

Italy 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

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: **Dan Cimpean, Johan Meire and Nicolas Roosens.**

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

ITALY	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	6
NIS GOVERNANCE	12
OVERVIEW OF THE KEY STAKEHOLDERS	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	13
FOSTERING A PROACTIVE NIS COMMUNITY	14
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	15
SECURITY INCIDENT MANAGEMENT	15
EMERGING NIS RISKS	15
RESILIENCE ASPECTS	16
PRIVACY AND TRUST	16
NIS AWARENESS AT THE COUNTRY LEVEL	17
RELEVANT STATISTICS FOR THE COUNTRY	19
INTERNET ACCESS OF POPULATION AND ENTERPRISES	19
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	20
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	21
OTHER STATISTICS	22
APPENDIX	23
NATIONAL AUTHORITIES ACTIVE IN NETWORK AND INFORMATION SECURITY	23
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	25
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	26
ACADEMIC BODIES ACTIVE IN NETWORK AND INFORMATION SECURITY	27
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	27
REFERENCES	28

Italy

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*
- *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

eGovernment Plan 2012

The President of the Council (Prime Minister) together with the Minister for Public Administration and Innovation unveiled the 'E-Government Plan 2012'¹ in January 2009. The Plan aims at promoting government innovation, spreading online services and reinforcing the accessibility and transparency of the Public Administration, so as to bring it closer to the needs of the citizens and the businesses. In 2010 no major update of the Plan has been identified. This Plan consists of 80 digital innovation projects structured around 4 intervention areas, namely:

- Sectoral, referring to Central Government and Universities;
- Local, covering either the Regions or their capitals;
- Structural, including infrastructure projects, e.g. projects for reducing the digital divide or for improving the accessibility of government services;
- International, to maintain Italy's major involvement in the European-scale networks focused on infrastructures, innovation and best practice dissemination.

The implementation of the Plan is being constantly monitored and its achievements are made public every three months. Citizens can follow the progress status of each planned project via the dedicated website www.e2012.gov.it. Here follows a brief description of the main projects and objectives listed in E-Gov 2012 on NIS:

- Digital interaction between schools and families - simplifying the communication schools/families by putting the main school documents online (e.g.: application for registration; electronic school reports and registers) and making the Internet, email exchange and SMS messages regular communication channels;
- Electronic passport and identity card - the police headquarters and the consulates will deliver the electronic passport with a microprocessor embedded to carry the holder's data and to prevent counterfeiting;
- A certified electronic mailbox for the citizens, the Public Administrations and the businesses with a view to digitise the exchange of documents between citizens/companies and the public authorities.

Strategic Plan for Innovation ("Piano Industriale dell'Innovazione")

The Minister for Public Administration and Innovation presented the Strategic Plan for Innovation in October 2008. Since then the Plan remains focus on the promotion of innovation through:

- Agreements with the central government;
- Agreements with the Regions and the Provinces (local government);
- Infrastructure programmes;
- Special projects.

Law and standards (amendments to the e-Government Code on issues such as the medical certificates online, electronic prescriptions, online advertising on institutional sites, the electronic

¹ See : <http://www.epractice.eu/en/document/288278>

identity card and the National services card, the VoIP -Voice over IP- and the Public Connectivity System -SPC).

The regulatory framework

The following Italian national regulations² have relevance and applicability in the domain of network and information security:

Decree of 6 May 2009 on the implementation of Law no.2/09

The Decree adopted by the Government (DPCM) on 6 May 2009 with the agreement of the Joint Conference State - Regions (Conferenza unificata Stato Regioni) defines:

- The procedures for delivering the certified electronic mailbox (PEC mailbox) to citizens;
- The procedures for activating the service via a tendering process, paying particular regard to the citizens at risk of exclusion (Article 8 of the e-Government Code);
- The use of the service and how to withdraw from it.

In 2010, no updates of the decree have been identified.

Law no. 2/09 of 28 January 2009

The law no. 2 of 28 January 2009 converts into law the Decree no.185 of 29 November 2008 which contains measures intended to overcome the economical crisis. The article 16-bis of the Decree states the following:

- Citizens receive a certified electronic mailbox (PEC box) upon request;
- The certified electronic mail is equivalent to a notification by regular mail as mentioned under the article 48 of the e-Government Code;
- The use of the certified electronic mail is free of charge for citizens;
- Each public administration uses the certified electronic mail for the communications with and the notifications to its employees (of the same public authority or a of a different one);
- The operating rules and the way of delivery of the certified electronic mailbox to the citizens are defined by a decree of the President of the Council of Ministers (DPCM), based on a proposal of the Minister for Public Administration and Innovation.

Since 2010 no updates of the law have been identified.

² Source: www.epractice.eu/en/document/288279. The same source was quoted in the case of several Italian laws mentioned in this section.

eGovernment Code

Adopted as a legislative decree on 7 March 2005 and published in the Italian Official Gazette on 16 May 2005, the e-Government Code ("Codice dell'Amministrazione Digitale") entered into force on 1 January 2006. It aims to provide a clear legal framework for the development of eGovernment and for the emergence of an efficient and user-friendly Public Administration.

Laying down a number of rules, obligations, recommendations and targets to promote the use of ICT in the public sector, it is intended to contribute to the removal of obstacles to further eGovernment development, such as "cultural difficulties" and "obsolete norms".

Among other things, the Code mainly mandates the public administrations to: share relevant information by electronic means in order to make life easier for citizens and businesses; make a minimum set of contents and services available on their websites, including a comprehensive organisation chart, an email directory, a list of eServices, the possibility to download forms and details on administrative procedures; communicate by email, namely for the exchange of documents and information; accept online payments from citizens and businesses (started in June 2007); use the electronic ID card and the National Services Card, as standard means of granting access to online services (starting on 1 January 2007).

This code was lastly amended by the Decree of 30 December 2010³ ("Decreto Legislativo 30 dicembre 2010, n.235"), published in the official journal on 10 January 2011. The Code furthermore grants citizens and businesses with the right to demand and obtain that public administration bodies use electronic means in their day-to-day relations with the users.

We notice also here that on 19 February 2010, the Italian Council of Ministers has approved the new version of the eGovernment Code proposed by the Ministry of Public Administration (PA) and Innovation.

This is one of the major steps towards achieving a new digital and simplified administration within the next three years, in compliance with the E-Gov Plan 2012. Following the reform of the Public Administration (legislative decree no. 150/2009), the new eGovernment Code will be the second pillar supporting the modernisation and digitisation of the Public Administration project.

The main novelties of the code regard: the re-organisation of the PA, the simplification of the PA's relationship with citizens and companies, the security of data exchange.

This is an important step towards the implementation of the eGovernment Plan 2012. Of particular interest are the Article 5-bis, 16 and 30 of the new Code:

- **Article 5-bis:** focuses on communication between businesses and the public administration. This article is important because for the first time, it is formalized in a law that the government and all actors exchanging data with them, are obliged to use ICT;
- **Article 16:** amending Article 23 of the old Code, states that an electronic document can be transformed into a similar document with the same evidential value, only if the analogue copy is attested by a public official;
- **Article 30:** speaks about the role of responsible for the electronic storage (Responsabile della conservazione sostitutiva). Another important role is the records and document manager ("Responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi").
- **Article 14:** this article amends the Article 21 of the old Code concerning the Digital Signature. In general the new Code introduces the advanced electronic signature concept

³ See: gazzette.comune.jesi.an.it/2011/6/6.htm

and modifies the definition of digital signature; on this basis advanced electronic signature may be used with the same legal effectiveness as qualified and digital signature.

Data Protection Code

The Data Protection Code⁴ was adopted as a legislative decree on 30 June 2003, and it entered into force on 1 January 2004. It replaces the previous Data Protection Law (Law no. 675/1996), as well as a number of other legislative and regulatory provisions.

The Data Protection Code has been meant to update, complete and consolidate Italy's data protection legislation since 1996 by introducing important innovations and conforming national legislation to European regulations, in particular the Data Protection Directive (95/46/EC) and the Directive on privacy and electronic communications (2002/58/EC).

In 2010 no major update of the Data Protection Code has been identified.

The code still aims to strengthen the data protection rights of individuals, allowing them to exercise their rights and instigate proceedings more easily. Individuals do not have to demonstrate that damage or distress has been caused as a result of a data protection breach; they merely have to demonstrate that their privacy has been breached.

The Data Protection Commissioner ("Garante Privacy") is in charge of supervising and enforcing the application of the Data Protection Code. In an effort to simplify the complaints process, the Commissioner has published a complaints form on its website.

Legislative Decree on Electronic Commerce

The Legislative Decree no. 70 of 9 April 2003 came into force on 14 May 2003. It regulates the use of electronic commerce means in Italy as well as the information that e-Commerce websites shall compulsorily provide to purchasers.

The Decree transposes the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Since 2010 no significant update to this decree has been monitored.

Electronic Communications Code

Adopted as a Legislative Decree on 31 July 2003, the Electronic Communications Code entered into force on 16 September 2003. It transposes four of the directives of the EU regulatory framework for electronic communications, the e-Privacy directive being transposed in the Data Protection Code. Since 2010 no significant update to this code has been monitored.

Decrees on certified electronic mail

With the Presidential Decree no. 68 of 11 February 2005⁵, emails transmitted through a certified electronic mail (Posta Elettronica Certificata – PEC) system have acquired legal validity.

Another decree, dated 2 November 2005, sets out the technical rules for the formation, the transmission and the validation of certified electronic mail.

⁴ Source: <http://www.epractice.eu/en/document/288279>. The same source was quoted in the case of several Italian laws mentioned in this section.

⁵ See: <http://www.epractice.eu/en/document/288279>

Legislative Decree no. 10 on Electronic Signatures

Italy has been among the first EU countries to give full legal value to electronic signatures. The Law no. 59 of 15 March 1997 on the simplification of the Public Administration provided in its article 15 that the use of electronic means would be legally valid for administrative procedures. Rules regarding the use of electronic signatures and documents were further detailed in a series of presidential and government decrees adopted between 1997 and 2001.

The Legislative Decree no. 10 of 23 January 2002 brought the Italian electronic signature regulations into line with the Directive 1999/93/EC on a Community framework for electronic signatures.

The eGovernment code defines a complete framework for the Digital Signature in Italy; as previously cited the code has been recently amended also in the articles concerning the digital signature.

Cybercrime legislation

In Italy computer crimes were introduced within the Criminal Code with by Act n°547 of 13 December 1993 concerning modification and integration of the Criminal Code and the Criminal Procedure Code involving cyber crime" (i.e. *Moficazioni ed Integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica*). The legislator did not create a specific section in the Penal Code for new issues, as has happened in some European countries.

Instead they were integrated using the old criteria. Computer system damages were incorporated near common damages, unauthorized access to computer or telecommunication systems near unauthorized access to private property, etcetera. Other criminal provisions related to ICT were introduced by Act. n° 269 of 3 August 1998 regarding Child pornography (i.e. *Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*), and Act. n° 438 of 15 December 2001 concerning conversion into Law, modifying D.L. n°364 of 18 October 2001, containing urgent provisions to combat international terrorism (i.e. *Conversione in legge del 18 ottobre 2001, n°374, recante disposizioni urgenti per contrastare il terrorismo internazionale*).

Last but not least is Legislative Decree n° 196 of 30 June 2003 that entered into force on 1 January 2004, the so called "data protection code", also known as the "Privacy code". It does not specifically concern cyber-crime, but some of its provisions refer to the telecommunications field.

The privacy code is divided into three parts:

- The first part sets out the general data protection principles that apply to all organisations;
- Part two of the code provides additional measures that will need to be undertaken by organisations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources;
- Part three relates to sanctions and remedies. It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice. Seven codes are planned (including surveillance, with particular regard to video surveillance, human resources, private investigators, and advertising/marketing) which will be developed in consultation with industry groups. The provisions relevant to us are in the second and third part, i.e. articles 167 and 130.

In Italy ICT crime investigations are lead by three main law enforcement bodies: the State Police (Polizia di Stato), the Carabinieri (Arma dei Carabinieri) and the Financial Guard (Guardia di Finanza).

Within the State Police there is a subsection dedicated to postal and communications crime (Polizia Postale e delle Comunicazioni), of which one particular section is devoted entirely to cyber crime investigation.

The Carabinieri have a subsection called the Carabinieri Scientific Investigations Group (Raggruppamento Carabinieri Investigazioni Scientifiche (Ra.C.I.S)), and its Telematics Section (Sezione Telematica) is entrusted with high tech crime investigations. The Financial Guard have the Special Technological Anti-Crime Cell (Nucleo Speciale Anticrimine Tecnologico).

Computer crimes, like any other common crimes, are judged by the Tribunal of First Instance (first court) and the Court of Appeal (appellate court). As a last possibly competent instance there is the Supreme Court (Corte di Cassazione), which rules only on points of law.

Guidelines for websites of public administrations

In 2010, the Ministry for Public Administration and Innovation, put online the guidelines⁶ concerning public administrations' websites ("**Linee guida per i siti web della Pubblica Amministrazione**", following the art. 4 of the Directive 8 / 09 of the Ministry for PA and Innovation). The objective of this project is to suggest criteria and tools for the rationalization of online content, and at the same time, the possibility of reducing the number of public websites that are considered obsolete. The goal is to provide accurate, timely and up to date information to citizens and businesses via the web. These guidelines will provide as well all public administrations with the main principles to discuss about innovative topics such as customer satisfaction, quality benchmarking between administrations, interactions with citizens. This will result in a continuous improvement of the quality of public websites.

Self-regulations

Self-regulatory Code of Conduct for Premium Services and Child Protection⁷

Mobile operators in Italy have signed the self-regulatory code of conduct for Premium Services and Child Protection.

Code of Practice for premium rate numbers in decade 4 – operative guidelines

The Italian 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 Italian mobile electronic telecommunications market and complies with applicable European and national legislation.

eIdentity

Italy uses a national ID card that is gradually being replaced by an e-ID card. This national ID card is mandatory for all the Italian citizens over the age of 15 as well as for foreigners mandated to reside in Italy. Italy also has a specification for smart cards, the National Service Card (CNS), aiming to ensure interoperability.

The authentication/attestation certificate in the e-ID card, issued through municipalities upon identification in person is based on PKI. The same goes for the authentication/attestation

⁶ Source: <http://www.epractice.eu/en/document/288277> and <http://www.innovazionepa.gov.it/comunicazione/notizie/2010/luglio/26072010-linee-guida-per-i-siti-web-della-pa.aspx>

⁷ Source: http://www.gsmeurope.org/documents/eu_codes/italy_child_protection.pdf

certificate in the CNS card and the authentication or signature certificate in the CMD (public servant card). The type of authentication mean is a hard crypto token.

In regards of future European interoperability, a small test was made with the Austrian e-ID scheme, through the STORK project. However, the results were mainly due to the flexibility of the Austrian system. Italy is also attendant in the Netcards⁸ project.

Italy is also active member of the European project STORK (Secure idenTity acrOss borders linKed) that is aimed at enabling businesses, citizens and government employees to use their national electronic identities in any Member State.

The consortium members include national authorities, non profit organisations, private companies and academic partners from: Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom and Iceland.

⁸ See: <http://netcards-project.com/web/frontpage>

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.

National Authorities	<ul style="list-style-type: none"> • Ministry of Economic Development – Communications Department – ISCOM (OCSI) • Ministry for Public Administration and Innovation • DigitPA (National Centre for Informatics in the Public Administration) • Italian Personal Data Protection Authority • Working Group on Critical Information Infrastructure Protection – Presidency of the Council of Ministers, Department of Innovation and Technology • Postal and Communication Police Service • National Technical Committee on Informatics Security – Presidency of the Council of Ministers, Department of Innovation and Technology • Network Security and Communications Protection Observatory • Department of Emergency Preparedness • Ministry of Interior • Communications Regulatory Authority (Agcom) • National Centre for Cybercrime and Protection of Critical Infrastructure (CNAIPIC) • Committee for the Diffusion of Broadband
CERTs	<ul style="list-style-type: none"> • CERT-IT • GARR-CERT • CERT-Difesa • CERT ENEL • CERT-RAFGV • GovCERT.IT • S2OC • SICEI-CERT
Industry Organisations	<ul style="list-style-type: none"> • ICT CE (Associazione Telecomunicazioni, Informatica ed Elettronica di Consumo) • AITech-Assinform • Clusit • Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) - Italian Association of IT Security Professionals
Academic Organisations	<ul style="list-style-type: none"> • Computer and Network Security Lab (LaSeR)
Others	<ul style="list-style-type: none"> • Accredia • ISACA Roma • ISSA IT • Association of Italian Experts in Critical Infrastructure (AIIC) • EASY • EDEN • OWASP IT • ISACA IT • Altroconsumo

For contact details of the above-indicated stakeholders we refer to the ENISA “Who is Who” – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁹.

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,

⁹ <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

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

Co-operation between national authority bodies

Italy does not have a single institution recognized among NIS stakeholders as the national security agency; there are various organizations sharing the responsibilities and competencies concerning the classified information. The Ministry of Economic Development acts as the institution from among all NIS stakeholders in Italy as the one responsible for coordinating the development and implementation of national information security strategy.

Italy is committed to data protection and ensuring compliance in this regard. Italian Personal Data Protection Authority ensures compliance with the Privacy Directive. It is accountable to the Italian Parliament, which has established its powers, defined its statutes and elected its members.

Additionally, Italy has a working group on critical information infrastructure protection, established in 2003 as part of the Prime Minister's Office, and composed of representatives from Government departments and agencies, and private sector operators. The country hosts a number of conferences on NIS - events organized prevalently by industry professionals and associations.

Other co-operation of NIS stakeholders to combat spam and malware

Cooperation between governmental bodies is in place¹⁰. Five years ago, a permanent observatory group for security and protection of networks and communications was created by the Minister of Communications, the Minister of Justice and the Minister for Internal Affairs. It has generic competences to verify the state of the art regarding network security, including the risks linked to malware and spyware attacks. Up to now the group has performed mainly research activities, as it does not have any real power to enforce legal bans.

The national DPA and the police of communications collaborate on a regular basis to stop and prevent criminal activities involving spam and spyware.

There is also cooperation between government and industry: the working group on privacy, phone interceptions and spam of the national ISPA has the duty to collaborate with the national DPA and to manage the relationships between the two entities. At the international level, the national DPA participates in the CNSA on behalf of Italy.

In terms of e-Security, new forms of cooperation have been established in 2010 between the Postal Police (*Polizia Postale*) and Symantec (leader in building security software for computers), and between the Postal Police and Facebook.

The Postal Police has signed an agreement to promote joint initiatives with Symantec¹¹. In 2010, the Postal Police reported 819 people for crimes related to e-Commerce and 37 were arrested. Of great significance was the number of people reported for hacking - equal to 2,913 with 76 arrested - and those for child abuse crimes - 475 reported and 51 arrested. The agreement is also

¹⁰ Source:

http://ec.europa.eu/information_society/policy/ecommerce/doc/library/ext_studies/privacy_trust_policies/spam_spware_legal_study2009final.pdf

¹¹ See: http://poliziadistato.it/articolo/20318-Lotta_al_crimine_informatico_accordo_tra_Polizia_e_Symantec

highlighting the effort made to achieve synergies between the public and the private sector to fight on line crimes.

Guidelines have also been established between the Italian Postal Police and Facebook Security members¹². The goal was to build a system of rules and structure of the site that encourages people to use real names and discourage criminal behaviours. The idea was to develop an effective operational process to eliminate spam and to be able to block users not complying with rules.

Fostering a proactive NIS community

No relevant information has been identified on this particular topic.

¹² <http://www.pubblicaamministrazione.net/e-government/news/2535/reati-online-accordo-polizia-postale-e-facebook.html>

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

Security incident management

Since 2003, a permanent observatory group for security and protection of networks and communications was created by the Minister of Communications, the Minister of Justice and the Minister for Internal Affairs. It has generic competences to verify the state of the art regarding network security, including the risks linked to malware and spyware attacks.

Up to now, the group has performed mainly research activities, as it does not have any real power to enforce legal bans. The national DPA and the police of communications collaborate on a regular basis to stop and prevent criminal activities involving spam and spyware.

Computer crimes, like any other common crimes, need to be reported to the competent authority before being prosecuted. This competent authority is the Public Prosecutor (Procura della Repubblica). The Public Prosecutor directs investigations and delegates the competent police section to execute the necessary measures.

Emerging NIS risks

Since the beginning of 2010, there were no major changes to the NIS risks identified previously.

The Università degli Studi di Napoli Federico II (Napoli) is an active partner in the FORWARD¹³ initiative of the European Commission to promote the collaboration and partnership between academia and industry in their common goal of protecting Information and Communication Technology (ICT) infrastructures.

The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defenses, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures.

No relevant information was identified on the participation of Bulgarian CERT, ISPs, etc., in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviours and Attack Threats (WOMBAT)¹⁴.

No other specific input was identified at this stage based on Italian relevant NIS sources.

¹³ See: <http://www.ict-forward.eu/home>

¹⁴ See: <http://www.wombat-project.eu/>

Resilience aspects

At the exception of the workshop¹⁵ on experimental platforms for Internet resilience, security and stability research facilitated two year ago by the Joint Research Centre¹⁶, on the need to create experimental platforms suitable for conducting empirical security research, no major resilience activities have been noticed in 2010. Such experimental platforms are expected to enable:

- Researchers to use rigorous scientific methods for studying vulnerabilities, threats, systemic faults, potential malicious actions, etc;
- Operators and technology providers to try new systems under different security scenarios;
- Authorities to better understand the security implications of the Internet infrastructure and the related applications.

No other specific input was identified at this stage on resilience aspects.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive was originally implemented by the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data Act (No. 675 of 31 December 1996) ("Law no. 675/96"). However, Law no. 675/96 has now been replaced by the Consolidation Act regarding the Protection of Personal Data (Data Protection Code - Legislative Decree No. 196 of June 30 2003) (the "DPC").

The competent national regulatory authority on this matter is the Italian Data Protection Authority: the "Garante per la protezione dei dati personali", or the "Garante". Since 2010 no updates on the implementation of the Data Protection Directive have been noticed.

Personal Data and Sensitive Personal Data

The definition of personal data in the DPC is based on the standard definition of personal data and also applies to data relating to legal entities, bodies or associations.

Sensitive data may be processed only with both the data subject's written consent and prior authorisation from the Italian Data Protection Authority (though there are exceptions for religious bodies and trade unions). For this purpose, the Italian Data Protection Authority has issued several general authorisations to the processing of sensitive data.

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

In addition to compliance with the general data security obligations, the Italian Data Protection Code requires, under criminal sanction, the implementation of specific technical, logical and organisational minimum security measures set forth by a "Disciplinare Tecnico" - "Technical Specifications".

¹⁵ See: http://sta.jrc.it/pdf/scni/ExperimentalPlatforms/ToR_WS_20090619.pdf

¹⁶ See the information on the Institute for the Protection and the Security of the Citizen, at: www.jrc.org

Enforcement and Data protection breaches

The Italian Data Protection Code does not contain any obligation to inform the Italian Data Protection Authority or data subjects of a security breach.

With regard to any breach of the DPC provisions, the data subject may apply either to the Garante or ordinary Court. The Garante may order the stop of the data processing or lay down conditions for the processing. Furthermore, the Garante may impose sanctions or administrative fines. In the event of crimes, the Garante has an obligation to inform the relevant criminal authorities.

Compensation for damages can be requested from the Civil Courts. The Garante has powers of investigation and can also use the Financial Police ("Guardia di Finanza"). Here also no major changes have been identified since 2010.

NIS awareness at the country level

Italy can be considered as a country where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software.

As an overall assessment, it is allowed to say that Italy is in a good position in combating online malpractices. There have been successful prosecutions in spam related cases and the Italian Data Protection Authority recently imposed relatively high fines. Also the DPA cooperates with the police and the national ISPA and participates in the CNSA at international level. Several ISPs offer to their clients spam filters or other security tools. Therefore, a lot of work has been done so far.

However, what seems to be compelling is the rationalisation and simplification of the existing legislative sources (especially in the criminal field: in other words, there are several laws that set criminal sanctions but these rules seem to be often not fully consistent, and therefore there are problems when they have to be applied to real cases) and of the enforcement powers of the relevant authorities. Sometimes, in fact, it is not very clear who is competent for what, and some clarifications by the lawmaker would undoubtedly render the work performed by the Privacy Authority and the Competition Authority more effective¹⁷.

Awareness actions to combat malware

Administrative decisions – The Italian Data Protection Authority issued an order to clarify the content of legislative provisions in the area of spam. It also issued a number of decisions in the field of spamming, ordering to stop the sending of spam via e-mail/SMS without consent, to stop the use of personal data and/or to provide the claimant with information about the processing of his personal data. In a case where the order was not followed, the DPA denounced the company in question to the competent prosecutor.

Awareness measures – The Police of Communications set up a website where citizens and enterprises can get information about illegal activities that take place on the Internet (including spam, malware and spyware).

Complaint channels – Via the website of the Police of Communications, victims can report cybercrimes. It is not possible to file an online complaint with the national DPA. This must be done

¹⁷ Source:

http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_sp_ware_legal_study2009final.pdf

via regular mail. The completion authority offers a toll free phone number for the reporting of aggressive commercial practices, including spam.

Measures have also been undertaken by the service provider industry: Several ISPs offer to their clients spam filters or other security tools. Telecom Italia, for instance, offers a 'total security' service to its clients against payment of a small fee of around 4 euro/month. This offers extensive protection against spam, viruses, spywares, etc.

Following the traces provided by the ENISA's "Information Package: Raising Awareness in information Security - Insight and Guidance for Member States", the partnership between CNIPA, CASPUR and the "Master in Information Security" is aimed to realize a multimedia project to broadcast guidelines for a conscious and secure utilization of the Internet, as a useful instrument for news, entertainment, communication and other useful and diversified services. Notably, the project is meant to fill the gap between citizens and new technologies, documented in other ongoing projects¹⁸.

Awareness actions targeting the consumers/citizens

Working within the Safer Internet programme and co-funded by the European Commission, since 2004. Adiconsum and Save the Children have been promoting EASY, a national awareness-raising campaign on safe and responsible internet and mobile phone use among young people. Since the 1st of January 2007, EASY has become the Italian Awareness Centre with the following objectives:

- To promote safe and responsible use of new media by children and adolescents;
- To promote a culture based on respect for children using the most diffused technologies, in accordance with the principles sanctioned by the UN Convention on the Rights of the Child.

The centre addresses pre-adolescents, parents and teachers, but its public awareness-raising task is actually much wider in scope, extending also to dealings with institutions, the media and the ICT industry, so that it comprises all the spheres that directly or indirectly impact young people's appropriate use of technological tools, reminding each of them of their specific responsibilities in this area.

A strong network of national stakeholders supports the awareness centre and ensures the dissemination of surveys, educational materials, information and advice. The Italian Awareness Centre coordinates the Italian celebration of Safer Internet day and cooperates with a large group of stakeholders on a variety of other campaigns¹⁹.

As a conclusion, we notice here that no major changes have been brought since 2010.

¹⁸ See the source:

http://ec.europa.eu/information_society/policy/ecommerce/doc/library/ext_studies/privacy_trust_policies/spam_sp_ware_legal_study2009final.pdf

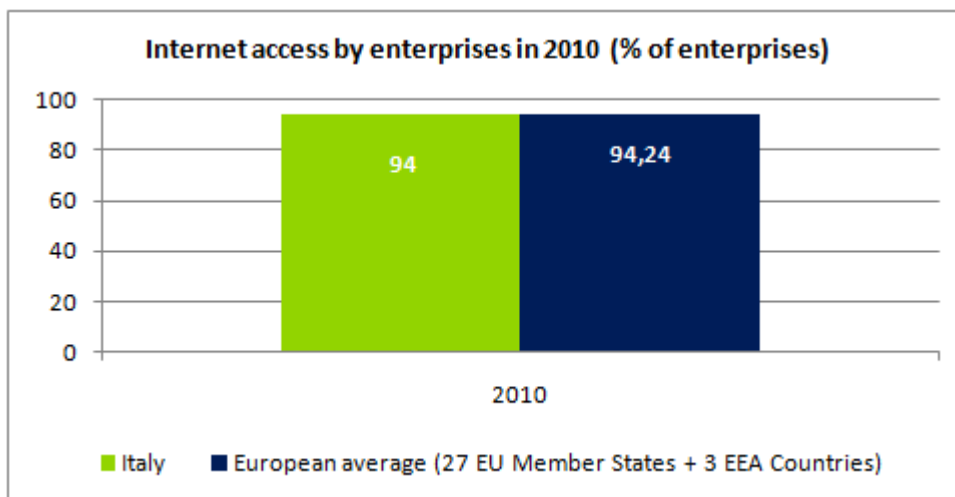
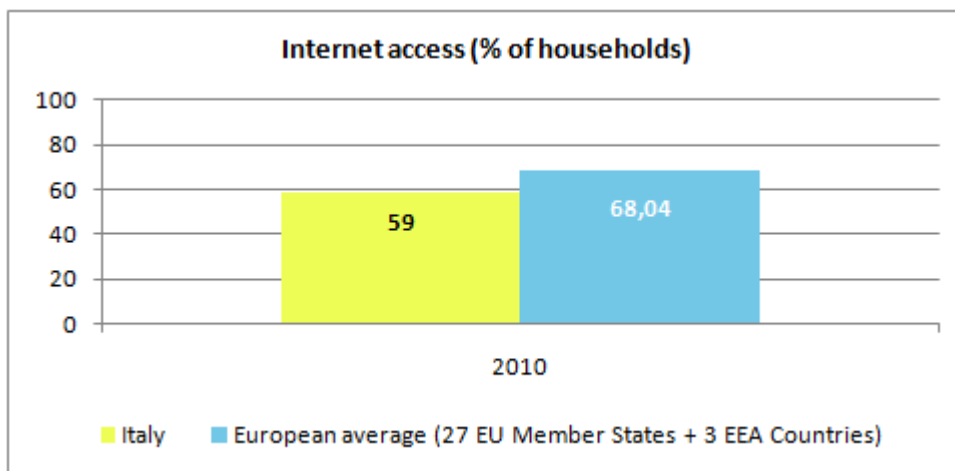
¹⁹ See: http://www.saferinternet.org/web/quest/centre/-/centre/italy?p_p_lifecycle=1&p_r_p_1607082367_country=Italy

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Italy, a series of relevant statistics are included in this section. Some of them indicate that the information society in Italy still needs some improvement, while others show progress and interesting trends.

Internet access of population and enterprises

The following graphs provide an overview of the situation²⁰ of Internet access in Italy for enterprises and respectively households, relative to the European average.

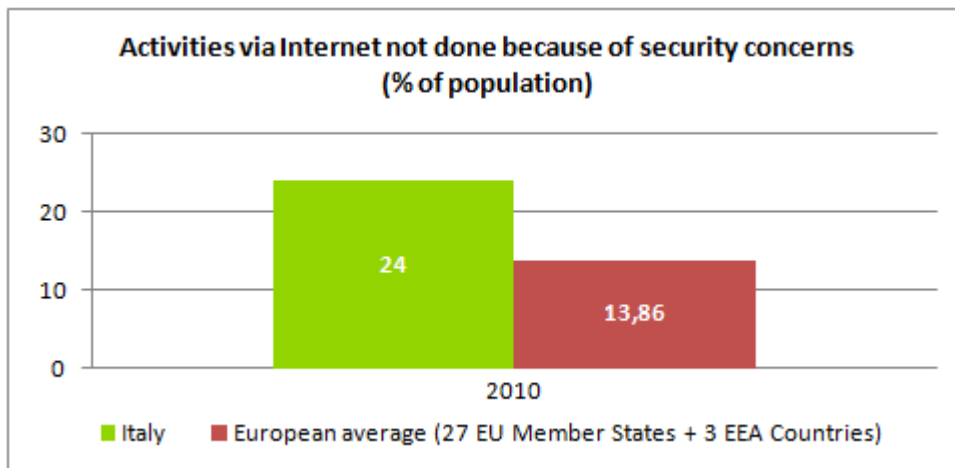


In 2010, the statistics indicate that the enterprises in Italy have the same level of Internet access as the European average, while more effort is required to close the gap on the households.

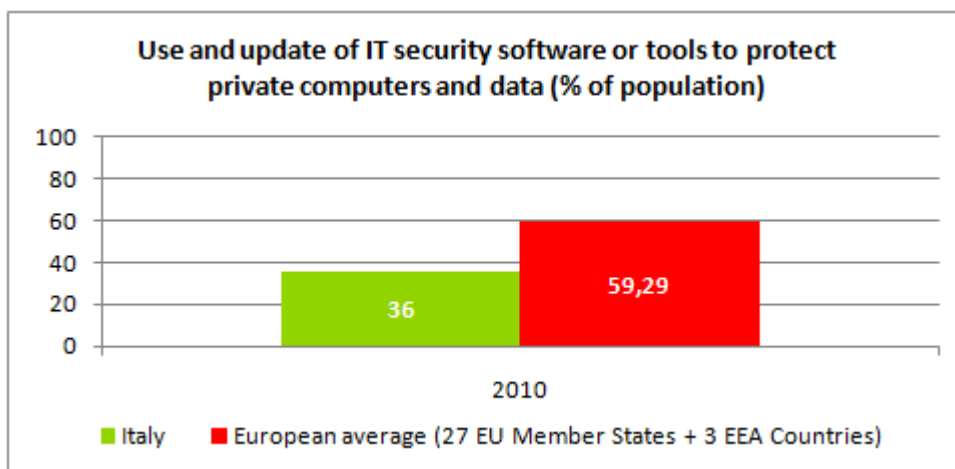
²⁰ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Italy 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 almost twice the European average:



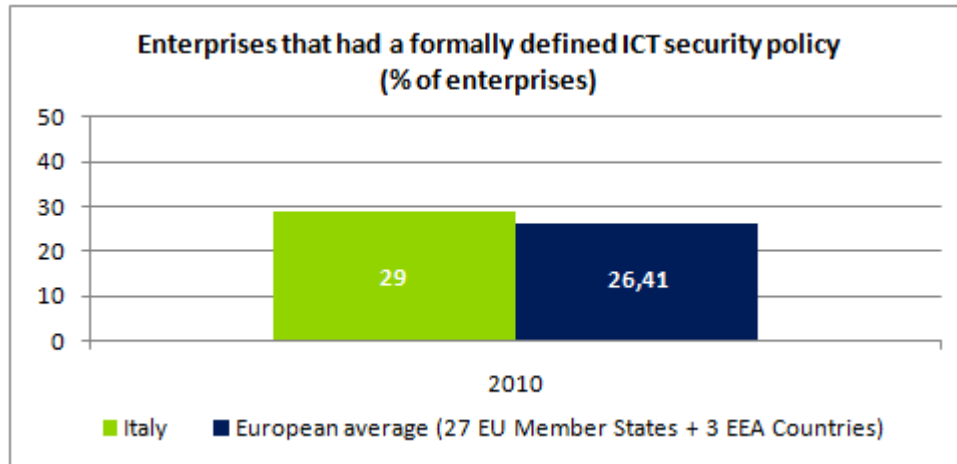
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



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

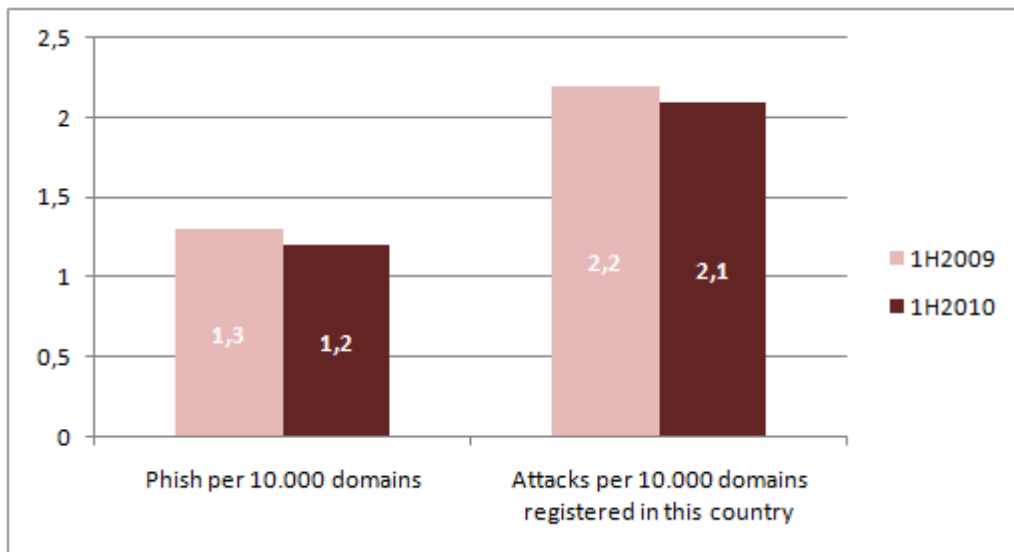
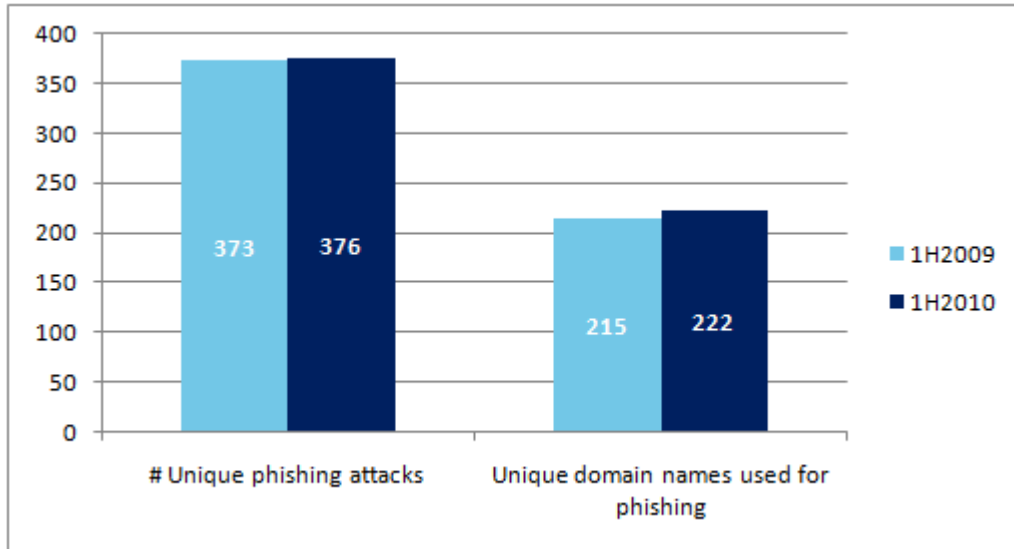
Statistics on use of Internet by enterprises and related security aspects

More enterprises in Italy have a formally defined ICT security policy, compared with their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Italy was mentioned in the global report²¹ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



²¹ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities active in network and information security

National authorities	Role and responsibilities	Website
1. Ministry of Economic Development – Communications Department	<p>The functions of the former Ministry of Communications and its inherent financial, material and human resources have recently been transferred to the Ministry of Economic Development.</p> <p>The Ministry of Economic Development:</p> <ul style="list-style-type: none"> • Supervises postal, financial products and telecommunications services; • Acts as a regulator, coordinator, supervisor and controller; • Represents the government at community and international meetings; • Examines and considers the evolution of opportunities in post and telecommunications, in economic, technical and legal terms at national and international levels; • Takes and publishes technical measures regarding the type of approval and the use of terminal apparatus to be connected, directly or indirectly, to telecommunications networks, granting relevant licences; • Approves telecommunications apparatus; • Grants licences, authorisations and permission, adopting the relevant provisions taking great care of their observance; • Determines technical regulations, considering both users' interests and service quality levels; • Arranges plans for the granting and allocation of radio frequency, granting and allocation, ensuring that these plans are observed. <p>ISCOM (Superior Institute for Communication and Information Technology) operates within the Ministry of Economic Development – Communications Department as research and technical body. It acts also as notified body under directive 1999/5/EC.</p> <p>OCSI is a division of ISCOM. It is the National security certification and accreditation body. It manages common criteria and ITSEC security certifications and acts in a mutual international recognition agreement framework, namely CCRA and SOGIS. The DPCM 10 february 2010, published in the Italian Official Gazette on 28 april 2010 designates OCSI as unique body for the assessment of the Hardware Security Module (HSM) devices related to their use in the digital signature . In particular OCSI is committed to verify the compliance of HSM devices to the requirements laid down in the Annex III of the 1999/93/EC Directive</p>	<p>www.comunicazioni.it www.sviluppoeconomico.gov.it</p> <p>www.isticom.it</p> <p>www.ocsi.isticom.it</p>
2. Ministry for Public Administration and Innovation	<p>The Ministry has been delegated to act on behalf of the Prime Minister in the areas of technological innovation, development of the information society and related innovations for government, citizens and businesses.</p>	<p>www.innovazionepa.gov.it</p>
3. DigitPA (National Centre for Informatics in	<p>It provides technical support to the Ministry for Innovation and Technologies. Its main technical</p>	<p>www.digitpa.gov.it</p>

National authorities	Role and responsibilities	Website
the Public Administration)	areas are: PKI, electronic signatures, ICT awareness, e-government.	
4. Italian Personal Data Protection Authority - Il Garante per la Protezione dei Dati Personali	Italian personal data protection authority.	www.garanteprivacy.it
5. Working Group on Critical Information Infrastructure Protection — Presidency of the Council of Ministers, Department of Innovation and Technology	Established in 2003 as part of the Prime Minister's Office. The Working Group is composed of representatives from government departments and agencies, as well as private sector operators involved in the management and control of national critical infrastructure.	No website available
6. Postal and Communication Police Service	Established in 1998, the Postal and Communication Police Service has field offices and units operating throughout the Italian territory. Its main activities concern the prevention of and response to computer crime and audiovisual piracy, cop-right protection, protection of postal services. It also acts as a national contact point for transnational emergencies connected with computer crimes in conformity with the specific G8 24/7 network.	http://www.poliziadistato.it/articolo/459-Polizia_postale
7. National Technical Committee on Informatics Security — Presidency of the Council of Ministers, Department of Innovation and Technology	Established in 2002 by the Ministry of Communication and Innovations and Technology Department, the committee is responsible for improving the informatics security of public bodies and for defining their nationwide ICT security plan.	No website available
8. Network Security and Communications Protection Observatory	Established in 1998, the observatory is made up of members from the Ministry of the Interior, Ministry of Communications and Ministry of Justice. The Internet sub-group deals with investigative and judicial matters relating to the Internet.	No website available
9. Department of Emergency Preparedness	The department is responsible for coordinating all initiatives in the event of a crisis.	http://www.protezionecivile.it
10. Ministry of Interior	Oversees aspects as national security, electronic identity (Electronic Passport), and Intelligence and Cybercrime policies.	http://www.interno.it/mininterno/export/sites/default/it/
11. Communications Regulatory Authority (Agcom)	The Communications Regulatory Authority (Agcom) is an independent authority, established in July 1997. Agcom is first and foremost a "guarantor". The two main tasks assigned to it: <ul style="list-style-type: none"> • To ensure equitable conditions for fair market competition; • To protect fundamental rights of all citizens in Italy. 	www.agcom.it
12. National Centre for Cybercrime and Protection of Critical Infrastructure (CNAIPIC)	Unit of the Postal and Communications Police Service specialized against attacks directed towards Critical Infrastructures.	No website available
13. Committee for the Diffusion of Broadband	Regional Affairs and Local Autonomies, and Public Administration and Innovation) is to identify the main Public actions needed to promote the diffusion of Broadband services over the Italian territory and to monitor the evolution and availability of those services; to coordinate different projects run out by single Regions; to set guidelines and provide technical recommendations for those projects.	www.comitatobandalarga.it

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST²² member • TI²³ listed 	
14. CERT-IT	<p>CERT-IT is the Italian Computer Emergency Response Team and was founded in February 1994. CERT-IT is a non profit organisation mainly supported by Dipartimento di Informatica e Comunicazione (DICO), Università degli Studi di Milano. CERT-IT became a member of the International Forum of Incident Response and Security Teams (FIRST) in 1995, as the first Italian CERT to be admitted.</p> <p>The main goal of CERT-IT is to contribute to the development of security culture in the computer world, in particular the Italian computer world.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: yes. 	http://security.dsi.unimi.it
15. GARR-CERT	<p>GARR-CERT is the Computer Emergency Response Team for GARR, the Italian Academic and Research Network. It deals with computer and network security incidents.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: yes. 	www.cert.garr.it
16. CERT-Difesa	<p>The CERT-Difesa mission is to assist the national army in protecting the communication networks and promoting the sharing of information around IT security.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: no. 	www.cert.difesa.it
17. CERT ENEL	<p>CERT ENEL is the reference in the Enel group for all problems related to ICT security. Services are provided solely within the company and seek to minimize information risk by ensuring compliance to the legal requirements, corporate standards and international best practices.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: no. 	www.enel.it/attivita/servizi_di_oversificati/informatica/cert
18. CERT-RAFVG	<p>CERT-RAFVG was born in 2005 following the acquisition by the Regione Autonoma Friuli Venezia Giulia, Insiel SpA. CERT-RAFVG acts as a reference point for the activities of cyber security within the region, and as a single contact point of the various components involved in the management of this problem. CERT-RAFVG work in various areas of IT Security to ensure the protection and security of information.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: no. 	http://cert-rafvg.regione.fvg.it
19. GovCERT.IT	<p>GovCERT.IT is the public administration computer emergency response team.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: no. 	www.cert-spc.it
20. S2OC	<p>CERT established and controlled by Telecom Italia Group.</p>	www.tuconti.telecomitalia.it
21. SICEI-CERT	<p>Computer Emergency Response Team, responsible for IT security related to Italy's Dioceses.</p> <ul style="list-style-type: none"> • First member: no; • TI listed: no. 	http://cert.chiesacattolica.it

²² See: <http://www.first.org/members/teams/>

²³ See: <http://www.trusted-introducer.nl/>

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
22. ICT CE (Associazione Telecomunicazioni, Informatica ed Elettronica di Consumo)	Association bringing together Italian Industry active in telecommunications, informatics and consumer Electronics. Its responsibility is to represent the electronic enterprises that operate in Italy.	www.ict-ce.it http://www.anie.it
23. AITech-Assinform	AITech-Assinform is the Italian association of ICT companies and an affiliate of Confindustria (Confederation of Italian Industry). AITech-Assinform member companies are suppliers of: <ul style="list-style-type: none"> • Both hardware and software; • Bespoke software development and software customisation services; • Installation and maintenance services; • Technical, application and management support and consultancy services; • Training services; • Outsourcing services; • Network services; • Multimedia content. 	www.assinform.it
24. Clusit	Clusit was born based on the experiences of other leading European information security associations such as Clusib (B), Clusif (F), Clusis (CH) and Clussil (L). Clusit aims to: <ul style="list-style-type: none"> • Raise computer security awareness among companies, public administrations and citizens; • Participate and contribute to the development of laws, practical codes, correct behavior in computer security both at national and international levels; • Contribute to the definition of learning programmes and of certifications for computer security professionals; • Promote the adoption of methodologies and technologies which can contribute to improving information infrastructure security at all levels. 	www.clusit.it
25. Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) - Italian Association of IT Security Professionals	AIPSI is a non-profit association founded in 2005 with the scope of representing the community of Italian security professionals. It is the Italian delegate of ISSA (Information Systems Security Association) that counts more than 13.000 associates in 100 organizations around the world. AIPSI activities are: organization of educational forum, documents publication, interactions and links between security experts in order to improve their knowledge, promotion of the correct management of security in public and private organizations.	www.aipsi.org

Academic bodies active in network and information security

Academic Organisations	Role and responsibilities	Website
26. Computer and Network Security Lab (LaSeR)	LaSeR is a research structure of the Dipartimento di Informatica e Comunicazione, at the Università degli Studi di Milano, Italy. The research focus is on applied computer security. In particular, their interests range from vulnerability analysis (both in web applications and executable code) to malware analysis and intrusion detection.	http://security.dsi.unimi.it
27. Università degli Studi di Napoli Federico II	The university is made up of three divisions (Poli), which operate as semi independent bodies for the teaching and research management of 13 schools and 82 departments grouped, within each division, according to academic and research profiles.	www.international.unina.it
28. Istituto Italiano per la Privacy (IIP)	The Istituto Italiano per la Privacy (IIP), or Italian Institute for Privacy, is a research center dedicated to the thematics of cybersecurity and protection of personal data in global ICT society. IIP is founding partner of the European Privacy Association.	
29. Institute for the Protection and the Security of the Citizen	Joint Research Centre	http://ipsc.jrc.ec.europa.eu

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
30. Accredia – Italian Accreditation System	Italian National Accreditation Body appointed by the State to perform accreditation activity concerning certification and inspection bodies	www.accredia.it
31. ISACA Roma	No-profit association for security experts, mainly interested to Educational activities.	www.isacaroma.it
32. ISSA IT	The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. The mission of the ISSA is to enhance the knowledge and skills of its, encourage exchange of information security techniques, approaches, and problem solving, be the global voice of the information security professional, and promote best practices in information security.	No website identified
33. Association of Italian Experts in Critical Infrastructure (AIIC)	No-profit organization with the intent of promoting in Italy many activities in the field of Critical Infrastructures, their security and interdependencies: <ul style="list-style-type: none"> • Research; • Education; • Analysis of risks; • Awareness; • Consulting services. 	www.infrastrutturecritiche.it/ aiic
34. EASY	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.	www.easy4.it
35. EDEN	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	http://eden.saferinternet.it

Others	Role and responsibilities	Website
	children. Its goal is also to fight against illegal content and content unwanted by the end-user. The initiative is part of the EU's coherent approach.	
36. OWASP IT	The Open Web Application Security Project (OWASP) is an open-source application security project with local chapters. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions. The chapter in Italy organizes local events such as the Mini-meetings, chapter meetings and specific events.	www.owasp.org/index.php/Italy
37. ISACA IT	ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems. The chapter in Italy organizes local events such as education and training, workshops, roundtables and other specific events.	www.aiea.it
38. Altroconsumo	A consumer organisation, its aim is to protect and educate consumers.	www.altroconsumo.it

References

- 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
- Italy - ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/italy>
- The "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator" published by the Italian Personal Data Protection Authority, available at: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1628774>

