

# Ireland Country Report



## About ENISA

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

## Contact details

For contacting ENISA or for general enquiries on the Country Reports:

### Mr. Giorgos Dimitriou

ENISA External Relations Expert

[Giorgos.Dimitriou@enisa.europa.eu](mailto:Giorgos.Dimitriou@enisa.europa.eu)

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



## Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Joris Lambrechts, Dan Cimpean and Johan Meire.**

## Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

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

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

© European Network and Information Security Agency (ENISA) 2011

## Table of Contents

<b>IRELAND .....</b>	<b>4</b>
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS .....	4
<b>NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES .....</b>	<b>5</b>
OVERVIEW OF THE NIS NATIONAL STRATEGY .....	5
THE REGULATORY FRAMEWORK .....	5
<b>NIS GOVERNANCE .....</b>	<b>9</b>
OVERVIEW OF THE KEY STAKEHOLDERS .....	9
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS .....	10
FOSTERING A PROACTIVE NIS COMMUNITY .....	10
<b>COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....</b>	<b>11</b>
SECURITY INCIDENT MANAGEMENT .....	11
EMERGING NIS RISKS .....	11
RESILIENCE ASPECTS .....	11
PRIVACY AND TRUST .....	12
NIS AWARENESS AT THE COUNTRY LEVEL .....	13
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY .....	13
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	13
<b>RELEVANT STATISTICS FOR THE COUNTRY .....</b>	<b>14</b>
INTERNET ACCESS OF POPULATION AND ENTERPRISES .....	14
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS .....	15
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS .....	16
OTHER STATISTICS .....	17
<b>APPENDIX .....</b>	<b>18</b>
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY .....	18
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs) .....	19
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	20
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES .....	21
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	22
REFERENCES .....	22

## Ireland

### The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
  - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
  - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
  - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
  - *Security incident management*
  - *Emerging NIS risks*
  - *Resilience aspects*
  - *Privacy and trust*
  - *NIS awareness at the country level*
  - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
  - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

## NIS national strategy, regulatory framework and key policy measures

### Overview of the NIS national strategy

In the frame of the consensual model, the key stakeholders know each other and providers share information with authorities easily. As the administration for resilience issues is a small one, public authorities need to share information with providers and engage in good exchange to enhance information level. Information is exchanged on all topics addressed here, i.e. information security policies, business continuity plans, preparedness measures, information on geographical, topological and technical network structures, locations with high infrastructure density.

In addition, information is exchanged about new technologies that have been rolled out. Within the cooperative model, information sharing, whereby formal requests are unnecessary is the norm. However, appropriate legislative requirements for information sharing are in place.

As regards the use of the information collected, ComReg holds a large stock of information. ComReg analyses the information appropriately according to various criteria. In the frame of the consensual model, the key stakeholders know each other and providers share information with authorities easily.

### The regulatory framework

The following Irish national regulations have relevance and applicability in the domain of network and information security:

#### Data Protection/Privacy Legislation

*Data Protection (Amendment) Act 2003*

The Data Protection Act of 1988 was amended in 2003 to ensure full compliance with the EU Data Protection Directive (95/46/EC). The aim of the Directive is to establish common standards of data protection across Member States in order to protect personal privacy and ensure the smooth operation of the internal market, while ensuring adequate levels of data protection in countries outside the European Economic Area in order to facilitate and encourage international trade (Department of Justice, Equality and Law Reform). The Data Protection Commissioner oversees and enforces the Act.

#### eCommerce Legislation

*Electronic Commerce Act, 2000*

The Electronic Commerce Act 2000 became law on 20 September 2000. It implements the EU Directive on a Community framework for electronic signatures (1999/93/EC) and, in part, the EU Directive on electronic commerce (2000/31/EC). The Act provides (with some exceptions) for the legal recognition of electronic signatures, electronic writing and electronic contracts. It authorises the use of encryption and sets the rights and obligations of Certification Service Providers (CSPs).

---

### *European Communities (Directive 2000/31/EC) Regulations 2003*

The Irish Minister for Enterprise Trade & Employment signed those regulations in 2003 with a view to give effect to those remaining provisions of the EU Directive on electronic commerce (2000/31/EC) not transposed into Irish law by the Electronic Commerce Act 2000.

### **eCommunications Legislation**

#### *Communications Regulation Act, 2002 2010<sup>1</sup>*

By means of the Communications Regulation Act 2002 and of secondary legislation (a number of Statutory Instruments), Ireland transposed all Directives under the EU regulatory framework for electronic communications, namely: Directive 2002/21/EC (Framework Directive); 2002/20/EC (Authorisation Directive); 2002/19/EC (Access Directive); 2002/22/EC (Universal Service Directive); and 2002/58/EC (Directive on privacy and electronic communications).

It was amended in 2010 by the Communications Regulation (Premium Rate Services and Electronic Communications Infrastructure) Act 2010 (No. 2 of 2010) which regulates so-called premium rate services. These services are defined as:

A "premium rate service" means a service having all of the following characteristics:

- (a) it consists in the provision of the contents of communications (other than a broadcasting service) through an electronic communications network or by using an electronic communications service, which may include or allow the use of a facility made available to the users of the service;
- (b) there is a charge for the provision of the service which exceeds the cost attributable to communications carriage alone;
- (c) the charge referred to in paragraph (b) is paid by the end user of the service directly or indirectly to the provider of the electronic communications network or electronic communications service used in connection with the provision of the service by means of a billing or other agreed payment mechanism.

### **eSignatures Legislation**

#### *Electronic Commerce Act, 2000*

The Electronic Commerce Act 2000, which became law on 20 September 2000, implements the EU Directive on a Community framework for electronic signatures (1999/93/EC). The Act provides (with some exceptions) for the legal recognition of electronic signatures, electronic writing and electronic contracts. It authorises the use of encryption and sets the rights and obligations of Certification Service Providers (CSPs).

The Revenue Commissioners also provide a Revenue Online Service (ROS) for business customers and self-assessing tax payers. This system provides a means to file returns online, make payments by laser card, debit instruction or online banking (Online Banking applies to Income Tax only), obtain online details of personal/clients Revenue Accounts, calculate tax liability, conduct business electronically and claim repayments. The ROS service is based on qualified electronic signatures.

---

<sup>1</sup> See: <http://www.irishstatutebook.ie/2010/en/act/pub/0002/print.html>

## Computer Crime Legislation

### *Criminal Justice (Theft and Fraud Offences) Act 2001*

The unlawful use of computers is covered by the Criminal Justice (Theft and Fraud Offences) Act 2001:

(1) A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

(2) A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

### *Criminal Damages Act 1991*

The Criminal Damages Act of 1991 Section 5 describes unauthorised access of data:

(1) A person who without lawful excuse operates a computer (a) within the State with intent to access any data kept either within or outside the State or (b) outside the State with intent to access any data kept within the State, shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding €500 or imprisonment for a term not exceeding 3 months or both.

(2) Subsection (1) applies whether or not the person intended to access any particular data or any category of data or data kept by any particular person.

## Self-regulations

### *Self-regulatory Code of Conduct for the Responsible and Secure Use of Mobile Services*

The Irish mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Irish mobile electronic telecommunications market and complies with applicable European and national legislation.

### *Industry Self-Regulation in Ireland*

Currently in Ireland the Internet Service Providers (ISPs) operate under a self-regulatory format<sup>2</sup> in relation to illegal and harmful content on the Internet, based on an industry Code of Practice and Ethics which is overseen by the Irish Government.

The Office for Internet Safety has primary oversight responsibility in respect to reviewing and ensuring the appropriate operation of the code and the wider self-regulatory system.

---

<sup>2</sup> See information available at: <http://www.internetsafety.ie/website/ois/oisweb.nsf/page/regulation-en>

---

## **eIdentification/eAuthentication**

### *Electronic Passports*

In October 2006, the Passport Office in the Department of Foreign Affairs have started to issue the Irish electronic passport. The Irish electronic passports use a secure, contact-less electronic chip that can store encrypted digital information. The chip holds personal details pertaining to the holder, along with a digital image of the person's face.

The chip technology allows the information stored on an ePassport to be read by special chip readers at close range. The chip also incorporates digital signature technology to verify the authenticity of the data stored on it.

### *Public Service Cards*

Ireland is planning to deploy public service cards, likely for natural persons subject to Irish health care and social services.

Some non-PKI systems are used, such as the Reach Services portal (Irish tax and customs). It uses a single factor authentication mechanism, based on electronic registration using the Personal Public Service (PPS) number.

Also worth mentioning is the HealthLinkOnline application, which allows secure transfer of patient information over the internet between general practitioners (GPs) and acute hospitals.

## NIS Governance

### Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

<b>National Authorities</b>	<ul style="list-style-type: none"> <li>• Department of Communication, Energy and Natural Resources</li> <li>• ComReg (Commission for Communications Regulation)</li> <li>• National Centre for Technology in Education</li> <li>• MakeITsecure</li> <li>• Irish Information Security Forum (IISF)</li> <li>• Department of Justice, Equality and Law Reform</li> <li>• National Crime Council</li> <li>• Internet Advisory Board</li> <li>• Data Protection Commissioner</li> <li>• Department of the Taoiseach - Information Society Policy Unit (ISPU)</li> </ul>
<b>CERTs</b>	<ul style="list-style-type: none"> <li>• HEANET-CERT - Higher Education Authority Net CERT</li> <li>• IRISS CERT - Irish Reporting and Information Security Service CERT</li> <li>• Jumper CSIRT - Computer Security Incident Response Team of the company Jumper</li> <li>• POPCAP-CSIRT - Computer Security Incident Response Team of POPCAP Games</li> </ul>
<b>Industry Organisations</b>	<ul style="list-style-type: none"> <li>• ICT Ireland</li> <li>• Irish Software Association (ISA)</li> <li>• Irish Chapter of the Information Systems Security Association (ISSA)</li> <li>• Telecommunications and Internet Federation (TIF)</li> <li>• Irish Telecommunications Security &amp; Fraud Forum</li> <li>• Irish Internet Association (IIA)</li> <li>• Internet Service Providers Association of Ireland (ISPAI)</li> </ul>
<b>Academic Organisations</b>	<ul style="list-style-type: none"> <li>• University College Dublin, School of Computer Science and Informatics</li> </ul>
<b>Others</b>	<ul style="list-style-type: none"> <li>• HEAnet</li> <li>• Consumers' Association of Ireland (CAI)</li> <li>• IISAN</li> <li>• Irish Computer Society (ICS)</li> <li>• Irish Reporting and Information Security Service</li> </ul>

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"<sup>3</sup> – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory<sup>4</sup>.

**NOTE:** only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

<sup>3</sup> The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

<sup>4</sup> See: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

## Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Providers and public authorities work closely together on issues of resilience of public networks.

The Communications Sector, ComReg and major operators come together on a regular basis. They have formed working groups on different levels, such as CEO level or technical level. In the working groups, so called "Structured Exercises" are discussed, designed and done. For example, the working group dealing with technical issues designs and stress tests networks, and addresses these issues in desktop exercises.

Two industry committees have been set up in Ireland in the past twelve months. One is at CEO level and the other is at technical level. The technical committee meets at least every two or three months plus when needs arise such as incidents occur.

### Co-operation via the Data Protection Commissioner

The Data Protection Review Group of the Irish from the Data Protection Commissioner has published a consultation paper<sup>5</sup> to discuss a number of areas of the broad topic of data protection. The main regulatory options available are identified and interested parties are asked to provide comments thereon to assist the group reach a balanced conclusion on how Ireland should address the issue of the most appropriate legislative response to data breaches.

### IRISS CERT

The IRISS (Irish Reporting and Information Security Service) CERT provides services to all users within Ireland. It is an independent not for profit company limited by guarantee founded in 2008 to provide a range of free services to Irish businesses and consumers in relation to information security issues to help counter the security threats posed to the Irish businesses and the Irish Internet space.

IRISS is funded by a combination of donations and corporate sponsorship and is not state-funded. IRISS also serves as a WARP for the Irish SME sector and is called IE1WARP<sup>6</sup>.

### Fostering a proactive NIS community

All Irish CERTs included in this document are listed on Trusted Introducer: This will facilitate cooperation with other international CERT and CSIRT teams (although none of the CERTs are a member of FIRST).

---

<sup>5</sup> See the Consultation Paper of the Irish Data Protection Review Group available at: [http://www.justice.ie/en/JELR/Pages/DPRG\\_Consultation](http://www.justice.ie/en/JELR/Pages/DPRG_Consultation)

<sup>6</sup> <http://www.warp.gov.uk/directory-ie1warp.html>

## Country-specific NIS facts, trends, good practices and inspiring cases

### Security incident management

Since beginning of 2010, there were no major changes to the security incident management stakeholders in Ireland.

Providers in Ireland use to report security incidents on a case by case basis - the reporting is structured as follows:

- An initial report about the incidents;
- A progress report, and;
- After damages from the incident are resolved, a closure report issued.

The Communication Sector follows this reporting procedure quite closely but increased formalisation of this is going to be considered. The Communications Sector must inform ComReg of significant outage issues, but defining "significant" has not been finalised yet.

In general, the reporting is confidential. However, if the incident happened in the public domain, for example if a network was off, it could be made public by ComReg.

### Emerging NIS risks

Since beginning of 2010, there were no major new risks identified.

In May 2009 Irish ISP Eircom experienced an unprecedented volume of traffic deliberately directed at its network which caused difficulties for customers.

Although the theft of sensitive IT assets is now a high-priority issue for most Irish organisations data from the ISSA cybercrime survey 2008 indicates that many organisations have significant work remaining to fully encrypt data stored on laptop and desktop PC's. No revised report has been issued as of 2008.

### Resilience aspects

Compared with 2009, no changes with regards to resilience were noted.

In Ireland, no central repository of good practices on the resilience of public networks exists. Each operator is obliged to follow good practice, and operators and stakeholders are engaging in good practice. Though not formalised, a good practice repository among various stakeholders in the sector exists.

A new cross sector platform has been built in Ireland by using Tetra technology. This platform is completely independent of all other infrastructure and was put in place to be used by key officials should the country ever suffer an attack or denial of service which affects the standard platforms and networks.

## Privacy and trust

### Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented in Ireland by the Data Protection Act 1988 (the "1988 Act") as modified by the Data Protection (Amendment) Act 2003 (the "2003 Act") and the EC (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003 (collectively, the "DPA").

The competent national regulatory authority on this matter in Ireland is the Office of the Data Protection Commissioner (the "DPC").

### Personal Data and Sensitive Personal Data

The DPA only applies to personal data, defined as "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller". This definition is therefore closely based on the standard definition of personal data. In particular, it only applies to living individuals as opposed to legal entities. The DPC has endorsed the Opinion on Personal Data.

Under the DPA, sensitive personal data includes both: (i) the standard types of sensitive personal data; and (ii) information about criminal offences or criminal proceedings.

Sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. Additional legitimate processing conditions are set out in the 2003 Act. These include processing for statistical purposes, political activities, the collection of taxes, assessment of entitlement to social welfare benefits and processing that is authorised by regulations made by the Minister for Justice for reasons of substantial public interest.

### Information Security aspects in the local implementation of the Data Protection Directive

Data controllers and data processors must comply with the general data security obligations. No explicit breach notification obligation is imposed on data controllers or data processors under the DPA. However, the Irish Data Protection Commissioner (DPC) recommends voluntary notification and early engagement with his office in the event of a security breach.

### Enforcement

The DPC may launch investigations into possible contraventions of the legislation and has the power to seek an amicable resolution or issue a decision. The DPC has no power to issue fines in respect of contraventions. However, the DPC in exercising its investigation powers may issue an Enforcement Notice which is subject to a right of appeal by either party to the courts. Prosecutions for criminal offences may be brought by the DPC before the Irish courts, who may then impose fines. The DPC has the power to conduct comprehensive privacy audits of data controllers, as the DPC thinks fit, in order to ensure compliance with the DPA. Such audits are supplementary to investigations carried out in response to specific complaints. In 2007, 12 privacy audits of data controllers were carried out by the DPC.

The DPC may also issue a Prohibition Notice in order to prohibit the transfer of personal data from Ireland to a country or territory outside of the EEA. Such a notice may prohibit the transfer concerned absolutely or until the data controller/data processor concerned has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned. The data controller/data processor may appeal to the court against the prohibition in the notice within 21 days of service. It is an offence to refuse or fail to comply with a prohibition specified in the notice.

## NIS awareness at the country level

### Awareness actions targeting the consumers/citizens

The Irish national campaigns “make it secure” are run every two years in Ireland involving radio, TV and seminars. The aim of the campaign<sup>7</sup> is to ensure that using computers, broadband and the Internet is a positive experience by providing some basic information on the issues that may affect computer users. The key information security awareness topics relate to:

- Phishing;
- Identity theft;
- Social networking risks;
- Spyware and viruses risks.

A successful initiative from the Irish Awareness Centre is “think B4U click” – it urges students to take responsibility for their own online privacy. Results of the 2009 web survey<sup>8</sup> show that 45% of teens claim to use Internet messaging services every day or almost every day, compared to one-in-ten in 2006. The Irish Awareness Centre is participating in the 2010 EU Kids Online survey.

### Country-specific activities for identifying and promoting economically efficient approaches to information security

Ireland has launched an awareness campaign on Internet security and runs **the “make it secure campaigns”** every two years. The IRISS (Irish Reporting and Information Security Service) CERT provides services to all users within Ireland free of charge.

## Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

### EC CIIP Action Plan

Ireland’s main CERT, IRISS, participated in NEISAS<sup>9</sup>. The NEISAS project is engaging with stakeholders in the public and private sector who are addressing Critical Infrastructure Protection through trusted information sharing on vulnerabilities, threats and good practice solutions. These national communities, often called Information Exchanges (IEs), meet face to face at regular intervals but also have a need to share information electronically via a trusted platform.

NEISAS is creating a framework and prototype national platform which will also provide the capability for bilateral exchange at the European level between national platforms. an EC funded project that will enhance critical infrastructure protection by supporting the trusted sharing of security related information between and within Member States.

---

<sup>7</sup> See: <http://www.makeitsecure.org/en/index.html>

<sup>8</sup> See the Webwise 2009 Survey of Children’s Use of the Internet in Ireland available at: [www.webwise.ie](http://www.webwise.ie)

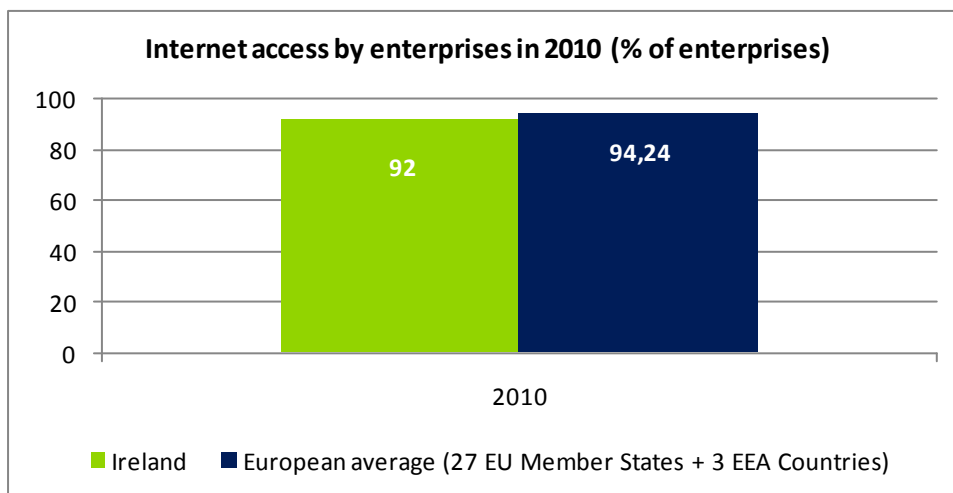
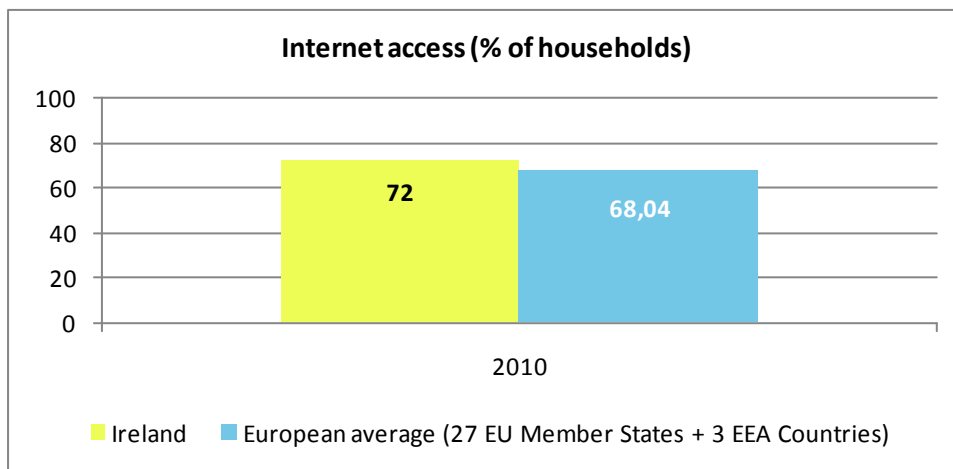
<sup>9</sup> <https://www.neisas.eu>

## Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Ireland, a series of relevant statistics are included in this section. Some of them indicate that the information society in Ireland is on par with the European average for most of the statistics listed below.

### Internet access of population and enterprises

The following graphs provide an overview of the situation<sup>10</sup> of Internet access in Ireland for enterprises and respectively households, relative to the European average.

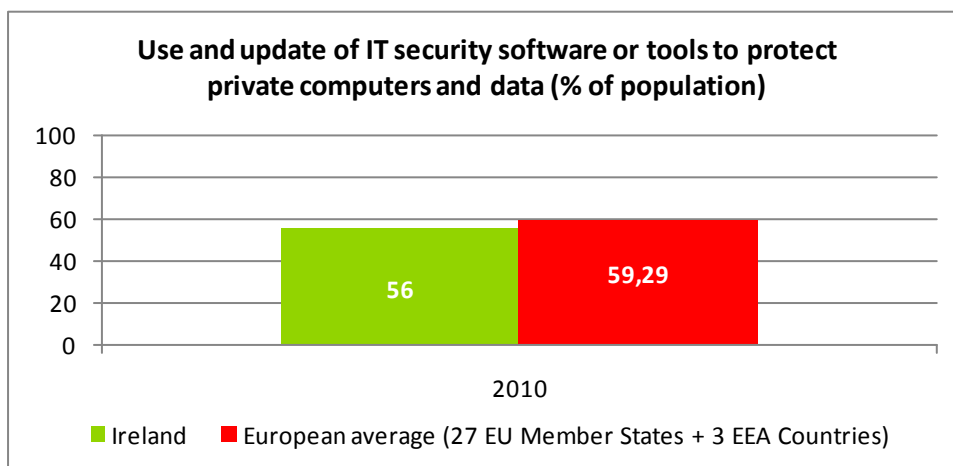
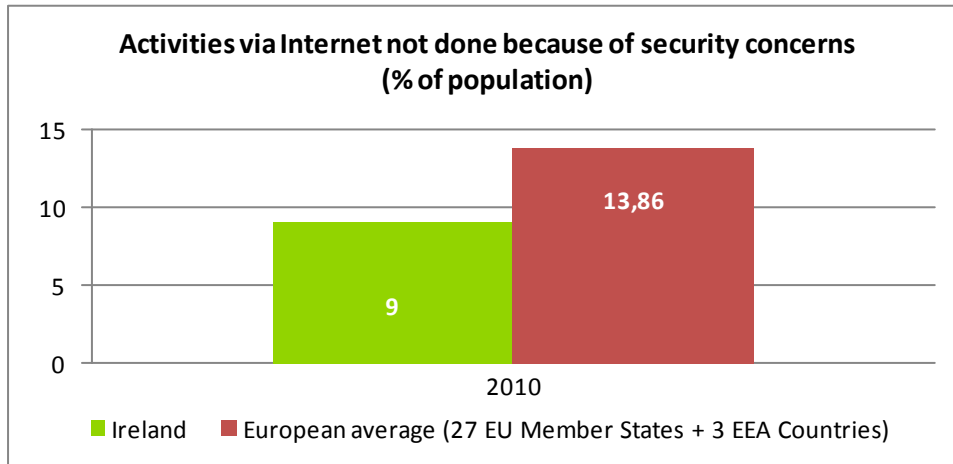


In 2010, the statistics indicate that the enterprises in Ireland have almost the same level of Internet access as the European average, while the households are slightly above the average.

<sup>10</sup> Source: Eurostat

### Statistics on use of Internet by individuals and related security aspects

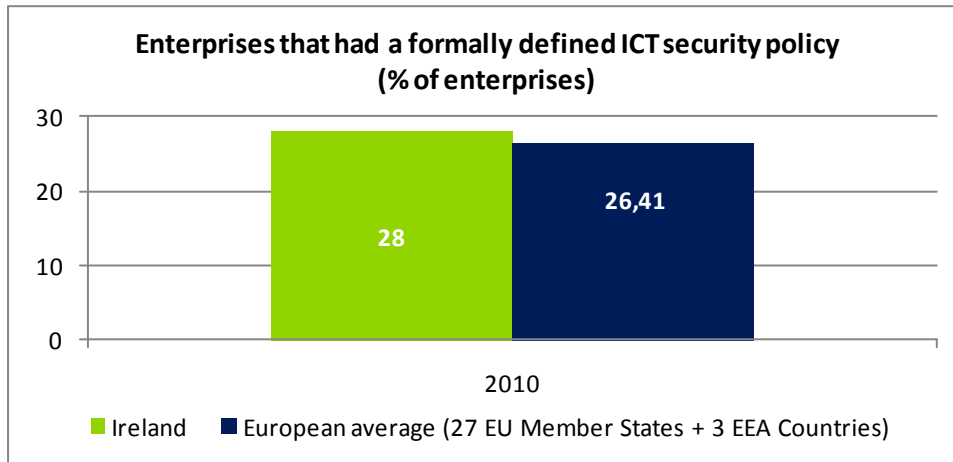
The percentage of population in Ireland that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is below the European average:



Meanwhile, it appears that the use of security tools to protect private computers and data is below the European average.

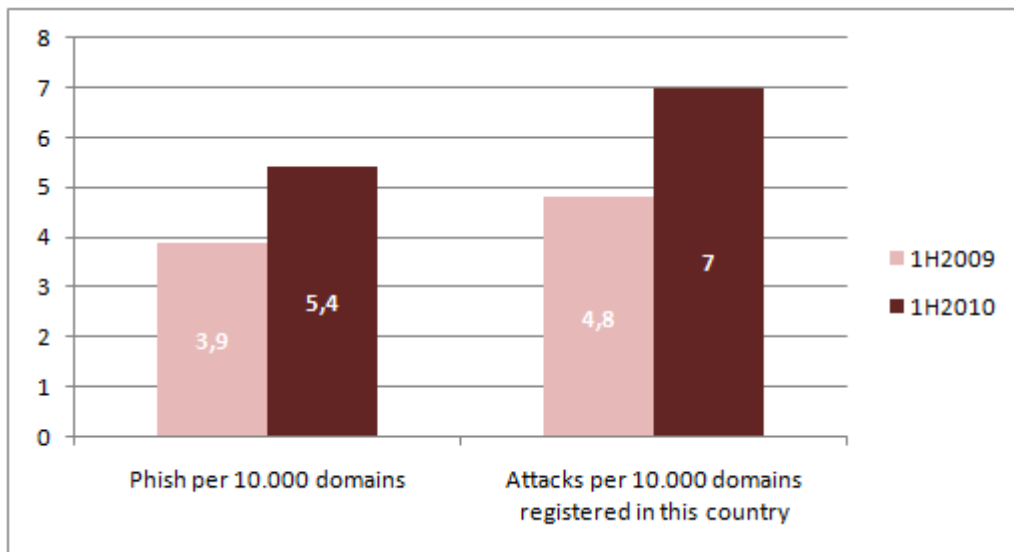
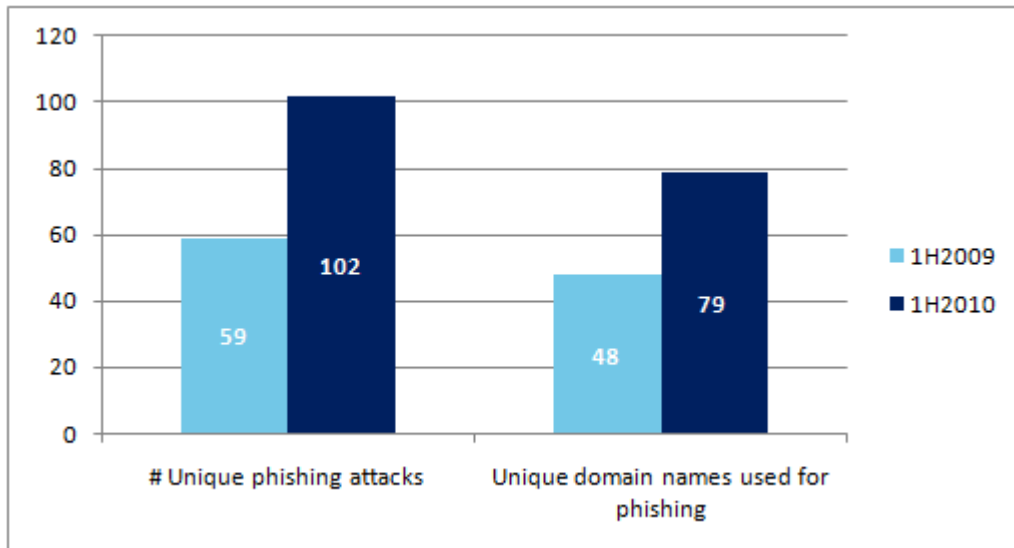
## Statistics on use of Internet by enterprises and related security aspects

More enterprises in Ireland have a formally defined ICT security policy, compared with their European peers.



## Other Statistics

It is interesting to also mention that during the 1<sup>st</sup> half of 2010, and respectively for the 1<sup>st</sup> half of 2009, Ireland was mentioned in the global report<sup>11</sup> published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



<sup>11</sup> See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_1H2010.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf)

## APPENDIX

### National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Department of Communication, Energy and Natural Resources	The Department of Communications, Energy and Natural Resources has responsibility for the Telecommunications, Broadcasting and Energy sectors. It regulates, protects and develops the Natural Resources of Ireland.	<a href="http://www.dcenr.gov.ie">www.dcenr.gov.ie</a>
2. ComReg - (Commission for Communications Regulation)	The Commission for Communications Regulation (ComReg) is the regulator for the electronic communications (telecommunications, radio communications and broadcasting) and the postal sector. The 2002 Communications Regulation Act sets out ComReg's statutory objectives. For the electronic communication sector these are to: <ul style="list-style-type: none"> <li>• Protect and inform consumers</li> <li>• Promote competition</li> <li>• Encourage innovation</li> </ul>	<a href="http://www.comreg.ie">http://www.comreg.ie</a>
3. National Centre for Technology in Education	The National Centre for Technology in Education is an Irish Government agency established to provide advice, support and information on the use of information and communications technology (ICT) in education.	<a href="http://www.ncte.ie">http://www.ncte.ie</a>
4. MakeITsecure	Provides awareness to the public on prevalent security issues, through to providing information and sources to counteract the risks.	<a href="http://www.makeitsecure.ie">http://www.makeitsecure.ie</a>
5. Irish Information Security Forum (IISF)	To improve the understanding and practice of information security within the business computer user community. Specific objectives are to: <ul style="list-style-type: none"> <li>• Facilitate the exchanging of information and sharing of experiences of mutual interest</li> <li>• Provide a focal point for the users of various information security products</li> <li>• Hold regular meetings and presentations on Information Security topics</li> <li>• Represent the views of IT Security practitioners on matters of public concern</li> <li>• Promote best security practice and standards</li> </ul>	<a href="http://www.iisf.ie">http://www.iisf.ie</a>
6. Department of Justice, Equality and Law Reform	The remit of the Justice family of agencies and services stretches across a range of human concerns. It touches on every aspect of national life from child protection and involvement in inquiries and tribunals to all elements involved in crime and punishment and the courts system, from the buying and selling of property to a range of immigration services and the areas of disability and diversity. On the international front, the Minister and the Department manage the interests of Ireland in relation to Justice and Home Affairs matters by participating fully in the European Union, the Council of Europe and the United Nations. The Office for Internet Safety is an Executive Office of the Department of Justice, Equality & Law Reform and takes responsibility for Internet safety in Ireland, particularly as it relates to children.	<a href="http://www.justice.ie">http://www.justice.ie</a> <a href="http://www.internetsafety.ie">www.internetsafety.ie</a>
7. National Crime Council	The council was established by the Minister for Justice, Equality and Law Reform. The Council has a broad mandate to provide a forum for the	<a href="http://www.irlgov.ie/crimecouncil">http://www.irlgov.ie/crimecouncil</a>

National authorities	Role and responsibilities	Website
	development, expression and contribution of a wide range of views on anti-crime strategies and policies and to raise public knowledge and awareness of crime.	
8. Internet Advisory Board	The IAB was established by the Minister of Justice, Equality and Law Reform in February 2000. The IAB assists and supports the Irish Internet Service Provider (ISPAI) industry to deliver an effective self-regulatory environment for internet content. The board also commissions research on internet downside issues and promotes awareness of internet safety, particularly with regard to children.	<a href="http://www.iab.ie">http://www.iab.ie</a>
9. Data Protection Commissioner	The Data Protection Commissioner is responsible for upholding the rights of individuals with respect to personal data. The Commissioner also has a role to play in the enforcement of Electronic Communications Data Protection and Privacy Regulations.	<a href="http://www.dataprotection.ie">http://www.dataprotection.ie</a>
10. Department of the Taoiseach - Information Society Policy Unit (ISPU)	The Information Society Policy unit (ISPU) part of the Department of the Taoiseach - has overall responsibility for developing, co-ordinating and driving implementation of the Information Society agenda. Our aim is to ensure that Ireland develops as a fully participative, competitive, knowledge-based Information Society, with all of the benefits that it entails.	<a href="http://www.taoiseach.gov.ie/eng/Department_of_the_Taoiseach/Policy_Sections/Knowledge_Society_and_eGovernment/About_the_Information_Society/">www.taoiseach.gov.ie/eng/Department_of_the_Taoiseach/Policy_Sections/Knowledge_Society_and_eGovernment/About_the_Information_Society/</a>

### Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> <li>FIRST<sup>12</sup> member</li> <li>TI<sup>13</sup> listed</li> </ul>	
11. HEANET-CERT	HEANET-CERT is the Higher Education Authority Net CERT. EAnet utilises the services of JA.net CSIRT to provide a single, trusted point of contact for our clients to deal with computer security incidents and their prevention. The aims of the service are to reduce the probability of successful attack, to reduce the direct costs of security to organisations and lower the risk of consequential damage. HEANET-CERT is: <ul style="list-style-type: none"> <li>Not a member of FIRST</li> <li>TI listed</li> </ul>	<a href="http://www.heanet.ie/services/cert">http://www.heanet.ie/services/cert</a>
12. IRISS CERT	IRISS CERT is the Irish Reporting and Information Security Service CERT. The Irish Reporting & Information Security Service (IRISS) is an independent not for profit company limited by guarantee founded in 2008 to provide a range of free services to Irish businesses and consumers in relation to information security issues to help counter the security threats posed to the Irish businesses and the Irish Internet space. HEANET-CERT is: <ul style="list-style-type: none"> <li>Not a member of FIRST</li> <li>TI listed</li> </ul>	<a href="http://www.iriss.ie/iriss/">http://www.iriss.ie/iriss/</a>
13. Jumper CSIRT	Jumper CSIRT is the Computer Security Incident Response Team of the company Jumper. Jumper CSIRT sells CERT services to its customers. HEANET-CERT is:	<a href="http://www.jumper.ie">www.jumper.ie</a>

<sup>12</sup> See: <http://www.first.org/members/teams/>

<sup>13</sup> See: <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> <li>FIRST<sup>12</sup> member</li> <li>TI<sup>13</sup> listed</li> <li>Not a member of FIRST</li> <li>TI accredited</li> </ul>	
14. POPCAP-CSIRT	<p>POPCAP-CSIRT is the Computer Security Incident Response Team of POPCAP Games.</p> <p>HEANET-CERT is:</p> <ul style="list-style-type: none"> <li>Not a member of FIRST</li> <li>TI listed</li> </ul>	<a href="http://www.popcap.com">www.popcap.com</a>

### Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
15. ICT Ireland	ICT Ireland is the voice of the information and communications technology sector in Ireland and represents over 300 companies. It is the representative lobby group for the high-tech or knowledge sector within the Irish Business Employers Confederation (IBEC) bringing together, among others, the Irish Telecommunications and Internet Federation (TIF) and the Irish Software Association (ISA).	<a href="http://www.ictireland.ie">www.ictireland.ie</a>
16. Irish Software Association (ISA)	The Irish Software Association (ISA) is a business association within IBEC for the Irish software, services and technology industry. The ISA is an affiliate association to ICT Ireland and IBEC. ISA has represented the interests of software and IT services companies in Ireland since 1978.	<a href="http://www.software.ie">www.software.ie</a>
17. Irish Chapter of the Information Systems Security Association (ISSA)	<p>The Information Systems Security Association is an international professional body for information security personnel.</p> <p>The ISSA / UCD Irish Cybercrime Survey is the result of a unique collaboration between the Irish chapter of ISSA and UCD's Centre for Cybercrime Investigation. This project is led by ISSA volunteers and conducted without any external funding, relying on the support of the Irish information security community.</p>	<a href="http://www.issaireland.org">www.issaireland.org</a>
18. Telecommunications and Internet Federation (TIF)	<p>The Telecommunications and Internet Federation (TIF) is the principal trade association for the electronic communications industry in Ireland. TIF is affiliated to ICT Ireland, the voice of technology within IBEC.</p> <p>The Regulatory Affairs Industry Group of TIF is active in monitoring the regulatory environment, at a domestic and at an EU level, for drafting legislation, laws and regulatory announcements of relevance to the sector in Ireland, and responding accordingly with the industry's position. Also, it responds to calls for consultation from ComReg on appropriate regulatory issues.</p>	<a href="http://www.tif.ie">www.tif.ie</a>
19. Irish Telecommunications Security & Fraud Forum	<p>The ITSFF has been established as an unincorporated association since April 1998 and has developed a reputation as an effective body operating in the field of telecommunication fraud and security issues within the industry.</p> <p>The Irish Telecommunications and Security &amp; Fraud Forum is affiliated to TIF.</p>	<a href="http://www.tif.ie">www.tif.ie</a>
20. Irish Internet Association (IIA)	<p>Areas of Activity: The Irish Internet Association is the professional body for those conducting business via the internet from Ireland. It has been and remains one of the driving forces behind the adoption of the medium. Established in 1997, the IIA provides leadership to</p>	<a href="http://www.iaa.ie">www.iaa.ie</a>

Industry Organisations	Role and responsibilities	Website
21. Internet Service Providers Association of Ireland (ISPAI)	<p>enterprises and society conducting business in Ireland.</p> <p>The Internet Service Providers Association of Ireland was formed in January 1998 by the leading Irish Internet Service Providers operating at that time. The aim of the association is to provide one voice for the Irish ISP industry at national, EU and International level. The ISPAI has agreed with the Irish government that a self-regulatory approach to the industry has greater opportunities for success and effectiveness. As part of this, the ISPAI established and funds the <a href="http://www.hotline.ie">www.hotline.ie</a> service to combat illegal content, especially child pornography, being hosted and distributed on the Internet. The ISPAI represents the industry on the Government's Internet Advisory Board.</p>	<a href="http://www.ispai.ie">www.ispai.ie</a>

### Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
22. University College Dublin, School of Computer Science and Informatics	<p>Areas of responsibility:</p> <ul style="list-style-type: none"> <li>• Knowledge Discovery: This theme deals with the application of machine learning techniques and other sophisticated algorithmic solutions to research in the sciences, industry and finance, extending to modelling and visualisation of phenomena.</li> <li>• Language and Cognition: This theme focuses on the modelling of cognitive phenomena relating to speech and language processing.</li> <li>• Software and Systems Engineering: This theme deals with the design and construction of large scale, distributed and embedded software systems, including sensor, autonomic and pervasive systems.</li> </ul> <p>Networks and Distributed Systems: This theme focuses on the design and optimisation of networks and distributed systems, including multimedia networking, mobile systems, and high-performance heterogeneous distributed systems.</p> <p>The University also has the UCD Centre for Cybercrime Investigation, which performs research and education activities in cybercrime and digital forensics.</p>	<a href="http://www.csi.ucd.ie">www.csi.ucd.ie</a>

## Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
23. HEAnet	HEAnet is committed to delivering, supporting and maintaining the most cost-effective and technically advanced solutions and services for national and international networking to meet the needs of its user community.	<a href="http://www.heanet.ie">www.heanet.ie</a>
24. Consumers' Association of Ireland (CAI)	A consumer organisation, its aim is to protect and educate consumers.	<a href="http://www.consumerassociation.ie">www.consumerassociation.ie</a>
25. IISAN	Part of the European 'Insafe' Internet safety network under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union.	<a href="http://www.webwise.ie/Contact.aspx">www.webwise.ie/Contact.aspx</a> <a href="http://www.webwise.ie">www.webwise.ie</a>
26. Irish Computer Society (ICS)	The Irish Computer Society was founded in 1967 as the national body for Information and Communication Technology (ICT) Professionals in Ireland. Since its foundation the ICS has promoted the continuous development of professional ICT knowledge and skills in Ireland by organising seminars, lectures and related activities.  The ICS represents the views of members to Government on topics of relevance, such as budgets and taxation, data protection, education and training. The Society is a nominating body for the Industrial and Commercial Panel of Seanad Éireann. ICS members serve from time to time on commissions, boards and committees appointed by government.	<a href="http://www.ics.ie">www.ics.ie</a>
27. Irish Reporting and Information Security Service	IRISS was set up by a private individual who works with the industry players to provide a range of high quality information security based services to aid Irish based organisations and citizens to better secure their information technology facilities and services in accordance with industry recognised standards and compliance requirements.	<a href="http://www.iriss.ie/iriss/">www.iriss.ie/iriss/</a>

## References

- The Consultation Paper of the Irish Data Protection Review Group available at: [http://www.justice.ie/en/JELR/Pages/DPRG\\_Consultation](http://www.justice.ie/en/JELR/Pages/DPRG_Consultation)
- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- ENISA, Information security awareness in financial organisation, November 2008, available at [http://www.enisa.europa.eu/doc/pdf/deliverables/is\\_awareness\\_financial\\_organisations.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf)
- Ireland - ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/ireland>

