

Belgium 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 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

BELGIUM	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	9
OVERVIEW OF THE KEY STAKEHOLDERS	9
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	10
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES	15
SECURITY INCIDENT MANAGEMENT	15
EMERGING NIS RISKS	16
RESILIENCE ASPECTS	17
PRIVACY AND TRUST	17
NIS AWARENESS AT THE COUNTRY LEVEL	18
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	19
RELEVANT STATISTICS FOR THE COUNTRY	21
INTERNET ACCESS OF POPULATION AND ENTERPRISES	21
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	22
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	23
OTHER STATISTICS	24
APPENDIX	25
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	25
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	28
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	29
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	30
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	32
REFERENCES	33

Belgium

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

NIS strategy

In Belgium there is not a single, independent government body recognized among NIS stakeholders as the security agency. Nor is there a single body solely responsible for development of national information security policy.

The Council of Minister constituted on September 30th, 2005 the Belgian Network Information Security platform ("BelNIS"). BelNIS meets regularly and groups the key federal government organisations which have a competencies and responsibilities in NIS. Despite the current lack of a mandated national cyber security strategy for Belgium, BelNIS created a white paper "Towards a national policy in information security" in 2007 which led to a number of actions that were taken by the government at that time such as the setup of a new national CERT, more specifically CERT.BE.

In 2010 an update of this paper was prepared in function of the ongoing government formation to bring forward updated key strategy recommendations. Belgium is also currently preparing a regulatory framework regarding the means of cooperation between network providers. These will be integrated into the new national CERT.

In another initiative by private associations and academic institutions, BISSI, a white paper "Towards a Belgian Strategy on Information Security" was published in 2008. Intended towards government and public authorities in the first place, the paper describes a number of focus areas that the public authorities should address in specific working groups:

- Information Security Awareness Forum
- Information security standardisation
- Education, training and research coordination
- Critical infrastructure and CERT
- Legal and regulations
- Belgian Information Security Body

Despite the lack of a formal national cyber security strategy, early 2011 the federal Justice Minister announced the creation of a Belgian cyber crime centre. The new centre must bring together the expertise of government, academia and industry to tackle cyber crime. The new centre on cyber crime is expected to be launched by June 2011 and is partially funded by Europe. The centre should organize training for magistrates and police officers, but also conduct research about cryptography and offer its expertise to the police in criminal investigations to computer criminals.

eGovernment national strategy¹

The Belgian eGovernment strategy aims to create a single virtual Public Administration while respecting the privacy of users, as well as the specificities and competences of all Government bodies and administrative layers. Its main objective is to improve public service delivery for

¹ <http://www.epractice.eu/en/document/288179>

citizens and businesses by rendering it faster, more convenient, less constraining and more open. In order to meet this, the Belgian eGovernment strategy has four main strategic streams:

- Re-engineering and integrating service delivery around user's needs and life events.
- Cooperation among all levels of Government so as to provide integrated services across organisational boundaries and administrative layers.
- Simplification of administrative procedures for citizens and businesses.
- Back office integration and protection of personal data

It should be noted that non-federal Belgian administrative entities have developed their own eGovernment strategies within their respective areas of competence. Wallonia and Flanders Regional Governments have created dedicated structures to implement their respective strategies.

ICT policy and e-Inclusion policy in Belgium is to a large extent demand and sector driven. This is partially explained by the institutional arrangements that govern the country. In social affairs many institutional channels exist through which social organisations and pressure groups can express their concerns. At governmental level, matters pertaining to e-Inclusion are dealt with by different ministries and administrations depending on their respective competencies.

The federal structure of Belgium allows also for a regionally diversified approach. In the federal context, the 'Regions' are competent for matters such as town and country planning, nature conservation, housing, water policy, environment, economics, energy policy, local authorities, employment policy, public works and transport. The language based 'Communities' are competent for personal matters (health, welfare), cultural matters, education and training, and co-operation between communities and regions. Each Region and Community has its own legislative and executive powers in its respective fields of competence, and its own parliament and government to exercise these powers. However, the Flemish Region and Community merged their executive and legislative powers, and transformed into one Flemish Parliament, one Flemish Government and one public administration competent for community and regional matters.

The regulatory framework

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

Data Protection/Privacy Legislation²

The so-called "Privacy Law" of December 1992 (Law on the protection of private life with regard to the processing of personal data) is intended to protect citizens against the abusive use of personal data. The law defines the rights and duties of both the data subject and the processor. Moreover it provides a legal basis for the creation of an independent body in charge of overseeing its respect, namely the Commission for the Protection of Privacy.

Since its promulgation, this law has undergone major modifications. It has notably been modified in 1998 in order to transpose the EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC). The Privacy law was last amended in 2003 to take into account the fast developments occurring within the Information Society. The status, composition and competences of the Commission for the Protection of Privacy have been modified in accordance with the new requirements. This law is now available in its 'consolidated version' dated of August 2007.

² Source: <http://www.epractice.eu/en/document/288180> - the same source was used for several other laws indicated in this section

In addition, it is worth noting that a specific law containing provisions relating to spamming was adopted on 24 August 2005, so as to transpose the related article of the EU Directive 2002/58/EC on privacy and electronic communications (the so-called 'ePrivacy Directive').

eCommerce Legislation

Two laws on certain legal aspects of Information Society services were adopted on 11 March 2003 and published in the Belgian Official Journal ('Monitor') on 17 March 2003. Both texts define the essential concepts underpinning electronic commerce. Among others, they lay down information and transparency requirements, with particular regard to consumers, while regulating advertisement on networks (including spamming), removing obstacles to the conclusion of contracts by electronic means, as well as determining the responsibilities and duties of intermediaries (site hosts, access providers, etc). Both 'eCommerce laws' transposed the EU Directive on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (the so-called "eCommerce Directive" - 2000/31/EC) into Belgian Law.

eCommunications Legislation³

The law on electronic communications was adopted on 13 June 2005 and published in the Belgian Official Journal on 20 June 2005. It was intended to transpose the EU regulatory framework for electronic communications into Belgian law. This legislation refers to the BIPT to coordinate the initiatives regarding the quality and security of public electronic communication networks and services. They are responsible for detecting, monitoring and analyzing security issues, and informing users of it. Companies that offer public e-communication services need to publish adequate and actual information regarding secure access to their services.

eSignatures Legislation

The Law on the use of Electronic Signature in Judicial and Extra-Judicial Proceedings of 20 October 2000 introduced the use of the electronic signature within judicial and extra-judicial proceedings. It has been the first law to address the eSignature issue in Belgium. Adopted on 9 July 2001, the so-called 'eSignature Act' transposed into Belgian Law the EU Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures. It gives legal value to electronic signatures and electronically signed documents while setting up a legal framework for certification services.

It furthermore literally translates the definitions of advanced and "qualified" electronic signature that are laid down in this directive. In accordance with the directive, the act foresees that the use of electronic signatures in the public sector may be subjected to additional requirements, provided that such requirements are objective, transparent, proportionate and non-discriminatory. It is worth mentioning that at regional level, a law on electronic forms signed with the eID card of December 2006 and two related decrees of July 2007 have been adopted by the Walloon Parliament and by the Walloon Government respectively. These decrees give the same legal value to electronic forms as that of paper forms. The user will fill in an electronic form and sign it with his/her eID. The Walloon Region is the first authority in Belgium to propose this possibility.

Moreover, the legal framework for the use of electronic identity cards is set in a series of Royal and Ministerial Decrees, namely: Royal Decree of 25 March 2003 on the legal framework of electronic ID cards; Ministerial Decree of 26 March 2003 on the format of electronic ID cards;

³ Source: <http://www.epractice.eu/en/document/288180> - the same source was used for several other laws indicated in this section

Royal Decree of 1 September 2004 on the generalisation of electronic ID cards; and Royal Decree of 18 October 2006 on the eID document for Belgian children under 12.

Cybercrime legislation

For cases where traditional crimes and investigation measures can not sufficiently deal with offences against the Confidentiality Integrity and Availability of offences, a law of 28 November 2000 introduced four specific computer crimes (informatics forgery, informatics fraud, data manipulation and hacking), three specific investigation measures (data seizure, network searching and expert involvement) and a provision imposing data retention obligations on operators and service providers of electronic communication. In addition, specific laws penalise spam, the interference with military communications to hinder their functioning and the unauthorised deliberate access to the national social security database.

The court most likely to deal with computer crime is the Court of First Instance, criminal section (Correctionele rechtbank/Tribunal correctionnel). Against its decisions, appeal can be lodged with the Court of Appeal (Hof van beroep/Cour d'appel). The Supreme Court (Hof van Cassatie/Court de Cassation) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate.⁴

Self-regulation

*Belgian Code of Conduct for Safer Mobile Use by Younger Teenagers and Children*⁵

The Belgian 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. This mainly relates to the protection of children (mobile users under 18 years) against the illegal or inadequate content that can be accessible via mobile.

The code has been tailored to the needs of the Belgian mobile electronic telecommunications market and complies with applicable European and national legislation.

⁴ ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf

⁵ http://www.gsmeurope.org/safer_mobile/national.shtml

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"> • Federal Ministry of the Interior (IBZ) • Federal Ministry of Economic Affairs • Federal Ministry of Justice • Federal Public Service Information and Communication Technology (Fedict) • Federal/Regional Computer Crime Unit (FCCU/RCCU) • Joint Committee for Telecommunications ("Comixtelec") • BIPT (Belgian Institute for Postal Services and Telecommunications) • The Commission for the Protection of Privacy • Banking, Finance and Insurance Commission (CBFA) • Crossroads Bank for Social Security (CBSS)
CERTs	<ul style="list-style-type: none"> • CERT.be • BELNET CERT • NCIRC CC
Industry Organisations	<ul style="list-style-type: none"> • Agoria • ISPA (Internet Service Providers Association Belgium) • BELTUG
Academic Organisations	<ul style="list-style-type: none"> • CETIC • ESAT-COSIC • FUNDP/CRID • KHID (Royal High Institute for Defence)
Others	<ul style="list-style-type: none"> • Belcliv-Clusib • SpamSquad • L-SEC • ISSA BE • OWASP BE • ISACA BE

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁶ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁷.

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.

⁶ 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

⁷ <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

Co-operation via the responsible Ministries

On a first level, the Ministerial Committee for Intelligence and Security is the political body which determines the general intelligence policy of the Government. It takes political and legislative initiatives with regard to intelligence and security.

The Committee is currently made up of the Prime Minister, the Deputy Prime Minister and Minister of Finance and Institutional Reforms, the Deputy Prime Minister and Minister of Health and Social Affairs, the Minister of Foreign Affairs, the Deputy Prime Minister and Minister of Employment and Equal Opportunities, the Minister of Justice, the Minister of Defence and the Minister of the Interior. The decisions made by the Committee are executed by the Board of Intelligence and Security and the different involved authorities.

Under the Ministry Economy, SMEs, Self-employed and Energy there is an information society program in place that includes three key components: develop the regulatory framework for Belgium, ensure information security (product certification), and stimulate innovation and new developments.

The ministry has also set up the Internet Rights Observatory as passive monitoring measure, where citizens, closely or remotely involved in Information and Communication Technologies (ICT), can provide feedback regarding their Internet rights. They also collaborated with the FCCU⁸ (Federal Computer Crime Unit) to create 'E-cops' an online reporting portal regarding illegal content on the internet and cybercrime⁹. Furthermore the Ministry has set up an awareness website called 'Saferinternet.be', as part of the European Ins@fe initiative. This website contains various awareness materials about technical risks, commercial threats, cyberhate, sex-related crime, e-gambling, etc.

The Council of Ministers instigated the Belgian Network Information Security platform (BelNIS) which is an information exchange platform for network- and information security issues, threats and good practices at federal level. This platform includes the following participants:

- Fedict, the Belgian federal ICT Office
- KSZ, responsible for the management and security of the personal data that are being used by the Social security sector
- FCCU, the federal computer crime unit
- BIPT, the Telecom and Internet regulator
- Belgian Intelligence services
- The commission for the defence of the Privacy which regulates everything about security.
- The Control service of the Federal Administration of Economy that treats and tries to detect Internet fraud
- NVO, the National Security Organisation that is responsible for the law on classified Information.
- ADIV or the military intelligence service

⁸ http://www.polfed-fedpol.be/crim/crim_fccu_nl.php

⁹ <https://www.ecops.be/>

Co-operation via the Belgian Information Security Support Initiative

In an answer to the current state of affairs of the Belgian State in terms of Information Security, the Belgian Information Security Support Initiative¹⁰ (BISSI) was founded in 2008 in order to support the development and promotion of a society that tries to improve its level in Information Security in Belgium today. The main goal is to ensure a more effective collaboration between associations, experts and the Belgian society as a whole (individuals, public and private organizations). By enhancing the capability of all actors, BISSI aims to prevent, address and respond to Information Security threats and incidents.

By implementing appropriate measures such as the correct infrastructures for the apparent threats, protecting critical infrastructures, networks, processes and services but moreover by reaching out as experts to remediate but also to prevent; the BISSI initiative will enhance the Belgian situation. One of the first initiatives of this 'Think Tank' was the publication of a White Paper in September 2008. This document presents the main directions that need to be addressed in order to achieve a state of the art and well balanced Information Security Management in Belgium.

Today the group has expanded with industry representatives, government officials, academic authorities and liaisons officers, working jointly to maintain this dialogue platform for Information Security. Early 2009, a number of Working Groups have been established on each of the identified tracks in the whitepaper. BISSI brings together a group of not for profit associations and organizations specialized or interested in Information Security, more in particular when information appears in electronic format. Members of BISSI include:

- Local representation of international professional associations (ISACA and ISSA)
- Enterprise clusters (LSEC, Infopôle Cluster TIC)
- Research centres (CETIC)
- Academia (FUNDP/CRID, KULeuven/ESAT/COSIC, SBS)
- Belgian ISO/IEC JTC1 SC27 (IT Security Techniques) Shadow Committee

The Belgian Information Security Initiative Group aims to:

- Activate working groups (WGs) to prepare proposals in each of the six areas;
- Be approachable at all national events related to Information Security;
- Regularly publish the status on its activities and work;
- Create awareness amongst all components of the Belgian society;
- Create and maintain the appropriate synergy between public and private sectors.

Co-operation via CERT BELNET / CERT.BE

CERT BELNET helps its constituency to react to incidents by means of information campaigns, advice, and its coordination and information centre, but also by making available a library with sources on safety and security, best practices, links to suppliers, etc.

Thanks to it serves as a central contact point in case of incidents, and a source of pertinent information concerning computer security. The BELNET CERT coordinates investigations and information flow regarding security incidents in which its constituency is involved, whether as source or as victim of an incident.

¹⁰ See: <http://www.bissi.be/>

Belgium is also currently preparing a regulatory framework regarding the means of cooperation between network providers. BELNET is also active in pan-European CERT co-ordination discussions¹¹.

Co-operation via the Data Protection Authority (Privacy Commission)

The Commission for the Protection of Privacy, better known as the Privacy Commission, is an independent data protection authority ensuring the protection of privacy during the processing of personal data. The Commission was established by the Belgian Federal House of Representatives with the Act of 8 December 1992.

The Commission issues opinions and makes recommendations, grants authorizations, checks the way in which personal data are processed, informs and provides assistance. Through direct collaboration with public and private organisations, the Commission wants to make sure that any individual's right to privacy is protected when personal data are processed, always respecting a certain balance.

Co-operation via the Telecommunications regulator

The BIPT supervises the postal sector and the telecommunications sector (now called electronic communications) within Belgium. BIPT exercises its regulatory authority through two kinds of activities in particular. The first concerns new regulatory tasks in the liberalised telecommunications markets. BIPT makes the necessary arrangements in order that the regulatory framework is observed, competition can develop, certain tasks of public interest are carried out and consumer interests are protected. The second concerns the exercise of supreme authority in specific technical fields.

Exchange of information regarding the resilience of the networks takes place in the framework of the agreements between the historical operator and the civil and military authorities. Other than that, information exchange is limited as operators resist due to claiming that it is proprietary information. Only incidents which become publicly known are reported to the regulator BIPT. For the reporting, no standard formats or maximum delays in time are given. Among measures taken to close the information gap, operators are contacted by BIPT, sometimes on site visits are made and it is controlled whether an operator found remedy for the incident.

Furthermore BIPT offers NIS information services in their scope of activities through a publicly available RSS feed. In addition, offers the possibility of being notified by email or SMS as soon as a new virus alert is launched. In this way, citizens and organisations are very rapidly informed about the imminent threat described in the alert, thus enabling them to take necessary measures (such as updating antivirus software, installing patches, fixing a vulnerability in a software etc.). The virus alerting service which was set up in 2000 and lived its peak in 2002 has since then declined and has become almost dormant due to the fact that the security services market has known a rapid grow since 2002. The BIPT is at this time studying the possibility to set up an "internet barometer" for the general public to indicate the level of harmful activity on the Internet.

Since its creation, the BIPT Network Security Department made staff available to partake in the Joint Commission on telecommunications (Comixtelec). As part of the activities of CoMixTelec, since June 4th 2008 they have the chair for three years of the Industrial Resources and Communication Systems Group (Telecommunication) working group which belongs to the "Civilian Emergency planning" branch of NATO. Belgium particularly participated in the activities aimed at

¹¹ We refer to ENISA report "CERT cooperation and its further facilitation by relevant stakeholders", available at: <http://www.enisa.europa.eu/act/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders> , page 24.

integrating Computer Security Incident Response Teams (CSIRTs) into the emergency and crisis planning for electronic communications via Comixtelec.

Co-operation via Academic Organisations

The Computer Security and Industrial Cryptography research group, commonly called COSIC¹², is a research group at the Department of Electrical Engineering of the Katholieke Universiteit Leuven. One of the well-known successes is the selection of Rijndael as the Advanced Encryption Standard (AES). Currently AES is used by millions of users in more than thousand products, such as the protection of US government information. COSIC is also coordinating ECRYPT, a European-wide Network of Excellence in the area of cryptology and watermarking. COSIC organizes bi-weekly seminars on Computer Security and Industrial Cryptography. Furthermore COSIC provides consultancy in the area of computer security and cryptography. It is also a research team of the Interdisciplinary Institute for Broadband Technology (IBBT).

The Research Centre on IT and Law (Centre de Recherches Informatique et Droit – CRID) has been created in 1979 by the Faculty of Law, the Faculty of Economics and the Faculty of Informatics of the University of Namur. Its main mission is the encouragement of interdisciplinary academic reflection on the legal and economic (but also technological and sociological) aspects of information and communications technologies.

In reply to questions raised by its partners, and in respect of its “Charter for Research Contract with CRID”, the centre has been led to inquire deeply into issues, which are fundamental for the future of our society and its citizens as well as for enterprises. In this way, CRID has carried out research on behalf of Belgian Parliaments and Governments, the EU, the Council of Europe, the UNESCO, private and public undertakings, administrations, etc.

Co-operation via Industry Organisations

Agoria¹³ is Belgium’s largest employers’ organisation and trade association for organisations in the technology sector. Agoria provides services for its members on international business development as well as specialized subject groups. Mainly in the IT subject group NIS related subjects are discussed between stakeholders. Furthermore Agoria often represents the private sector in NIS discussions with the other NIS stakeholders in Belgium

ISPA is the Internet Service Providers Association of Belgium. This non-profit organisation was created to promote the interests of Belgian companies providing Internet services. The key areas of activity of the ISPA include:

- Offering a forum for discussions with government and other organisations of relevance to the Internet Industry
- Promoting the availability of accurate information about the Internet in Belgium
- Creating, promoting and maintaining a Code of Conduct for Internet Providers in Belgium
- Communicating with related organisations in Belgium and worldwide

BELTUG is the largest Belgian independent user group of ICT decision makers, working on communications services. More than 900 members actively share their knowledge and experience with each other, while benefiting from free reports, conferences, round tables, case stories and lobbying. In an on-line environment or in person, members learn from each other, each taking their communications technology and services a step forward. Particularly regarding NIS, BELTUG has launched a specific security SIG (Special Interest Group) in 2011.

¹² See: <http://www.esat.kuleuven.be/cosic/>

¹³ See: <http://www.agoria.be/>

Co-operation via LSEC

LSEC is an internationally renowned Information security cluster, a not for profit organization that has the objective to promote Information Security and the expertise in Flanders and Belgium. It is supported by the Flemish institute for sciences and development (IWT) and has a broad membership base of Information Security specialized companies, and numerous individual Information Security Professionals.

The organization represents a unique platform of world-class e-security expertise and professionals and contributes to innovation and high-tech entrepreneurship through its synergy with other organizations and networks. This is to support the members staying at the forefront of innovation by stimulating and supporting knowledge exchange and collaboration. The main mission for L-SEC has been to create IT security awareness in the industry at large. This has resulted in the organization of major IT security events in Belgium.

LSEC continues to organize a series of events on a yearly basis on important IT Security Topics, but will also increase awareness by divulging information on its diversity of expertise via its web portal that will consist out of a wide range of Information and topics of Information Security. LSEC is also supporting the future growth of the market by supporting innovation at large in the industry.

This will be reflected by a number of start-up projects, and an incubation facility to host small start-up companies. Finally LSEC participates as an active member in a number of research programs such as ADAPID (Advanced Applications for electronic Identity Cards) and SEC SOA (Secure Service Oriented Architectures).

Co-operation via Other Organisations

Furthermore there are very active information security organisations, such as ISSA, OWASP, ISACA, etc. where stakeholders from the academic world, the public sector and the private sector come together to share knowledge and best practices regarding various NIS topics.

Additionally there are a number of annual conferences (privately organized) such as Infosecurity.be¹⁴ and BRUCON¹⁵ that significantly foster co-operation and interaction between the diverse groups of professionals in the Belgian NIS environment.

¹⁴ www.infosecurity.be

¹⁵ www.brucon.org

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

Security incident management

For a long time, Belgium did not have a real national CERT. As a result of the publication in 2007 of the BelNIS' white paper, a number of new initiatives were started including the setup of a new national CERT, more specifically CERT.BE. Since the start of September 2009, BELNET has been charged with the task of operating the Belgian National Computer Emergency Response Team, CERT.be.

This service is an extension of BELNET CERT, which since 2004 has been helping BELNET customers handle computer security incidents and informing them concerning computer threats. The first phase only concerns critical infrastructure suppliers and telecommunications and ICT professionals in general. The second phase will add security information and services intended for the general public. CERT BELNET/CERT.BE provides a broad set of services including:

- **Reactive Services:** reactive services are offered in reaction to an occurring incident, be it detected by BELNET staff or a constituency's staff. They focus on short-term issues and include:
 - Alerts and Warnings
 - Incident handling (Detection, Triage, Response)
 - Vulnerability handling and response coordination
 - Artefact handling, analysis and response coordination
- **Proactive Services:** proactive services aim to prevent incidents from happening and reduce their impact when they occur. They focus on medium- to long-term issues and include:
 - Announcements
 - Technology Watch
 - Configuration of Tools
 - Security-Related Information Dissemination
- **Security Quality Management Services:** security quality management services leverage the CERT's expertise and focus on long-term issues, including:
 - Awareness Building
 - Education and Training
 - Advice to Legislative Bodies

Emerging NIS risks

In an answer to the current state of affairs of the Belgian State in terms of Information Security, BISSI - the Belgian Information Security Support Initiative was founded in 2008 in order to support the development and promotion of a society that tries to improve its level in Information Security in Belgium today. One of the first initiatives of this 'Think Tank' was the publication of a White Paper in September 2008.

This document presents the main directions that need to be addressed in order to achieve a state of the art and well balanced Information Security Management in Belgium, based on emerging NIS risks. The document highlights the following:

Over the past two decades there has been substantial investment in research, development, deployment and auditing, which has resulted in better protection against some NIS risks. But unfortunately numerous incidents show that overall information security is not really improving. There are several reasons for this:

- 1) Information systems are evolving very quickly and becoming ever more complex (we link computers made of hundreds of millions of small components in networks consisting of hundreds of millions of computers) and as humans we are not very good at securing complex systems that have many failure modes.
- 2) As more and more applications go online, the greater the financial incentives for online criminal behaviour. However, it is important to note that we may not hear so much about such problems because it is not in the perpetrators' interest to publicise their successes.
- 3) Information security is highly interdisciplinary. Developing solutions requires an integrated management approach that combines technology with internal and external regulation. Economic and human or social factors also need to be studied and taken into account. So in order to make progress there needs to be close collaboration between government, companies and research institutions.

The development and deployment of secure ICT systems requires the development of standards, the evaluation of products or systems and global coordination and enforcement. Although many of these issues need to be addressed at an international level, it is clear that national governments share a major responsibility. In Belgium there is no information security body for providing recommendations and support to Belgian administrations, institutions and organisations, at any level. This is in contrast to the situation in many European countries, including most of Eastern Europe [see Annex A].

The Belgian Defence Ministry has also done risk management exercises; these were not shared with other authorities due to lack of communication. In order to improve sharing of information, the Belgian Defence Ministry permitted BelNIS to share information with other agencies and stakeholders.

Resilience aspects

In Belgium, two authorities are responsible for matters of resilience of public e-communications networks: The Belgian Institute for Postal Services and Telecommunications (BIPT) and The Mixed Committee for Telecommunications (Comixtelec). The former, together with the Ministry of Defence shares responsibility and has oversight of Comixtelec.

Telecom operators act on a minimum of level of resilience. A regulation following Art 114 of the law on electronic communications on obligations regarding security measures and resilience of communication networks is still missing.

The Belgian electronic communications act stipulates that operators should take all necessary measures to assure continuity of its service offering. The measures to be implemented by the historical operator (incumbent operator – Belgacom) under the universal service provision have been defined. Their application to other operators is currently being prepared. In order to facilitate this implementation, BIPT has established an inventory based on a survey among operators which started in February 2007 and is still going on.

As regards future strategies, a working group of representatives of different federal public services is discussing the ongoing critical issues for the ICT-sector and proposing possible measures to be put in place. Contacts will be held with different parties from the different sectors to come to sector specific emergency planning: ISPs, operators, data centres, Government and manufacturers.

The Belgian Network of Information Security (BelNIS), being a governmental dialogue platform has prepared a white paper on information security, in which network security and dependability is also discussed¹⁶. This white paper, initially published in 2007 but updated in a new version end 2010, should actually serve as a general guideline to the government to define resources, priorities and actions to improve resilience.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the law of 11 December 1998 modifying the law of 8 December 1992 on privacy protection in relation to the processing of personal data (the "DPA"). Some provisions of the DPA have been modified, mainly by the law of 22 August 2002 on patients' rights and by the law of 26 February 2003 regarding the status, composition and functioning of the national regulatory authority. The competent national regulatory authority on this matter is the Commission for the Protection of Privacy (the "Commission").

Personal Data and Sensitive Personal Data

The definition of personal data in the DPA is based on the standard definition. In particular, the notion of personal data only applies to individuals as opposed to legal entities. However, Belgium has widened its interpretation of the concept of personal data: as soon as a data subject can directly or indirectly be identified on the basis of a set of data, this data will be considered as personal data. This is true even if the person with the means to identify the individual behind the data is not the data controller

¹⁶ We also refer to ENISA report "Analysis of Member States policies and regulations - Policy Recommendations" available at: <http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations> . See page 37.

Under the DPA, sensitive personal data is defined by reference to the standard types of sensitive personal data. In addition, data of a judicial nature such as information about criminal offences or criminal proceedings is treated as sensitive personal data.

Standard types of sensitive personal data may only be processed if the standard conditions for processing sensitive personal data are met. Consent from a data subject to process standard types of sensitive personal data must be in writing. In addition, for the processing of sensitive personal data the data controller must ensure that the persons having access to such data will comply with the obligation of confidentiality in relation to such data by means of legal, statutory or contractual provisions. The data controller has to keep a list with the categories of persons having access to such data and a precise description of their duties in relation to the data.

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

The data controller must comply with the general data security obligations and must also: (i) secure access to the data; (ii) inform its personnel about their obligations under the DPA; and (iii) ascertain that no unlawful use is made of the software programs used for the automatic processing of personal data;

Data protection breaches

The DPA does not contain any obligation to inform the Commission or data subjects of a security breach. However, data controllers in certain sectors may be required to inform sectoral regulators of particular types of breach.

Enforcement

The Commission's mission is, amongst other things, to monitor overall compliance with the DPA. To this end, the Commission has general power of investigation with respect to any type of processing of personal data. Furthermore, the Commission may file a criminal complaint with the Public Prosecutor. The Commission may also institute a civil action before the President of the Court of First Instance. However, the Commission cannot impose fines upon individuals or organisations.

NIS awareness at the country level

There are several good initiatives, such as for example 'Saferinternet' to increase awareness among the Belgian population. This program is an initiative of the government, and its objective is also creating awareness regarding security and the possible risks in the digital environment.

As awareness centre 'Saferinternet' develops awareness tools on safe and responsible use of the Internet and informs parents, teachers and the public about children's use of the Internet and new technologies. The aim is to provide children, parents and teachers knowledge and tools for guidance and to empower children using information and communication technologies. Child Focus also has a hotline against child abuse images found on the Internet and permits the public to sent reports. These activities are funded by the European Commission under the Safer Internet Programme.

The Belgian awareness centre seeks to give children, parents and teachers advice and tips to avoid risks when using the Internet. At the same time the centre emphasizes the positive aspects of using information and communication technologies. A strong and large network of national stakeholders works very intensively together with the awareness centre in guiding the development of tools, giving advice and information on new technologies. Furthermore, these stakeholders help us to disseminate information.

Child Focus initiates, coordinates and participates in a broad range of activities and initiatives with the aim to raise awareness in the area of online safety and child abuse images. Among others:

National campaigns - The Belgian Awareness Centre coordinates the Belgian celebration of Safer Internet Day and launches different campaigns on Internet safety in collaboration with industry, Ministries and other partners.

Reaching different target groups - In order to reach and learn from the different target groups (children, parents and teachers), Child Focus developed different strategies. The Awareness centre gives regularly presentations for parents in schools, institutions... about children's use of Internet and provides parents with information and educational advice. Different tools, e.g. board games, pocket cards, are being developed to empower young people in their use of new technologies. The Awareness centre gives regularly training and advice to teachers on cyber bullying in schools.

Youth Panel - The Awareness centre is guided by a youth panel consisting of young people between 14-17 years old. The youth panel provides information on their youth culture and their online life and gives feedback on the tools developed. They also play an active and creative role by developing peer-to-peer communication tools for young people.

National collaboration - The awareness centre is highly respected and seen as key resource and knowledge centre for children's use of Internet and mobile phones. The centre has a large network of relevant stakeholders (government, law enforcement, industry, non- governmental and welfare organisations...) and is regularly consulted for information, advice and collaboration.

The Belgian Safer Internet Centre - From October 1st 2008, Child Focus, Foundation for Missing and Sexually Exploited Children and Sensoa, Flemish expert organization on sexual health form the Belgian Integrated Network Safer Internet, now Belgian Safer Internet Centre.

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

In 2010, the Royal Higher Institute for Defence Studies (KHID) published a very interesting study on the protection of national critical infrastructure against the asymmetric threat of proliferation. In a previous study, "Weapons of mass destruction: legacy of the Cold War and threat to the future," recommendations were formulated applicable to several domains in order to improve national emergency planning.

Risk analysis can help determine what improvements should be made to existing plans, or what infrastructure should be better protected. Future threats will materialize in proliferation, international terrorism, unequal distribution of wealth, organized crime and pandemics. This threat is further increasing due to consequences of globalization as the growing energy demand, climate change, urbanization, demographic explosion and its sociological consequences as well as the present economic crisis. This study aims to shed some light on the consequences of aforementioned problems; hence risk analysis and critical infrastructure protection are key words in an environment of asymmetrical proliferation.

In a first part, the framework will clearly be defined by the explanation of relevant definitions, for concepts like risk, threat and impact are often interchangeably used: this can result in unclear contextual documents which are useless. Once these foundations laid out, the methodology for the development of a sound critical infrastructure protection planning can be detailed.

The second part of this study focuses on the international interpretation that was given to the concept of critical infrastructure (protection). Therefore, both the approach of the European Union and NATO are highlighted. In the final part, the national policy is analyzed and recommendations

are proposed. National legislation in the European framework, procurement, Communications Security, and market regulation of private partners as well as the availability of information are fundamental national requirements.

Furthermore, a network of national computer emergency response teams, protection of critical (information) infrastructure in expeditionary capabilities, supranational relevant treaties and a European strategic vision on critical infrastructure protection are expressed as important on the international level. Network enabled capabilities, protection of information flows and interoperability (UN, NATO, EU, ...), dependency and cascade effects, defining rules of engagement and cyber activity concepts, operational cooperation in research and development, as well as EU-NATO rationalization of networks contribute to a holistic approach for defence forces.

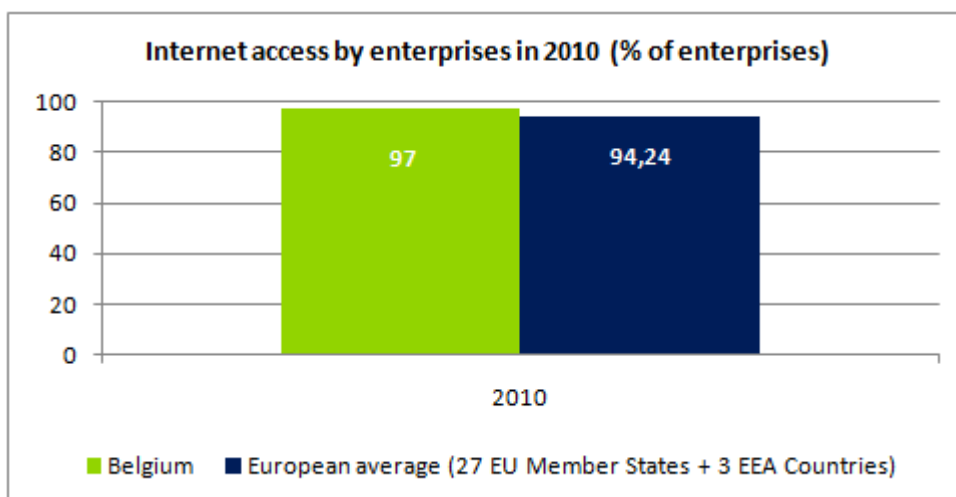
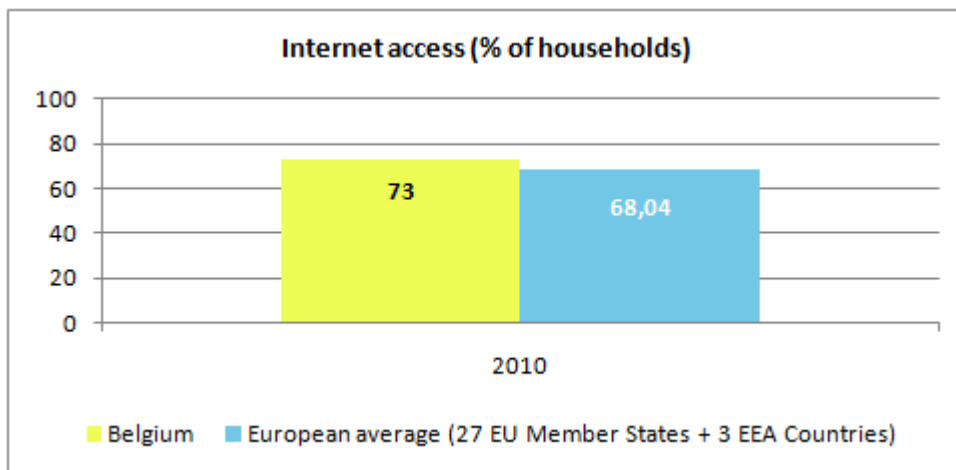
These policy recommendations could improve homeland protection as well as capabilities for expeditionary forces.

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Belgium, a series of relevant statistics are included in this section. These statistics mainly show that Belgium is slightly above the European average in regards of NIS and ICT development.

Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation¹⁷ of Internet access in Belgium for enterprises and respectively households, relative to the European average.

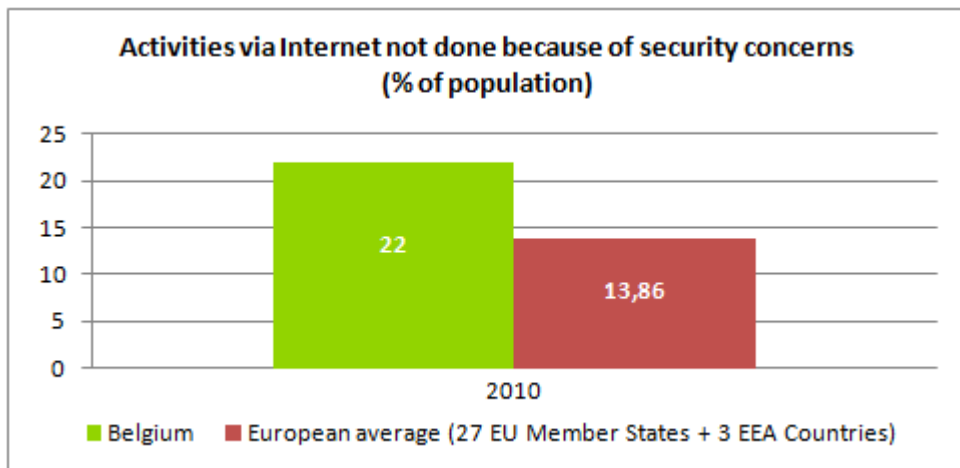


In 2010, the statistics indicate that both the enterprises and the households in Belgium have a level of Internet access that is lightly above the European average.

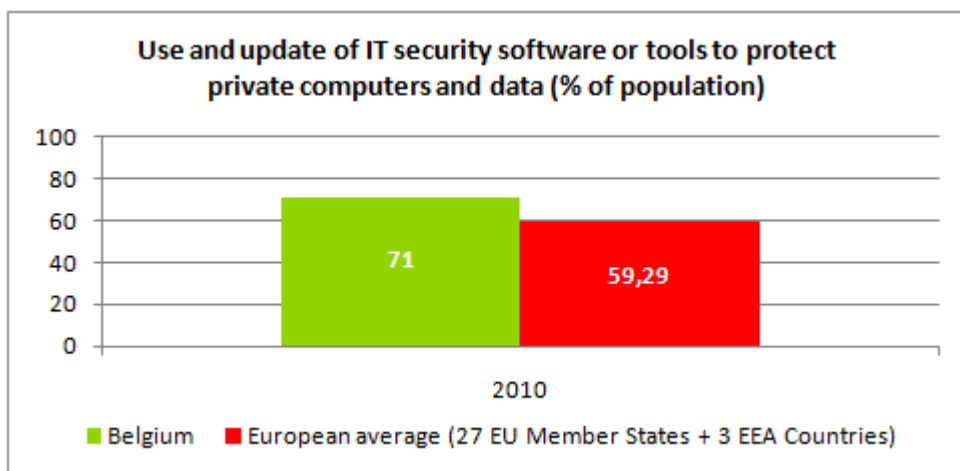
¹⁷ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Belgium 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 highly above the European average:



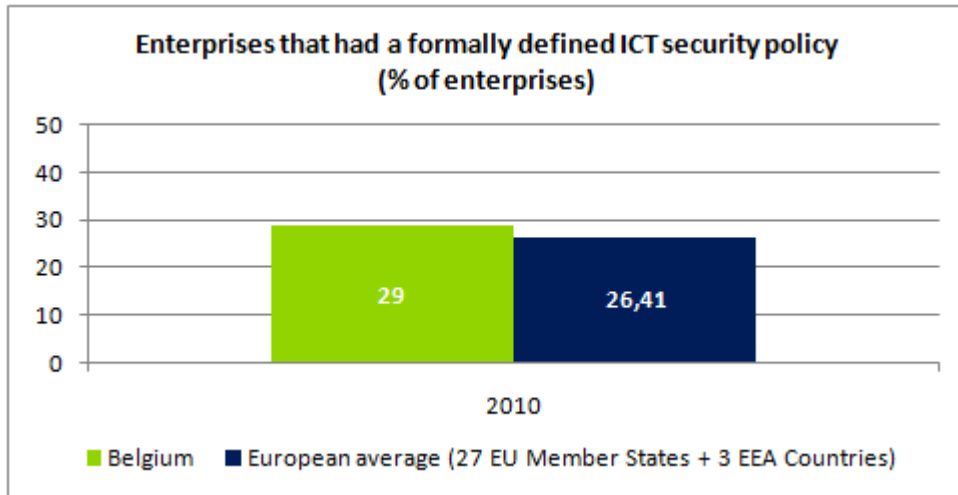
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



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

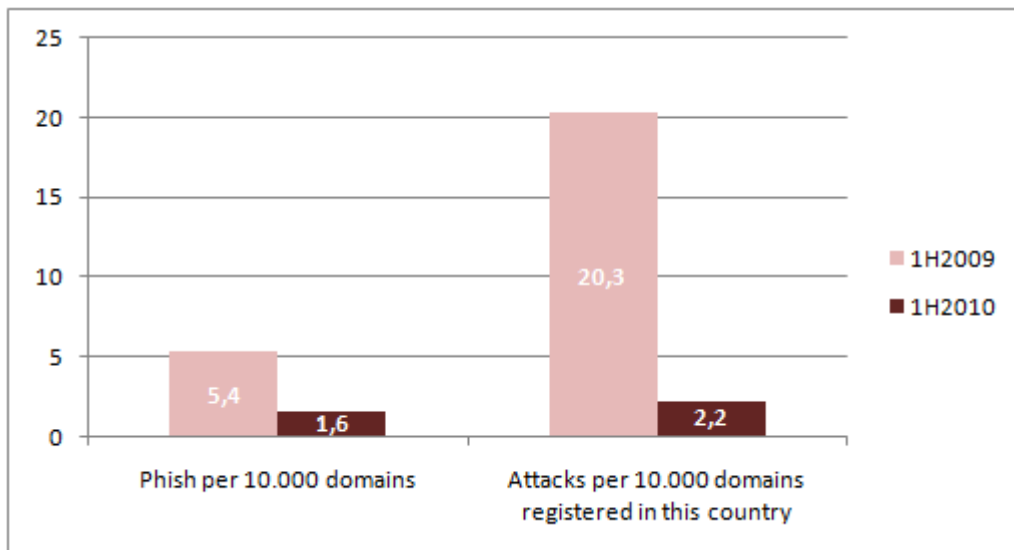
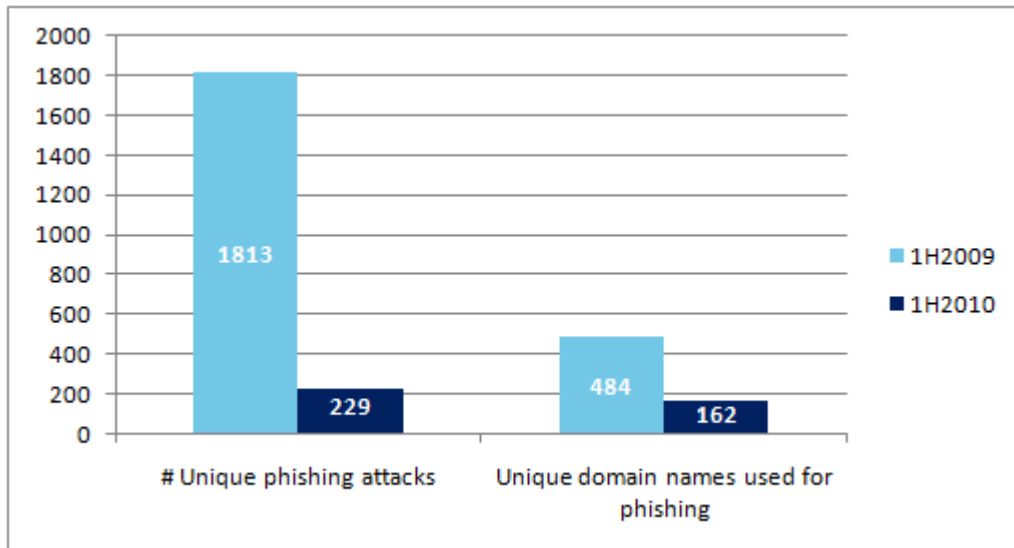
Statistics on use of Internet by enterprises and related security aspects

More enterprises in Belgium 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, Belgium was mentioned in the global report¹⁸ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



¹⁸ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Federal Ministry of the Interior (IBZ)	<p>The Federal Ministry of the Interior is also called the Federal Public Service for the Interior in Belgium. It formulates policy, prepares legislation and regulations, and is also responsible for coordination, supervision and policy implementation regarding national security measures. From that perspective, they have a principal role regarding general Critical Infrastructure protection planning and preparedness.</p> <p>A specific role within the IBZ is the operation of the crisis coordination centre which coordinates the management of crises at a national level and provides support to the regional and local level. Furthermore IBZ is responsible for the police, and therefore also for the FCCU.</p>	<p>www.ibz.be www.crisis.ibz.be</p>
2. Federal Ministry of Economic Affairs	<p>The Federal Ministry of Economic Affairs is also called the Federal Public Service 'Economy, SMEs, Self-Employed and Energy'. Its numerous responsibilities include a principle role regarding e-commerce and the development of the information society.</p> <p>There is an information society program in place that includes three key components: develop the regulatory framework for Belgium, ensure information security (product certification), and stimulate innovation and new developments.</p> <p>The Federal Public Service for Economy, SMEs, Self-employed and Energy has also set up the Internet Rights Observatory as passive monitoring measure, where citizens, closely or remotely involved in Information and Communication Technologies (ICT), can provide feedback regarding their Internet rights. They also collaborated with the FCCU (Federal Computer Crime Unit) to create 'E-cops' an online reporting portal regarding cybercrime.</p> <p>Furthermore the Ministry has set up an awareness website called 'SaferInternet.be', as part of the European ins@fe initiative. This website contains various awareness materials about technical risks, commercial threats, cyber hate, sex-related crime, e-gambling, etc.</p>	<p>economie.fgov.be www.internet-observatory.be www.saferinternet.be</p>
3. Federal Ministry of Justice	<p>The Federal Ministry of Justice is also called the Federal Public Service Justice in Belgium. It has the principal role regarding NIS from the perspective of NIS-related law enforcement and combating cybercrime in terms of investigation and prosecution.</p> <p>State Security is the civil intelligence service, and this service is primarily under the authority of the Minister of Justice. Sometimes, however, it acts under the authority of the Minister of the Interior.</p>	<p>www.just.fgov.be</p>
4. Federal Public Service Information and Communication Technology (Fedict)	<p>FedICT was created in May 2001 as part of the plans of the federal government to modernise the federal administration. It is a so-called horizontal unit as it provides services to the other federal public services (ministries) and related</p>	<p>www.fedict.belgium.be eid.belgium.be</p>

National authorities	Role and responsibilities	Website
5. Federal/Regional Computer Crime Unit (FCCU/RCCU)	<p>authorities. FedICT became operational in 2002 and is responsible for implementing e-government, development of an e-society, and promoting Belgium as a knowledge area regarding ICT.</p> <p>FedICT wants to develop a common strategy for e-government by developing a solid base infrastructure, additional services and supporting projects. A good example of this is their principal role in the implementation and support of EID (electronic ID card) services.</p> <p>The parts of the police that are specialised in the investigation of computer and telecommunication systems are organized in two levels: The federal Computer Crime Unit (FCCU) on national level and Regional Computer Crime Units (RCCU) within the different juridical regions. The Computer Crime Units are responsible for support to police and justice regarding ICT matters in the context of general investigations, as well as other specifically regarding cybercrime issues.</p> <p>The role of the Federal Computer Crime Unit (FCCU) includes combatting all forms of cybercrime through specialisation, prevention, proactive and reactive interventions, etc. Their mission also includes fighting other crime by providing specialized investigations in ICT environments, such as child pornography, Internet fraud, telecom fraud, etc.</p> <p>The Regional CCU's ensure minimally qualitative forensic ICT investigations of PC equipment, data carriers and small networks. For more specialized or larger investigations the FCCU is involved as national centre of expertise. Furthermore the FCCU executes awareness raising campaigns with regards to NIS directed at private organisations, and manage an online reporting portal regarding illegal content on the internet and cybercrime called 'E-cops'.</p>	<p>www.polfed-fedpol.be</p> <p>www.ecops.be</p>
6. Comixtelec	<p>Comixtelec is the joint commission on telecommunications created by the royal decree of 10 December 1957. Its main objective is to optimise the use of all means of telecommunication for the benefit of both military and civil authorities. It has to determine and oversee measures, preventive and reactive, to be taken by designated operators in case of crises or exceptional situations.</p>	<p><i>Not applicable</i></p>
7. Belgian Institute for Postal Services and Telecommunications (BIPT)	<p>The BIPT supervises the postal sector and the telecommunications sector (now called electronic communications) within Belgium.</p> <p>BIPT exercises its regulatory authority through two kinds of activities in particular. The first concerns new regulatory tasks in the liberalised telecommunications markets. BIPT makes the necessary arrangements in order that the regulatory framework is observed, competition can develop fully and fairly, certain tasks of public interest are carried out and consumer interests are protected. The second concerns the exercise of supreme authority in specific technical fields. Certain resources, such as the electromagnetic spectrum or the numbering space, are scarce: a regulator is required to share, regulate and monitor their use with accuracy.</p> <p>The BIPT carries out yet more technical tasks of</p>	<p>www.bipt.be</p>

National authorities	Role and responsibilities	Website
	<p>public interest, such as relating to the security and QoS of public electronic communications networks. It also runs a virus alerting service for the general public and SMEs, which is to be replaced by an "internet barometer" planned in 2011.</p>	
<p>8. The Commission for the Protection of Privacy</p>	<p>The Commission for the Protection of Privacy, better known as the Privacy Commission, is an independent data protection authority ensuring the protection of privacy during the processing of personal data. The Commission was established by the Belgian Federal House of Representatives with the Act of 8 December 1992. The Commission issues opinions and makes recommendations, grants authorizations, checks the way in which personal data are processed, informs and provides assistance. This is how the Commission wants to make sure that any individual's right to privacy is protected when personal data are processed, always respecting a certain balance.</p>	<p>www.privacycommission.be</p>
<p>9. Crossroads Bank for Social Security (CBSS)</p>	<p>To improve the service delivery to the socially insured people and the companies and to solve the above mentioned disfunctionalities, the Crossroads Bank for Social Security (CBSS) was created 16 years ago. The mission of the CBSS is to be the motor of e-government in the social sector, i.e.</p> <ul style="list-style-type: none"> • to stimulate and to support the actors in the Belgian social sector to grant more effective and efficient services with a minimum of administrative formalities and costs for all the involved; based on a common and concerted vision, the actors in the Belgian social sector benefit from the new technologies to improve and re-organize radically their mutual relationships and processes; • to promote the information security and the privacy protection by the actors in the Belgian social sector so that all the involved institutions and people can have justified confidence in the system; • to deliver integrated statistical information to the politicians and the researchers in order to support the social policy. 	<p>www.ksz-bcss.fgov.be</p>
<p>10. Banking, Finance and Insurance Commission (CBFA)</p>	<p>The Banking, Finance and Insurance Commission (CBFA) is the single Belgian authority in charge of supervising most financial institutions and financial services offered to the public. The CBFA was established in order to ensure protection of savers and policy-holders, public confidence in financial products and services, and the proper operation of markets in financial instruments. In order to achieve these goals, Parliament entrusted the CBFA with a very wide range of tasks, including NIS related responsibilities in the financial sector such as security requirements for e-banking.</p>	<p>www.cbfa.be</p>

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST¹⁹ member • TI²⁰ listed 	
11. CERT.be	CERT.be is the Belgian national Computer Emergency Response Team. Appointed by FedICT in collaboration with BIPT, CERT.be is the primary Belgian contact point for dealing with Internet security threats and vulnerabilities affecting Belgian interests. We operate within a worldwide network of information security experts and provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Belgium. CERT.be is FIRST Member and TI Listed.	www.cert.be
12. BELNET CERT	The BELNET CERT coordinates investigations and information flow regarding security incidents in which its constituency is involved, whether as source or as victim of an incident. BELNET CERT.be is FIRST Member and TI Listed.	cert.belnet.be
13. NCIRC	The NCIRC is the NATO Computer Incident Response Capability. This team doesn't belong only to Belgium, but serves for all NATO countries. NCIRC is FIRST Member and TI Listed.	www.ncirc.nato.int

¹⁹ <http://www.first.org/members/teams/>

²⁰ <http://www.trusted-introducer.nl/>

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
14. Agoria	<p>Agoria is Belgium's largest employers' organisation and trade association for organisations in the technology sector. The companies represented by Agoria are active in 13 branches of the technology industry: aerospace, automotive, construction products, contracting & maintenance, electrical engineering, industrial automation, ICT, mechatronical engineering, metals & materials, metal processing, mounting & cranes, plastics, security & defence.</p> <p>Agoria provides services for its members on international business development as well as specialized subject groups. Mainly in the IT subject group NIS related subjects are discussed.</p>	www.agoria.be
15. ISPA (Internet Service Providers Association Belgium)	<p>ISPA is the Internet Service Providers Association of Belgium. This non-profit organisation was created to promote the interests of Belgian companies providing Internet services. Its members account for 97% of the Internet connections in Belgium.</p> <p>The key areas of activity of the ISPA include:</p> <ul style="list-style-type: none"> • Offering a forum for discussions with government and other organisations of relevance to the Internet Industry • Promoting the availability of accurate information about the Internet in Belgium • Creating, promoting and maintaining a Code of Conduct for Internet Providers in Belgium • Communicating with related organisations in Belgium and worldwide 	www.ispa.be
16. BELTUG	<p>BELTUG is the largest Belgian independent user group of ICT decision makers, working on communications services. More than 900 members actively share their knowledge and experience with each other, while benefiting from free reports, conferences, round tables, case stories and lobbying. In an on-line environment or in person, members learn from each other, each taking their communications technology and services a step forward. Particularly regarding NIS, BELTUG has launched a specific security SIG (Special Interest Group) in 2011.</p>	www.beltug.be

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
17. CETIC	CETIC is the Centre of Excellence in Information and Communication Technologies, focusing on applied research and technology transfer in the field of software engineering, Service oriented technologies and embedded systems. CETIC is a connecting agent between academic research and industrial companies.	www.cetic.be
18. ESAT-COSIC	<p>The Computer Security and Industrial Cryptography research group, commonly called COSIC, is a research group at the Department of Electrical Engineering of the Katholieke Universiteit Leuven.</p> <p>The goal of COSIC's research activities is to create a secure electronic equivalent for interactions in the physical world such as confidentiality, signatures, identification, anonymity, payment and elections. The research concentrates on the design, evaluation, and implementation of cryptographic algorithms and protocols, on the development of security architectures for information and communication systems and on the development of security mechanisms for embedded systems. COSIC's theoretical work is mainly based on discrete mathematics such as number theory, finite fields, Boolean algebra, but also includes statistics and optimization. The aim is to achieve efficient and secure solutions. The broader goal is to achieve efficient and secure multi-party computation. These mathematical tools are applied to increase our understanding of the strengths and weaknesses of cryptographic algorithms and to develop new and better algorithms such as block ciphers, stream ciphers, public-key encryption algorithms and zero-knowledge identification protocols.</p> <p>One of the well-known successes is the selection of Rijndael as the Advanced Encryption Standard (AES). Currently AES is used by millions of users in more than thousand products, such as the protection of US government information. COSIC is also coordinating ECRYPT, a European-wide Network of Excellence in the area of cryptology and watermarking.</p> <p>COSIC organizes bi-weekly seminars on Computer Security and Industrial Cryptography. Furthermore COSIC provides consultancy in the area of computer security and cryptography. It is also a research team of the Interdisciplinary Institute for Broadband Technology (IBBT).</p>	www.esat.kuleuven.be/cosic
19. FUNDP/CRID	<p>The Research Centre on IT and Law (Centre de Recherches Informatique et Droit – CRID) has been created in 1979 by the Faculty of Law, the Faculty of Economics and the Faculty of Informatics of the University of Namur. Its main mission is the encouragement of interdisciplinary academic reflection on the legal and economic (but also technological and sociological) aspects of information and communications technologies. Based on its research activities, CRID is also active in teaching.</p> <p>Currently, CRID counts some forty researchers, including six professors. In reply to questions raised by its partners, and in respect of its</p>	www.fundp.ac.be

Academic Organisations	Role and responsibilities	Website
	<p>"Charter for Research Contract with CRID", the centre has been led to inquire deeply into issues, which are fundamental for the future of our society and its citizens as well as for enterprises. In this way, CRID has carried out research on behalf of Belgian Parliaments and Governments, the European Union, the Council of Europe, the UNESCO, private and public undertakings, administrations, etc.</p>	
20. KHID	<p>The Royal High Institute for Defence (RHID) is a 'think tank' and a forum for discussing matters of Security and Defence, open to anyone interested in them. One of its most important objectives is to set up co-operation with similar organizations outside the Defence Ministry.</p> <p>The Royal Higher Institute for Defence determines and manages the research programmes of the Belgian Defence Ministry. To that end, it has at its disposal its own researchers in the domain of 'Defence and Security' policy. Where scientific and technological research is concerned, it relies upon the research network of the Defence Ministry (which includes other universities and research institutions, as well).</p> <p>The IRSD also organizes the programme of Advanced Defence Studies for the higher echelons of the military and public authorities. The programme is a series of seminars where senior officers, senior officials of other ministries, managers and those who influence opinion meet one another and discuss themes related to 'Security and Defence' in the broadest sense of the words.</p> <p>It also organizes evening lectures, seminars, symposiums and workshops. Not only does it issue its own publications, but its researchers publish in national and international revues.</p>	<p>http://www.mil.be/rdc</p>

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
21. Belcliv-Clusib	<p>Belcliv-Clusib (Belgian Club for Internet Security) is an organisation that aims to foster the security of information systems and networks in Belgium. More precisely their objectives include:</p> <ul style="list-style-type: none"> introducing and spreading methods and technical recommendations concerning the security of information systems and networks; presenting summaries about the state of the art and the technologies in this field; promoting the exchange of experience and ideas among its members; providing on-going training for its members, e.g. conferences, training seminars and publications. 	<p>www.clusib.be</p> <p>www.belcliv.be</p>
22. SpamSquad	<p>SpamSquad is an informal working group with participants from the academic world, public sector and private sector on the topic of spam emails. They focus on methods to measure spam and develop possible measures to fight spam.</p>	<p>www.spamsquad.be</p>
23. L-SEC	<p>LSEC is an internationally renowned Information security cluster, a not for profit organization that has the objective to promote Information Security and the expertise in Flanders and Belgium. It is supported by the Flemish institute for sciences and development (IWT) and has a broad membership base of Information Security specialized companies, and numerous individual Information Security Professionals.</p>	<p>www.l-sec.be</p>
24. ISSA BE	<p>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.</p> <p>The Brussels European ISSA Chapter in Belgium (ISSA BE) is an independent chapter of the Information Systems Security Association (ISSA). It facilitates, among other things, knowledge sharing events on various information security topics throughout the year in the Belgium.</p>	<p>www.issa-be.org</p>
25. OWASP BE	<p>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 Belgium organizes local events such as seminars and other specific events.</p>	<p>www.wasp.org/index.php/Belgium</p>
26. ISACA BE	<p>ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems.</p> <p>The chapter in the Belgium organizes local events such as education and training, workshops, roundtables and other specific events.</p>	<p>www.isaca.be</p>

References

- ENISA report "Analysis of Member States policies and regulations - Policy Recommendations" available at: <http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations>
- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- ENISA report "Information security awareness in financial organization", November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- ENISA report "Stock taking of policies and regulations - Resilience of communication networks" published in September 2008: <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report>
- See BISSI - BIIB - IBSI web site, available at: <http://www.bissi.be>



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu