISA conducts surveys and produces papers, reports and studies on the current state of play in NIS in Europe. Over the last five years these have included – among many others – issues such as the risks to children on the Internet, the security of USB drives and printing devices, information sharing, exercises, incident reporting mechanisms, spam, standards, risk assessment, risk management, certification schemes, eID, security economics, Business Continuity, Computer Emergency Response Teams (CERTs), and how to obtain the CEO's support for NIS awareness raising.

Identifying risks

The Agency has published Position Papers to explain NIS risks presented, for example, by virtual worlds and online gaming, botnets and Web 2.0 – and has suggested mechanisms to mitigate against them. And, recognising the importance to Europe's economic growth of small and medium enterprises (SMEs) which represent 99% of all enterprises in the EU and around 65 million jobs, ENISA is addressing the specific problems of SMEs and microenterprises.



Disseminating information

ENISA co-organises conferences, runs workshops and provides expert speakers at events around the world. The Agency produces the ENISA Quarterly Review, a magazine to encourage the NIS debate. It compiles directories and databases and provides training materials, for example to improve the efficiency of CERTs.

Providing assistance and advice

The Agency assists the governments of Member States and EU institutions with their specific security problems, ranging from help with training to advice on Internet security.

A global player

ENISA is aware that NIS is a global challenge that does not recognise borders. In 2008 the Agency took its expertise to another continent, bringing together Finland and South Africa in the establishment of a South African Computer Security and Incident Response Team (CSIRT). ENISA regularly participates as a technical expert in the work of various international organisations such as the OECD and ITU, and has hosted visits to its headquarters by delegations from China, Japan and South Korea.

Improving Resilience in eCommunication Networks



We have become so reliant on Information and Communication Technologies (ICT) that life grinds to a standstill with any network outage. Physical phenomena, software and hardware failures, human mistakes or intentional attacks can all affect the proper functioning of eCommunication networks and jeopardise both public welfare and economic stability.

ENISA is working to improve resilience in eCommunication networks. A stocktaking exercise was successfully completed in 2008, which examined national policies and regulations, measures deployed by operators and the use of existing technologies which can enhance resilience. The Agency is now analysing the results to identify common measures and good practices deployed in the different Member States – as well as gaps and inconsistencies. After further consultations, ENISA will then be able to recommend action to the different categories of stakeholder. The Agency has also begun to deal with the impact of cloud computing on the availability and integrity of networks and is working on the development of good practice guides on information sharing, incident reporting mechanisms and exercises.

Business Continuity

While important for many organisations, business continuity is vital for the resilience of IT systems and their components. ENISA is contributing to the generation of a publicly available information base on Business Continuity with inventories, good practices and applicability guides.

To complement its analysis of measures deployed by operators to safeguard the resilience of public communication networks, in 2008 ENISA conducted a survey on availability and continuity issues among providers of eCommunication infrastructures. The Agency also produced an inventory of Business Continuity methods and tools which will help users to understand their needs and acquire information about the various approaches to Business Continuity.

The Digital Fire Brigades – CERTs

Recent major cyber-attacks in Estonia and towards governments in Germany, Sweden, France and other countries have increased interest in Computer Emergency Response Teams (CERTs). Like a fire brigade, CERTs are called out when a security 'fire' occurs. Besides responding to security incidents, CERTs usually also provide a comprehensive portfolio of other security services for their customers, such as alerts and warnings, advisories and security training.

ENISA has produced a setting-up guide and other material to help organisations in the establishment of national/governmental CERTs, which have been used for example in Latvia, Austria, Cyprus and the former Soviet Republics. ENISA's expertise is even sought outside Europe: in 2008, ENISA and Finland together supported the setting up of a national CSIRT in South Africa. The number of national/governmental CERTs has risen from 8 in 2005 to 18 with 4 more in the pipeline. In total, there are currently (June 2009) 128 listed CERTs in the European Union and the number is growing – in no small part due to the efforts of ENISA!

The Agency organises CERTs training and has produced a collection of 'Good practices for CSIRT exercises'.

Co-operation is a necessity for successful incident response because attacks on the Internet do not stop at national borders and affect all aspects of the Information Society. ENISA therefore conducted a study on how certification of CERTs could act as a mechanism for building trust among the teams which in turn would stimulate the exchange of information about incidents and help enhance the general level of CERT performance in Europe.



The Agency also organises an annual Workshop on CERTs in Europe, giving CERT members an opportunity to meet together to share their experiences and learn good practices.



Unless people know about the threats and risks in today's modern information and communication technologies, how can they protect themselves?

ENISA therefore facilitates the activities of the EU Member States in raising awareness. Targeting primarily users, ENISA has produced: 'A Users' Guide: How to Raise Information Security Awareness' which has been released in different languages, as well as information security awareness programmes. The Agency has produced a White Paper on 'Obtaining support and funding from senior management', together with a related publication specifically for the financial sector, and organises numerous workshops to disseminate information.

By encouraging the use of appropriate tools and behaviour, the Agency helps to build the trust that is essential for the acceptance of new technology and the growth of the digital economy.

ENISA has launched the **Awareness Raising Community** as a subscription-free forum designed to spread information security knowledge. By July 2009, the community already included 46 nations, comprising 317 members, from both within and outside the EU.

Examples of key publications produced include:

- **Children on Virtual Worlds** – With every passing day, a new social networking website seems to spring up, and entertainment companies are rushing to exploit the latest new market – the younger generation. Children are on the Internet at an earlier age than ever before and (according to research conducted by EMarketer Inc) around 20 million children and tweens will visit virtual worlds by 2011 – up from 8.2 million in 2007. Inevitably, this raises enormous safety concerns. ENISA has produced a White Paper, 'Children on virtual worlds: what parents should know', to provide clear and comprehensive information about virtual worlds, the risks children can encounter and what parents can do to protect their children and help them understand how to behave in virtual worlds so that they can reap the many potential benefits whilst avoiding the dangers.



- **'Social Engineering** – Exploiting the 'Weakest Links' – a paper explaining how to avoid the pitfalls of social networks and email (also known as 'Nigeria-letters' or 'advance-fee frauds'), instant messaging and Voice over Internet Protocol (VoIP).
- **Secure printing** – Unintended disclosure of sensitive information, such as invoices, employee records and customer details, may jeopardise crucial company assets. ENISA has published a White Paper highlighting the inherent risks to businesses if secure printing policies are not in place.
- **Secure USB flash drives** – This White Paper advises on the threats from accidental loss or theft of confidential corporate data on unsecured USB flash drives.

The Risks in Emerging Technologies

ENISA has published a number of Position Papers to help policy-makers and other decision-makers to better understand the nature of NIS threats – and to counter them. Each provides an introduction to security issues in specific areas, highlights the most important threats, and makes recommendations for action and good practices to reduce the security risks to users. They have all received high level, general media attention. Topics covered include:



- **Virtual Worlds, Real Money**

The growth in malicious programmes that specifically target online games and virtual worlds has increased phenomenally in recent times. Such malware is invariably aimed at the theft of virtual property accumulated in a user's account and its sale for real money. At the same time, online gaming offers a significant risk in the disclosure of private data.

- **Web 2.0 Security and Privacy**

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

- **Online Social Networks**

Social Networking Sites (SNSs) have been one of the big growth businesses of the last few years. Their commercial success depends heavily on the number of users attracted. Combined with the strong human desire to connect, this encourages online behaviour where security and privacy are not always the first priority. As a result, SNS members often broadcast sensitive information too widely and sometimes unadvisedly, either by choice or unwittingly.

- **Reputation-based Systems**

Reputation-based systems are used by an increasing number of applications as risk management mechanisms to facilitate trust by allowing users to form an expectation of behaviour based on the judgements of others. They are an integral part, for example, of the strategy behind eBay. Electronic reputation is a valuable asset – and is thus becoming the target of attacks.

- **Botnets – the Silent Threat**

Typically botnets are used for identity theft, unsolicited commercial email, scams, Distributed Denial of Service (DDoS) attacks and other frauds. Most owners of infected computers do not even know that their machines have been compromised. Botnets represent a steadily growing problem threatening governments, industries, companies and individual users with devastating consequences.

- **Emerging and Future Risks**

In years to come, new application scenarios and technologies are expected to emerge which will generate new risks. Early and accurate identification of such risks will increase our capability to reduce and control their impact. ENISA has developed a framework model for the identification and assessment of risks based on specific scenarios and has successfully run a pilot test on Remote Health Monitoring and Treatment. Further scenarios are now being assessed.



Access Everywhere – Secure Nowhere?

Mobile devices

Mobile devices such as smart phones and Personal Digital Assistants (PDAs) can act as an identity or payment card for online services. In the near future, for example, we might use our phone to pay our taxes, buy tickets, elect a president or open a bank account. But when we use a mobile device, we leave traces of our identities and transactions behind. The theft of such devices is rising and, due to their increasing complexity, they are now also prone to virus attacks. ENISA has produced a Position Paper which identifies various security threats and suggests key mechanisms to counteract them. In doing this, the Agency is helping to make it possible for the citizens of Europe to enjoy the enormous opportunities which are becoming available with mobile devices – securely.



eID cards

Europe lacks a co-ordinated strategy for how to protect the private data stored by the electronic identity (eID) card, which is a significant obstacle to cross-border interoperability and limits the acceptance of eID cards by users. ENISA has conducted a study and produced a Position Paper which gives the first overview of the vast disparity between privacy features in eID cards across Europe and explains the technologies that can protect privacy – ‘Privacy Features’. The analysis sets the stage for a privacy baseline in European eID cards.

Authentication assurance

Authentication Assurance Levels have been defined to foster eID interoperability using a common policy language for describing authentication assurance strength. ENISA has mapped these authentication levels to a machine readable format using the OASIS SAML standard, making them now widely accessible. At the same time, the Agency has produced a gap analysis with guidance on how to implement these authentication levels in eGovernment applications using SAML context classes.

Responding to Requests

The EU Member States, the European Parliament and the European Commission seek ENISA's advice or assistance. These requests range, for example, from help with establishing CERTs to advice on Internet security matters. Other requests for assistance have included:

Security and Anti-Spam Measures

At the request of the European Commission, ENISA undertook a study into how providers of electronic communication services (e.g. Internet Service Providers, telecommunication companies) secure their services and protect their clients from spam and other threats. The findings provided valuable information about the current situation and formed the basis for recommendations to enhance security and combat spam. ENISA followed up its work with a second study a year later.

Developing a Trusted Partnership for a Data Collection Framework

ENISA was asked by the European Commission to examine whether it would be feasible to create a data collection framework for security incidents. The long term goal was a partnership of public and private entities which would benefit from or contribute to a data-sharing initiative and enable decision-makers to see the big picture. As a result of ENISA's study, a new information exchange, called 'Partnership for ICT Security Incident and Consumer Confidence Information Exchange (PISCE)', was established.

EISAS – NIS Information for Home-users and SMEs

There is evidence that, for various reasons, the computers of home-users and small and medium enterprises (SMEs) are the most popular victims of targeted attacks. Although immensely important to the economy, due to their size, SMEs rarely employ dedicated security personnel so the protection of their information assets is often left to non-security experts. The European Commission asked ENISA to "examine the feasibility of a European information sharing and alert system (EISAS)". ENISA's report made a number of recommendations regarding the EU's future role in this area.



The Future

ENISA fully supports the European Commission's strategy on Critical Information Infrastructure Protection (CIIP) and its moves to protect Europe from cyber-attacks and disruptions. The Agency will intensify its efforts to encourage a greater dialogue between all actors, to maximise the exchange of information, increase co-operation and disseminate the knowledge required to combat these threats.

There is a 10-20% probability that telecom networks will be hit by a major breakdown in the next 10 years, with a potential global cost of around €193 billion.

To maximise the effect of its limited resources and increase its impact on key areas, ENISA has defined a number of strategic priorities, with a series of rolling Multi-annual Thematic Programmes (MTPs) focusing on:

- **Improving resilience in European eCommunication networks** – including the identification of current good practices, gap analysis of policy and providers' measures and the investigation of innovative actions.
- **Developing and maintaining co-operation models** – including developing the awareness raising community and a security competence circle for CERTs, building information confidence among microenterprises, and facilitating co-operative initiatives through the European NIS Good Practice Brokerage.
- **Identifying emerging risks for creating trust and confidence** – including establishing an Emerging Risks framework that will enable decision-makers to better understand and assess 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.

NIS is crucial for the European economy and touches the daily lives of citizens in Europe. The balance between security, privacy and trust and, at the same time, continuous access guarantees that NIS will remain on the agenda and that the need for NIS will be a decisive political and economic factor for the EU and its Member States for the foreseeable future. ENISA is well placed to meet the evolving challenges in NIS and, in no small part as a result of its work to date, the Member States are becoming increasingly equipped to meet them.

ENISA: 2004-2009 – and Beyond

A recent resolution² of the European Council recognises that
“the establishment of ENISA has been a major step forward in the EU’s efforts to respond to the challenges relating to network and information security”.

In March 2004, the proposal for a European Network and Information Security Agency was formally adopted. The founding Regulation 460/2004 for the Agency, defines its mandate as being to address the security of communication networks and information systems.

Initially established in Brussels, the Agency moved to its current headquarters and began operations in Heraklion, Crete, on 1 September 2005.

With its success well documented, in 2008 the Agency’s mandate was extended until 2012. There is no doubt that the challenges to Europe and the world in Network and Information Security will extend for many years to come. The need for secure networks, systems and services will not suddenly disappear at the expiry of the current ENISA mandate – despite the work we undertake; the threats and risks can only increase. The stability and growth of the European economy, as well as our ability to exploit the benefits offered by new technology, depend on how well we manage Network and Information Security. ENISA is prepared to meet this challenge. Following the EU parliamentary elections in June 2009 and the establishment of a new European Commission, we now have the necessary time to reflect thoroughly upon the activities of ENISA ‘post-2012’.



² 15768,01.12.2006



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

