France Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

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, please use the following details: Mr. Jeremy Beale, ENISA Head of Unit - Stakeholder Relations, Jeremy.Beale@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 the **France Country Report** on behalf of ENISA: Dan Cimpean, Johan Meire and Aurore Pellé.

Legal notice

Table of Contents

France

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:*
        - *National authorities*
        - *CERTs*
        - *Industry organisations*
        - *Academic organisations*
        - *Other organisations active in NIS*
    - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
- *Country specific NIS facts, trends, good practices and inspiring cases.*

For more details on the general country information, we suggest the reader to consult the web site: http://europa.eu/abc/european_countries/index_en.htm

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Context

France conducted a thorough review of its defence and national security policies. New priorities have been set and endorsed by the president Sarkozy in the so called French White Paper on Defence and National Security, published on June 17th, 2008.[1] This White Paper has identified cyber attacks as one of the main threats to the national territory. Indeed, society's growing dependence on information and communication technologies has made prevention and reaction to cyber attacks a major priority in the organisation of national security:

"Over the next 15 years, the proliferation of attempted attacks by non-State actors, computer pirates, activists or criminal organisations is a certainty. Some of these could be on a massive scale."

"The State must powerfully develop, maintain and disseminate its information systems security expertise among economic actors, and particularly among network operators. The instantaneous, near-unpredictable nature of attacks also calls for a crisis management and post-crisis management capability able to maintain the continuity of activities, and to prosecute and punish attackers."

"Faced with a growing threat, whether State-backed or otherwise, France must in the short term acquire reactive capability to protect the nation's information systems.

Early-warning systems will be developed to detect cyber attacks by setting up a detection centre in charge of the permanent monitoring of critical networks and implementation of appropriate defence mechanisms.

To combat the threat, greater use will be made of security products and trust networks. This in turn will require sufficient national capacity in the industry to master and develop very high-security products to protect State secrets, as well as a range of guaranteed "trusted products and services" for use by government agencies and services which will be made widely available to the business sector.

Regulatory provisions will also be introduced to ensure that electronic communications operators implement the technical and organisational measures necessary to protect their networks against the most serious failures and attacks. In this respect, the Internet will need to be considered as critical infrastructure and considerable effort will be made to improve its resilience.

A new agency responsible for information systems security (agence de la sécurité des systèmes d'information) will be set up to reinforce the coherence and capacity of State resources. Reporting to the Prime Minister and operating under the aegis of the General Secretariat for Defence and National Security (SGDSN), the agency will take over, and substantially expand, the staff and resources of the SGDN division currently responsible for this task. The agency will operate a centralised capability to detect and defend against cyber attacks. It will have the resources to sponsor the development of, and acquire, the security products essential to protect the Government's most sensitive networks.

---

[1] *http://merln.ndu.edu/whitepapers/France_English2008.pdf*

The agency will also take on an advisory role to the private sector, particularly in areas of critical strategic importance, and will participate actively in the development of security for the information society. The development of Internet sites dedicated to information system security and accessible to all will be one of its responsibilities.

More generally, the Government administration will enhance its expertise by increasing the numbers of specialised personnel in the ministries, creating a reservoir of competencies available to serve the needs of government departments and operators of critical infrastructures.

In view of the international dimension of the threats to communication networks, the agency will maintain close links with our main partners, particularly in Europe, and will encourage the development of a Europe-wide communication networks security policy.

A nationwide network of experts will also be established in the form of information system security observatories in the defence and security zones. These observatories will report to the zone Prefects and their principal tasks will include support (training, advice) to local government, organisation of networks and reporting early warning-signs of incidents."

Creation of a new agency: The French Network and Information Security Agency (FNISA) - Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) created on July 7th, 2009.[2]

In order to strengthen France's capabilities to face the challenges posed by information system security, the White Paper on Defence and National Security has planned the creation of a French Network and Information Security Agency (FNISA or ANSSI in French, standing for "Agence Nationale de la Sécurité des Systèmes d'Information"), in a similar way to France's main partner nations. This new agency is placed under the authority of the Prime Minister and is attached to the Secretary General for National Defence.

One year after the publication of the French White Paper, the ANSSI is now established by a decree issued in the Journal Officiel de la République Française of July 8th, 2009 — the creation process being under way since January 1st, 2009. The agency replaces the present Central Directorate for Information System Security (DCSSI), and is assigned wider missions and resources.

The creation of the French Network and Information Security Agency is a milestone in the process of improving France's capability to protect its sensitive information systems.

The core missions of the new agency are:

- To detect and early react to cyber attacks, thanks to the creation of a strong operational center for cyber defence, working round-the-clock and being in charge of the continuous surveillance of sensitive Governmental networks, as well as the implementation of appropriate defence mechanisms ;
- To prevent threats by supporting the development of trusted products and services for Governmental entities and economic actors ;

[2] *http://www.ssi.gouv.fr/site_article76.html*

- To provide reliable advice and support to Governmental entities and operators of Critical Infrastructure ;

To keep companies and the general public informed about information security threats and the related means of protection through an active communication policy.

The regulatory framework

eGovernment Act

Ordinance on electronic interactions between public services users and public authorities and among public authorities

This ordinance – also referred to as the 'teleservices ordinance' – has been adopted on 8 December 2005 on the basis of the Legal Simplification Law of 9 December 2004.

It aims at establishing a comprehensive legal framework for the shift to an 'electronic administration' by 2008, by creating the conditions for simple and secure electronic interactions between citizens and public authorities. The text covers all exchanges of electronic documents, email or digital communications among, on the one hand, public authorities, and on the other hand, citizens and central administration, regional governments and private organisations licensed to carry out public services.

It grants the same legal status to email as that of traditional paper-based correspondence and legalises the use of electronic signatures by public authorities. Moreover, the ordinance includes a provision for users to have the option of securely storing and receiving official correspondence and administrative forms on personalised online mailboxes. Lastly, the text lays down provisions on both the security of exchanges and the interoperability of information systems.

Data Protection / Privacy Legislation

France adopted the Law on 'Informatics and Liberty' on 6 January 1978, becoming one of the first European countries to have a data protection legislation.

The Law provides a legal framework for the use of identifiers in databases and the processing of personal data by public and private sector organisations. The Law created a National Commission for Informatics and Liberty (CNIL), which is in charge of overseeing its implementation and observance. The CNIL also has an advisory role in the planning of administrative data systems.

The Law on Informatics and Liberty was amended by law no. 2004-801 of 6 August 2004 implementing the EU Data Protection Directive (95/46/EC).

eCommerce Legislation

Adopted on 21 June 2004, the Law for trust in digital economy implements the EU Directive on electronic commerce (2000/31/EC) and sets the legal framework for the development of eCommerce services in France. Among others, this law lays down the opt-in principle for receiving advertisement email messages and regulates the liability of certification service providers issuing qualified digital certificates.

eCommunications Legislation

The postal and electronic communications Code is a legal code which defines regulations related to electronic communications amongst others. Section L.35-1 and followed sections cover the mobile telephony and the access to Internet. Section L.45 defines the organization that manages Domain Names french. The Version in force at December 18, 2009 of the code of postal and electronic communications is available on Legifrance website[3].

eSignatures / eIdentity Legislation

The Law of 13 March 2000 on electronic signature gives legal value to electronic signatures and electronically-signed documents, and further implements the EU Directive 1999/93/EC on a Community framework for electronic signatures. This law was complemented by an application decree issued on 30 March 2001.

Ordinance on electronic interactions between public services users and public authorities and among public authorities

The so-called 'teleservices ordinance' of 8 December 2005 gives the same legal force to an eSignature on public documents as that of a hand-written signature.

Cyber crime legislation[4]

France was one of the first European nations to draft specific cyber-crime provisions, through the Information Technology and Liberty Act (Loi Informatique et Libertés) of 1978, and more significantly the so-called Godfrain Act (Loi Godfrain) of 5 January 1988. The Godfrain Act updated the French penal code by introducing a section regarding the intrusion in information systems (articles 323-1 to 323-7). This section has been updated several times since its introduction. The most recent modification occurred through the Act of 21 June 2004 Reinforcing Trust in the Digital Economy (Loi du 21 juin 2004 pour la Confiance dans l'Economie Numérique).

Additionally, several other provisions have been adapted in the past few years to ensure their applicability in the information society, e.g. regarding fraud, the distribution of child pornography, commercial communications (including spam), and interception of private communications. Specific provisions have also been introduced in the Penal Procedure Code, e.g. regarding encryption/decryption, communications monitoring, and data seizure.

[3] *http://www.legifrance.gouv.fr/WAspad/UnCode?&commun=CPOSTE&code=CPOSTESL.rcv (Legislative Part)*

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

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	• **Secrétariat Général de la Défense et de la Sécurité Nationale – SGDSN** • **Agence Nationale de la Sécurité des Systèmes d'Information - The French Network and Information Security Agency – ANSSI** • **Commission Nationale de l'Informatique et des Libertés– French Data Protection Authority – CNIL** • **Autorité de Régulation des Communications Électroniques et des Postes– French Telecommunications and Posts Regulator – ARCEP** • **Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication– Central Office for the Fight against Crime Related to Information Technology and Communication – OCLCTIC** • **The Ministry of Economy, Industry and Employment – Haut Fonctionnaire de Défense et de Sécurité** • **Délégation aux usages de l'internet– Internet Usage Delegation – DUI** • **Direction du développement des médias – Directorate for Media Development - DDM** • **Direction générale de la modernisation de l'Etat – State administration modernisation directorate – DGME**
CERTs	• COSSI (ITSOC) • CERT-Renater • APOGEE SecWatch (devoteam) • Computer Emergency Response Team - Industrie, Services et Tertiaire (Cert-IST) –Computer Emergency Response Team - Industry, Services, and Tertiary • CERT-LEXSI • CERT-Société Générale
Industry Organisations	• Alliance TiCS
Academic Organisations	• Renater - Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche
Others	• Club de la Sécurité de l'Information Français– French Information Security Club – CLUSIF • Confiance Project • Observatoire de la Sécurité des Systèmes d'Information et des Réseaux– Observatory of Information Systems and Network Security – OSSIR • OWASP France • Association Française de l'Audit et du Conseil Informatiques - ISACA France – AFAI • UFC-Que choisir • CLCV - Confédération de la Consommation, du logement et du cadre de vie • OR.GE.CO - Organisation générale des consommateurs

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 Inventory[5]

[5] http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country

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.

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

Dialogue platform with the CICREST[6]

This platform in charge of defence and public security includes, amongst others, the commissioner of defence telecommunication, representatives of different ministries, the president of the regulating authority of the telecommunications a representative of France Télécom, a representative of the telecommunication networks, a representative of the suppliers of telecommunication services.

Through this platform, CICREST informs the ministerial departments on the performance of the authorized networks. The platform harmonizes the conditions in which the performances have to be ensured and, if applicable, proposes the needed changes.

In case of crisis, the CICREST will ensure the coordination of the actions of the different operators so that performances can be delivered adapted to the needs of the ministries and the companies and organisations. They will also inform the governmental authorities on the condition of the national en international telecommunications.

Information exchange between the telecom operators and the governmental authorities

Following the 2006 decree[7] on CIP, every operator or provider designated has to submit a **masterplan** for security. It is used to check whether the operator or provider is compliant with national security guidelines (confidential not published). Once the operators have submitted their security master plan, the HFDS (The Ministry of Economy, Industry and Employment – Haut Fonctionnaire de Défense et de Sécurité) follows up to verify if the plan has been implemented properly and satisfactorily. The work is still in progress. By 2010 these masterplans will have been a) submitted and, most importantly, b) implemented. In turn, HFDS will have the necessary data and can, if necessary, change regulation accordingly. The security masterplan, as to be submitted by each operator, allows addressing risk management issues. Specifically, this will be useful for evaluating how the operator tries to address which risk using what measures to reduce the likelihood of network failure.

Information platform on the legal framework

A permanent working group among the public authorities and the telecommunication operators called — Commission interministérielle de coordination des réseaux et services de télécommunications pour la défense et la sécurité publique— (CICREST) discusses the evolution of the legal framework.

---

[6] *http://www.droit.org/jo/20010529/PRMX0104748A.html*

[7] *http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000634536&fastPos=3&fastReqId=1619653505&categorieLien=id&oldAction=rechTexte*

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

Emerging NIS risks

Since its inception, the operational center of the security of information systems (COSSI) in France identifies each year an increasing number of attacks. Even if unsolicited messages (spam) and disfigurements of websites are the most visible attacks, they are actually the background noise of the Internet. New forms of cybercrime, such as botnet networks, and targeted attacks are real strategic threats.

Widespread attacks targeted

The use of malicious code (Trojan horses ...) in order to steal sensitive information does not limit the scope of the sensitive state. It affects all activities in which competition exists among States or between businesses, which represent a prime target for hackers. The observed shift of massive attacks by means of computer virus attacks to more focused and discrete attacks, is the result of a professionalization of hackers, now motivated by profit rather than by recognition of their expertise. They can also make available pharmacies, businesses or state, for compensation, their technical or learn how.

Incredible capabilities of botnets networks

Botnets, large networks of infected computers controlled remotely, offer the aggressors capacity of attacks without limit. Today mostly used to spread massively unsolicited messages, they can also be used to conduct blocking operations (denial of service). Thus the attacks against Estonia in 2007 were largely carried out through networks of botnets. When we know that larger networks have reached the million compromised machines and the attacks in Estonia were conducted from a few thousand computers, we can better understand the threat posed by these networks.

The systematic use of computer attacks in protest

In 2006, following the publication of cartoons of Prophet Mohammed in the newspaper France Soir and Charlie Hebdo, the French websites have been defaced. Many others have been defaced during debates and subsequent the adoption by the National Assembly of the draft law aimed at punishing Armenian genocide denial in October 2006.

This development has reached a level never seen before in connection with computer attacks suffered by Estonia in 2007. This event caused riots and different computer attacks to government websites and private websites (media, banks) in Estonia. These attacks were aimed at making government websites inaccessible but also render useless the entire Internet in Estonia. In 2009, in Iran, several disfigurements of government sites have been identified following the publication of results of the presidential election of June 12.

The vulnerability of control systems and industrial control

Emerged in the 1960s, the SCADA systems (Supervisory Control and Data Acquisition) are used in most industrial processes to ensure real-time acquisition data, supervision and control processes. They are present in many sectors of vital activities, such as transportation and power generation, transformation of chemicals and hydrocarbons,

control of water quality and effluent. These systems designed to maximize availability and efficiency of industrial processes, can introduce vulnerabilities that could be exploited for malicious purposes.

Some figures

In 2008, nearly a million websites have been defaced in the world. Phishing literally exploded since 2005. Banks and electronic communication operators are regularly affected. In 2008, the operational center of the security of information systems (COSSI) has been close more than 2,200 phishing sites, against 400 in 2006.

Resilience aspects

The national risk management process and preparedness measures[8]

Each Ministry is tasked with doing a risk assessment regarding network resilience and information security by using a specific method. Most ministries and government agencies use EBIOS (Expression of Needs and Identification of Security Objectives). Other approaches exist, such as the Méthode Harmonisée d'Analyse de Risque (MEHARI) offered by CLUSIF (Club de la Sécurité de l'Information Française). Both approaches lead more or less to the same results. All knowledge and results are centralised at the Secretariat-General for National Defence and Security (SGDSN).

The Ministry of the Interior manages national crises, while the operational end is with the inter-ministerial operational centre of crisis management.

France approaches the preparedness and recovery measures challenges on two levels: national and local level. Every master security plan submitted by an operator has to address both two levels in detail. France conducts exercises regularly as far as the security of information systems and data are concerned.

Incident response capabilities[9]

For communication networks breakdown, incident response depends on the very nature of the failure and must take into account that networks are geographical. Nevertheless, for security breaches, cooperation between CERT's, software vendors and so on is used. Past records show that a major outage in the public communications networks occurs every two to three years. Most likely it will be a software-related problem that triggered an incident. All major failures require submission of a special report and later investigations.

Guidelines for procurement

An incident in 2007 resulted in recommendations and specifications that will be part of the service level agreement (SLA) for new contracts between the government and telecom providers. The recommendations culminating from analysing the 2007 incident were passed on to a working group that developed new procurement guidelines.

---

[8] *http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies*

[9] *http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies*

Regulatory issues of resilience of public and other essential eCommunications networks[10]

ARCEP's main focus is not on dependability and resilience but, on innovation, pricing, regulatory compliance and so forth. France Telecom, the incumbent and universal service provided can be fined by ARCEP if its service does not function properly such as due to a blackout in a region of the country. Investigation regarding such an incident will be done by the Ministry of Economy, Industry and Employment - HFDS group (Commissariat aux Télécommunications de Défense) since this would be identified as a matter of national security. In general, guidelines are written by the ANSSI and must be implemented by the HFDS of the different ministries. These guidelines are made available to private companies.

Audits related to resilience[11]

Audits on the resilience master plan do not take place. The operators, and above all the historical incumbent are very active in the area of resilience and their work is appreciated. CGIET and HFDS are familiar with their procedures and networks. Trust' and prove' play an important role here. Newer or small communication operators may be under more cost pressure than more established ones. In turn, this might affect or at least influence their risk management to some degree. France's state authorities are aware of this and, therefore, keep careful watch regarding resilience and dependability of these networks. Security master plans must be submitted by critical infrastructure operators. In turn, once submitted, HFDS will have to assess through an audit how well the operators have implemented the plan. A third party may conduct part of such an audit.

Privacy and trust

Status of implementation of the Data Protection Directive

After a long legislative process, France (being the last EU Member State to do so) finally implemented the Data Protection Directive into national law pursuant to Law no. 2004-801 of 6 August 2004 relating to the protection of individuals against the processing of personal data and decree no. 2005-1309 of 20 October 2005, as amended by decree no. 2007-451 of 25 March 2007. This last law modifies the French Data Protection Act of 6 January 1978 (the "DPA").

The competent national regulatory authority on this matter is the Commission Nationale de l'Informatique et des Libertés (the "CNIL").

Personal Data and Sensitive Personal Data

The definition of personal data in the DPA is closely based on the standard definition of personal data. It only applies to individuals as opposed to legal entities.

---

[10] *http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies*

[11] *http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies*

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

The data controller or any person acting under its instructions must comply with the general data security obligations.

Data protection breaches

The DPA does not contain any obligation to inform the CNIL or data subjects of a security breach. In practice, contracts with sub-contractors will include an obligation on the sub-contractor to notify any breach of the DPA (and/or of the contract) to the data controller.

Enforcement

The CNIL has the power to take enforcement action in France. It has the ability to fine organisations itself as it may issue financial sanctions (i.e. administrative fines). Prosecutions for criminal offences are brought before the French criminal courts, which have the power to impose criminal fines and/or imprisonment.

NIS awareness at the country level

Awareness actions related to Information Security in general

The French Network and Information Security Agency set up an information portal (www.securite-informatique.gouv.fr) to offer practical information and advice to citizens, professionals and SMEs. The information includes a glossary of computer security jargon, guidelines on how to configure softwares, technical information regarding the Information security, on-line trainings, solutions to protect computers, security threats alerts,...

Signal Spam [12] is an association which gathers together most French organisations concerned by the anti-spam's fight. The association's goal is to fight spam (unwanted or illegal e-mails) and its effects, with users and professionals, in France as in international. This association invites Citizens and professionals to participate in the anti-spam's fight by adopting best practices. A series of recommendations is available on-line related to the confidentiality, filtering and security. Moreover, Plugins Signal Spams are available on-line and the members have the possibility to notify a spam address.

The fourth edition of the SecurityDay took place in place in France on April 29th, 2009. The thematic 2009 was the Security Management. The Clusif provided a presentation on the malicious acts over the phone.

Each year, the Observatory of the Information Security of systems and networks or OSSIR ("Observatoire de la Sécurité des Systèmes d'Information et des Réseaux") organized a day on the Information Security, called JSSI ("Journée de la Sécurité des Systèmes d'Information"). The JSSI'2010 took place on March 17th, 2009. The main topic was the new faces of the IT insecurity.

[12] *www.signal-spam.fr*

Awareness actions related to Internet Security for teenagers

The European Commission supports an awareness program in France, composed of:

- Internet Sans Crainte, an awareness project [13]
- NetEcouteFamille, phone assistance
- Point de contact, On-line service to notify illegal websites

Internet Sans Crainte is the French node of the European awareness raising network, part of the Safer Internet Program. The program aims both at reaching children and teenagers directly and at addressing their parents and educators. It also federates at the national level the main actors involved in the protection of minors over the Internet, and supports e-prevention actions. It relays the Safer Internet European campaigns in France. Internet Sans Crainte youth panel gathers about 30 young people aged 13-17 issued from diverse commissions of a local authority council (Conseil Général de l'Oise). The panel meets five times per year and is called upon both as a study group on Internet uses and behaviour and as a consulting committee for the creation of adapted Internet Sans Crainte awareness tools. Internet Sans Crainte provides awareness kits to help educators, teachers and other professionals to organize workshops in schools, educational and leisure centers and shows and exhibits. This material is available on demand on the website, for example: Children corner with cartoons and games; Teenager's corner with videos, advices, and a serious game soon to come; Information and advices for parents; Pedagogical tools and to help teachers organize workshops in schools and News. Addressing young people directly, the Vinz and Lou cartoons are given as the starting point for workshops for teachers and educators and in B2i (IT and Internet Certificate) classes. vinz and lou on the Internet is broadcast by M6 and has been adapted for print as a strip (M6 Editions). It has also been widely distributed in primary schools.

e-enfance is a French non-profit organization funded by private donors[14]. It aims at informing parents and children about responsible Internet use, via PCs, mobile phones, and gaming consoles. The e-enfance mission focuses on making adults more aware of their "cyberparent" role. E-enfance has set up phone assistance at the national level for the teenagers' protection on Internet. Several advices on the Information security are available on-line.

A Non-governmental organisation, located in all French-speaking countries in Europe, called "Action Innocence" [15] contributes to preserve the dignity of children on the Internet. The association cooperates with the Canton of Geneva Department of Justice, Police and Safety, as well as the Canton's Department of Public Education. "Action Innocence" develops the following actions:

- Behaviour survey of teenagers using Internet
- Risk analyse for which teenagers could be faced with on Internet
- Development and diffusion of prevention programs
- Creation and distribution of materials for prevention
- Development of new technologies in collaboration with the policy Departments in Europe

[13] *www.internetsanscrainte.fr*

[14] *www.e-enfance.org*

[15] *www.actioninnocence.org*

Leaflets, cartoons, webcasts and pedagogical tools (advices and videos) for parents and teachers are available on the website.

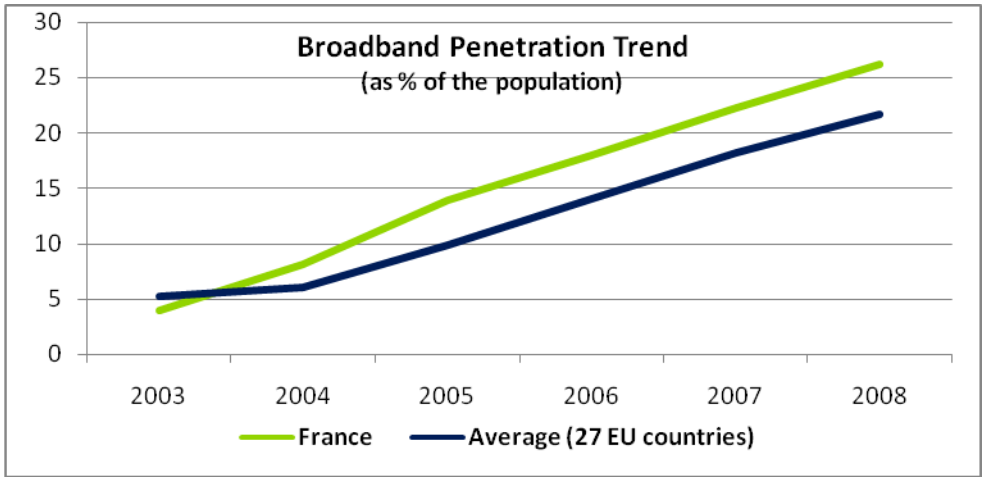
Awareness actions related to electronic administration

By opening a new website [16], the state administration modernisation directorate (Direction générale de la modernisation de l'Etat) –would like to facilitate the access to reference documents giving a state of art on the electronic administration. On this website, several referential are available such as the General Security Referential. The purpose of this referential is to fix a security baseline to promote the information security. The referential contains a set of security rules that the administrative authorities and their suppliers have to comply with.

Relevant statistics for the country

The information society in France is at a relatively average maturity stage of development. The progress made can considered as constant over the last years: averaged rankings on broadband penetration, of Internet usage and e-Governance and its constant progression through the years show that France is a bit in progress regarding the European trend.

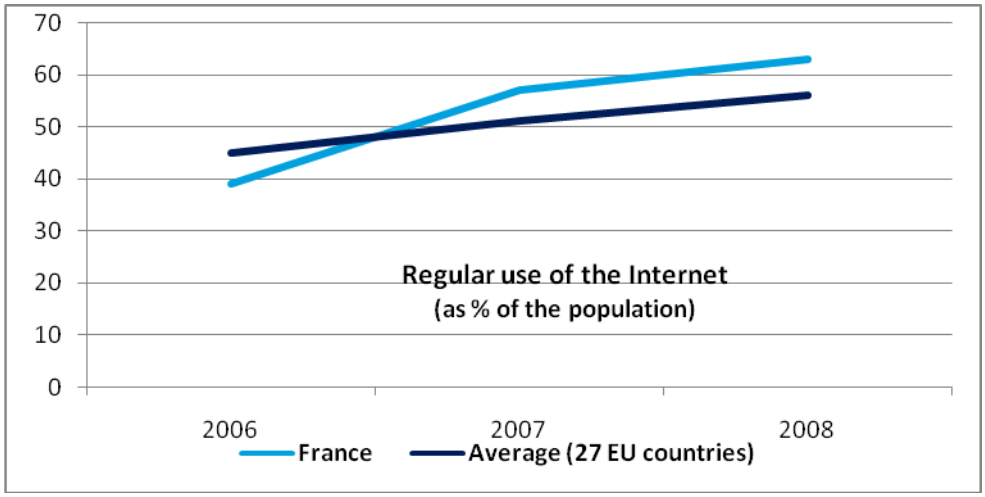
Based on the Eurostat[17] information, it appears that the broadband penetration trend for Sweden is significantly currently above the EU average:



Based on the same source of information, the regular use of Internet by the population (use as % of the population) is since 2007 above the EU average but it continues on an increasing path. Rates of internet usage have been gradually improving over the last few years. Nevertheless, take-up of the Internet in France is still low and a certain segment of the population has never used the Internet. But we may conclude that the usage of Internet services is correspondingly averaged.

[16] *www.references.modernisation.gouv.fr*

[17] *Source: Eurostat*


70
60
50
40
30
20
10
0
Regular use of the Internet
(as % of the population)
2006
2007
2008
France
Average (27 EU countries)

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Agence Nationale de la Sécurité des Systèmes d'Information - The French Network and Information Security Agency - ANSSI	The agency replaces the present Central Directorate for Information System Security (DCSSI), and is assigned wider missions and resources. The creation of the French Network and Information Security Agency on July 7th, 2009 is a milestone in the process of improving France's capability to protect its sensitive information systems. The core missions of this new agency are to: • Detect and early react to cyber attacks, thanks to the creation of a strong operational centre for cyber defence, working round-the-clock and being in charge of the continuous surveillance of sensitive Governmental networks, as well as the implementation of appropriate defence mechanisms ; • Prevent threats by supporting the development of trusted products and services for Governmental entities and economic actors ; • Provide reliable advice and support to Governmental entities and operators of Critical Infrastructure In the agency, there is a service in charge of training public officials in the field of system security information (SSI), called the CFSSI. The agency contains a certification body of the Central Directorate for Information Systems Security as well. This Certification body is responsible for examining certifications according to the directives given by the certification management committee.	http://www.ssi.gouv.fr/
2. Commission Nationale de l'Informatique et des Libertés– French Data Protection Authority - CNIL	CNIL's overall responsibility is to ensure that the development of information technology remains at the service of citizens and does not breach human rights, privacy, or personal or public liberties. CNIL holds specific competences to access on behalf of citizens' state security, defense and public security files, including those of the security and investigation branches of the police force. The authority supervises compliance with the law by inspecting IT systems and applications. It authorizes the implementation of sensitive files, such as the ones including biometric data. Furthermore, it puts forward statutory and regulatory measures to adjust liberties and privacy protection to IT and technical changes.	http://www.cnil.fr
3. Autorité de Régulation des Communications Électroniques et des Postes– French Telecommunications and Posts Regulator	ARCEP is the National Regulation Agency for Telecoms, driven by Telecom Paquet's EU Framework. In the telecommunications sector, ARCEP is responsible for applying the legal framework resulting from transposition of the European directives on electronic	http://www.arcep.fr

- ARCEP	communications.	
4. Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication– Central Office for the Fight against Crime Related to Information Technology and Communication - OCLCTIC	The office was established in May 2000 and has operational and technical competence in the area of cyber-crime. The main task of the office is to facilitate and coordinate police activities against cyber-crime at the national level. The OCLCTIC is the international contact point in the area of cyber-crime. The tasks of the OCLCTIC include carrying out investigations and assisting the police, the gendarmerie & the Directorate General for Competition, Consumption and Fraud Prevention in their judicial activities. OCLCTIC supports local and regional police with IT expertise, IT data collection, and other IT crime-related needs	http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organization/dcpj/cyber-criminalite
5. Délégation aux usages de l'internet– Internet Usage Delegation - DUI	The overall remit of the DUI is to bridge the digital gap in France. The DUI's tasks include: the creation of public access points to the Internet; the promotion of alternative access technologies; the Internet safety for the public (especially the protection of minors) and the ICT training and support.	http://www.delegation.internet.gouv.fr/mission/index.htm
6. Direction du développement des médias– Directorate for Media Development - DDM	The DDM is responsible for implementing public policy in the realm of the media and the information society. The DDM sets up the Signal Spam initiative.	http://www.ddm.gouv.fr/ http://www.signal-spam.fr/
7. Direction générale de la modernisation de l'Etat – State administration modernisation directorate - DGME	The State administration modernisation directorate created in 2005 is part of the Budget Ministry. The DGME advices the ministries in their egovernment strategies, identifies the egovernment possibilities and assists them in th e implementation of new strategies.	http://www.modernisation.gouv.fr

Computer Emergency Response Teams (CERTs): roles and responsibilities

CERT	FIRST member	TI Listed	Role and responsibilities	Website
8. Centre opérationnel pour les systèmes et sécurité de l'information – Operational Centre for Information Systems Security - COSSI (ITSOC)	No	Yes	COSSI is part of the French Network and Information Security Agency (ANSSI), it is the French cyber defense centre. For governmental authorities, it is in charge of prevention, detection and protection against cyberattacks and coordinates the governmental answer to cyber crisis. COSSI includes the French governmental CERT (CERTA) which acts as the technical cell for COSSI.	http:///www.ssi.gouv.fr http:///www.cerca.ssi.gouv.fr
9. CERT-Renater	Yes	Yes	CERT RENATER, founded in 1995, serves the members of the National Telecommunications Network for Technology, Teaching, and Research (RENATER) in matters of information security, particularly in the areas of security protection and threat detection and resolution.	http://www.renater.fr/Securite/CERT_Renater.htm

			Its prime function is to be a point of contact: the structure to call when help is needed and that organizes the help in case of an incident. This structure offers the possibility to centralize and divulgate information through secure channels.	
10. APOGEE SecWatch (Devoteam)	No	Yes[18]	Devoteam is a consultancy and engineering company in information system infrastructures in Europe, specialising in information system infrastructures. They offer consulting services: Strategy, organisation, business process and independence and proven methodologies. They also design and implement solutions which are appropriate to the needs defined by our clients with suitable technology: Implementing solutions, Commitment to results and a transfer of skills. Devoteam has developed the Business Relationship Management (BRM) approach, answering the main concerns of all of our clients: information system alignment, costs, quality and risks. Knowledge management and training are the key factors for differentiation and growth for our workforce and our clients. Their project rests on 3 pillars: a Permanent University, a team dedicated to Knowledge Management and the Knowledge Communities. Devoteam works with all sectors of the private (industry and services) and public (public services) economy. The Group focuses on a large number of these sectors in which it has developed its expertise.	http://www.devoteam.com
11. Computer Emergency Response Team - Industrie, Services et Tertiaire (Cert-IST) – Computer Emergency Response Team - Industry, Services, and Tertiary	Yes	Yes	Cert-IST was created by a consortium of French companies in 1998. The association has four partner members – CNES, France Telecom, Sanofi Aventis, and the Alcatel-Lucent group – that have access to all Cert-IST services, and adherent members that have partial access to services. Cert-IST (Computer Emergency Response Team - Industry, Service and Tertiary) is a not for profit association, which goal is to provide to its adherents risk prevention services and assistance for incident handling. Cert-IST is a centre for alert and reaction to computer attacks dedicated to French enterprises, member of FIRST, and with several partners, both French and European.	http://www.cert-ist.com

[18] The APOGEE SecWatch CSIRT is a private group Devoteam - the TF-CSIRT lists this CERT, which is under accreditation; https://www.trusted-introducer.org/teams/teams-a.html#APOGEE-SECWATCH.

			Principal activities are measures for risk prevention and incident handling. Cert-IST associative mode guarantees its independence towards editors. It works for the community by sharing resources and experience. Cert-IST durability is ensured by its adherents and the involvement of partner members. The adherent confidence in the Cert-IST is strengthened daily by: • The truthfulness and the exhaustive character of the information released • The confidentiality of private information always demonstrated • The guarantee of objectivity • The sustainable activities • Cert-IST commits itself to provide rated information in the best delays to qualified persons. Cert-IST works to make its products and services CVE compliant. Its Knowledge Base has been submitted to the CVE consortium review board as a candidate to the "CVE compatible" label. Cert-IST is currently in-line with CVE version: 20040901.	
12. CERT-LEXSI	No	Yes	The CERT-LEXSI is the monitoring and investigation division of LEXI, aimed at protecting online assets of organisations. It is implemented in Europe, Asia and North America. The CERT-LEXSI proposes a unique combination of technologies and talent to reduce the risks linked to the internet. Accredited CERT, the CERT-LEXSI proposes a response force to an incident and investigation 24/7. Their analysts, developers, and investigators work closely with the research community and the anti-fraud services worldwide.	http://www.lexsi.com/francais/certlexsi
13. CERT-Société Générale	No	Yes	The CERT of the Société Générale, a large international institution in France.	http://cert.societegenerale.com

Industry organisations active in network and information security: role and responsibilities

Industry organisations	Role and responsibilities	Website
14. Alliance TiCS	Alliance TiCS is a professional union created in 2003 by two unions SFIB (Technologies de l'Information) and GITEP TICS (Télécommunications) to represent the ICT industry and its related service industry both in France and in the European Union. Alliance TiCS contributes to the technological, economic and social development of French industry by participating directly or through its union members in the work of different national and European organisations. The mission of Alliance TiCS is to foster solidarity among its members and to act as a common platform advocating their interest at local and global levels.	http://www.alliance-tics.org/index.htm

Consumer organisations: role and responsibilities, tasks

Academic bodies	Role and responsibilities	Website
15. Renater - Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche	Renater is a national telecommunications research network, founded to bring together the telecommunication infrastructure for the purpose of research and education. The organisation also operates a CERT, more specifically CERT-Renater. This public interest body brings together many different research stakeholders such as CNRS, CPU, CEA, INRIA, CNES, INRA, INSERM, ONERA, CIRAD, CEMAGREF, IRD, BRGM, as well as the ministries of labour and education.	http://www.renater.fr

Other bodies and organisations active in network and information security: role and responsibilities

Other organisations active in NIS	Role and responsibilities	Website
16. Club de la Sécurité de l'Information Français– French Information Security Club - CLUSIF	CLUSIF, created in 1984, is a non-profit organization allowing professionals dealing with information security (including IT security) to meet, work, exchange opinions, and progress together. CLUSIF contributes to information security education, improvements, and awareness via publications resulting from the activity of its work groups, market studies, and public conferences. Most of the documents resulting from these activities are made publicly available. CLUSIF also regularly	http://www.clusif.asso.fr/

	initiates public studies on cyber-crime and security policies. An important contribution of CLUSIF to the management of information-related security is a comprehensive risk management methodology, called MEHARI, which is built around a set of modules, tools, and questionnaires.	
17. Confiance Project	The 'Confiance' project is a joint awareness initiative of the public and private sector, and 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.	http://www.delegation.Internet.gouv.fr/confiance/ presentation.html
18. Observatoire de la Sécurité des Systèmes d'Information et des Réseaux– Observatory of Information Systems and Network Security - OSSIR	Originally created inside the Military Academy for Telecommunications, OSSIR is a user organization which is still linked to the defense and military sectors. Widely opened to the IT security community, OSSIR gathers many experienced users in the public sector. It aims at promoting the security of information systems and networks in all its forms. It therefore operates forums in the form of mailing lists and monthly work and discussion groups, organises an annual conference, and publishes IT security-related materials to share knowledge.	http://www.ossir.org/
19. OWASP France	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 France organizes local events such as seminars and other specific events.	http://www.owasp.fr
20. Association Française de l'Audit et du Conseil Informatiques - ISACA France - AFAI	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 the France-Paris organizes local events such as education and training, workshops, roundtables and other specific events.	http://www.afai.fr/
21. UFC-Que choisir	A consumer organisation, its aim is to protect and educate consumers.	http://www.quechoisir.org
22. CLCV - Confédération de la Consommation, du logement et du cadre de vie	The CLCV, created in 1952, is one of the most important national associations for the consumers and clients. This association takes place in all the areas related to the daily life and the lifestyle.	http://www.clcv.org
23. OR.GE.CO - Organisation générale des consommateurs	This consumer organisation provides advices on method and legislative and regulatory information on the rights of the consummation.	http://www.orgeco.net

Country specific NIS glossary

ANSSI	French Network and Information Security Agency - Agence Nationale de la Sécurité des Systèmes d'Information
BEFTI	Brigade for investigation of ICT fraud - Brigade d'enquêtes sur les fraudes aux technologies de l'information
BPM	Brigade for the protection of minors - Brigade de Protection des Mineurs
CADA	Commission of Access to Administrative Documents
CERTA	French Governmental Computer Emergency Response Team
CICREST	Commission regulating networks and telecommunication services for Defense and Security - Commission interministérielle de coordination des réseaux et services de télécommunications pour la défense et la sécurité publique
CLUSIF	Club for Information Security - Club de la Sécurité de l'Information Française
CNIL	National Commission for Informatics and Liberty
COSSI - ITSOC	Information Technology Security Operational Center
DCSSI	Central Directorate for Information System Security
DPA	Data Protection Act
DNRAPB	National division for infractions against persons and goods - Division nationale de répression des atteintes aux personnes et aux biens
FFTelecom	French Federation of Telecoms and Electronic Communications - Fédération Française des Télécommunications et des Communications Électroniques
FNISA	French Network and Information Security Agency
HFDS	The Ministry of Economy, Industry and Employment – Haut Fonctionnaire de Défense et de Sécurité
JSSI	Day of the Information Security - Journée de la Sécurité des Systèmes d'Information
MEHARI	Harmonised Method for Risk Assessment - Methode Harmonisée d'Analyse de Risque
O.C.L.C.T.I.C.	Central Office for the Fight against ICT crime - Office Central de Lutte contre la Criminalite liee aux Technologies de l'Information et de la Communication
PCI	Payment Card Industry
Personal Data	The definition in the DPA is based on the standard definition of personal data. In particular, information is not personal data if identifying the relevant individual would require an unreasonable amount of time, cost and manpower.
SCADA	Supervisory Control and Data Acquisition
SGDSN	Secretariat-General for National Defence and Security
SLA	Service level agreement
STRJD	Technical service of criminal investigations - Service technique de recherches judiciaires et de documentation

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
- France - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/france
- French White Paper on Defence and National Security, published on June 17th, 2008: http://merln.ndu.edu/whitepapers/France_English2008.pdf
- Creation of a new agency: The French Network and Information Security Agency (FNISA): http://www.ssi.gouv.fr/site_article76.html
- Decree No. 2006-212 of February 23, 2006 on the safety of vital activity: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000634536&fastPos=3&fastReqId=1619653505&categorieLien=id&oldAction=rechTexte

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