

Sweden Country Report



About ENISA

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

Contact details

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

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

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



Acknowledgments:

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

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Dan Cimpean, Johan Meire and Nicolas Roosens.**

Legal notice

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

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

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

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

SWEDEN.....	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	8
NIS GOVERNANCE	12
OVERVIEW OF THE KEY STAKEHOLDERS.....	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS.....	13
FOSTERING A PROACTIVE NIS COMMUNITY	16
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	17
SECURITY INCIDENT MANAGEMENT	17
EMERGING NIS RISKS	18
RESILIENCE ASPECTS	19
PRIVACY AND TRUST.....	20
NIS AWARENESS AT THE COUNTRY LEVEL	21
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY.....	23
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	23
RELEVANT STATISTICS FOR THE COUNTRY	24
INTERNET ACCESS OF POPULATION AND ENTERPRISES	24
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS.....	25
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	26
OTHER STATISTICS.....	27
APPENDIX.....	28
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY	28
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	31
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	32
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	32
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY.....	33
REFERENCES	34

Sweden

The structure of the individual country reports

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

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS governance model at country level:

- *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
- *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
- *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
 - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
 - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

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

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

The objectives for the work on information security at societal level are stated in the national strategy. The strategy is currently expressed in several versions with unclear status and mutual order - work is currently in progress on updating and clarifying the strategy for societal information security.

The information-security investigation summarised its view of national strategy in ten points, which were in part based on the text of the government bills.

These points are summarized as following:

- To develop Sweden's position within the EU and in international contexts;
- To create confidence, security and safety, and to increase protection of integrity;
- To promote increased use of IT;
- To prevent and be able to deal with disturbances in information systems and communication systems;
- To reinforce the work of the intelligence and security services and to develop service of process;
- To reinforce capacity in the field of national security;
- To exploit society's combined capacity;
- To focus on critical societal functions;
- To increase awareness of security risks and possibilities of protection;
- To guarantee provision of staff.

Action plan for information security in Sweden

The government has commissioned MSB (the Agency for Civil Protection and Preparedness) with administrating the national plan of action for information security drawn up in 2008 and updated in 2010. The plan is based on the national information security strategy and was created in collaboration with a number of other authorities and organisations with crucial remits in the field.

Four areas have been identified as priorities:

- There is a need for improved multi-sector and inter-sector work on societal information security. Comprehensive information security regulations could be designed so as to apply to all authorities under government control. Responsibility by sector simultaneously needs clarifying. Opportunities to issue appropriate recommendations to other sections of society are also needed;
- A basic security level for societal information security needs to be established. It is a prerequisite for safeguarding the information assets that have increasingly become fundamental to both commerce and the public sector;
- Society must be able to handle extensive IT-related disturbances and crises. An operational national coordinating function should be established;
- There is a lack of information security expertise at all levels of society. The rapid development also means that lack of skill in individual users is having bigger and bigger consequences. Several proposals are thus being presented that together constitute a wide-ranging investment in skills enhancement in the field.

The proposed measures also take into consideration, among other things:

- The Commission's report Information Security on Secure Information;
- The Government bill for improved emergency preparedness ;
- The Committee directive for a new agency with responsibility for emergency preparedness and security matters¹.

Efficient work on information security can be described in various ways. The model described in the regulations of the MSB⁴ recommends clear responsibility, a well thought-out management system, and risk and vulnerability analyses with feedback.

Action Plan for eGovernment

Since 2008 an Action Plan² called "New grounds for IT-based business in Public Administration" has been set up. This plan highlights the prioritised policy areas until 2010, indicates the responsible Government departments and defines the necessary coordination with municipalities and regions (county councils). No major updates of it were identified in 2010.

Among other aspects, the information handling of the public authorities will be made more efficient, information security should increase and automatic IT-support for case handling and procurement will be introduced.

Key elements of the Action Plan include:

- Safe electronic communication and secure/efficient information exchange, such as the issue of eIdentification;
- Simplified access to information;
- IT-standardisation and common demand specifications;
- Automatic handling of cases;
- Common administrative interface for safe communication and documentation;
- Accessibility and usefulness.

In order to strengthen the development of eGovernment and create good opportunities for inter-agency coordination, a delegation for eGovernment is being established. The first task of the Delegation - to propose a strategy for the government agencies work on eGovernment - has been submitted to the Government on 19 October 2009.

The Delegation is subsequently required to coordinate the IT-based development projects of government agencies and to follow up their impact on citizens, business operators and public administration employees. A further task of the Delegation is to coordinate specific IT standardisation issues and assist the Government in the international work in this area.

The eGovernment Delegation has received an additional mandate on public information and social media. The Delegation is instructed to promote and coordinate the agencies' efforts to improve the conditions for the re-use of documents. These efforts are to be based on the Act on the re-use of public sector documents proposed in the Government bill 'Public administration for democracy, participation and growth' (Govt. Bill 2009/10:175). Within the framework of its remit to develop instructions, the Delegation is also to draft guidelines for government agencies' use of social media.

¹ See: <http://www.msb.se/sv/Tools/News/Information-security-in-Sweden---Situational-assessment-2009/>

² See: <http://www.epractice.eu/en/document/288378>

Every year, the Delegation is to submit interim reports to the Government, containing background material and proposals. A final report is to be submitted by 31 December 2014 at the latest.

Action plan for internet security

The aim of a strategy for a more secure internet in Sweden is to safeguard critical functions in internet infrastructure which, if not maintained, would create extensive disturbances or interruptions and thus impede or prevent use of the internet by large groups of individual users or societal important companies, authorities and organisations. Large parts of the infrastructure are provided by private operators. Since beginning of 2010 no key changes to the Action plan for internet security were identified.

The starting point for security in internet infrastructure is thus the providers' responsibility for networks and services based on market requirements. The public undertaking is based on there being requirements that the market cannot meet³.

National Strategy for eHealth

The strategy lays down a set of basic principles⁴ for national collaboration on ICT development in the health care sector. It first establishes a common vision of how eHealth should be used to support and improve healthcare.

The work to be jointly undertaken is grouped into six action areas with the following objectives:

- Bring laws and regulations into line with extended use of ICT;
- Create a common information structure;
- Create a common technical infrastructure;
- Facilitate interoperable, supportive ICT systems;
- Facilitate access to information across organisational boundaries;
- Make information and services easily accessible to citizens.

Furthermore, this strategy will be followed by implementation plans and the problems identified during its application will be considered for possible strategy updates. The relevant work is to be undertaken by High-Level Group for eHealth.

With regards to the report of 2009, there are no key additional highlights worth to be mentioned.

³ See : <http://www.msb.se/sv/Tools/News/Information-security-in-Sweden---Situational-assessment-2009/>

⁴ See : <http://www.epractice.eu/en/document/288378>

The regulatory framework

Overview of the Swedish security policy

The conditions governing Sweden's security policy have fundamentally changed in the last decade. Sweden's security policy can be expressed as follows:

- "The aims of Sweden's security policy are to preserve the country's peace and independence, contribute to stability and security in the vicinity and strengthen international peace and security";
- "Sweden is not a member of any military alliance. This security policy approach, which allows us to remain neutral in the event of conflicts in the region around Sweden, has served us well";
- "Looking to the future, it is clearer than ever that security is more than the absence of military conflicts. Threats to peace and the security can best be averted collectively and in cooperation with other countries. At global level, the primary expression of this is the Swedish support for the United Nations. As a member of the European Union, we are part of a community characterized by solidarity, whose primary purpose is to prevent war on the European continent".

The only form of cooperation that Sweden excludes is agreements on binding mutual defense guarantees. Sweden is prepared to take part in all other cooperation that can contribute to achieving these overall goals to the best of its ability and after a decision is taken in each individual case.

Sweden's security policy is based on a broad perception of security. Today, threats to the Swedish security are different and more complex than the traditional military threats. The new, expanded concept of security also includes non-military threats.

The rights and security of individuals are of major importance, not just those of states⁵.

eGovernment Legislation

There is currently no overall eGovernment legislation in Sweden. eGovernment activities are regulated by general laws and ordinances on Public Administration, public registers and data security⁶. No major changes to the eGovernment legislation have been identified since the previous country report of 2010.

Data Protection/Privacy Legislation

The Personal Data Act lists certain fundamental requirements concerning the processing of personal data. These demands include, inter alia, that personal data may only be processed for specific, explicitly stated and justified purposes. Once these requirements are satisfied, personal data may only be processed if the person registered gives his/her consent.

Exemptions to this rule include the exercise of official powers or the fulfilment of a legal obligation by the controller of personal data⁷. Since 2010 no update of the Data Protection/Privacy legislation has occurred.

⁵ See : <http://www.sweden.gov.se/sb/d/3103/a/116839>

⁶ See : <http://www.epractice.eu/en/document/288379>

⁷ See : <http://www.epractice.eu/en/document/288379>

Cybercrime Legislation

Offences against the Confidentiality, Integrity and Availability of information in Sweden are mainly managed through the Swedish Criminal Code and in particular through chapter 4 which deals with "Crime Against Liberty and Peace", chapter 12 which deals with "Crime Inflicting Damage" and chapter 13 that deals with "Crimes Involving public Danger".

Chapter 4 of the Swedish Criminal Code is the one most frequently used to handle these CIA offences. Section 8 deals with the "breach of postal or telecommunications secrecy": it is a provision dealing with unauthorised access to a communication or its unauthorised interception.

Other provisions relating to these offences are Section 9, 9a and 9c of the same chapter. In particular, Section 9 deals with "intrusion into a safe depository" establishing that it is an offence to open letters or telegrams or to otherwise obtain access to something kept under seal or lock or otherwise enclosed.

Section 9a establishes that it is an offence to unlawfully and secretly listen to or record by technical means for sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which the person doing the listening has improperly obtained access.

All these conducts are defined as "eavesdropping". Section 9c deals with the "breach of data secrecy", the case in which a person unlawfully obtains access to record automatic data processing activities or unlawfully alters or erases or inserts such a recording device.

Chapter 12 of the Swedish Criminal Code deals with the infliction of damage: the first section deals with persons who destroy or damage property to the detriment of another's right thereto. The penalty provided is a fine or a term of imprisonment up to one year. The third section of the article deals with serious cases of inflicting damage.

Damage is to be considered serious when it causes a risk to anyone's life or health, or when the damage was to something of great cultural or financial importance. In this case the penalty is a term of imprisonment of up to 4 years.

Another important chapter of the Swedish Criminal Code that has to be taken into consideration in relation to these sorts of offences is Chapter 13 which deals in general with "Crimes Involving Public Danger." This also applies to anyone who destroys or damages or seriously disrupts or obstructs public traffic or the use of telegraph, telephone, radio or other similar public services, or the use of an installation for the supply of water, light, heat or power to the public. The penalty for this offence is a term of imprisonment up to 4 years.

Sweden has two parallel types of court - general courts, which deal with criminal and civil matters, and general administrative courts, which deal with administrative matters. There are three levels of general courts - the district courts (tingsrätt), the courts of appeal (hovrätt) and the Supreme Court (Högsta domstolen). There are also three levels of administrative courts - the county courts (lansrätt), the administrative courts of appeal (kammarrätt) and the Supreme Administrative Court (Regeringsrätten).⁸

⁸ Source : ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf

Cybercrime – law enforcement

A great emphasis is placed on the computer crime awareness of individual law enforcement officers in Sweden. All officers are given a basic understanding of computer crime and dealing with computer evidence (at a basic level) when they pass through Police College.

At the local level, there are 21 independent state police departments which cover distinguished geographic regions. In each unit there are 1 or 2 specially trained investigators. This number can be higher in the major departments with other local experts being present.

Furthermore, each regional state unit is able to call upon the national unit for support if required. The IT crime squad (ITbrottsroteln) forms part of the National Criminal Investigation Department (Rikskriminalpolisen). There are 15 officers in the IT crime squad, who are a mix of police officers and special profile technicians. The IT Crime Squad is divided into subunits concerned with search and seizure and internal surveillance, which mirrors the structure of other national units (e.g. the UK NHTCU).

The responsibilities and supportive measures are first and foremost directed to local police units in each state department, but also to international liaisons, specifically with Interpol, Europol and the G-8 24/7 reporting points. This unit does not, however, cover national intelligence related liaisons regarding computer crime, which is handled by the Swedish Security Service (Sakerhetspolisen, Sweden's internal intelligence agency).

The IT Crime Squad also cooperates with the military and other national research agencies. This co-operation is normally along the lines of seminars and workshops as well as the more obvious operational assistance.

In the Swedish National Forensic Laboratory (Statens kriminaltekniska laboratorium), five engineering staff members deal exclusively with computer forensics. They can be called upon by the National Criminal Investigation Department as well as state forces.

The Police College programme includes a basic level of digital and computer evidence awareness in basic training, but a special 13 week course also exists for specialist investigators. This consists of a 10 week introductory course with regards to computing and information technology, covering operation of Information Technology at an advanced level. A further 3 weeks provide training on legal considerations, software and forensic tools. Other advanced training courses are available on a topical basis (e.g. the rise in popularity of Distributed Denial of Service attacks).

The level of sophistication of cyber crimes remains quite high, and outside civilian experts are only called in 5 to 6 times a year for specific assistance on investigations.

Self regulations

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

- Code of Conduct - Mobile Premium Services
- Self-regulatory Code of Conduct for Premium Rate Call Services⁹
- Code of conduct- Safer use of mobile phones and services by younger teenagers and children.

⁹ See: http://www.gsmeurope.org/safer_mobile/national.shtml

eIdentity

Sweden uses electronic ID cards issued by companies selected in a government frame agreement procurement. These cards can also be soft certificates.

Swedish citizen and others that have been introduced in the population register can get cards. Most issuers today are banks

Another form of identity is the National Swedish identity card which can be issued by the police but is still not fully initiated for electronic use. There is also an ID-card issued by the Swedish Tax Agency, which is currently being used by one Certificate Service Provider as well as by the only issuer of qualified certificates in Sweden.

Advanced certificates, either soft or hard and based on a PKI system, are available through public/private partnerships. Two separate certificates are present on each token, one for authentication and one for signature. The issuance is based on a compulsory prior identification in person and information recorded in the national population register.

Certificates are therefore issued by private sector partners as well as the police, through the national Swedish identity card.

A national electronic health record system, known as National Patient Summary, is in place (Nationell Patientöversikt – NPÖ¹⁰). This system will, at a later stage, allow Swedish residents to access their own medical records through the Internet. At the moment, however, the National Patient Summary mainly gives authorized care staff access to critical patient information.

The validation methods used are either the Online Certificate Status Protocol (OCSP) or the Certificate Revocation Lists (CRLs), though OCSP is the main method used.

eSignatures Legislation

The Act on Qualified Electronic signature does not make a literal translation of the eSignature definition stated in the European Directive. Rather, a Swedish electronic signature includes both authentication and integrity requirements. Electronic signatures indeed defined as “data in electronic form attached to or logically associated with other electronic data and used to verify that the content originates from the alleged issuer and has not been altered.”¹¹

¹⁰ See: <http://www.npö.nu/index.php?s=english>

¹¹ See: <http://www.epractice.eu/en/document/288379>

NIS Governance

Overview of the key stakeholders

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

National Authorities	<ul style="list-style-type: none"> • Ministry of Enterprise, Energy and Communications • Swedish Post and Telecom Agency (PTS) • Swedish Data Inspection Board • Media Council • Ministry of Justice • Ministry of Defence • Swedish Defence Materiel Administration • National Defence Radio Establishment (Försvarets radioanstalt - FRA) • Agency for Civil Protection and Preparedness (MSB) • Swedish Defence Research Agency (FOI) • National Police Board • Swedish National Financial Management Authority (ESV) • Swedish Board for Accreditation and Conformity Assessment (SWEDAC) • Answer
CERTs	<ul style="list-style-type: none"> • CERT SE • SIST • SUNet CERT • Swedbank SIRT • TS-CERT
Industry Organisations	<ul style="list-style-type: none"> • Swedish IT and Telecom Industries • SIG security • Swedish Risk Management and Security organization
Academic Organisations	<ul style="list-style-type: none"> • ICT, Royal Institute of Technology (KTH) • Department of Computer and Systems Sciences (DSV) • Chalmers • Blekinge Institute of Technology (BTH) • Linköping Institute of Technology (LITH) • Swedish Institute of Computer Science (SICS)
Others	<ul style="list-style-type: none"> • The Swedish Association of Local Authorities and Regions • The Swedish Consumers' Association • ISACA Sweden

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"¹² – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory¹³.

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.

¹² 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

¹³ <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

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

Co-operation between public authority bodies

Sweden does not have a single government body that is recognized among NIS stakeholders as the national security agency. Various institutions such as the Swedish Post and Telecom Agency (PTS), Swedish Data Inspection Board, Swedish Civil Contingencies Agency, National Defense Radio Establishment, Swedish Defence Materiel Administration and Swedish Security Service share the tasks and competencies.

The Ministry of Enterprise, Energy and Communications, Ministry of Justice and Ministry of Defense are responsible for the coordination of the development of national information security policy/strategy, legislation and research in the NIS domain. The execution of strategic policies is carried out by the organizations that are overseen by the mentioned ministries.

The PTS also exercises supervision to ensure compliance with legislation and decisions concerning obligations and requirements, in addition to regulations issued under law. If there is reason to suspect that an operator is not complying with these rules, PTS may inform the operator of the circumstance. In case of dispute between operators a decision issued by PTS to resolve the situation can only regulate the terms between the parties in the specific dispute, and only the parties to the dispute are to be directly encompassed by a decision issued by PTS to resolve the dispute.

The Swedish Data Inspection Board is an independent oversight body responsible for protection of the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. The Board works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes. Sweden has security response teams in place to handle security breaches and other incidents.

As part of the Ministry of Culture, the Swedish Media Council is an expert committee on children and media in Sweden. The aim of the Council's work is to protect children and minors from harmful effects of media content and media use.

Co-operation via the NTSG

The National Telecommunications Coordination Group (NTSG) was founded in August 2005 and is a voluntary cooperation platform aimed at supporting the restoration of the national infrastructure for electronic communications in connection with extraordinary events in society. The criterion for NTSG membership is that the operator/organisation possesses its own technical equipment, skills or resources that affect Sweden's critical infrastructure for electronic communications. Through their role, they have a potentially major influence on the critical national infrastructure for electronic communications. New members may join the group following a joint decision in NTSG. PTS chairs the NTSG.

Those participating in NTSG meet up twice a year to ensure that NTSG is well established and has been trained to be able to function in a national emergency, to test and develop the forum, to update documentation, to develop contacts and for coordination exercises. In addition to this, the group's procedures for convening meetings are tested every third month. These virtual meetings also offer the opportunity to discuss issues within the group's area of interest. The group's members also participate in various collaboration projects with the power sector and the stakeholders responsible for the area, such as the county administrative boards and municipal authorities.

During an emergency, the group's work is initiated by a group member requesting that the group convenes; following which PTS makes a decision regarding this. The group then convenes either virtually or physically at a predetermined location. Work starts with a start-up meeting, which follows an agenda drawn up in advance and the members report on the current situation. After that, regular telephone and web meetings are held as often as the situation requires. This work is characterised by collaboration within the sector, collaboration across sectors, private-public collaboration and civil-military collaboration.

In the event of an emergency, the group summarises the damage situation, reports back on the situation to the parties affected and proposes measures as required. If needed, the group may also coordinate initiatives.

Collaboration with other stakeholders in society is an important area for NTSG. Routines for collaboration with, for example, county administrative boards and other important stakeholders in an emergency situation are gradually being developed.

Co-operation via the MIMER

In the spring of 2006, work started on a prototype for a joint situation assessment (MIMER). The MIMER project was cofounded by the EPCIP programme.

The objective was to enable the creation of a joint situation assessment within the electronic communications sector in the event of major disruptions to the electronic communications networks. It is now in production.

The aim of MIMER is to reduce disruptions within the electronic communications sector and minimise the effects of disruptions for other sectors of society whose operations are dependent on electronic communications. The aim is also to increase the capacity of society to deal with the consequences of disruptions and interruptions to electronic communications.

The main domains where MIMER is active are¹⁴:

- Increased cooperation between stakeholders in society;
- MIMER-P facilitates reporting to SOS Alarm.

Co-operation of NIS stakeholders to combat spam and malware

SAMFI is a collaboration group which supports agencies within the information security field¹⁵. The group consists of the Swedish Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Post & Telecom Agency, the Swedish Armed Forces, the Swedish Civil Contingencies Agency & the Swedish Police. We notice here that the SAMFI cooperation is broader than the above mentioned cooperation to combat spam and malwares¹⁶.

¹⁴ For more detailed information on implementation projects related to the MIMER please visit the following websites : <http://www.telenor.se/privat/kundservice/tackning-och-driftinformation/aktuella-storningar.html>
http://www.telia.se/privat/link.do?tabId=3&channelId=-103360&sl=teliaservice_driftinfo_mob

¹⁵ Source:

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

¹⁶ The MSB intends to, in collaboration with the agencies that make up SAMFI, investigate whether a more structured technical intrusion detection and warning system for important societal functions and critical infrastructures could be introduced in Sweden.

Sweden can be considered as a Member State where moderate information can be found on a diversified series of actions and measures related to the combat against online malpractices such as spam, spyware or malicious software.

It is noted that the Swedish Post and Telecom Agency (overseen by the Ministry of Enterprise, Energy and Communications), the Swedish Data Inspection Board (overseen by the Ministry of Justice), the MSB (which has a role which was taken before January 2009 by the Swedish Emergency Management Agency), the National Defence Radio Establishment (overseen by the Ministry of Defense) and the Swedish Security Service cooperate together to ensure information security in Sweden.

Co-operation between public and private stakeholders for internet security

The SurfaLugnt¹⁷ national campaign for a safer Internet is one of the most successful partnerships between the IT industry and relevant authorities.

The partnership leveraged respective expertise and access to channels and was formed as an alliance is viewed as being more credible and has more opportunity of gaining attention among the target groups and the media.

INFOSAFE is an international EU network with a local presence, organizing events and promoting awareness. The Swedish node for internet safety awareness is coordinated by the Swedish Media Council.

Safer Internet Day is organized by INSAFE each year in February to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people across the world.

Internetsakerhet¹⁸ also exists - a practical site that provides SMEs and citizens with helpful information on Internet security.

The website "Computer security test for consumers" is aimed at the Swedish citizens. Through this web service, a consumer who is connected to the Internet from home can obtain a grade relating to whether their computer is vulnerable to security abuse when they surf.

The e-Security¹⁹ is campaign initiative initiated by the city of Stockholm. As the public administration increase their service and contact with their citizens there is an increased demand for e-Security. Citizens using the new services expect the same security, confidentiality and reliability as when they get the service over-the-counter. For citizens to accept and start using the new services they must have confidence in them and therefore e-Security is a very important issue for all governments and local-governments.

There are a number of e-Security initiatives but most within awareness raising programs towards citizens and businesses. With the increased pressure towards cities to provide a secure and confidential service, there is a strong need for cities to work together in establishing standards and sharing best practices within e-Security.

¹⁷ See: <http://surfaluqnt.se/>

¹⁸ See: <http://www.pusha.se/nyckelord/internetsakerhet>

¹⁹ See: <http://www.esecurity.se/>

Information exchange platform on regulation and personal data processing

Regarding exchange mechanisms, the Swedish Post and Telecom Agency website provides information about its decisions and regulations and also informs and provides tips to around:

- Consumer interests;
- Sustainable competition;
- Efficient utilization of resources and;
- Secure communications.

As a public authority, PTS is encompassed by the right of public access to official information. This means that all documents, including personal data, submitted to PTS become public documents which may be provided to any party requesting them. In some cases, however, information may be deemed to be confidential and is consequently not provided to third parties. Read more about the right of public access to official information and confidentiality on the website of the Swedish Government. PTS may transfer personal information submitted via the website if the Agency is the wrong authority to receive such information, which means that it should be transferred to the correct body. In addition to this, information related to marine radio licences is provided to the Swedish Maritime Administration on a regular basis.

Fostering a proactive NIS community

For Sweden the security has been deepened and expanded to a great extent: Estonia, Latvia and Lithuania. The security policy cooperation with Finland is particularly close. In 2010, Sweden actively participated in the Arctic, Barents Sea and Baltic Sea cooperation, and contributed to the EU's Northern Dimension. Security in the Baltic Sea region has been fundamentally strengthened now that Estonia, Latvia and Lithuania have become members of the EU and NATO.²⁰

In February 2009, an extraordinary meeting of Nordic foreign ministers took place in Oslo²¹. The goal of this meeting was to present a certain number of proposals relative to co-operation between the Nordic Countries. One of these proposals described a project for a "Nordic Resource Network", a cooperation network between the Nordic Countries which would aim at protecting against cyber attacks. The main task of this network would be to facilitate exchange of experience and coordinate national efforts to prevent and protect against such attacks and provide advice to Nordic countries that are in the process of building capacity in this area. In the longer term, the resource network could develop and coordinate systems for identifying cyber threats against the Nordic countries.

On 3 November 2010, a request²² was made for the set-up of this network, the "Nordic CERT Information Sharing Network". Also, Baltic countries have been invited to participate in this network as soon as feasible. It is also worth mentioning that similar co-operation had already begun in some form before the Stoltenberg report.

²⁰ See: <http://www.sweden.gov.se/sb/d/3103/a/116839>

²¹ Source: www.regjeringen.no/upload/UD/Vedlegg/nordicreport.pdf

²² Source: www.um.dk/NR/rdonlyres/153EA335-238A-405B-854B-816BC4B56AA7/0/Erkl%C3%A6ringfradetnordiskeudenrigsministern%C3%B8deiReykjavikd.pdf

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

Security incident management

In recent years, many countries have introduced, or are about to introduce, new national collaborative functions in order to coordinate the handling of IT incidents. Sweden has good prerequisites for creating strong structures to prevent and handle IT incidents. In Sweden, many of the competencies and resources needed in order to create a sustainable system for the preventing and handling of IT incidents are already available, both in the private and public sectors. However, these collective resources have to be supplemented in order to improve their suitability, coordination, availability and dimension.

The Swedish Civil Contingencies Agency (MSB) was tasked by the Government to submit proposals for the prevention and handling of IT incidents in Sweden, before mid January 2010.

The main results presented were:

- **Creation of national structure:** one of the main proposals has been made by the MSB. The objective is to create a coherent structure to strengthen the national ability to prevent and handle serious IT incidents²³;
- **Creation of a national operational centre:** the MSB intends to set up a national operational coordination centre for cybersecurity at the agency. The coordination centre will be assigned to support Sweden's preventive cybersecurity work and to help coordinating the handling of serious IT incidents;
- **Development of measures to strengthen the national structure:** Besides the establishment of a national operational coordination centre, the following measures should be implemented in order to create a structure that aims to increase the national ability to prevent and handle serious IT incidents. The main objective here are:
 - Development of measures to improve management, cooperation & coordination;
 - Improvement of information sharing;
 - Improvement of situational awareness;
 - Improvement of situational responsiveness.

More emphasis is put on incident response, critical infrastructure activities and active contributions to joint international development and co-operation projects. Clearer focus is put on the ability to gather data through the operation of traffic monitoring systems. Proprietary periodic statistics reports are substituted by continuous situation information.

The main collaborators are the utilities because power is essential to the functioning of a public e-communication network. Nevertheless, when the utility tries to repair power lines or a transformer station, communication with people involved is a necessity. In Sweden, whenever dependability and reliability become an issue, the root is very likely the power supply. Issues relating to vulnerability concern a very large number of actors and interests in society, and it is a highly dynamic sphere of activity.

²³ Source :

http://www2.msb.se/Shopping/pdf/upload/Publikationsservice/MSB/0163_10_Measures_to_Prevent_Handle_IT_Incidents.pdf

Accordingly, consumers call operators about network failures or issues affecting reliability and dependability of public e-communication networks. Often, before they call the operator, consumers try to investigate themselves by using an online facility.

Training and exercises in crisis management

Within the framework of its robustness work, the Swedish Post and Telecom Agency has a strategy for training and exercises that is based on an integrated approach which includes all components, from an individual and corporate level to an overall sectorial level.

The aim of the strategy and the training and exercises conducted within this framework is to increase the capacity of the sector to deal with emergencies and extraordinary events to in turn minimise the consequences for society as a whole. The target group for training and exercises includes individuals and undertakings or other organisations within the sector that possess their own technical equipment, skills or resources that affect Sweden's critical infrastructure for electronic communications.

- **Individual emergency training in three modules:** the aim of the individual training programme is to make participants aware of their opportunities and limitations during extraordinary events;
- **Training and exercises tailored for undertakings:** the aim of the training and exercises at a corporate level is to provide undertakings with the knowledge and experience to enable them to deal with crises and stressful situations in the best way possible;
- **Training at a sectorial and cross-sectorial level:** the training at a sectorial and cross-sectorial level is primarily aimed at improving collaboration and increasing understanding of the operations of various stakeholders and creating networks of contacts;
- **Exercises at a sectorial and cross-sectorial level:** these exercises are an effective way of evaluating how organisations, operations and collaboration function during an emergency and they are basically necessary for developing crisis management capabilities within the sector. In a liberalised market, all stakeholders are an important piece of a large puzzle, where collaboration is a prerequisite for being able to deal optimally with emergencies.

One of the tasks of PTS is to strive for robust electronic communications and it also has certain financial resources for various measures to strengthen electronic communications networks. The measures taken using PTS's resources are only those not generated on commercial grounds or following other regulatory requirements imposed on operators and where society needs improved robustness in order to be able to deal with an extraordinary situation.

Emerging NIS risks

At societal level the main risks are mainly related to the following areas: electronic communications, digital control systems, cryptographic functions, the media sector, the public sector, financial services, medical care and healthcare and crime-fighting.

They are all characterised by the fact that inadequate information security means an adverse effect on society. Sensitive information can get into the wrong hands, payment streams can be stemmed or rerouted and suspected crime cannot be investigated. The residents of Sweden assume that information management in these areas will function and be secure. Under the

heading organisation and the individual level we highlight here briefly the functions that are crucial to the functioning of the businesses of individual organisations or persons. It should be mentioned that a completely unexceptionable subdivision into the societal level and the organisational and individual level is impossible. We inform the reader that more detailed information is available in the document²⁴: **“Information security in Sweden - Situational assessment 2009”**.

Resilience aspects

Good practice on resilience

There is no repository for good practices on resilience. However, a strategy for improving robustness exists as well as does regulation that should help to build more robust networks and network nodes. These efforts focus on organisations that build infrastructure. Information exchange between the regulator and vendors is limited. Consultations are indirect, whereby operators may bring vendors to meetings. As well, informal discussions may be held with a vendor. Regulation regarding Universal Service Obligations (USO) exists in Sweden. However no operator has been issued any obligations under USO.

Traditionally, the incumbent TeliaSonera has been the provider of fixed telephony access. However, in recent years this has become a challenge because the operator does not longer repair or deploy fixed lines in the more rural areas. PTS is at the moment evaluating different approaches to the USO-problem. One way is to have a type of USO-obligation with some operators for particular geographical regions.

There is also a financial issue since the costs could be exorbitant. Finally, the Robust Communications Unit uses a three year strategy to decide prioritized areas. In turn, this may result in a shift of funding priorities for resilience work regarding public e-communication networks.

Regulatory issues of resilience of public e-Communications networks

The Electronic Communications Act²⁵ (2003:389) does address resilience in chapter 5 article 6a. This part of the law has been translated except for this critical article. An unofficial translation looks like this: “A party that provides a public electronic communication service or a public electronic communication network shall ensure that the service and the public network satisfy reasonable demands for good function and technical security and also for sustainability and accessibility in the case of extraordinary events during peacetime” [Chapter 5 of the Electronic Communications Act (LEK)].

Sweden follows the principled-based standard approach. Accordingly, in contrast to rule-based standard descriptions regarding continuity planning as well as incident planning are quite general. In turn, much interpretation is left to the operator who experiences pressure by the market to provide adequate resilience at a competitive price. As well, regulations require that operators demonstrate adequate measures were taken to assure satisfactory reliability and dependability of public e-communication networks.

²⁴ Source:

http://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0119_09_Information_security_in_Sweden.pdf

²⁵ See the ENISA report: <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies>

Audits related to resilience

Sweden prefers to conduct supervision activities instead of full-blown audits. All regulatory work is conducted by the PTS.

Whilst it may hire outside experts to do part of the job, it will keep responsibility and will be the lead on the project. The Robust Communications Unit at PTS stays away from regulatory work and compliance issues because its focus is to work closely together with operators to improve resilience. Enforcing regulation, however, might jeopardize trust and reduce operators' willingness.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented through the Swedish Personal Data Act (Sw. Personuppgiftslagen (1998:204)) (the "Act"). The competent national regulatory authority on this matter is the Datainspektionen (the "Data Inspection Board"). No updates to this were identified in 2010.

Personal Data and Sensitive Personal Data

The definition of personal data in the Act is closely based on the standard definition of personal data. In particular, it only applies to living individuals, as opposed to legal entities or dead persons. The Swedish courts and regulator tend to interpret the concept of personal data broadly. The guidelines issued by the regulator are, however, in all relevant respects in line with the Opinion on Personal Data.

IP addresses are considered in Sweden as personal data. This has been confirmed by the Administrative Court of Appeal who stated that an IP address is referable to a natural person and shall therefore be considered as personal data.

Under the Swedish Personal Data Act, sensitive personal data includes the standard types of sensitive personal data. Certain alternative provisions apply to information about legal offences and personal identity numbers (the Swedish equivalent to social security numbers). In general, sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. A data subject's consent does not have to be made in writing but must be voluntary, explicit and informed.

Data concerning legal offences may only be processed by public authorities unless permission is granted by the Data Inspection Board. Personal identity numbers may, in the absence of consent, only be processed when it is clearly justified with regard to the purpose of the processing, the importance of secure identification or some other noteworthy reason.

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

The data controller must comply with the general data security obligations. This applies also when processing personal data in accordance with the Unstructured Material Rule.

Enforcement and data protection breaches

The Swedish Personal Data Act contains a general obligation for the personal data representative to inform the Data Protection Board of any suspected breaches.

The Data Inspection Board has the authority to fine organisations and/or to prohibit them from processing personal data. The Data Inspection Board may also apply to the Swedish Administrative Courts to delete unlawfully processed personal data.

We notice that in term of privacy and trust no major changes have been identified in 2010.

NIS awareness at the country level

Awareness actions for all players in society who are involved in managing information-security issues

Since 2008, MSB redacts an assessment on Information security in Sweden. We notice here that no updated English version of the situational assessment has been identified. The results presented in this section are thus the key highlights related to 2009 situational assessment that are still applicable and valid in 2010.

Such a situational assessment provides a picture of the level of societal security presents the latest developments made, the threats, the vulnerabilities, the risks and the measures carried out. This assessment is used in order to compare the Swedish Information security situation with the situation targeted. Such an exercise can thus be used as a basis for prioritisation of the areas to which particular attention needs to be devoted.

MSB's remit is to support and coordinate the work on societal information security and to analyse and assess outside developments in the area. The situational-assessment work forms part of the monitoring of outside events and the analytical work, and constitutes support in the work on the national plan of action for information security administrated by MSB. The situational assessment constitutes support for players in society who are involved in managing information-security issues.

Awareness actions targeting the safe use of the internet

Specific actions on awareness include the Swedish Post and Telecom's websites on Internet security and the establishment of the CERT Swedish IT Incident Centre (CERT SE).

It is also worth noting that awareness raising is often a natural part of the work plan in an agency or a business and would come about with or without a national strategy. Examples are consumer protection agencies, sector agencies (electronic communication, financial services etc.) and law enforcement agencies.

The Swedish Consumer Agency for example provides information on safe e-commerce, provides a tool to protect IT users from modem hi-jacking (which for a period of time was a very large problem), and provides the ability to measure the actual bandwidth delivered by an ISP.

The Swedish strategy – from a governmental point of view focuses mainly on educating users to increase the security level of their computer equipment and less on administrative actions against malicious software.

A lot of practical work is most likely done at the level of ISPs who offer security packages and filter spam and e-mails containing viruses. There seems, however, not too much cooperation between

ISPs and software companies except in cases of information campaigns. The government and the ISP industry created a PPP initiative to create a more secure web for the public.²⁶

The Swedish Safer Internet Centre is coordinated by the Swedish Media Council. In collaboration with BRIS – Children’s Right in Society, a Swedish NGO, they will use their position as national awareness centre to coordinate a strong, consistent and up-to-date safety message and ensure that it reaches all relevant target groups²⁷. The main initiatives are:

- The Young Internet campaign;
- Development and distribution of educational materials;
- Helpline support services;
- Youth panels – advice from the real experts.

We highlight here the “Young Internet” which is a campaign promoting safer use of the Internet among children and young people. The campaign is run by the Media Council in collaboration with BRIS (Children’s Rights in Society), a Swedish NGO, and is partly funded by the European Commission. Through its work with The Young Internet campaign, the Media Council represents Sweden in Insafe, a European network of e-safety awareness. The Young Internet aims to raise awareness²⁸ about Internet safety and promote dialogue between children and adults.

Other awareness-raising events

The Swedish Media Council is a committee of inquiry in the Swedish government offices, working with children’s and young people’s media situation, with an aim to reduce the risks of harmful effects of the media. The Council covers all moving image media, i.e. the Internet, film, television, computer and video games.

The Media Council gathers relevant research in this area for the purpose of dissemination and coordination of educational efforts. With this knowledge the Media Council²⁹ tries to raise awareness about the risks and benefits of media use, offering advice to parents, as well as those engaged in professions that deal with children and youth.

Here also we mention here the very successful campaign SurfaLugnt initiative in terms of awareness raising.

²⁶ Source of information:

http://ec.europa.eu/information_society/policy/ecomms/doc/library/ext_studies/privacy_trust_policies/spam_spaware_legal_study2009final.pdf

²⁷ Source: <http://www.saferinternet.org/web/guest/centre/>

[/centre/sweden?p_p_lifecycle=1&p_r_p_1607082367_country=Sweden&](http://www.saferinternet.org/web/guest/centre/-/centre/sweden?p_p_lifecycle=1&p_r_p_1607082367_country=Sweden&)

²⁸ Source: <http://www.medieradet.se/Om-Medieradet/About-the-Swedish-Media-Council-in-English/>

²⁹ Source: <http://www.medieradet.se/Om-Medieradet/About-the-Swedish-Media-Council-in-English/>

Country-specific activities for identifying and promoting economically efficient approaches to information security

No specific information has been identified on this particular topic. But nevertheless we notice that the Government intends to create a Public Administration that emanates from the needs of both the citizens and the entrepreneurs, to achieve significant changes in their daily lives. Likewise, the Government has set the goal to reduce administrative costs by at least 25 % by 2010.

The organization responsible for new legislation and regulations are obliged to make a written assessment of the consequences for the actors covered by the legislation and regulation. The assessment covers proportionality as well as a specific part of consequences for SME.

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

Digital control systems (SCADA) that control the electricity and water supply and other basic infrastructure are core components of critical societal functions. The area has attracted increased attention as a result of the creation of a public, available and easy-to-use attack code that exploits a well-known vulnerability in a relatively well disseminated SCADA system. Vulnerabilities arising when older SCADA systems are connected to modern administrative systems still persist, and bearing in mind the increasingly sophisticated threats their management has become a priority. It is important that more measures in this area be carried out over the coming years.

IT-related threats are directed at critical societal functions such as financial services, media companies and medical care and healthcare.

Cybercrime is a complex threat to critical societal functions. Crime-fighting is in part impeded by a lack of resources, undisclosed cases and problems that are hard to categorise. Businesses are handling events internally as technical problems, whilst they are by the same token being exposed to cybercrime.

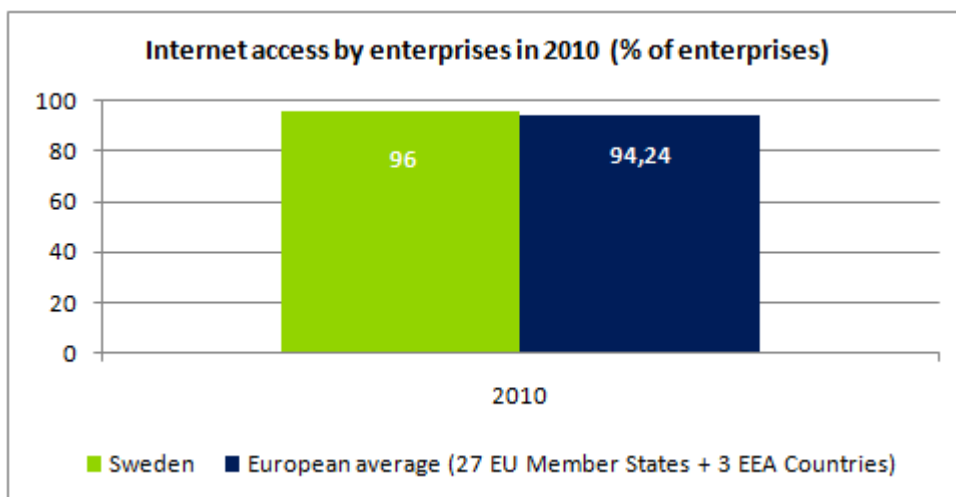
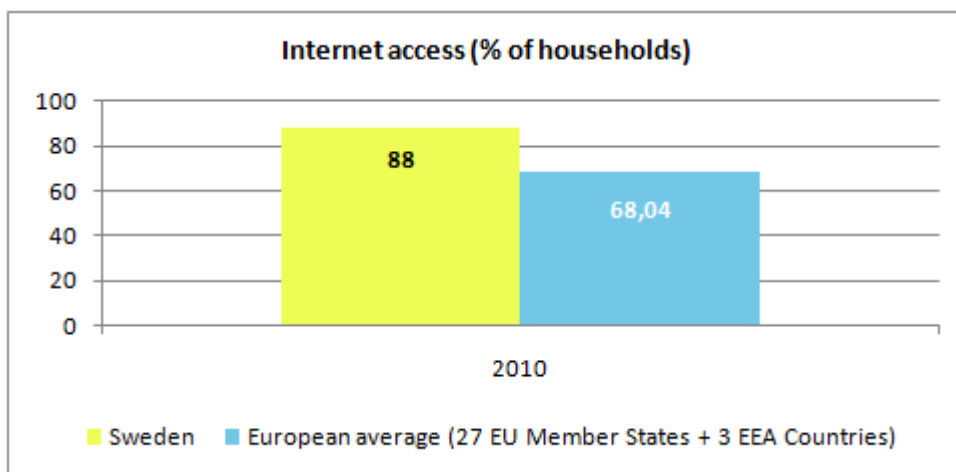
Security work and crime-fighting related to IT constitute a field in which private companies are occupying an unusually large area and are assuming particular responsibility.

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Sweden, a series of relevant statistics are included in this section. These statistics show that, overall, Sweden is ahead of the European average in Information Technology and NIS matters.

Internet access of population and enterprises

The following graphs provide an overview of the situation³⁰ of Internet access in Sweden for enterprises and respectively households, relative to the European average.



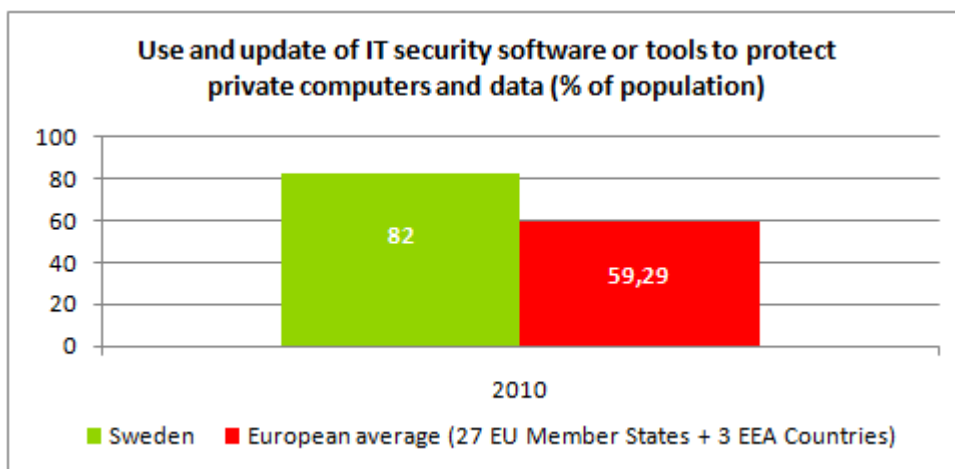
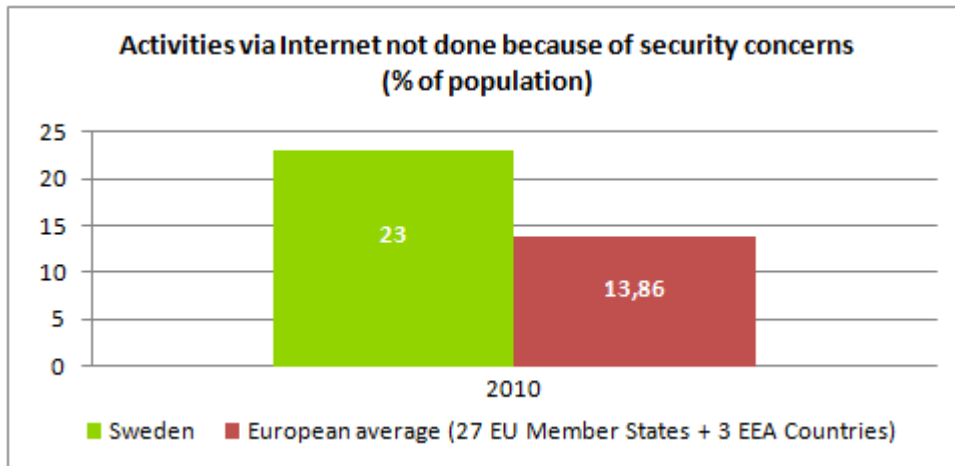
In 2010, the statistics indicate that both the enterprises and the households in Sweden have a level of Internet access that is above the European average. It appears that the Swedish business sector is leading the way for the other European countries.

³⁰ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Sweden that is reluctant to perform activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) is above the European average.

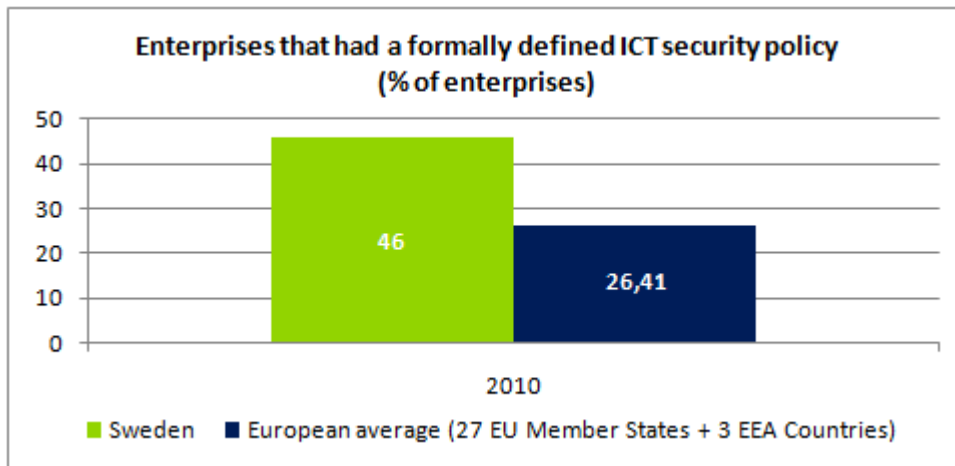
Swedish citizens, although very connected, are also very aware of the security concerns. This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



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

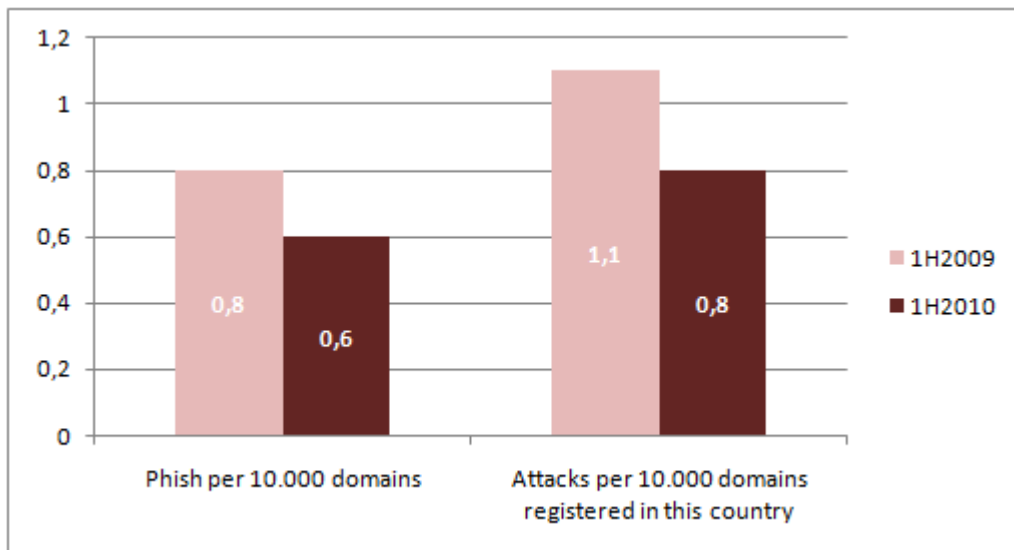
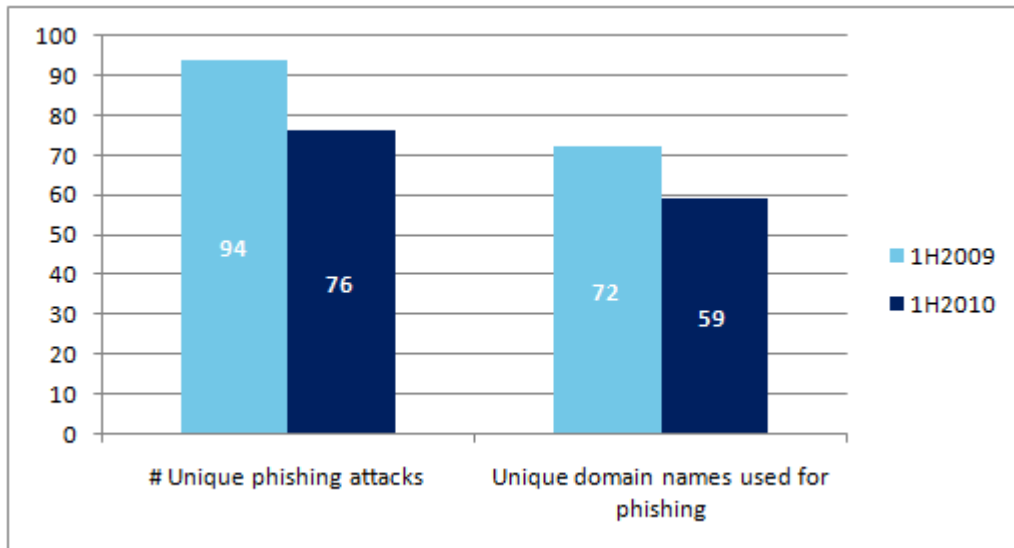
Statistics on use of Internet by enterprises and related security aspects

More enterprises in Sweden have a formally defined ICT security policy, compared with their European peers.



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Sweden was mentioned in the global report³¹ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



³¹ 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

National authorities	Role and responsibilities	Website
1. Ministry of Enterprise, Energy and Communications	<p>The main responsibility area of the ministry of Ministry of Enterprise, Energy and Communications are the:</p> <p>The Ministry of Enterprise, Energy and Communications is responsible for handling government business in the following areas:</p> <ul style="list-style-type: none"> • Business development; • Competition; • Electronic communications; • Energy; • ICT Policy; • Postal communications and cashier service; • Regional growth; • Development Perspective (ESDP). • Tourism; 	www.sweden.gov.se/enterprise
2. Swedish Post and Telecom Agency (PTS)	<p>The authority is an independent agency according to the Swedish public authority model. PTS's work concerning secure communications involves supervision under the Electronic Communications Act. The Swedish Post and Telecom Agency:</p> <ul style="list-style-type: none"> • Monitors the electronic communications and postal sectors in Sweden; • Acts as regulating authority for security in electronic communications (Telecommunications, Internet and radio) and in the use of electronic signatures. <p>The Agency works with consumer and competition issues, efficient utilization of resources and secure communications.</p> <p>The authority may require that all networks for electronic communications should satisfy reasonable requirements for good functionality and security. One important component of enhancing security on the Internet is well-informed and aware users. PTS has consequently taken initiatives to inform consumers about these areas. Furthermore, supervision is conducted in this area to verify that the stakeholders in the market comply with the legal provisions concerning protection of privacy. This supervision comprises for example dealing with complaints received, inspections and follow up of demands imposed.</p>	www.pts.se
3. Swedish Data Inspection Board	<p>Protecting the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. The government has given the task of creating the preconditions for the processing of personal data so as not to lead to undue privacy infringement.</p> <p>The Board works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes. The Board also handles complaints and carries out inspections. By examining government bills the Data Inspection Board ensures that new laws and ordinances protect personal data in an adequate manner.</p>	http://www.datainspektionen.se
4. Media Council	<p>The Swedish Media Council was founded January 1st, 2011, when the former Statens biografbyrå</p>	http://www.medieradet.se

National authorities	Role and responsibilities	Website
	<p>(National Board of Film Classification) merged with Medierådet (formerly also called The Swedish Media Council). The Media Council is a national authority working with children's and young people's media situation, with an aim to reduce the risks of harmful effects of the media and to empower the children in their media use.</p> <p>The Media Council gathers relevant research and continuously publishes reports and other material on developments in the media, media effects and the media situation of children and young people. The Council is also responsible for the Swedish film classification on films that are going to be public screened to determine whether films are liable to harm the well-being of children in different age groups.</p> <p>Also the Swedish Media Council represents Sweden in Insafe, a European network of Safer Internet Centres. It is done through the campaign The Young Internet, aims to raise awareness about internet safety and promote dialogue between children and adults. We stress the benefits of the internet and online media, as well as the importance of being a critical media user. Our awareness message is based on facts and knowledge and we have chosen to put the issue of safer internet use into a broader context of children's everyday life.</p>	
5. Ministry of Justice	<p>Development of Security Technology and Standards Policy, Implementation of Security Technology and Standards. More globally the area of responsibility of the Ministry of Justice are:</p> <ul style="list-style-type: none"> • Legislation; • The Judicial System; • Criminal Matters; • International Judicial Cooperation; • Strategy to meet the threat of terrorism; • Migration and Asylum Policy; • The Principle of Public Access; • Plain Language Work; • Transparency in the EU. 	http://www.sweden.gov.se/ju stice
6. Ministry of Defence	<p>The Ministry of Defence is responsible of:</p> <ul style="list-style-type: none"> • Protection and preparation against accidents; • Severe peacetime emergencies; • Security policy in the field of defence; • International operations; • Intelligence issues; • Gender equality and diversity. <p>The Ministry has the National Defence Radio Establishment organization to assist it with IT security matters.</p>	http://www.sweden.gov.se/d efence
7. Swedish Defence Materiel Administration	<p>FMV is a civil government agency with the task of boosting the overall capability of the total defence organisation.</p> <p>The aim is to be a defence-equipment supply agency that is skilled and is in demand, including in an international perspective. A business-like approach, know-how in system development and a high level of cooperation capability are characteristic features of FMV.</p> <p>FMV is also a supervisory authority with regard to electromagnetic compatibility (EMC) for the Swedish Armed Forces, the National Fortifications Administration, the National Defence Radio Establishment and the Swedish Defence Research Agency. EMC means the ability of a device,</p>	www.fmv.se

National authorities	Role and responsibilities	Website
	<p>equipment or system to function satisfactorily in its electromagnetic environment without introducing unacceptable electromagnetic interference into its surroundings.</p> <p>In addition, FMV has to establish a certification function to draw up and maintain a Swedish system based on the international standard ISO/IEC 15408 Evaluation and Certification of Products and Systems. This standard is more generally known as Common Criteria (CC).</p>	
8. National Defence Radio Establishment (Försvarets radioanstalt - FRA)	<p>FRA is engaged in information assurance. On demand, the Authority supports government authorities and state owned companies regarding current IT threats as well as giving general advice to improve security.</p> <p>FRA's main customers are the Foreign Ministry, the Ministry of Defence, the Military Intelligence & Security Directorate (MUST) and the Security Police.</p>	www.fra.se/
9. Agency for Civil Protection and Preparedness (MSB)	<p>The task of the MSB is to enhance and support societal capacities for preparedness for and prevention of emergencies and crises. When one does occur, MSB supports the stakeholders involved by taking the right measures to control the situation.</p> <p>In collaboration with other stakeholders the MSB develops the individual's and society's capacity to prevent, deal with and learn from emergencies and disasters.</p> <p>Knowledge development plays also a strategic role in the MSB's work for a safer society. As research is the most important way of developing knowledge the MSB has the task of directing, ordering and ensuring the quality of research conducted on its behalf.</p> <p>The MSB primarily supports applied, needs-oriented research. The aim is to generate practical applicable research findings that will lead to an increased ability to solve societal problems. MSB research covers a wide field and encompasses several disciplines and is carried out in cross-sector and international context.</p>	www.msb.se
10. Swedish Defence Research Agency (FOI)	<p>FOI is one of Europe's leading research institutes in the defence and safety area. The agency is financed on contracts basis and is responsible to the ministry of defence. The core business is research, method and technology development and studies.</p> <p>FOI carries out security policy studies and analyses evaluate different types of threats and develop tools for, as an example, adaptation of society due to climate change. FOI develops systems for crisis management in connection with major accidents and catastrophic events.</p>	www.foi.se
11. National Police Board	<p>The Police inform about IT security and crime in addition to enforcing IT-related legislation.</p> <p>The Swedish National Police Board (Rikspolisstyrelsen) is the central administrative and supervisory authority of the police service. It is also the supervisory authority of the National Laboratory of Forensic Science.</p> <p>The SNPB is headed by the National Police Commissioner who is appointed by the government. The current National Police Commissioner is Bengt Svenson. Among other things, the SNPB is responsible for the</p>	www.polisen.se

National authorities	Role and responsibilities	Website
	development of new working methods and technological and administrative support. It is also - through the National Police Academy - responsible for the training of police officers. It is also the principal agency for the Swedish National Laboratory of Forensic Science.	
12. Swedish National Financial Management Authority (ESV)	As part of the ministry of finance the Swedish National Financial Management Authority is responsible for implementing e-invoicing.	www.esv.se
13. Swedish Board for Accreditation and Conformity Assessment (SWEDAC)	SWEDAC is the national accreditation body in Sweden. It is a government authority under the Ministry for Foreign Affairs as well as the Ministry of Enterprise, Energy and Communications. SWEDAC is a public authority which duties are funded by a Government grant, while its commercial work is funded by fees. This commercial work is self-financing, i.e. its costs are completely covered by its fees.	www.swedac.se
14. Answer	The Swedish Media Council coordinates the Swedish node for internet safety awareness. In February 2007 BRIS-Children's Right in Society joined the project as helpline partner. Together they coordinate a strong, consistent and up-to-date safety message and ensure that it reaches all relevant target groups.	http://www.saferinternet.org/en/en/pub/insafe/focus/sweden.htm

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST³² member TI³³ listed 	
15. CERT SE	<p>CERT SE is the Swedish government CERT. CERT SE is the national alert, warning and response system and is responsible for technical vulnerability disclosure co-ordination. CERT SE provides information and advice regarding proactive measures, and compiles and publishes statistics. It is part of the National Post and Telecom Agency.</p> <p>We notice here that CERT SE is:</p> <ul style="list-style-type: none"> FIRST member; TI listed. 	www.cert.se/
16. SIST	<p>SIST (The SNIC IT Security Team) coordinates and supports the local IT security staff at the Swedish high performance computing sites within the SNIC (Swedish National Infrastructure for Computing) meta-centre.</p> <ul style="list-style-type: none"> Not a FIRST member; TI listed. 	http://www.snic.vr.se/snic-committees/sist
17. SUNet-CERT	<p>SUNet-CERT is the Swedish University Network Computer Emergency Response Team. SUNet CERT helps University, college and other organisation connected to SUNET network with coordination of incidents. SUNet CERT will also help to keep the competence at IT security organisation within University's and colleges. SUNet CERT will also keep a close contact with other ISP in Sweden and abroad and cooperate with national and international CERT organisation.</p> <p>We notice here that SUNet-CERT is:</p>	www.cert.sunet.se

³²See: <http://www.first.org/members/teams/>

³³See: <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST³² member TI³³ listed 	
	<ul style="list-style-type: none"> FIRST member; TI listed. 	
18. Swedbank SIRT	Swedbank is Sweden financial sector incident response team. We notice here that SUNet-CERT is: <ul style="list-style-type: none"> Not a FIRST member; TI accredited. 	https://www.trusted-introducer.org/teams/teams-s.html#SWEDBANK-SIRT
19. TS-CERT	TS-CERT is the CERT of Telia Sonera, a major Internet service provider. We notice here that SUNet-CERT is: <ul style="list-style-type: none"> Not a FIRST member; TI accredited. 	https://www.trusted-introducer.org/teams/ts-cert.html

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
20. Swedish IT and Telecom Industries	Swedish IT and Telecom Industries promotes the increasing use of IT in Sweden and provides vital support to the development of individual member companies by promoting business opportunities, removing barriers and providing member service.	http://www.itforetagen.se
21. SIG security	The organization's main issue is to give rise to the understanding of and inspire to the work within the information security area.	www.sigsecurity.se
22. Swedish Risk Management and Security organization	The organization's task is to promote awareness in the field of risk by monitoring current events, expert interaction etc.	www.svensktnarinsqliv.se

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
23. ICT, Royal Institute of Technology (KTH)	The ICT faculty provides IT-related research and education.	www.kth.se
24. Department of Computer and Systems Sciences (DSV)	The Department of Computer and Systems Sciences (DSV) is a joint department between Stockholm University and the Royal Institute of Technology. The DSV hosts SecLab, a laboratory for research and education in Computer Security and Security Informatics.	www.dsv.su.se/en/seclab/
25. Chalmers	It is a progressive university situated in Gothenburg. The implementation of education and research is taking place within 17 departments in research groups of varying size. In these departments, a departmental advisory team exists made up of external and internal members and equipped with an external chair to be consulted on issues of strategic importance. Department heads are responsible for providing departmental operational leadership	www.chalmers.se
26. Blekinge Institute of Technology (BTH)	Institute for higher education that has a clear focus on applied IT and innovation for sustainable growth. At BTH the research activities are ranging from engineering and mathematics to spatial planning, the humanities, business administration and	http://www.bth.se

Academic Organisations	Role and responsibilities	Website
27. Linköping Institute of Technology (LITH)	<p>health. The common characteristic for the research is the profile on applied IT and sustainable development of business and society.</p> <p>With a body of more than 9 000 students, a faculty of more than 1 000 employees and a budget exceeding 1 billion Swedish kronor, the Institute of Technology is one of the largest higher engineering education institutions in Sweden. The Institute of Technology is a fully integrated part of Linköping University.</p>	www.lith.se
28. Swedish Institute of Computer Science (SICS)	Swedish Institute of Computer Science, SICS, is a research organisation focusing on applied computer science	www.sics.se

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
29. The Swedish Association of Local Authorities and Regions	<p>The Swedish Association of Local Authorities and the Federation of Swedish County Councils represent the governmental, professional and employer related interests of Sweden's 290 local authorities, 18 county councils and two regions. The association strives to promote and strengthen local self-government and to create the best possible conditions for the work of their members. Membership fees largely finance the activities.</p> <p>The association has published information on information security policy adapted to local and regional authorities. Security issues are discussed at conferences and best practice from a local authority could be highlighted. Information such as advice on new and relevant legislation is published on the website.</p>	http://kikaren.skl.se/artikel.asp?C=756&A=180
30. The Swedish Consumers' Association	<p>The Swedish Consumers Association is an independent, non-partisan cooperative organisation consisting of 28 member organisations.</p> <p>The Swedish Consumers Association aims to strengthen the position of consumers in order to improve people's ability to bring their consumer power to bear. Our goal is to ensure that political, business, and government decision makers always have the best interests of the consumer in mind.</p>	http://www.sverigeskonsumenrad.se/start.asp?sida=3241
31. ISACA Sweden	ISACA provides security certificates.	http://www.isaca.se

References

- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- ENISA, Information security awareness in financial organisations, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Sweden- ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/sweden>



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