

France 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: **Vincent Bouckaert, Dan Cimpean, Johan Meire and Nicolas Roosens.**

Legal notice

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

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

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

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

FRANCE	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
FOSTERING A PROACTIVE NIS COMMUNITY	11
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	13
SECURITY INCIDENT MANAGEMENT	13
EMERGING NIS RISKS	13
RESILIENCE ASPECTS	13
PRIVACY AND TRUST.....	15
NIS AWARENESS AT THE COUNTRY LEVEL	16
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	18
RELEVANT STATISTICS FOR THE COUNTRY	19
INTERNET ACCESS OF POPULATION AND ENTERPRISES	19
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS.....	20
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	21
OTHER STATISTICS.....	22
APPENDIX	23
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	23
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	24
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	26
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	26
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	26
REFERENCES	28

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 on the following Network and Information Security (NIS) related topics:

- *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*
 - *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

Context

As stated in the 2010 ENISA Country Report for France, this country conducted a thorough review of its defence and national security policies in recent years. New priorities have been set and endorsed by the president Sarkozy in the so called French White Paper on Defence and National Security¹, published on 17 June 2008.

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.

France's national strategy for the defence and security of information systems

In July 2009, the French government took a first step in this policy with the creation of ANSSI, the French Network and Information Security Agency, which acts as the national authority for cyber-security. Following these efforts, France issued a national strategy for the defence and security of information systems in February 2011².

This strategy relies on four major objectives: being a global power in cyber-defence and belong to the first circle of major nations in this area, while maintaining its autonomy; guarantee France's freedom of decision by the protection of sovereignty information; reinforce the French national vital infrastructures' cyber-security; and ensure security in the cyber-space.

Being a global power in cyber-defence

While maintaining its strategic autonomy, France must undertake the necessary efforts in order to belong to the first circle of major nations in the area of cyber-defence. Therefore, France will benefit from the multiplier effect of co-operations on both the operational level and the establishment of a unified strategy to tackle mutual threats.

Guarantee France's freedom of decision by the protection of sovereignty information

Government authorities as well as crisis management actors must have the means to communicate confidentially in every possible situation. Networks that correspond to this need must be extended, in particular to the territorial level.

The confidentiality of the information that transit through these networks requires the implementation of well-mastered security products. France must therefore keep the necessary skills for their conception and optimize their development and production modes.

Reinforce the national vital infrastructures' cyber-security

Society relies increasingly on information systems and networks, and in particular on the Internet. A successful attack against a critical information system or against the French Internet may cause

¹ Source: http://merln.ndu.edu/whitepapers/France_English.pdf

² Source: www.ssi.gouv.fr/site_article318.html

serious human or economical consequences. It is therefore important that the State, in close co-operation with the concerned providers and operators, works towards ensuring and improving the security of these critical systems.

Ensure security in the cyber-space

The French national strategy for the defence and security of information systems takes into consideration the fact that threats against information systems affect indistinctively administrations, enterprises and citizens, especially in France. As a matter of action to be taken by the French authorities, the administration must be exemplary and improve the protection of its information systems as well as the protection of the data entrusted to it.

Regarding enterprises and individuals, French national strategy foresees that an information and awareness program must be committed. As for fighting against cyber-crime, France will encourage the strengthening of the law and international judiciary mutual help.

In order to meet these objectives, seven "effort-axes" are chosen:

1. Better anticipate and analyze the environment in order to take the appropriate decisions.
2. Detect attacks and counter them, alert the potential victims and help them.
3. Increase and perpetuate France's scientific, technical, industrial and human capabilities, in the objective of keeping the necessary autonomy.
4. Protect the information systems of the State and of the operators of vital infrastructure, for a better national resilience.
5. Adapt the law as to take into account the evolutions in technology and the new uses.
6. Develop France's international collaborations in the areas of information systems security, fight against cyber-crime, and cyber-defense, in order to better protect the national information systems.
7. Communicate, inform and convince, so as to enable French individuals to better understand the issues linked to information systems security.

The regulatory framework

eGovernment Act

As stated in last year's report, an ordinance on electronic interactions between public service users and public authorities and among public authorities. Since 2010, no major updates were brought to this.

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.

In May 2010, a referential on the security of information systems³ (RGS) was issued in order to enforce this ordinance. This referential is a general legal framework to promote and harmonize the use of trustworthy products within the administration.

Data Protection / Privacy Legislation

France adopted the Information Technology and Liberty Act (*Loi Informatique et Libertés*) on 6 January 1978, becoming one of the first European countries to have 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 organisation 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 website⁴.

Cyber crime legislation

France was one of the first European nations to draft specific cyber-crime provisions, through the Information Technology and Liberty Act of 1978⁵, 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*).

³ Source: www.ssi.gouv.fr/rgs

⁴ See: <http://www.legifrance.gouv.fr/WAspad/UnCode?&commun=CPOSTE&code=CPOSTESL.rcv> (Legislative Part)

⁵ See: ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf

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.

eIdentification/eAuthentication

General overview

France uses a national ID card for its citizens, and has plans to implement an e-ID card (INES) in the future. Other e-IDM tokens are also used, such as the Vitale Card (health insurance), the Healthcare Professional Card ("Carte Professionnelle de la Santé") or the Daily Life Card ("Carte de la Vie Quotidienne").

The certificate contained in the Daily Life Card is issued by local authorities through a PKI based system. The Vitale card's certificate (contained in hard crypto token) is also issued through a PKI based system, by the health insurance funds. Additionally, the national register acts as the authentic source for civil status information.

France is also experimenting a unique portal for the management of the federation of identities, <https://mon.servicepublic.fr/portail/>.

Activity via STORK

France is also active member of the European project STORK⁶ (Secure idenTity acrOss borders linKed) that is aimed at enabling businesses, citizens and government employees to use their national electronic identities in any Member State.

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

eSignatures/eIdentity specific 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 e-Signature on public documents as that of a hand-written signature.

⁶ The STORK project consortium consists of 29 participants representing 13 Member States and Iceland. A full list of participants in the STORK project is available at www.eidstork.eu

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"> • 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 générale de la modernisation de l'Etat – State administration modernisation directorate – DGME
CERTs	<ul style="list-style-type: none"> • COSSI (ITSOC) • CERT-Renater • 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	<ul style="list-style-type: none"> • Alliance TiCS
Academic Organisations	<ul style="list-style-type: none"> • Renater - Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche
Others	<ul style="list-style-type: none"> • 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"⁷ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁸.

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.

⁷ 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

⁸ <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

Dialogue platform with the CICREST

The French *Commission Interministérielle de Coordination des Réseaux et des Services de Télécommunication pour la Défense et la Sécurité Publique* - CICREST⁹ 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 decree¹⁰ on Critical Infrastructure Protection (CIP), every operator or provider designated has to submit a **masterplan** for security. This is used to check whether the operator or provider is compliant with national security guidelines (these guidelines are confidential, not published). Once the operators have submitted their security master plan, the French Ministry of Economy, Industry and Employment – *Haut Fonctionnaire de Défense et de Sécurité* (HFDS) follows up to verify if the plan has been implemented properly and satisfactorily.

The work is still in progress, and it was scheduled that by 2010 these masterplans should have been submitted and implemented. In turn, HFDS will have the necessary data and can, if necessary, change regulation accordingly. The security masterplan, as planned 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 French legal framework.

⁹ See: www.droit.org/jo/20010529/PRMX0104748A.html

¹⁰ See:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000634536&fastPos=3&fastReqId=1619653505&categorieLien=id&oldAction=rechTexte>

Fostering a proactive NIS community

International co-operation facilitated via the Franco-German Council of Ministers

The 12th Franco-German Council of Ministers, held in February 2010 under the chairmanship of both French President Nicolas Sarkozy and German Chancellor Angela Merkel, defined the roadmap of the bilateral cooperation between Germany and France for the coming years. Amongst the 80 measures accepted, France and Germany agreed to work together on strengthening the protective measures against cyber attacks and especially in the appropriate international forums¹¹.

The German and French authorities in charge of information systems security, namely the Bundesamt für Sicherheit in der Informationstechnik (BSI) and the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) are long used to work together, yet the development of new threats requires the partnership to be further reinforced. The year 2010 saw the reinforcement¹² of the bilateral co-operation between ANSSI and BSI.

International co-operation with the United States, via Cyber Storm III

ANSSI participated in September 2010 to the Cyber Storm III exercise, organised by the United States Department of Homeland Security (DHS), which involved thirteen countries¹³ and sixty private companies. This exercise lasted three days and had the aim of bringing a coordinated answer to a major IT crisis.

European co-operation via Cyber Europe 2010

On 4 November 2010, France and the other members of the European Union, as well as Iceland, Norway and Switzerland, participated in an exercise¹⁴ organised by ENISA simulating a massive attack against the European Internet interconnection points, paralyzing the network and disabling electronic communications.

International co-operation via NATO: Cyber Coalition 2010

From 16 to 18 November 2010, 24 NATO member states took part in a cyber-defence exercise¹⁵, aiming at the coordination of civil and military means of defence. ANSSI represented France, along with the French Ministry of Defence.

International co-operation via the European Government CERTs (EGC) group

CERTA is amongst the active members¹⁶ of the European Government CERTs (EGC) group. EGC is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.

¹¹ Source: BSI, see https://www.bsi.bund.de/cln_174/ContentBSI/EN/Press/pressreleases/BSI-ANSSI_050210.html

¹² See: www.ssi.gouv.fr/IMG/pdf/2010-02-05_Communique_commun_du_BSI_et_de_l_ANSSI.pdf

¹³ The 13 countries involved were: Australia, Canada, France, Germany, Hungary, Italy, Japan, New-Zealand, Sweden, Switzerland, Netherlands, UK, USA.

¹⁴ Source: www.ssi.gouv.fr/IMG/pdf/2010-11-05-Cyber_Europe_2010.pdf

¹⁵ Source: www.ssi.gouv.fr/IMG/pdf/2010-11-24-cyber_coalition.pdf

¹⁶ The members of the European Government CERTs group include: Austria - GovCERT.AT, Finland - CERT-FI, France - CERTA, Germany - CERT-Bund, Hungary - CERT-Hungary, Netherlands - GOVCERT.NL, Norway - NorCERT, Spain - CCN-CERT, Sweden - CERT-SE, Swiss - GovCERT.ch, United Kingdom - CSIRTUK, United Kingdom - GovCertUK; See more details at: www.egc-group.org

To achieve this goal, the EGC group members:

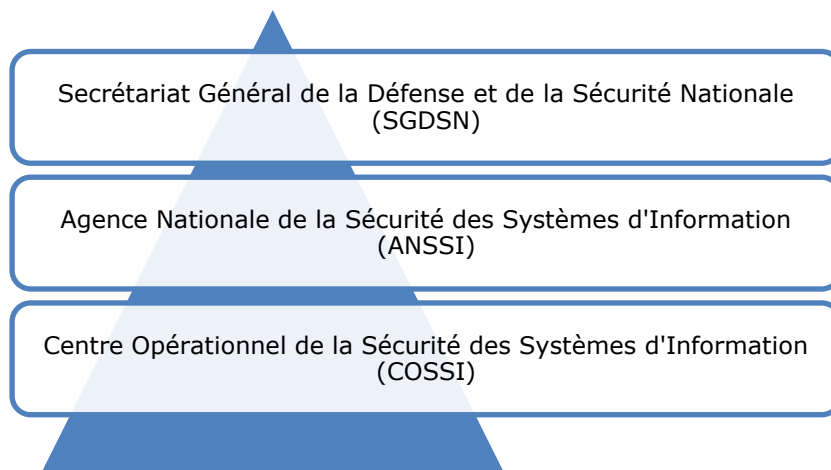
- Jointly develop measures to deal with large-scale or regional network security incidents;
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities;
- Identify areas of specialist knowledge and expertise that could be shared within the group;
- Identify areas of collaborative research and development on subjects of mutual interest;
- Encourage formation of government CSIRTs in European countries;
- Communicate common views with other initiatives and organisations.

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

Security incident management

As stated above, France has been involved in large scale exercises with international partners, enabling it to assess its reaction capacity towards major IT threats.

In order to defend governmental networks and information systems, the SGDN runs the Information System Security Operation Center (COSSI) which, in addition to its general preventive tasks, coordinates the action of French ministries and draws up protection and reaction measures. The centre also prepares and implements the Vigipirate plan against terrorist threats. COSSI operates around the clock, 365 days a year.



Emerging NIS risks

As described in the 2010 ENISA Country Report for France, 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.

Since the beginning of 2010, there were no major changes to the NIS risks identified in this country. The main ones are still botnets and the resulting spam and/or related attacks (phishing, pharming, DOS, etc.).

Resilience aspects

Compared with 2009, no major changes were identified on the grounds of resilience.

The national risk management process and preparedness measures

Each Ministry is tasked with doing a risk assessment regarding network resilience and information security by using a specific method¹⁷. Most ministries and government agencies use EBIOS

¹⁷ See: <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies>

(Expression of Needs and Identification of Security Objectives). Other approaches exist, such as the Méthode Harmonisée d'Analyse de Risque (MEHARI) offered by CLUSIF. 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 - *Secrétariat général de la défense et de la sécurité nationale* (SGDSN).

The French 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.

SGDSN did organised in June 2010 a national-wide exercise ¹⁸for responding to a major crisis affecting the critical information technology and telecommunication infrastructure: PIRANET 2010.

Incident response capabilities

For communication networks breakdown, incident response depends on the very nature of the failure and must take into account that networks are geographical¹⁹. 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.

Regulatory issues of resilience of public and other essential eCommunications networks

ARCEP's main focus is not on dependability and resilience but, on innovation, pricing, regulatory compliance and so forth¹⁶. 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

Specific audits on the resilience master plan¹⁶ do not currently take place in France on a large scale. 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

¹⁸ See more details on PIRANET 2010 at: http://www.ssi.gouv.fr/IMG/pdf/2010-06-25_Communique_de_presse_Piranet_2010.pdf

¹⁹ <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies>

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.

French 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 be involved to conduct part of such an audit – this is decided by HFDS.

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 French Data Protection Authority - *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.

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 and enforcement aspects

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.

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.

On 17 March 2010, CNIL published a report concerning on-site inspections and outlined its objectives for the coming year. In the report, which was adopted on 18 February 2010, CNIL indicated that it intends to conduct at least 300 on-site inspections throughout France in 2010, with a special focus on the following issues:

- Ensuring compliance with CNIL decisions, in particular the CNIL's standards for simplified notifications;
- Verifying that data controllers comply with the technical recommendations defined in their registration forms;
- Assessing the effectiveness of data protection officers within organisations.

CNIL also intends to focus on certain business sectors and concerns, such as:

- The airline industry, including customer relations (customer databases, mileage programs, “no-fly” lists, passenger name record data), airport security (body scanners, cameras in airports) and biometric passports;
- The real estate industry, including the collection of personal data by real estate agencies, test screenings, blacklisting and discriminatory practices;
- The protection of minors, including verifying the collection of personal data about minors, particularly in the context of direct marketing to minors by online merchants;
- The use of closed-circuit television (CCTV) for video surveillance, including verifying that such surveillance systems comply with the Data Protection Act and respect the privacy rights of individuals.

In 2009 CNIL conducted 270 on-site inspections, representing a 27% increase over 2008. According to CNIL, this increase in inspections and more effective enforcement is a result of a strengthening of CNIL’s powers in 2004. Of the 270 inspections, 22% led to warnings or sanctions and 85% of the inspections targeted private sector entities. The CNIL also noted that 92% of the organisations it inspected had not appointed a data protection officer²⁰.

NIS awareness at the country level

Awareness actions related to Information Security in general

No particular changes were noticed since the previous issue of this report on the grounds of awareness action related to general information security. As stated before, the French Network and Information Security Agency offers an information portal²¹ which contains information and advice for citizens, professionals and SMEs. The information includes a glossary of computer security jargon, guidelines on how to configure software, technical information regarding the Information security, on-line trainings, solutions to protect computers, security threats alerts, etc. In particular, a new good practice guide on outsourcing and cloud computing was issued in 2010.

Signal Spam²² 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.

Also worth mentioning is the association CLUSIF²³, which organises a certain number of conferences on IT security matters each year.

On the same grounds, the Observatory of the Information Security of systems and networks (OSSIR- “Observatoire de la Sécurité des Systèmes d’Information et des Réseaux”) organises a one-day event on Information Security, called JSSI (“Journée de la Sécurité des Systèmes d’Information”), on a yearly basis. The JSSI’2010 took place on March 16th, 2010 on the theme “Attack/Defense. Score 2.0”.

Awareness actions related to Internet Security for teenagers

²⁰ Also, more information about the CNIL’s agenda for 2010 may be found (in French) on the [CNIL’s website](#)

²¹ See: www.securite-informatique.gouv.fr

²² See: www.signal-spam.fr

²³ Club de la Sécurité de l’Information Français – www.clusif.asso.fr

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

- Internet Sans Crainte, an awareness project ²⁴;
- 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 organise workshops in schools, educational and leisure centers and shows and exhibits.

E-enfance is a French non-profit organisation funded by private donors²⁵. 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"²⁶ 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;
- 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 website²⁷, 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 RGS (see regulatory framework).

²⁴ See: www.internetsanscrainte.fr

²⁵ See: www.e-enfance.org

²⁶ See: www.actioninnocence.org

²⁷ See: www.references.modernisation.gouv.fr

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

The French Secteur d'activités d'importance vitale (SAIV) decree²⁸, issued in February 2006, addresses the particular topic that represents the security of "activities of vital importance". As such, it identifies all the sectors which are of vital importance for the country and for which it is essential to avoid any sort of neutralization. It also identifies the major actors in those sectors (OIV – "Opérateurs d'Importance Vitale").

Under the authority of a coordinating minister, a national security directive (DNS) will be written by the state in order to determine the menaces and possible attack scenarios for each sector.

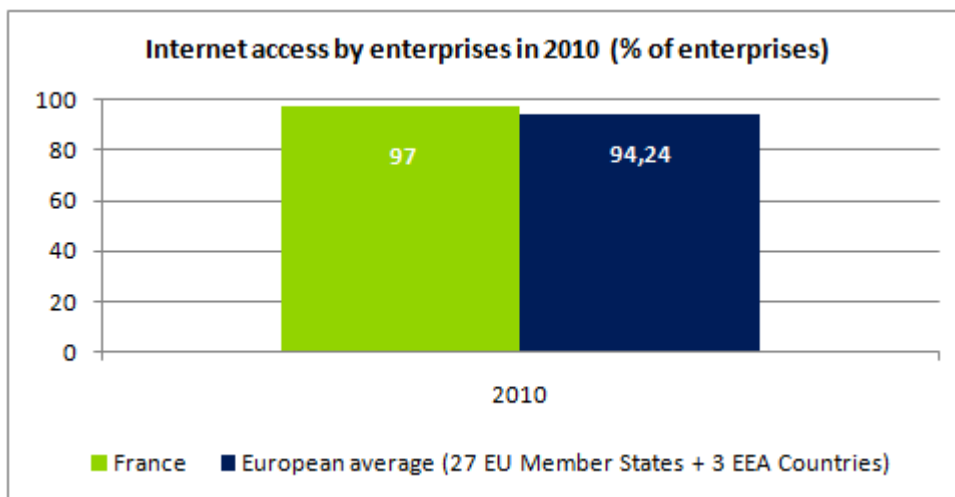
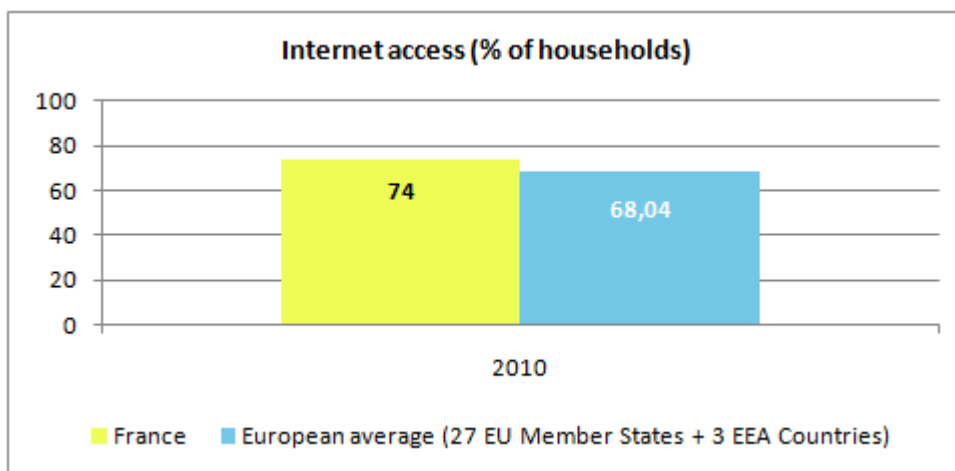
²⁸ Source: http://www.circulaires.gouv.fr/pdf/2009/04/cir_1338.pdf

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in France, a series of relevant statistics are included in this section. These statistics show that France is slightly above the European average regarding information technology matters.

Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation²⁹ of Internet access in France for enterprises and respectively households, relative to the European average.

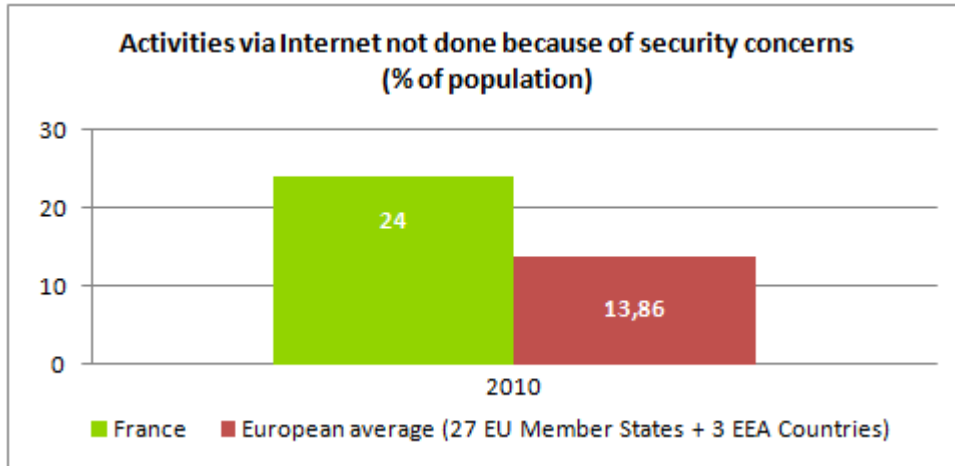


In 2010, the statistics indicate that both the enterprises and the households in France have a level of Internet access that is above the European average.

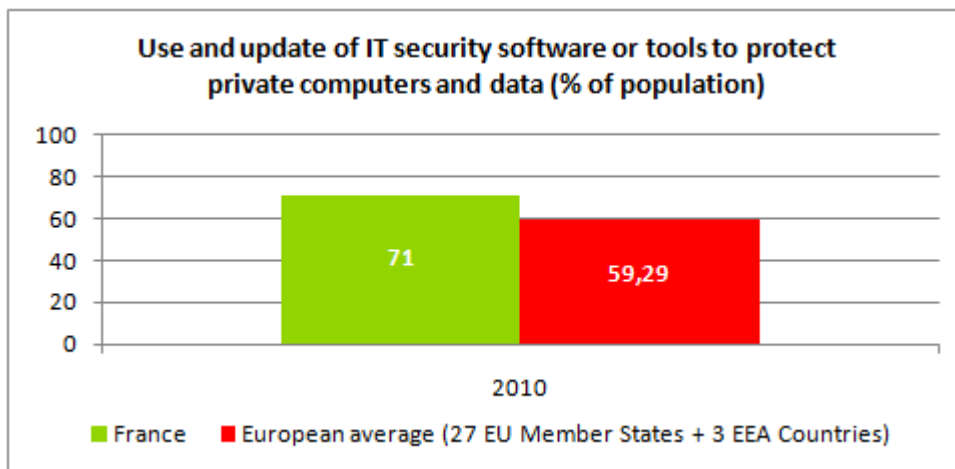
²⁹ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in France 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 nearly twice the European average:



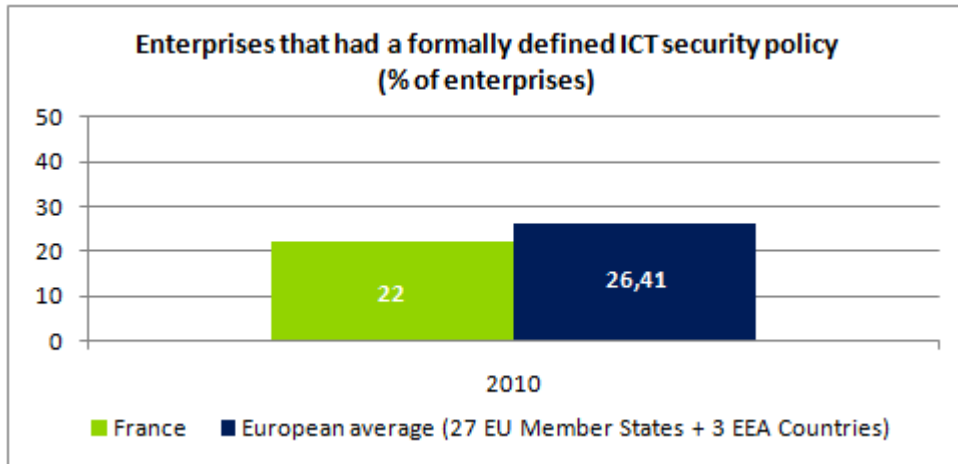
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



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

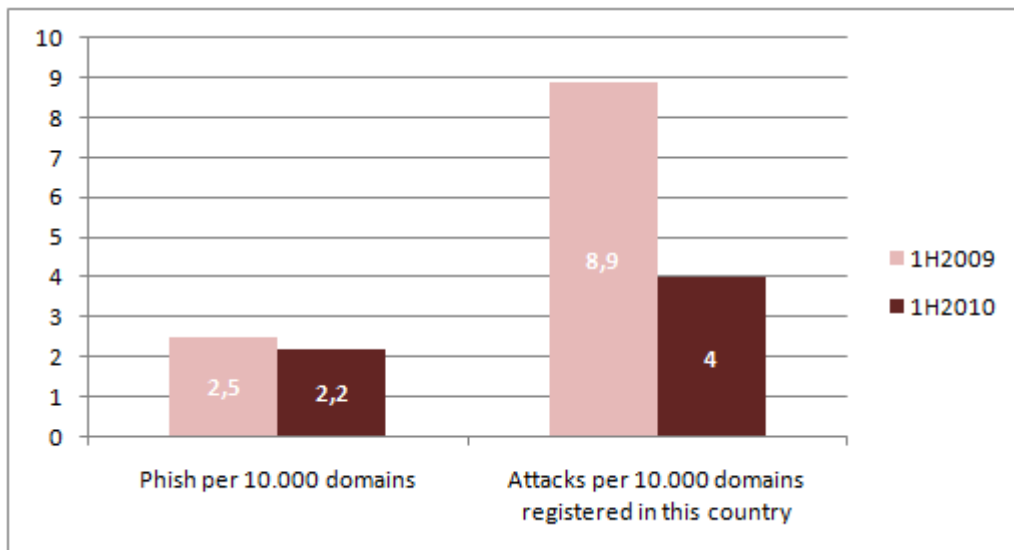
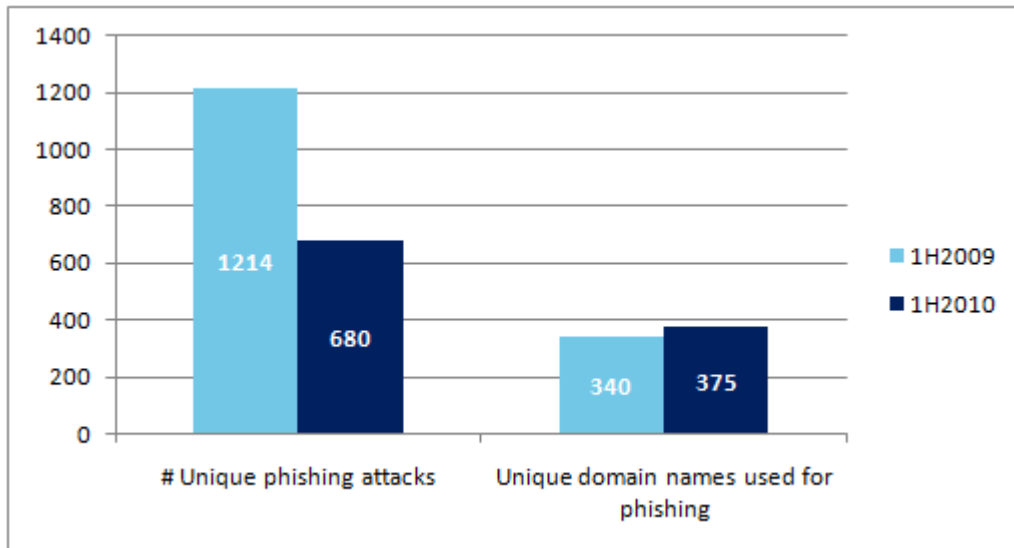
Statistics on use of Internet by enterprises and related security aspects

Fewer enterprises in France 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, France was mentioned in the global report³⁰ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



³⁰ 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. Agence Nationale de la Sécurité des Systèmes d'Information - The French Network and Information Security Agency - ANSSI	<p>ANSSI is now responsible to respond "immediately" in case of computer attacks "violent and paralyzing" the infrastructure of the state. Since February 13, 2011 the institution has seen its powers strengthened by a decree giving it the authority function of national defense information systems.</p> <p>The core missions of this agency are to:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>	www.ssi.gouv.fr/
2. Commission Nationale de l'Informatique et des Libertés- French Data Protection Authority - CNIL	<p>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.</p> <p>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.</p> <p>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.</p>	www.cnil.fr
3. Autorité de Régulation des Communications Électroniques et des Postes- French Telecommunications and Posts Regulator - ARCEP	<p>ARCEP is the National Regulation Agency for Telecoms, driven by Telecom Paquet's EU Framework.</p> <p>In the telecommunications sector, ARCEP is responsible for applying the legal framework resulting from transposition of the European directives on electronic communications.</p>	www.arcep.fr
4. Office Central de Lutte contre la Criminalité liée aux	<p>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</p>	www.interieur.gouv.fr/section/contact/police/questions-

National authorities	Role and responsibilities	Website
Technologies de l'Information et de la Communication – Central Office for the Fight against Crime Related to Information Technology and Communication - OCLCTIC	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.	cybercriminalite
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.	www.delegation.internet.gouv.fr/mission/index.htm
6. 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 advises the ministries in their eGovernment strategies, identifies the eGovernment possibilities and assists them in the implementation of new strategies.	www.modernisation.gouv.fr

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST³¹ member TI³² listed 	
7. Centre opérationnel pour les systèmes et sécurité de l'information – Operational Centre for Information Systems Security - COSSI	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 cyber attacks and coordinates the governmental answer to cyber crisis. COSSI includes the French governmental CERT (CERTA) which acts as the technical cell for COSSI. <ul style="list-style-type: none"> Not FIRST member; TI listed. 	www.ssi.gouv.fr www.certa.ssi.gouv.fr
8. CERT-Renater	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. Its prime function is to be a point of contact: the structure to call when help is needed and that organises the help in case of an incident. This structure offers the possibility to centralize and divulgate information through secure channels. <ul style="list-style-type: none"> FIRST member; TI listed. 	www.renater.fr/Securite/CERT_Renater.htm
9. Computer Emergency Response Team - Industrie, Services et	Cert-IST was created by a consortium of French companies in 1998. The association has four partner members – CNES, France Telecom, Sanofi	www.cert-ist.com

³¹ <http://www.first.org/members/teams/>

³² <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
<p>Tertiaire (Cert-IST) – Computer Emergency Response Team - Industry, Services, and Tertiary</p>	<p>Role and responsibilities</p> <ul style="list-style-type: none"> • FIRST³¹ member • TI³² listed <p>Aventis, and the Alcatel-Lucent group – that have access to all Cert-IST services, and adherent members that have partial access to services.</p> <p>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. Principal activities are measures for risk prevention and incident handling.</p> <p>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:</p> <ul style="list-style-type: none"> • The truthfulness and the exhaustive character of the information released • The confidentiality of private information always demonstrated • The guarantee of objectivity • The sustainable activities <p>Cert-IST commits itself to provide rated information in the best delays to qualified persons.</p> <p>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.</p> <ul style="list-style-type: none"> • Not FIRST member; • TI listed. 	
10. CERT-LEXSI	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> • Not FIRST member; • TI listed. 	<p>www.lexsi.com/francais/certlexsi</p>
11. CERT-Société Générale	<p>The CERT of the Société Générale, a large international institution in France.</p> <ul style="list-style-type: none"> • FIRST member; • TI listed. 	<p>cert.societegenerale.com</p>

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
12. Alliance TiCS	<p>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.</p> <p>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.</p>	<p>www.alliance-tics.org/index.htm</p>

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
13. Renater - Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche	<p>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.</p> <p>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.</p>	<p>www.renater.fr</p>

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
14. Club de la Sécurité de l'Information Français- French Information Security Club - CLUSIF	<p>CLUSIF, created in 1984, is a non-profit organisation allowing professionals dealing with information security (including IT security) to meet, work, exchange opinions, and progress together.</p> <p>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.</p> <p>CLUSIF also regularly 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.</p>	<p>www.clusif.asso.fr/</p>
15. Confiance Project	<p>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</p>	<p>www.delegation.Internet.gouv.fr/confiance/presentation.html</p>

Others	Role and responsibilities	Website
	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.	
16. Observatoire de la Sécurité des Systèmes d'Information et des Réseaux – Observatory of Information Systems and Network Security - OSSIR	<p>Originally created inside the Military Academy for Telecommunications, OSSIR is a user organisation 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.</p> <p>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.</p>	www.ossir.org
17. OWASP France	<p>The Open Web Application Security Project (OWASP) is an open-source application security project with local chapters. The OWASP community includes corporations, educational organisations, and individuals from around the world.</p> <p>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 organises local events such as seminars and other specific events.</p>	www.owasp.fr
18. Association Française de l'Audit et du Conseil Informatiques - ISACA France - AFAI	<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 France-Paris organises local events such as education and training, workshops, roundtables and other specific events.</p>	www.afai.fr/
19. UFC-Que choisir	A consumer organisation, its aim is to protect and educate consumers.	www.quechoisir.org
20. 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.	www.clcv.org
21. 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.	www.orgeco.net

References

- 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>
- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- French White Paper on Defence and National Security, published on June 17th, 2008: http://merln.ndu.edu/whitepapers/France_English2008.pdf
- 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>
- France's national strategy for the defence and security of information systems: www.ssi.gouv.fr/site_article318.html
- "Network Resilience within the French NIS strategy" presentation available at: <http://www.enisa.europa.eu/act/res/workshops-1/2009/providers-measures/resilience-workshop-folder/ENISA%20resilience%20workshop%20-%20French%20network%20resilience%20ANSSI.pdf>

