

# Finland Country Report



## About ENISA

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

## Contact details

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

### Mr. Giorgos Dimitriou

ENISA External Relations Expert

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

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



## Acknowledgments:

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

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **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.

## Table of Contents

<b>FINLAND .....</b>	<b>4</b>
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS .....	4
<b>NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES .....</b>	<b>5</b>
OVERVIEW OF THE NIS NATIONAL STRATEGY .....	5
THE REGULATORY FRAMEWORK .....	7
<b>NIS GOVERNANCE .....</b>	<b>11</b>
OVERVIEW OF THE KEY STAKEHOLDERS .....	11
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS .....	12
FOSTERING A PROACTIVE NIS COMMUNITY .....	14
<b>COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....</b>	<b>15</b>
SECURITY INCIDENT MANAGEMENT .....	15
EMERGING NIS RISKS .....	16
RESILIENCE ASPECTS .....	17
PRIVACY AND TRUST .....	18
NIS AWARENESS AT THE COUNTRY LEVEL .....	18
<b>RELEVANT STATISTICS FOR THE COUNTRY .....</b>	<b>21</b>
INTERNET ACCESS OF POPULATION AND ENTERPRISES .....	21
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS .....	22
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS .....	23
OTHER STATISTICS .....	24
<b>APPENDIX .....</b>	<b>25</b>
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY .....	25
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs) .....	29
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	30
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES .....	31
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	32
REFERENCES .....	33

## Finland

### The structure of the individual country reports

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

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

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

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

### Overview of the NIS national strategy

The first National Information Security Strategy in Finland was adopted in 2003. In December 2008 the Finnish Government adopted its second resolution on National Information Security Strategy. Since beginning of 2010, there were no changes to this strategy called "*Everyday security in the information society – a matter of skills, not of luck*".

The aim of this of this strategy remains focus on the fact that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services.

By 2015 Finland still aims to be the leading country in terms of information security. The Finnish Information security strategic objectives remain built on three main pillars which are:

- **Basic skills in the ubiquitous information society:** Information security involves more than just technology. In the ubiquitous information society, people need new kinds of basic skills that they did not possess before. Information security is still too often seen as being a disconnected part of overall ICT development. There are many kinds of information, and information security risks should be evaluated on the basis of the type of data concerned. Trust in the information society is built upon the service providers' and users' understanding of their rights and responsibilities. It is also important to improve the skills of business owners and corporate information security professionals;
- **Information risk management and process reliability:** Electronic services and communications are increasingly to be found at the heart of the service system in both the public and private sectors. At the same time, dependence on information technology is making services more vulnerable. People must be able to trust that the services they use are secure and that no confidential data will end up in the wrong hands. When a breach of information security occurs, for example in identity theft, people and businesses must be able to rely on adequate support from the authorities;
- **Competitiveness and international network cooperation:** Finland is part of the global information network economy, which means that a significant percentage of information security threats and attacks (e.g. denial-of-service attacks) originate outside the country's borders. Finland must be active in international cooperation between national authorities to prevent information security threats and minimise any possible damage. As well as making its own national regulatory environment simpler and more predictable for businesses, Finland must actively seek ways of influencing international regulation.

The implementation of the Strategy started when the Action Plan was adopted in November 2009. In the beginning of 2011 the first results of these projects have been presented. The action plan is based on the priorities set out in the Resolution.

The measures and follow-up necessary for the implementation of the Strategy are included in the Action Plan. There are in total nine projects constituting the action plan<sup>1</sup>.

The first pillar of the Finnish NIS strategy ("Basic skills in the ubiquitous information society") is covered by the action plan via the deployment of the two following projects:

- **Increasing information security awareness:** this project is aimed at assessing what basic security related skills in the ubiquitous information society mean and, based on this, has prepared information security communications for all the main population groups;
- **Service provider's responsibilities, rights and obligations:** the purpose of the project was to review the current situation in terms of service providers' responsibilities, rights and obligations. based on the results a recommendation on best practices was proposed. The project released its final report in February 2011. The report includes a study on current status of legislation concerning information security obligations of service providers and also a proposal for related best practices to be used in a situation in which a small and medium-sized enterprise (service provider) acquires websites or other online services from another company<sup>2</sup>.

The second pillar of the Finnish NIS strategy ("Information risk management and process reliability") is covered by the Finnish action plan through the deployment of the two following projects:

- **Identifying information risks and data protection requirements:** the project has surveyed appropriate risk management tools and inspected possibilities promoting their adoption. The project has also considered how training related to risk management and service continuity could be promoted, particularly in SMEs;
- **Safeguarding continuity of business activities and the public's access to services:** The purpose of the project is to review the means by which the functionality of information and communications services can be safeguarded.

The third pillar of the Finnish NIS strategy ("Competitiveness and international network cooperation") is covered in the current action plan via the deployment of the three following projects:

- **Promoting Finnish information security expertise and active participation in international standards development work:** this project will result in the preparation of a plan to improve the image of Finland as an information security country. Another focus of the project is to investigate how to promote Finland's opportunities to actively influence international standards development work and how to promote the wide scale utilisation of international standards;
- **Business competitiveness and the NCSA:** the project's purpose was to accelerate the establishment of a National Communications Security Authority (NCSA) in Finland and to find the necessary funding for this, particularly in terms of the future. The NCSA-FI functions started January 1<sup>st</sup> 2010 under the Finnish Communications Regulatory Authority;
- **Enhancing and activating national cooperation in international information security issues:** The project has contemplated on establishing a national forum to

<sup>1</sup> See: [http://www.lvm.fi/c/document\\_library/get\\_file?folderId=339549&name=DLFE-10210.pdf&title=Julkaisuja\\_51-2009](http://www.lvm.fi/c/document_library/get_file?folderId=339549&name=DLFE-10210.pdf&title=Julkaisuja_51-2009)

<sup>2</sup> See: <http://urn.fi/URN:ISBN:978-952-243-220-9> (in Finnish)

improve exchange of information and also considered other measures to enhance national cooperation in international information security issues.

Also the action plan supports two other projects not specifically related to one of the pillar of the Finnish NIS strategy which are:

- **Research project on near-future information security trends:** the project has surveyed near-future information security threats, which relate for example to new technologies, services, production models and corporate structures. The project also identified new trends as well as the risks and opportunities related to them;
- **Measuring information security:** The project has reviewed how the level of information security is currently monitored in Finland and, based on this, suggested a proposal on available measuring methods and mechanisms.

## The regulatory framework

### Overview of the Finish security policy

The national information society policy has not changed in comparison with previous year and still aims at increasing citizens' wellbeing and economic productivity by utilizing information and communications technology. In 2010 no changes in terms of foundation of the national information society policy have been identified. The national information society policy is still based on the two following elements<sup>3</sup>:

- On 21 June 2007, the Government appointed a minister-led Ubiquitous Information Society Advisory Board. The Advisory Board's task is to ensure the implementation of the national information society strategy as well as the aims outlined in the Government resolution. During its term of office, the Ubiquitous Information Society Advisory Board is expected to provide insight on the identification of priorities for the national information society policy as well as on the setting of ambitious but realistic goals;
- The Ubiquitous Information Society Advisory Board will report to the Government annually on the progress of key projects presented in the action programme. The action programme will be supplemented flexibly during the Government's term of office and updated according to new measures or perceived shortcomings.

The Internal Security Programme supports both the reduction of the number of offences highlighted in the Government Programme and the improvement cooperation between public authorities.

### Cyber attack legislation

Finland ratified the Council of Europe Convention on Cybercrime on 24 May 2007. In this connection, a number of the Criminal Code's provisions on cyber offences were amended by an Act (540/2007) that took effect on 1 September 2007. There is an updated English translation of the amended provisions<sup>4</sup> (amendments up to 940/2008 included). In Finland, cyber offences are criminalized to a great extent. The Coercive Measures Act (450/1987) sets the requirements to the authorities to act e.g. to launch the wiretapping. Since 2007 no major changes have been identified.

---

<sup>3</sup> See the following source:

[http://www.intermin.fi/intermin/images.nsf/files/7E16BE52F11364AEC2256F47002D6874/\\$file/internal\\_security\\_programme\\_summary\\_en.pdf](http://www.intermin.fi/intermin/images.nsf/files/7E16BE52F11364AEC2256F47002D6874/$file/internal_security_programme_summary_en.pdf)

<sup>4</sup> See: <http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf>

We also notice here that when detected, websites used for terrorist purposes in Finland would immediately be monitored with a view to a criminal investigation and possible prosecution. Where such websites and/or the users are located outside Finland, the relevant information is shared with the competent authorities according to national legislation on information sharing and data protection.

### **eCommunications Legislation**

The eCommunication legislation is still based in 2010 mainly on two acts:

- The Communications Market Act transposed the new EU Regulatory Framework for Electronic Communications through the Finnish legal framework. The Communications Market Act (393/2003) states that if a communications network or equipment item causes danger or interference to a communications network, equipment, communications network user or another person, the telecommunications operator or the keeper of another communications network or equipment shall take measures immediately to rectify the situation and, if necessary, isolate the communications network or equipment from the public communications network." (131 § paragraph 1);
- The Act on the Protection of Privacy in Electronic Communications transposed the "ePrivacy Directive" (2002/58/EC) into Finnish Law. Section 19 of the Act defines telecommunications operators and value added service providers obligation to maintain information security and Section 20 defines the measures taken to implement information security. Section 21 includes provisions concerning information security notifications in case where a violation or a threat is posed to the information security.

In 2010 the objective of the Act remains to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the balanced development of a wide range of electronic communications services.

### **eGovernment Legislation**

The eGovernment legislation has not been changed in 2010 and is still based on the Finnish Act on Electronic Services and Communication in the Public Sector (i.e. "the Act"). This Act has been developed to improve the smoothness and rapidity of services and communication as well as information security in the administration, courts and other judicial bodies, including the enforcement authorities by promoting the use of electronic data transmission.

The Act contains provisions on the rights, duties and responsibilities of the authorities and their customers in the context of electronic services and communication.

### **eCommerce Legislation**

The Act on the Provision of Information Society Services enacts the EU Directive on electronic commerce (2000/31/EC). The main issues governed by this Act revolve around the freedom to provide Information Society services, information requirements for service providers, electronic orders and electronic contracts, as well as related liabilities. In 2010 no updates of this eCommerce legislation have been noticed.

### **eProcurement Legislation**

The eProcurement Legislation is based on the following: Act on Public Procurement, Act on Public Procurement in Special Sectors, Government Decree on Public Contracts, Re-use of Public Sector Information (PSI).

## Self-regulations

### *Regulation on Barring Categories in Telecommunications (PDF)*

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

## eIdentity

### *General overview*

Finland uses e-ID cards (FINEID) for its citizens and for the non-nationals registered in Finland. Additional e-ID tokens are also used, such as the healthcare professional card.

The authentication certificate in the Finnish e-ID card is issued by local police stations through a PKI based system. The national ID card uses 4 certificates: two CA certificates and two user certificates (authentication and non-repudiation), which are all protected by different PIN codes. Certificate Revocation Lists (CRLs) are used for validation/management of the certificates' lifecycles. Other systems, notably KATSO and VETUMA, allow an authentication respectively for organisations and citizens and provide access to a range of online services from public administrations.

Non-PKI systems are also in use, notably the TUPAS system which was implemented by Finnish banks for use in e-banking applications.

Additionally, since 29 June 2009, all new passports issued in Finland include **fingerprints**. The fingerprints stored on the passport chip will improve passport security and contribute to establishing a more reliable link between the travel document and its holder.

Fingerprint data will also be entered in a national register which will help authorities to reliably identify people who apply for a passport or in situations where people need to travel. The aim of registration is to protect people's identity, improve personal security and prevent identity misuse that violates the right to privacy.<sup>5</sup>

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

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

### *eSignatures legislation*

The eSignatures legislation is based on the act on Strong Electronic Identification and Electronic Signatures (617/2009). This Act enforces the EU Directive on a Community framework for electronic signatures (1999/93/EC) and gives legal value to the use of electronic signatures for eCommerce and eGovernment services. In 2010 no updates of this eSignature legislation have been noticed.

---

<sup>5</sup> See: <http://www.epractice.eu/en/document/288223>

The **Act on Strong Electronic Identification and Electronic Signatures** entered into force on *1 September 2009* replacing the Act on Electronic Signatures issued in 2003. The objective of the new Act is to create common rules for the provision of strong electronic identification services.

It will likewise promote the provision of identification services and the use of electronic signatures. The Act is founded on the principle that users must be able to trust information security and protection of privacy when they use strong electronic identification services<sup>6</sup>.

---

<sup>6</sup> See: <http://www.epractice.eu/en/document/288223>

## NIS Governance

### Overview of the key stakeholders

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

<b>National Authorities</b>	<ul style="list-style-type: none"> <li>• Ministry of Transport and Communications Finland</li> <li>• Information Security Group of the Ubiquitous Information Society Advisory Board</li> <li>• FICORA (Finnish Communications Regulatory Authority)</li> <li>• Ministry of Finance</li> <li>• Ministry of Defense</li> <li>• VAHTI (Government Information Security Management Board)</li> <li>• Ministry of the Interior</li> <li>• The Advisory Board for Defence Information (ABDI)</li> <li>• Security and Defence Committee</li> <li>• Finnish Defence Forces (FDF)</li> <li>• Data Protection Ombudsman</li> <li>• National Emergency Supply Agency, NESA</li> <li>• National Board of Economic Defence, NBED</li> </ul>
<b>CERTs</b>	<ul style="list-style-type: none"> <li>• CERT-FI</li> <li>• Ericsson PSIRT</li> <li>• Funet CERT</li> <li>• Nokia NIRT</li> <li>• FSLabs</li> </ul>
<b>Industry Organisations</b>	<ul style="list-style-type: none"> <li>• FiCom (Finnish Federation for Communications and Teleinformatics)</li> <li>• EK (Confederation of Finnish Industries)</li> <li>• OWASP Helsinki Local Chapter</li> <li>• ISACA FI</li> </ul>
<b>Academic Organisations</b>	<ul style="list-style-type: none"> <li>• AALTO</li> <li>• VTT Technical Research Centre of Finland</li> <li>• Tekes, the Finnish Funding Agency for Technology and Innovation</li> <li>• Helsinki Institute for Information Technology</li> <li>• University of Helsinki / Department of Computer Science</li> <li>• University of Oulu</li> <li>• University of Jyväskylä</li> <li>• The University of Tampere</li> <li>• University of Turku</li> </ul>
<b>Others</b>	<ul style="list-style-type: none"> <li>• Finnish Consumer Agency and Consumer Ombudsman</li> <li>• Children On-Line</li> <li>• FISA (Finnish Information Security Association)</li> <li>• Mannerheim League of Child Welfare / Children online</li> <li>• CSC (IT Center for Science Ltd)</li> <li>• NESO</li> </ul>

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"<sup>7</sup> – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory<sup>8</sup>.

<sup>7</sup> The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

<sup>8</sup> See: <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**

### **Co-operation between public authority bodies**

The Ministry of Transport and Communications is responsible for legislation and strategy development concerning information security in communications services. Finnish Communications Regulatory Authority (FICORA) is a general administrative authority under the Ministry of Transport and Communications for issues concerning electronic communications and information society services in Finland. FICORA is the national security authority in Finland and the Finnish national Computer Emergency Response Team (CERT-FI) and National Communications Security Authority (NCSA-FI) functions are situated in FICORA.

The Finnish Government has appointed The Ubiquitous Information Society Advisory Board, chaired by the Minister of Communications. The Advisory Board aims to transform Finland into an internationally recognized, competitive, competence-based service society with a human touch. One of its focus areas is information security, and a group on information security issues has been established: The Information Security Group.

The tasks of the group remain the promotion of information security in the information society, monitor the progress that is made, and suggest improvements. The group will pay attention to present and future challenges in information security, and act as a national “think-tank” in information security issues.

The group should also firmly and determinedly draw attention to controversial issues in information security, too, and encourage discussion. Also The new National Information Security Strategy was drawn up by the Information Security Group.

The Ministry of Defence (MOD) provides direction and control over its administrative sector. In addition, the MOD remains responsible for its own security. Furthermore, within the purview of the National Security Authority, the MOD is responsible for Designated Security Authority services with the exception of issuing Facility Security Clearances or Personal Security Clearances, or security obligations related to communications security.

The Ministry of Interior is responsible for internal security and steers the Internal Security Programme of Finland.

The Ministry of Finance is responsible for driving and developing the information security of the Government of Finland. In 2010 no major changes have been identified (compared to prior years) with regards to the current mechanisms of co-operation between public authority bodies.

### **Co-operation on information security incidents**

The CERT teams prevent, monitor and solve information security incidents and distribute information on information security threats.

At FICORA, the group focusing on information security incidents and their control is called CERT-FI (Computer Emergency Response Team FICORA). In its activities, it strives to implement the principles of overall CERT activities and to promote security in the information society.

The CERT-FI cooperates with national and international CERT players and representatives of trade and industry, and public administration. FICORA also coordinates a CERT working group, which acts as a cooperative body for different players in the field of information security incident disclosure and solution. This working group also monitors and promotes the general development in the field and distributes information about it.

### **Co-operation and Information exchange mechanisms on emergency supply**

The National Emergency Supply Organisation (NESO) consists of a strategic level Council for Security of Supply and Infrastructure (CSSI), a planning committee network (Clusters and Pools) and an executive National Emergency Supply Agency (NESA) under the Ministry of Employment and the Economy.

There is a long tradition of partnership between the public and private sectors in Finland. The new National Emergency Supply Organisation operates on this very basis. The National Emergency Supply Organisation includes a planning committee network of clusters and pools. The clusters, which focus on priority areas for Finland's security of supply, are broad-based, sector-specific collaborating organisations consisting of experts representing the authorities, relevant bodies and the main parties involved.

These collaborating organisations have the task of guiding, coordinating and monitoring the contingency preparations within their own particular sphere of the arrangements for the security of supply. The responsibility for the security of supply with regard to information society needs rests with the National Emergency Supply Organisation's information society cluster.

NESA will be launching a secure partnership system portal early in 2010. The portal will be a forum for information exchange among the partners. It will include a self-assessment tool to check the maturity of business continuity management in each organisation. National maturity reports will be available for each industrial sector, although the assessments of individual companies will be kept confidential. The reporting will also provide benchmarking for the individual partners.

With regards to previous year report no major changes have been identified.

## Fostering a proactive NIS community

CERT-FI is amongst the active members<sup>9</sup> 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. 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 organizations.

Finland participates actively in the information security cooperation in the European Union and other international level bodies. Various ministries and other organizations participate in several working groups and forums.

FICORA participated actively in the work of EU's Communications Committee, Radio Spectrum Committee and Spectrum Policy Expert Group. FICORA has also held bilateral meetings with the EU Commission to discuss decisions on significant market power, the implementation of the EU legislation and pricing and expenses of call termination on mobile networks.

By co-operating with the European regulators' groups IRG and ERG, FICORA has been able to have an influence on EU regulation. The authority also contributed to the working groups of the European Network and Information Security Agency ENISA and IRG. The groups planned an action for ensuring communications networks and services in the event of emergency or interference.

In addition, FICORA participated in the work of the ECC (Electronic Communications Committee) of CEPT and its sub-groups. Several frequency-related reports, recommendations and spectrum decisions were adopted by the ECC. The common national opinions adopted in the executive group of telestandardisation were promoted in the general assemblies of ETSI.

Also the National Communications Security Authority Finland (NCSA-FI) specialized in information assurance matters related to the electronic communications and handling of classified information, is also responsible for duties arising from international information assurance responsibilities related to the above matters. In fact Finland has selected a decentralised organising model for ensuring the implementation of international information assurance responsibilities.

The Finnish Ministry for Foreign Affairs acts, in accordance with the Act on international information security obligations, as Finland's National Security Authority (NSA). The Act also prescribes other Designated Security Authorities (DSA). Authorized by act, FICORA executes tasks pertaining to the role of the National Communications Security Authority (NCSA).

---

<sup>9</sup> 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: <http://www.egc-group.org/>

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

### Security incident management

Security incidents are reported according to FICORA's order. The kind of information to be disclosed is specified in:

- Publicity Act;
- Act on the Protection of Privacy in Electronic Communications;
- Act on Competition.

Incidents can be reported to the CERT FI using an online form. Faults and disturbances in communication networks and services are reported to FICORA also online.

The most important incidents response capabilities in Finland are the owners and operators of the networks who bare the burden to response.

In 2010 FICORA and NESA still give support to the operators facing an incident. FICORA has its own incident response capability CERT-FI. NESA participates in the working groups and finances CERT-FI activities from a Security of Supply Fund. Private companies and other organisations like universities have their own CERTs. Domestic cooperation is pretty well organised as is international one, too.

### Autoreporter

Autoreporter is a fully automated service provided by CERT-FI for collecting and reporting information security incidents in the Finnish network space. The development started in late 2005 as an internal trial funded by an almost nonexistent budget.

Back then, the service did not even have a name. Now, the name of the service has been branded and some much needed functionality has been added. Safe to say, Autoreporter has become a vital part of the daily operations of CERT-FI.

Autoreporter's customers range from major Finnish Internet service providers (ISPs) to small domestic enterprises. If you administer your own network space and your business is concentrated in Finland or if you have an Autonomous System (AS) registered under the Finnish country code, then you are probably a customer of Autoreporter. Currently, Autoreporter is continuously tracking and reporting incidents for roughly 170 Autonomous System Numbers.

Currently Autoreporter is fed with information from intrusion detection systems, honeynets and sinkholes run by trusted third parties. The correctness of this information is evaluated on the basis of customer feedback and also, from time to time, internally.

## Emerging NIS risks

### Relevant emerging NIS risks

In Finland's information society, ICT still plays two different roles in the activities of telecommunications operators and organisations: an implementing role and an enabling role. ICT can be used to support and improve the efficiency of existing structures and processes. ICT can also enable new types of operating model and, in extreme cases, it could even change the structure of an entire industry.

The operation of all intelligent systems is based on different levels of information. Systems need information on the world around them; they interpret this data within their own framework; and, through their actions or by distributing information, they have an impact on other systems. The structure of a system, in terms of the information it holds and processes, consists of its physical components, their relationship to each other, and the data stored in the system.

The extent of computerised equipment and systems in Finland's information society highlights the essential nature of information. The computer-based processes rely on various software applications, which at their simplest are off-the-shelf packages requiring no user-specific customisation. At the other extreme are extensive families of software applications, which can be complex and purpose-specific software packages. Any information society will be reliant on information processes. Typically, the entire process must function successfully in order that a certain desired action or service is properly available. However, the more critical a specific function in the process, the greater will be its impact. In terms of the functioning of the information society, network products and services constitute a critical element of this.

### The national risk management process

In 2010 the focus of Finland has remained on preparedness, whereby dependability and resilience of e-communication networks is part of these efforts. For instance, ministries preparedness obligations include, but are not limited to, the special situations. Ministries have to prepare for all estimated risks and threats within their purview. The NESCA pools use a 5 criteria indicator set, defined by NESCA and NESCA together, to assess annually the level of security of supply in all critical sectors (CI, CII and others). The indicators used are:

- Capacity redundancy;
- Availability redundancy;
- Domestic controllability;
- Security arrangements;
- Level of contingency planning.

The analysis is done by breaking down each infrastructure (and services) to components (typically tens of them), including supporting functions from other sectors. In addition, NESCA and NESCA have used a linear risk analysis method for identifying the most critical areas in the interdependent infrastructures. This method gives higher risk value to those elements / areas on which many others depend. The mathematical method is well established and public. The method has been used to rank infrastructure risks on a national level. It has also been applied to a detailed analysis of ICT-infrastructure in order to rank the functions of CII by their criticality. Telecom operators in Finland are obliged to notify FICORA about major faults and disturbances in communication networks and services. Based on that information and also information gathered from telecom operators by other means FICORA has made estimations on risk levels and has given regulations for telecom operators to reduce those risks.

## Resilience aspects

There are a few aspects that remains worth be mentioned in 2010 - not in any particular order, namely

- Communication Market Act articles 90, 128 and 129;
- Act on the Protection of Privacy in Electronic Communications articles 19-23, 26-33;
- Radio Act, Act on Communications Administration;
- Government Decree on Communications Administration;
- Preparedness Act (Renewal in Finnish Parliament);
- MTC's Code of Conduct for Preparedness.

As far as electronic information and communication technologies (ICT) are concerned, again the strategy is quite specific, too, but the main mandatory issues come from Communications Market Act. Finland renewed its CIP strategy in 2010. "The Security Strategy for Society" was adopted by a Government resolution in December 16<sup>th</sup> 2010. It constitutes the common basis of preparedness planning and crisis management for all the actors in the society in normal conditions as well as in exceptional conditions. The preparedness of the different administrative branches is harmonised in the Security strategy for society.

The goal of the strategy is to ensure the functioning of society, safeguard Finland's national sovereignty and promote the security and well-being of citizens. Functioning of the economy and infrastructure has been identified as a vital function of the society. It is the responsibility of the authorities to ensure that telecommunications function not only in normal conditions but also during disruptions and exceptional conditions.

Threat models have been compiled as the basis of preparedness for the security strategy for society and a serious disruptions to telecommunications and information systems has been identified as one of the threat models.

Special attention must be paid to teleoperators preparedness obligations, including relevant authority-teleoperator cooperation, data security in networks and services as well as to guaranteeing services to selected user groups.

There are also resilience audits realized by NESAs. These audits are inspections of readiness in telecommunications companies together with MINTC and FICORA every year. MINTC, FICORA and NESAs/NESCs in co-ordination with each other perform inspections related to integrity and availability of public networks particularly in disruptive situations and exceptional conditions.

Today there is still no central register making information accessible as far as resilience is concerned. Many of the regulations given by FICORA are resilience targeted – the meaning of the regulation is to enhance resilience within a certain context, i.e. e-mail, Internet access, network maintenance and so forth.

Another kind of a set of best practices is the work done by Ministry of Finance under the umbrella called VAHTI. It has published several resilience related guidelines. Numerous guidelines will come up in English. As far as information security is FICORA (the regulator) has a good website with lots of pertinent information. Another useful link for good practice on resilience issues and vulnerabilities is to be found on their web site. All here referred materials are publicly available.

## Privacy and trust

### Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Finnish Personal Data Act (Henkilötietolaki 1999/523) (the "DPA") dated 22 April 1999. Here also no relevant changes have happened in 2010.

The competent national regulatory authority on this matter remains The Office of the Data Protection Ombudsman (supervises the processing in order to achieve the objectives of the DPA) (the "Ombudsman").

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

The data controller still must comply with the general data security obligations.

### Data protection breaches

The Finnish DPA does not contain any particular obligation to inform the Ombudsman or data subjects of a security breach.

### Enforcement

The Ombudsman promotes good processing practice and issues directions and guidelines so as to ensure unlawful conduct against the DPA is not continued or repeated. Where necessary, the Ombudsman shall refer the matter to be dealt with by the Board or report the matter for prosecution. In addition, the Ombudsman shall decide matters brought to the Ombudsman's attention by data subjects by ordering data controllers to grant rights of access to the data subject or to rectify an error.

Prosecutions for criminal offences are brought before the Finnish District Courts and may lead to fines or imprisonment. Claims for damages by data subjects are also brought before the Finnish District Courts as independent claims or integrated with criminal proceedings.

## NIS awareness at the country level

### Awareness actions targeting the consumers/citizens

Finnish Internet Awareness and Safety (FIAS) is a joint action of three individual organizations: Save the Children Finland, The Mannerheim League for Child Welfare (MLL) and The Finnish Communications Regulatory Authority (FICORA). Save the Children Finland acts as the coordinator of the project.

Finnish Internet Awareness and Safety project consists of three main activities: awareness work, helpline and hotline. Awareness centre is coordinated by FICORA, Hotline is maintained by Save the Children Finland and Helpline is run by MLL. All three participants initiate and implement awareness work actively.

The aim of the awareness work is to provide children, parents and teachers with knowledge and tools for guiding and empowering children in the internet society.

The Safer Internet Day (SID) actions are coordinated by FICORA in Finland. Safer Internet Day is a nationwide campaign that is organized in a unique set of private-public partnerships including a considerable amount of voluntary work. The project is active all through the year and has more

than 30 partners. The day is actively promoted with targeted communications and marketing actions around the country.

The National Information Security Day is the primary project of the governmental Information Security Committee. Among the committee's other important projects are "Information security program", "Information network crime as an information security problem" and "Situation awareness of national information security risks".

Schools and PTAs can book an internet safety trainer from the online pool of SID trainers or MLL trainer pool. Trainers will speak about the safer use of the internet for pupils, parents and teachers. The briefings cover topics such as basic tips for safer internet use and reasons to act responsibly online, understanding the nature of privacy and publicity online, encouraging critical attitude towards the online information, online bullying, and the possibilities and pitfalls of the popular websites among young people.

The FIAS consortium has developed training modules and awareness raising material that can be combined to provide education tailored for various target groups and in a variety of contexts. The modules will cover topics such as grooming, legal issues, cyber bullying, technical security, gaming, online interaction and social networking. Training is also offered for the moderators acting in the social online services used by the children and youth.

The Safer Internet Day newsletter is sent to all comprehensive schools in Finland 3 to 4 times a year giving teachers current information on Safer Internet Day themes and materials available.

### **Co-operation between public and private stakeholders for Internet security**

In Finland there is a long tradition in the co-operation between the public and private stakeholders for Internet security. One good example is The Information Security Group, which consists of over 20 members, both from the public and private sector.

National Safer Internet Day, jointly organised by the public administration, the business world and various organisations, is held every year. Its goal is to improve citizens' awareness of the opportunities offered by the Internet as well as the related information security threats and means of protection from these threats

The "www.tietoturvakoulu.fi" website has been broadened and updated based upon users' feedback. Two new comic book-type stories have been added emphasising three basic elements of safer internet use: follow rules, protect yourself and safeguard your computer. The stories can be read individually, in groups or together with teachers. They contain information about safety and on line competitions to test the level of knowledge of information safety. Over 15,000 pupils have participated to the competition so far and 80% of school teachers have visited the web site.

### **Other awareness actions**

Service providers are called on by the government to inform users on various online risks and how to mitigate the risks, to offer information security services, to actively monitor for suspicious network activities and to respond to them accordingly. Service providers are explicitly entitled by law to take the necessary measures to ensure information security by removing malicious software from messages or preventing transmission of e - mail messages if necessary for safeguarding the network and their services in general. Finally, they are also asked to cooperate effectively with the national CERT.

The Finnish IT association FiCom together with Finnish MNO's and data security companies has launched an Information Security Manual for Mobile users. The site offers a collection of practical

advice on how to protect against security threats common to mobile devices and on how to act in the case an incident occurs.

Internet service providers have an obligation to inform their customers on the different information security risks they might be exposed to, and to advise on the available methods for mitigating those risks. In practice, the main service providers sponsor awareness campaigns and offer contractual services to easily include information security services with other network services.

Service providers are also obliged to monitor their networks and services in order to detect fraud and in the case of information security breaches. The obligations require that any found irregularity will need to be corrected by switching off, re - routing or by filtering network traffic.

The ubiquitous information society action programme aims to secure the strong, rapid and balanced development of Finland's information society. Action programme projects and measures seek to safeguard the current service offering and to create new services for citizens and companies. The projects will also help enhance the productivity of Finnish society as well as international competitiveness.

The typical projects set up in Finland to develop information society infrastructure are:

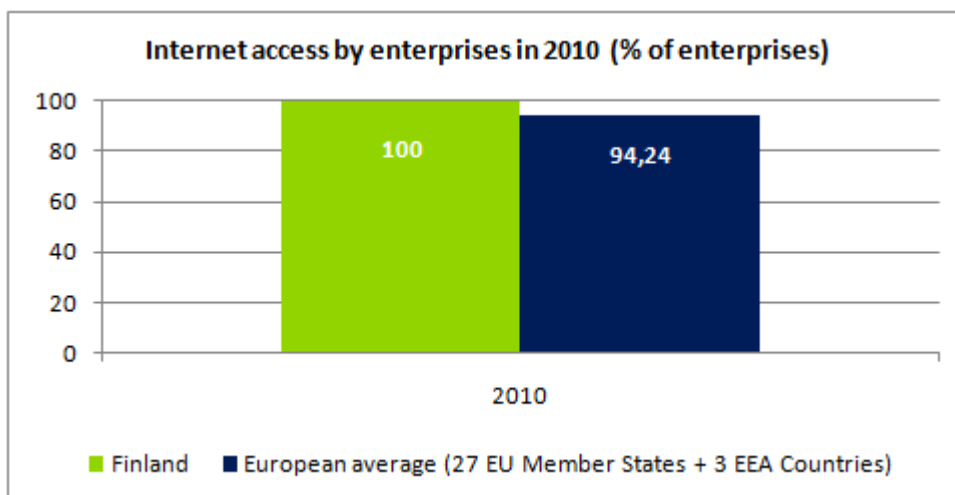
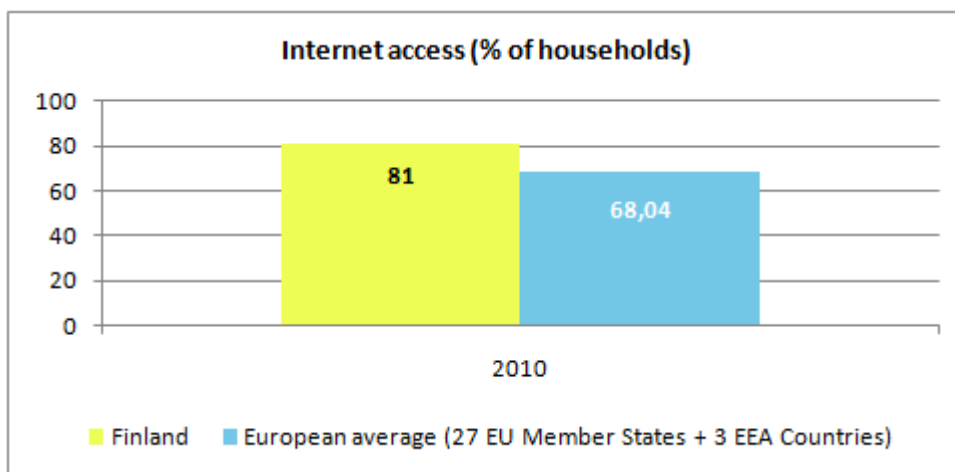
- Information security strategy was prepared in a national working group and published by a government resolution in December 2008. A action programme to implement the strategy was published in December 2009. The action programme has been implemented in 2010 in nine different projects.
- Conditions for the introduction of mobile identification were established in a working group. Reform of legislation on certification services was initiated. Finland has issued a modern electronic identification legislation, which has enabled a clear and strong national infrastructure in the field of electronic identification. The act on strong electronic identification and electronic signatures came into force September 2009 and it paved the way for the birth of eg. mobile identification markets
- The national broadband strategy was updated and published as a Government resolution in 2008. The level of universal service obligation covering the whole country was evaluated and as of the beginning of July telecom operators defined as universal service providers must be able to provide every permanent residence and business office with access to a reasonably priced and high-quality connection with a downstream rate of at least 1 Mbit/s.;
- Under the Advisory Board, an Electronic Invoicing Working Group was established with the task of assessing measures to accelerate the adoption of electronic invoicing both in the public and private sectors and particularly in the consumer segment. The Group gave its recommendation in 2009.

## Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Finland, a series of relevant statistics are included in this section. These statistics show that Finland is ahead of Europe in the Information Technology domain.

### Internet access of population and enterprises

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

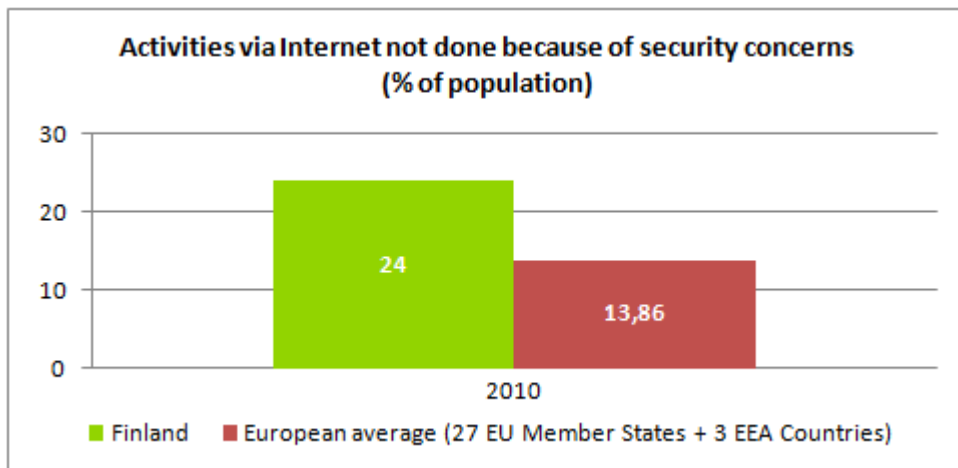


In 2010, the statistics indicate that both the enterprises and the households in Finland have a level of Internet access that is above the European average. It is also worth noting that **all the enterprises** in Finland have access to the Internet.

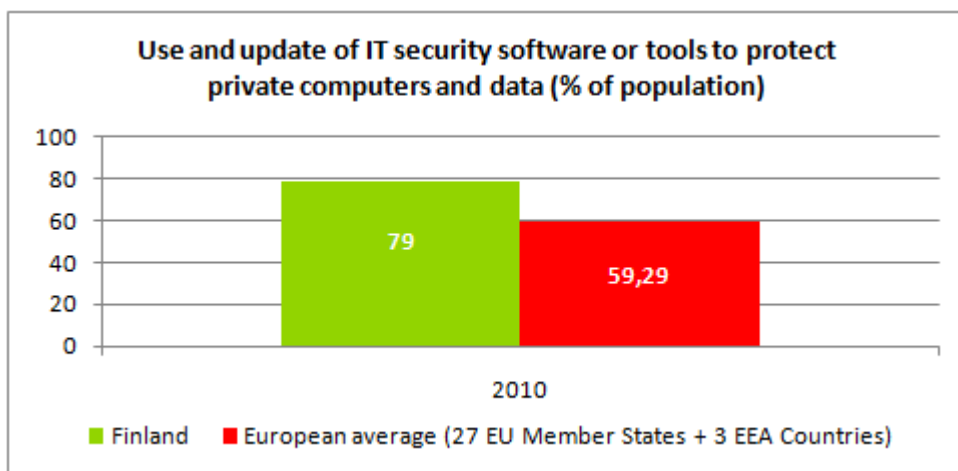
<sup>10</sup> Source: Eurostat

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

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



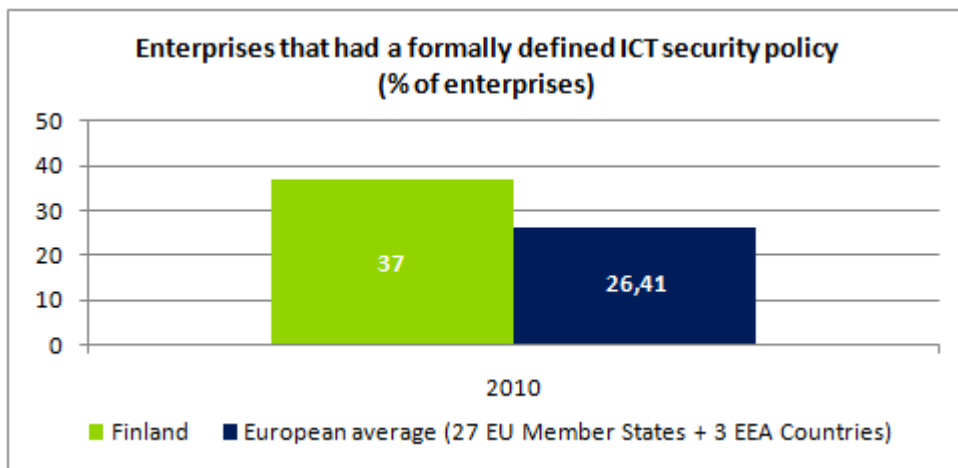
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



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

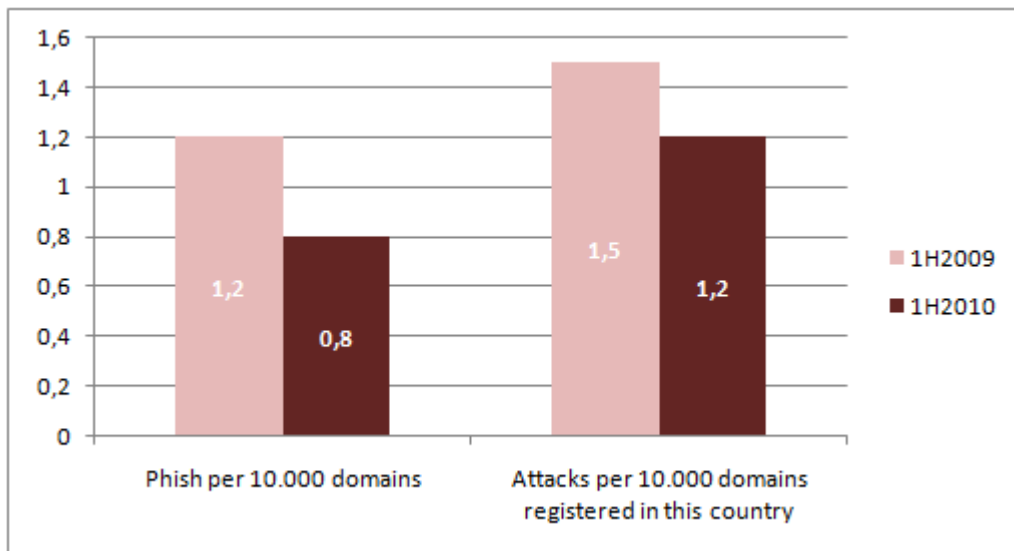
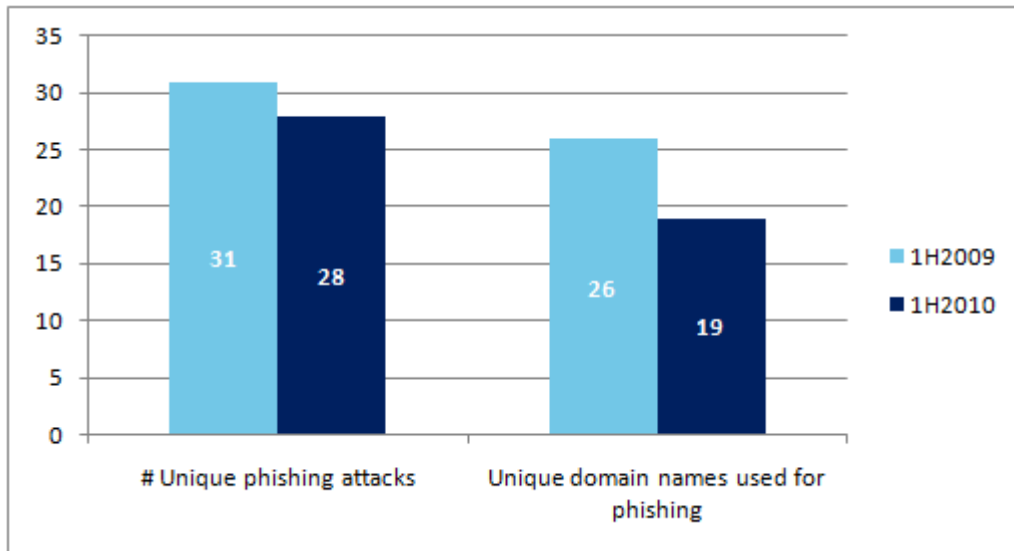
### Statistics on use of Internet by enterprises and related security aspects

More enterprises in Finland 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 1<sup>st</sup> half of 2010, and respectively for the 1<sup>st</sup> half of 2009, Finland was mentioned in the global report<sup>11</sup> published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



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

## APPENDIX

### National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Ministry of Transport and Communications Finland	<p>The responsibility and roles of the Ministry of transport and communication is to provide general guidance and develop the communications market and information society including information security.</p> <p>The Ministry is responsible for legislation and strategy development concerning information security in communications services. Its mission is to ensure that the general public, businesses and government all have confidence in the usability, security and privacy protection of services provided in the information society.</p> <p>It was responsible for the co-ordination of the first National Information Security Strategy adopted in 2003 and of the new National Information Security Strategy adopted in 2008.</p>	<a href="http://www.mintc.fi">www.mintc.fi</a>
2. Information Security Group of the Ubiquitous Information Society Advisory Board	<p>The Finnish Government has appointed an advisory board for information society issues, chaired by the Minister of Communications. One of its focus areas is information security, and a group on information security issues has been established. The Information Security group has the duty to:</p> <ul style="list-style-type: none"> <li>• Draw up an action plan for the national information society strategy;</li> <li>• Monitor and coordinate the implementation of the action plan;</li> <li>• Accommodate the measures of the action plan and ensure that they are consistent with one another;</li> <li>• Maintain cooperation with other players in the information society development;</li> <li>• Integrate and coordinate information security work in the information society;</li> <li>• Promote the introduction and development of reliable electronic identification systems;</li> <li>• Take new initiatives to speed up the national information society development;</li> <li>• Monitor the information society development at international and EU level; and</li> <li>• Report annually to the Government about the implementation of the action plan.</li> </ul>	<a href="http://www.arjentietoyhteiskunta.fi/index.phtml?s=5">www.arjentietoyhteiskunta.fi/index.phtml?s=5</a>
3. FICORA (Finnish Communications Regulatory Authority)	<p>FICORA is the national security agency/authority in Finland. FICORA is a governmental agency under the Ministry of Transport and Communications. FICORA maintains an overview of the functionality of electronic communications networks and information security and reports of eventual information security threats. FICORA</p>	<a href="http://www.ficora.fi">www.ficora.fi</a>

National authorities	Role and responsibilities	Website
	<p>also aims to increase the awareness of information security in homes and companies, and arranges the Information Security Day. FICORA is the national information security authority.</p> <ul style="list-style-type: none"> <li>• FICORA is a general administrative authority for issues concerning electronic communications and information society services;</li> <li>• It also has duties concerning protection of privacy and data security in electronic communications and is, among other things, involved in Comsec (communications security) work;</li> </ul> <p>It also has a role in CERT (Computer Emergency Response Team) activities involving detection and resolution of data security infringements (CERT-FI).</p> <p>The NCSA-FI functions as the national communications security authority under FICORA. NCSA-FI specializes in information assurance matters related to the electronic communications and handling of classified information, and is responsible for duties arising from international information assurance responsibilities related to the above matters.</p>	
4. Ministry of Finance	<p>Steering and development of the Finnish Government's information security.</p> <p>The Ministry of Finance is part of the Government. It provides a macroeconomic and fiscal policy framework for the government, drafts the annual Budget and offers experience in tax policy matters. The Ministry is responsible for strategic policy on the financial markets, and State employer and personnel policy, and for overall development of government. Moreover, the Ministry is in charge of the legislative and financial requirements of local government functions. It also participates in the work of the European Union and several international organizations.</p> <p>The Ministry works to safeguard stability and secure opportunities for growth, and to ensure a competitive tax system and the competitiveness and service provision of Finland's public administration. The Ministry's vision emphasizes the importance of stable economic development in order to safeguard the opportunities of future generations.</p>	<a href="http://www.ministryoffinance.fi">www.ministryoffinance.fi</a>
5. Ministry of Defense	As a Government department and the ministry	<a href="http://www.defmin.fi/index.phtml?/">www.defmin.fi/index.phtml?/</a>

National authorities	Role and responsibilities	Website
	<p>providing the guidelines for defence administration, the Ministry of Defence is in charge of national defence policy and security and international defence policy cooperation. In addition, the Ministry is responsible for national military defence resources and the operating framework of the Defence Forces. It coordinates Finnish participation in international crisis management and contributes to shaping the European security structures to safeguard Finland's national interests.</p> <p>The Ministry of Defence coordinates total defence arrangements and works for maintaining the resolve of Finns to defend the country. The Ministry also acts as a link between the Government and the Defence Forces.</p> <p>The Government controls the Defence Forces via the Ministry of Defence and the needs of the Defence Forces are brought to the attention of the Government via the Ministry.</p>	<p><a href="#">=en&amp;s=2</a></p>
6. VAHTI (Government Information Security Management Board)	The board, set up by Ministry of Finance, assists the latter in steering, developing and coordinating the Finnish Government's information security.	<a href="http://www.ministryoffinance.fi">www.ministryoffinance.fi</a>
7. Ministry of the Interior	The Ministry of the Interior has a broad operative field, which includes areas such as internal security, regional and administrative development as well as municipal affairs. The ministry steers also the Internal Security Programme of Finland.	<a href="http://www.intermin.fi">www.intermin.fi</a>
8. The Advisory Board for Defence Information (ABDI)	<p>The Ministry of Defence gives strategic level guidance to the Defence Forces related to information security.</p> <p>Set up by the Government for the Parliament's term of office, the Advisory Board for Defence Information (ABDI) is a permanent parliamentary committee. Administratively, it is in the Ministry of Defence.</p> <p>The work of the ABDI includes national defence information for normal and exceptional conditions and observing the development of Finns' opinions regarding matters closely related to national defence. The work is primarily carried out in the Work Branch, Research Branch, Media Branch, Education Branch and Organisation Branch. The ABDI has its own Secretariat and close connections with corresponding organisations in other Nordic countries</p>	<p><a href="http://www.defmin.fi/index.phtml?l=en&amp;s=179">www.defmin.fi/index.phtml?l=en&amp;s=179</a></p>
9. Security and Defence Committee	The Security and Defence Committee is a cooperation body between the various ministries concerning the issue of the 'total defence' concept and actions to secure vital functions of society, including anti-cyber war issues.	<a href="http://www.defmin.fi">www.defmin.fi</a>
10. Finnish Defence Forces (FDF)	The FDF implements all the information security actions within its own structure in accordance	<a href="http://www.mil.fi/">www.mil.fi/</a>

National authorities	Role and responsibilities	Website
	<p>with the MoD's guidance. It participates in the cross-sectoral work with other security-related authorities.</p> <p>As one of the Ministries of the Finnish Government and leading authority in the area of national defence, the Ministry of Defence is in charge of national defence policy and national security as well as of international cooperation in defence policy matters.</p> <p>In carrying out its tasks in a changing operational environment and in cooperation with its interest groups, the Ministry is responsible for:</p> <ul style="list-style-type: none"> <li>• The resources and operational prerequisites necessary for an independent military defence;</li> <li>• Preparedness for international crisis management as well as cooperation with the security structures in Europe to safeguard Finland's national interests;</li> <li>• Maintenance of the strong will of the Finns to defend their country.</li> </ul>	
11. Data Protection Ombudsman	<p>The office of the Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice. The ombudsman guides and controls the processing of personal data and provides related consultation. The Objective of our Office is to maintain and promote the right to privacy, one of the basic rights of each citizen, by:</p> <ul style="list-style-type: none"> <li>• Fulfilling the duties assigned to the Data Protection Ombudsman by legislation ;</li> <li>• Co-operating with data subjects and controllers and organisations representing them as well as other related bodies, aiming at preventing violation of privacy in advance;</li> <li>• Promoting the development of, and compliance with, good data processing practices ;</li> <li>• Assisting and supporting the development and use of systems supporting and safeguarding privacy.</li> </ul>	<a href="http://www.tietosuoja.fi">www.tietosuoja.fi</a>
12. National Emergency Supply Agency, NESAs	<p>The Agency plans with actors in the ICT industry to reduce vulnerabilities and create preparedness for exceptional circumstances. The Agency finances ICT backup systems of national importance.</p>	<a href="http://www.nesa.fi">www.nesa.fi</a>
13. National Board of Economic Defence, NBED	<p>The National Board of Economic Defence (NBED) is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyse threats against the country's security of supply and to plan measures to control these threats.</p> <p>NBED makes plans and formulates guidelines,</p>	<a href="http://www.nesa.fi/organisation/national-board-of-economic-defence">www.nesa.fi/organisation/national-board-of-economic-defence</a>

National authorities	Role and responsibilities	Website
	which public authorities implement when disturbances occur. NBED also promotes companies' contingency planning. NBED does not have the power of public authorities, but its assembled expertise constitutes an important resource of national security.	

### Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> <li>FIRST<sup>12</sup> member</li> <li>TI<sup>13</sup> listed</li> </ul>	
14. CERT-FI	<p>CERT-FI is the Finnish national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security.</p> <p>CERT-FI also:</p> <ul style="list-style-type: none"> <li>Makes and maintains situation awareness of information security threats and informs of incidents;</li> <li>Gives recommendations, advice and guidelines for improvement of information security;</li> <li>Distributes information on how to prevent information security incidents;</li> <li>Helps solve information security problems ;</li> <li>Cooperates with equipment, networks and software suppliers ;</li> <li>Cooperates with the Police and other authorities ;</li> <li>Coordinates information security cooperation;</li> <li>Maintains international contacts between authorities in CERT activities.</li> </ul>	<a href="http://www.cert.fi/">www.cert.fi/</a>
15. Ericsson PSIRT	Ericsson PSIRT is the Ericsson Product Security Incident Response Team.	<a href="http://www.ericsson.com/">www.ericsson.com/</a>
16. Funet CERT	Funet CERT is the Finnish University and Research Network CERT.	<a href="http://www.cert.funet.fi">www.cert.funet.fi</a>
17. Nokia NIRT	Nokia NIRT is the Nokia Incident Response Team.	<a href="http://www.nokia.com/">www.nokia.com/</a>
18. FS Labs	FS Labs is the Fsecure Security lab.	<a href="http://www.f-secure.com/">www.f-secure.com/</a>

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

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

## Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
19. FiCom (Finnish Federation for Communications and Teleinformatics)	<p>The Finnish Federation for Communications and Teleinformatics (FiCom) is a cooperation organisation for the ICT (information and communications technology) industry in Finland and looks after its interests.</p> <p>FiCom's members are companies and other entities that operate in the communications and teleinformatics sector in Finland. FiCom's task is to promote business opportunities for its members and to enhance their competitiveness.</p>	<a href="http://www.ficom.fi">www.ficom.fi</a>
20. EK (Confederation of Finnish Industries)	<p>The Confederation of Finnish Industries (EK) is Finland's the leading business organisation. It represents the entire private sector, both industry and services, and companies of all sizes.</p> <p>EK's member companies represent more than 70 % of Finland's gross domestic product and over 95 % of exports from Finland.</p> <p>It promotes the interests of its member companies in Finland, the European Union and internationally, and its mission is to improve the competitiveness of companies in Finland.</p>	<a href="http://www.ek.fi">www.ek.fi</a>
21. OWASP Helsinki Local Chapter	<p>The Open Web Application Security Project (OWASP) is an open-source application security project with local chapters. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions.</p> <p>The chapter in the Finland organizes local events such as the OWASP Helsinki Cafe, Mini-meetings, chapter meetings and specific events.</p>	<a href="http://www.owasp.org/index.php/Helsinki">www.owasp.org/index.php/Helsinki</a>
22. ISACA FI	<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 local chapter organizes local events such as education and training, workshops, roundtables and other specific events.</p>	<a href="http://www.isaca.fi">www.isaca.fi</a>

## Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
23. AALTO	<p>Established in 2010, the Aalto University is a new university with centuries of experience. The Aalto University was created from the merger of three Finnish universities: The Helsinki School of Economics, Helsinki University of Technology and The University of Art and Design Helsinki. Aalto University School of Science and Technology has been divided into four new schools starting from 1st of January 2011. The six schools of Aalto University are all leading and renowned institutions in their respective fields and in their own right.</p> <p>The combination of six schools opens up new possibilities for strong multi-disciplinary education and research. The new university's ambitious goal is to be one of the leading institutions in the world in terms of research and education in its own specialized disciplines.</p>	<a href="http://www.aalto.fi/en/about/">www.aalto.fi/en/about/</a>
24. VTT Technical Research Centre of Finland	<p>VTT Technical Research Centre of Finland is the biggest multi-technological applied research organisation in Northern Europe. VTT provides high-end technology solutions and innovation services.</p> <p>From its wide knowledge base, VTT can combine different technologies, create new innovations and a substantial range of world class technologies and applied research services thus improving its clients' competitiveness and competence.</p> <p>Through its international scientific and technology network, VTT can produce information, upgrade technology knowledge, create business intelligence and value added to its stakeholders.</p>	<a href="http://www.vtt.fi">www.vtt.fi</a>
25. Tekes, the Finnish Funding Agency for Technology and Innovation	<p>Tekes, the Finnish Funding Agency for Technology and Innovation is the main government financing and expert organisation for research and technological development in Finland.</p> <p>Tekes funds innovative research and development projects in companies, universities and research institutes.</p>	<a href="http://www.tekes.fi">www.tekes.fi</a>
26. Helsinki Institute for Information Technology	<p>HIIT is a joint research institution of Helsinki University of Technology TKK and the University of Helsinki (UH).</p> <p>Key competences: Internet architecture and technologies, mobile and human-centric computing, user-created media, analysis of large sets of data, and probabilistic modelling of complex phenomena</p>	<a href="http://www.hiit.fi/">www.hiit.fi/</a>
27. University of Helsinki / Department of Computer Science	<p>The Department of Computer Science at the University of Helsinki is known for its quality research and teaching among other in the Information Security area.</p>	<a href="http://www.cs.helsinki.fi/index.en.html">www.cs.helsinki.fi/index.en.html</a>
28. University of Oulu	<p>The University of Oulu is an international scientific community known for high-quality research and education that provides experts for demanding</p>	<a href="http://www.oulu.fi">www.oulu.fi</a>

Academic Organisations	Role and responsibilities	Website
29. University of Jyväskylä	<p>tasks on both national and international level. The University promotes well-being and education in Northern Finland and is a significant player in the Finnish and European re-search based system of innovation and education.</p> <p>The University offers undergraduate and postgraduate degrees, teacher training programmes and over 120 subject area disciplines. The university is currently divided into seven faculties:</p> <ul style="list-style-type: none"> <li>• Faculty of Humanities</li> <li>• Faculty of Information Technology</li> <li>• Faculty of Education</li> <li>• Faculty of Sport and Health Sciences</li> <li>• Faculty of Mathematics and Science</li> <li>• School of Business and Economics</li> <li>• Faculty of Social Sciences</li> </ul>	<a href="http://www.jyu.fi">www.jyu.fi</a>
30. The University of Tampere	<p>The University of Tampere embraces many fields of science and its research profile is extensive and multidisciplinary. There are six faculties and nine independent institutes. The University of Tampere is the biggest provider of higher education in Finland for social sciences and the accompanying administrative sciences.</p>	<a href="http://www.uta.fi">www.uta.fi</a>
31. University of Turku	<p>The University of Turku is a highly international university, where education and research are closely intertwined. The university offers academic education based on high quality and often multidisciplinary research. The University of Turku offers talented and ambitious students and scholars a versatile, inspiring and attractive academic environment and educational setting in which they can develop their potential in full. As a part of a vibrant academic community, our students learn much more than knowledge and skills. The University of Turku offers education for life.</p>	<a href="http://www.utu.fi">www.utu.fi</a>

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

Others	Role and responsibilities	Website
32. Finnish Consumer Agency and Consumer Ombudsman	<p>The task of the Finnish Consumer Organisation and Consumer Ombudsman is to ensure consumers' economic, health and legal position and to implement consumer policy. The consumer ombudsman monitors compliance with legislation concerning the protection of consumers' rights.</p>	<a href="http://www.kuluttajavirasto.fi">www.kuluttajavirasto.fi</a>
33. Children On-Line	<p>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.</p>	<a href="http://www.pelastakaalapset.fi/netti_vihje/sahkoposti.php">www.pelastakaalapset.fi/netti_vihje/sahkoposti.php</a> <a href="http://www.pelastakaalapset.fi/netti_vihje/english">www.pelastakaalapset.fi/netti_vihje/english</a>
34. FISA (Finnish Information Security)	<p>FISA is the largest information security association in Finland.</p>	<a href="http://www.tietoturva.fi">www.tietoturva.fi</a>

Others	Role and responsibilities	Website
Association)	It is a non-profit association, whose objective is to promote professionalism, awareness and best practices in information security. Activities include member meetings, discussion groups, company visits, conferences, CISSP-certification and participation of various information security programmes.	
35. Mannerheim League of Child Welfare / Children online	The Mannerheim League is an NGO, which promotes the wellbeing of children, increases respect for childhood, and sees that children's views are taken into account in public decision-making.	<a href="http://www.mll.fi/">www.mll.fi/</a>
36. CSC (IT Center for Science Ltd)	CSC, the Finnish IT center for science, is administered by the Ministry of Education. CSC is a non-profit company providing IT support and resources for academia, research institutes and companies: modelling, computing and information services. CSC provides Finland's most powerful supercomputing environment that researchers can use via the Funet network. CSC has an active role in developing information and network security measures in its own services and among its constituents. Funet CERT (Finnish University and Research Network, Computer Emergency Response Team) coordinates security incidents and offers support and help with minimising exposure to security risks.	<a href="http://www.csc.fi">www.csc.fi</a>
37. NESO	National Emergency Supply Organisation (NESO) consists of a high level Council for Security of Supply and Infrastructure (CSSI), a planning committee network (Clusters and Pools), and an executive National Emergency Supply Agency (NESA). The five NESO Clusters and 24 Industry Pools are a network of committees consisting of the leading 1000 experts from both the public administration and the business world. Their tasks are to analyze threats against the country's security of supply, including ICT infrastructure, to plan measures to control these threats, and to promote readiness planning in individual industrial sites.	<a href="http://www.nesa.fi/organisation">www.nesa.fi/organisation</a>

## 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](http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf)
- An overview of the eGovernment and eInclusion situation in Europe, available at: <http://www.epractice.eu/en/factsheets>
- CIRCA-FI: [http://www.enisa.europa.eu/cert\\_inventory/pages/04\\_01.htm#02](http://www.enisa.europa.eu/cert_inventory/pages/04_01.htm#02)



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280  
[www.enisa.europa.eu](http://www.enisa.europa.eu)